UTS UNIVERSITY OF TECHNOLOGY SYDNEY

Adaptive Digital Identity Verification Reference Architecture (ADIVRA) Framework

by Memoona Javeria Anwar

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy (C02029)
Information Systems

under the supervision of:
Dr Asif Q.Gill
Dr Farookh Hussain
Dr Ghassan Beydoun

University of Technology Sydney
Faculty of Engineering and Information Technology
School of Computer Science
July 2021

Certificate of Authorship

I, Memoona Javeria Anwar, declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy in Information Systems in the Faculty of Engineering and IT, School of Computer Science at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature: Production Note:
Signature removed prior to publication.

Date: 06-07-2021

Acknowledgments

I have been privileged to have Dr Asif Gill, Dr Ghassan Beydoun and Dr Farookh Hussain as my supervisors. I want to express my sincere gratitude to my principal supervisor, Dr Asif Gill, for giving me the opportunity to work with him on this research project. His highly valuable support, coaching, encouragement, quick feedback, and guidance helped me finish this research project. Dr Asif Gill was always there to provide support in meetings, phone conferences, and by email. His valuable understanding in the field of information security, privacy, and digital ecosystems as an academic, researcher, and practitioner provided a wealth of knowledge that I used in this research project.

This study would not have been possible without the support of my family. I am very grateful to my parents, Hameeda Begum (late) and Muhammad Anwar Sheikh (late), for their precious love, blessings, support, encouragement, sacrifice, and care since my childhood. I am thankful for the support of my husband, my children, and siblings. Their genuine care gave me confidence and peace of mind during my busy life. I am blessed to be a member of such a loving, caring, and supportive family.

I want to express my sincere thanks to all my colleagues and friends for their valuable feedback and support.

I also wish to thank the Australian Government for its support for providing the funding for my research project for the length of my PhD study period.

I am thankful to all of the reviewers for their valuable feedback and comments.
Thank you all.

Research Contributions and Publications

During this PhD research project, I collaborated with my supervisor and other colleagues. I published the components of this research work (ADIVRA) in several rigorously reviewed international conference papers and scientific journals. The publication of these papers was an opportunity to present my work for review before including it in this thesis. Appendix F presents a list of the publications that have been included in this thesis.

Publication	Status	Reference	Source
Publication-1	Published	Anwar, M., Gill, A., and Beydoun, G. 2018. "A review of information privacy laws and standards for secure digital ecosystems", in ACIS, 2018, Sydney, Australia.	http://www.acis2018.org/wp-content/uploads/2018/11/ACIS2018_paper_78.pdf
Publication-2	Published	M. J. Anwar and A. Q. Gill, "A Review of the Seven Modelling Approaches for Digital Ecosystem Architecture," 2019 IEEE 21st Conference on Business Informatics (CBI), Moscow, Russia, 2019, pp. 94-103, doi: 10.1109/CBI.2019.00018.	https://ieeexplore.ieee.org/document/8807801
Publication-3	Published	M. Anwar, A. Gill, and G. Beydoun, "Using Adaptive Enterprise Architecture Frame-work for Defining the Adaptable Identity Ecosystem Architecture," 2019.	https://acis2019.io/pdfs/ACIS2019_PaperFIN_176.pdf
Publication-4	Published	M. Anwar and A. Gill, " Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model," 2020.	https://www.datazoo.com/wp-content/uploads/ISO27701-and-GDPR-Gaps-and-Overlaps.pdf
Publication-5	Published	Secure Big Data Ecosystem Architecture: Challenges and Solutions	https://doi.org/10.1186/s13638-021-01996-2
Publication-6	In Review	A Privacy Assessment Model for GDPR Compliant Blockchain enabled Identity Management: An Action Design Research	Journal of Information and Management
Publication-7	Accepted	PESTLE+ risk analysis model to assess the pandemic preparedness of identity ecosystems	Security and Privacy journal
Publication-8	In Review	Decentralised Digital Identity Requirements Model: Regulatory Perspective	Computer and Security Journal
Publication-9	In Review	Using ArchiMate for Modelling the Secure Digital Identity Ecosystem Architecture	Computer and Security Journal

Table of Contents

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Description
ADIVRA	Adaptive Digital Identity Verification Reference Architecture
DigI	Digital Identity
DDigI	Decentralized Digital Identity
PII	Personally Identifiable Information
eIDV	Electronic Identity Verification
ADR	Action Design Research
BIE	Build, Intervene and Evaluate
RL	Reflection and Learning
FL	Formalization of Learning
SP	Service Provider
IdP	Identity Provider
IO	Identity Owner
II	Identity Issuer
VC	Verifiable claim
GDPR	General Data Protection Regulation
eIDAS	electronic Identification, Authentication and trust Services
B2B	Business-to-Business
B2C	Business-to-Customer

Abstract

Digital ecosystems comprise interacting actors such as organizations, people and things that are supported by digital platforms. The interconnection of actors may involve sharing personally identifiable information such as digital identity information for verification within the digital ecosystem. One of the key privacy challenges in digital ecosystems is the verification of a digital identity in a manner that is secure and compliant with regulatory requirements. The identity verification process is compromised if personally identifiable information is lost, which can lead to identity theft and more serious instances of data breaches. Therefore, a practical digital identity verification solution should enable secure digital identity verification for actors operating in the inherently complex and diverse regulatory environment of digital ecosystems.

Several research and industry initiatives have been taken to address this challenge however, there is a lack of capability in existing solutions and guidance for implementing a digital identity verification solution that can comply to regulatory requirements and securely verify an identity without storing personally identifiable information. Hence, this thesis aims to address a pressing research need: how to ensure regulatory compliance and the privacy of personally identifiable information involved in digital identity verification in a digital ecosystem? This thesis aims to address this practice-oriented research question by proposing an adaptive digital identity verification reference architecture (ADIVRA) framework. The ADIVRA has been incrementally developed by the iterative cycles of build, intervene, and evaluate, reflection and learning, and the formalization of learning research activities following the principles of well-known action design research.

ADIVRA comprises three main components: Assess, Design and Evolve. The Assess component helps to assess the environmental risks and gaps. The Design component fills the gaps identified by Assess component. The third and final component of the ADIVRA framework is Evolve, which analyzes the changes and identifies the adjustments against changing privacy risks, regulatory requirements, and business needs. The proposed ADIVRA framework is evaluated via design and review workshops in industry partners' organizational settings and industry experts' field survey. The results of this evaluation indicate that the proposed ADIVRA framework could be helpful for guiding the development of adaptive digital identity verification solutions that are privacy aware and support regulatory compliance. ADIVRA is intended for use by industry practitioners, law makers, regulators, and researchers as a comprehensive reference architecture for developing privacy aware and regulatory compliant digital identity verification solutions.

Chapter 1: Introduction

Digital ecosystems comprise interacting actors such as organizations, people and things that are supported by digital platforms (French 2019;Nischak & Hanelt 2019; Schmitz 1996). Digital identity (DigI) consists of personally identifiable information (PII) that is used to identify actors in digital ecosystems (Naik & Jenkins 2020; Ben Ayed 2014; Cameron 2005; Windley 2005). With the increase in the number of online services and users, identity fraud is on the rise (Berghel 2012). From bank account hacks to stolen funds, to social media takeovers, identity-related crimes have become a routine threat to everyone's life, and this continues to increase with digitization (Adeyemo Kingsley 2012). This is mainly due to a central body controlling a user's PII (Bartolomeu et al. 2019; Othman & Callahan 2018). To address this important issue, this research presents an adaptive digital identity verification reference architecture (ADIVRA). ADIVRA is enabled by blockchain technology. The use of blockchain technology promises to embed security and privacy into the design of the DigI verification solution (Mukta et al. 2020). This first, introductory chapter provides the research background, research problem and research questions. This chapter also presents the aims and objectives, significance and scope and contribution of this research work in the form of a novel ADIVRA framework. In the end, it discusses the research strategy and overviews the thesis structure.

1.1. Research Context

The research presented in this thesis has been conducted in the area of information systems, mainly in the context of the DigI ecosystem. A broader definition of information systems by Buckingham et al. (1987) in Avison & Wood-Harper (1990, p.4) is: “an information system is any system which assembles, stores, processes and delivers information relevant to an organization (or society), in such a way that information is accessible and useful to those who wish to use it, including managers, staff, clients and citizens. An information system is a human activity (social) system which may or may not involve the use of computer systems”. A DigI is single or multiple elements of PII about an individual or an entity that is processed or stored in digital form (Der, Jähnichen & Sürmeli 2017). Since the advent of the Internet, DigI has been a major element (Ben Ayed 2011; Hu et al. 2014; Takemiya & Vanieiev 2018). DigI is composed of PII and free-flowing PII endangers individuals to identity fraud, consequently reducing the trustworthiness of DigI for verification (Ben Ayed 2014; Cameron 2005; Windley 2005). The lack of efficient DigI verification solutions exposes individuals and organizations to increased identity theft and fraud. In this thesis, we approach the problem of DigI verification with a primary focus on the compliance and privacy of PII.

As a concept, privacy is commonly applied in every walk of life and it is widely dependent on social, professional, business, academic and legal contexts, as pointed out by (Gürses 2010). Thus, as a first step, the research context is developed by defining privacy, DigI and the related terms that are used throughout this thesis.

1.1.1. Privacy

There are many definitions of privacy, which makes it difficult to select a single source for defining privacy. The varying definitions of privacy are discussed in the literature review chapter (Chapter 2). At a higher level, privacy can be defined as: the "right to be left alone" (Samuel D. Warren & Brandeis 1890). In this digitally transformed world of connected online platforms and systems, privacy is usually described as the capability of individuals to have control over the sharing of their PII. Alternatively, Westin (1967) defines privacy as: "the right of the individual to decide what information about himself should be communicated to others and under what circumstances."

The recognition of a general right to privacy is a comparatively new trend (Gavison 1980). In this thesis, the focus is on the privacy of DigI information and its verification. This kind of privacy is identified as information privacy. Hence, information privacy empowers the organization or individual in deciding and controlling the extent to which DigI information is shared with and disclosed to third parties. However, on the Internet, the concept of privacy is greatly misunderstood, and it can be complicated to correctly handle sensitive data due to the range of privacy legislations and regulations that exist (Erramilli 2012; Huo et al. 2020; Li & Palanisamy 2019). Therefore, there are different aspects to privacy. Privacy is a combination of what you do (behaviour) and who you are (form) (Pilton, Faily & Henriksen-Bulmer 2021). What you do is, for example, your digital footprints i.e., the information you search for on Google, the sites you visit, where you work, the books you read, even your online shopping. Who you are is your identity, which is based on PII attributes. The PII attributes can be a person's name, birth details, home address, driving licence number, social security number, salary package, skillset and more.

Widespread debate on information privacy, augmented by the known or unknown storage of PII in centralised databases, was initiated in the 1960s (Prosser 1960). Therefore, before agreeing on one definition of privacy, we discuss what is PII.

1.1.2. Personally Identifiable Information (P I I)

The term PII is quite broad. It refers to pictures, comments, places, tweets, likes, IP addresses, business profiles, professional information, social information, behavioural information, and of course identity information. The definition of PII according to NIST (McCallister, Grance & Kent 2010:ES-1) is as follows:

"PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

PII is alternatively known as personal data as defined by EU's General Data Protection Regulation (GDPR) (European Union 2018:Art.4):

"'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

PII is one of the very fundamental notions in information privacy. The applicability of privacy legislations and regulations is usually determined by the involvement of PII. Nevertheless, there is no standardised definition of PII given by legislation. In some cases, non-PII linked with individuals can be formed in unimaginable ways and de-identified information linkage can be re-identified (European Union 2018). PII and non-PII therefore can be classified as mutable types, with the possibility of transformation to PII of a previously categorised non-PII. This debate of PII with non-PII is never ending; however, the undeniable sensitivity of PII that constitutes an individual's DigI is certain. What PII attributes constitute DigI varies according to the context.

1.1.3. Privacy Principles

Since the time of the Bell-La Padula and the Biba models, which mentioned confidentiality and integrity individually (Dhillon & Backhouse 2001), the phrases 'confidentiality', 'integrity' and 'availability' have been generally used in information privacy practice and in the academic literature (Doherty, Anastasakis & Fulford 2011; Gomi 2011; Radhakrishnan, Kharrazi & Memon 2005; Shaw 2000; Thomas & Meinel 2010; Windley 2005). Of the foundational privacy concepts in DigI verification are confidentiality, integrity, and availability, referred to as the CIA triad (ISO 2015). Confidentiality makes sure that only authorised people or processes can access information. Integrity guarantees that the information has not been altered. Availability specifies that the information is available to authorised users when required. In some circumstances, these properties are bonus features, while in others, their absence can cause serious damage. Realising their importance and need is crucial to a DigI verification. The concept of privacy used in this thesis entails all three components of the CIA triad. Therefore, privacy refers to decisions like which information can be shared with others (confidentiality), how that information can be shared safely (integrity), and how it can be made available to authorised users (availability). In addition, we have added a fourth feature to the CIA triad i.e., non-repudiation to broaden the range and effectiveness of the triad to signify a deeper insight into privacy management in the DigI ecosystem. Non-repudiation ensures that someone cannot deny the authenticity of their digital signature in relation to a transaction or a message.

1.1.4. Digital Identity (DigI)

A DigI is related to the physical identity of an entity such as a person, a company, a device, or a car (Der, Jähnichen & Sürmeli 2017). According to the International Telecommunication Union, DigI is: "a digital representation of an entity, detailed enough to make the individual distinguishable within the digital context." Thus, its definition is generally reliant on its use, context, aim, and numerous other considerations (Phiri & Agbinya 2006). The DigI is characterized by upholding similar identifying information as in the physical world; however, it is published on the web, with the addition of elements such as digital signatures and email. In addition, DigI includes other non-PII information related to individuals i.e., business information,

social information, and professional information. As DigI invariably includes elements from the physical identity of a person, it is exposed to privacy and security risks and contains a possibility of identity theft and fraud. Hence, it is important to know the interconnection between physical identity and DigI and how it can be protected. In this context, DigI information is a critical asset that needs to be securely verified to avoid data breaches, lawsuits, or loss of business. DigI verification is used to verify that the DigI holder is also the real owner of the physical identity as claimed.

There are four main models for DigI verification, namely centralised, federated, user-centric and decentralised (L'Amrani et al. 2016; Naik & Jenkins 2020). In the centralised model, a central body, such as the organization, has full control of the identity owner's information. With the federated DigI verification model, customers can use DigI credentials issued by one domain to reach another domain, such as Microsoft Passport and Facebook Connect. In the user centric DigI verification model, the identity owner is given more control and verification is performed indirectly through the user so that the central body does not have to be directly involved in every transaction. However, this approach still relies on the user selecting an individual identity provider and agreeing to their terms and governance for the user's personal data. The decentralised DigI (DDigI) verification model puts the management and charge of DigI data straight under the control of the identity owner (L'Amrani et al. 2016; Mukta et al. 2020). The decision to choose the DigI model depends on the level of regulatory and compliance requirements applicable to the corresponding sector. The scope of this thesis is limited to the DDigI verification model, which is made possible via blockchain technology.

1.1.5. Blockchain

An anonymous researcher or a team of researchers published an article titled "Bitcoin: A Peer-To-Peer Electronic Cash System" in 2008 using the alias of Satoshi Nakamoto (Nakamoto 2008). This technology is also known as blockchain or distributed ledger technology. In this thesis, we refer to this technology as blockchain. The key concepts that surround blockchain are a distributed database, peer-to-peer communication, irreversibility, and computational logic. Blockchain is often referred to as the next upcoming big trend in the literature (Kshetri 2017). Most of the world's large organizations are exploring ways to integrate blockchain into their products and services (Castillo 2018). Personal health records management, supply chain management, property management, and even the management of our DigIs are some of the use cases that are already leveraging blockchain. Blockchain is an immutable (integrity) and transparent distributed database, a ledger which has global consensus by all participants (non-repudiation). The data on blockchain can be hashed or encrypted (confidentiality) and can be accessed by all the trusted participants in a transparent manner (availability). With privacy constraints in mind, blockchain technology can offer a DigI verification solution with better regulatory compliance. Hence, in this research, blockchain is used as the supporting technology for the design of the proposed reference architecture.

1.1.6. Regulations

As the new world of connectivity creates a set of challenges, many countries have begun outlining guidelines for the ways a DigI verification system should operate. The aim of these guidelines is

to promote increased information privacy practices to keep an individual's PII secure. Within each country, national (such as the Privacy Act 1988 in Australia) and international (such as GDPR, NIST, eIDAS) regulations pose opportunities and risks that may affect the efficiency, reputation, and commercial viability of DigI ecosystems. For DigI verification solutions to grow and be widely adopted, they must be designed in line with relevant regulations to guarantee operational efficiency coupled with the effective management of risk and opportunity. To support the widespread adoption of secure DigI verification and promote interoperability, several laws, regulations, and standards have been devised across many countries. In these laws, regulations and standards, the privacy of information is the topmost priority. This revival of privacy regulations has resulted in organizations struggling to ensure compliance. Many of them, initially compliant, fail to keep up with the speed of changing regulations and risks. It is crucial for DigI verification solutions to evolve and adapt to the heightened information protection and privacy obligations. In this research, different privacy regulations and standards are evaluated to determine which regulation covers the maximum concepts of DigI verification. It is found that the EU's GDPR (European Union 2018) covers the maximum facets of privacy aware DigI verification (Anwar, Gill & Beydoun 2018a). Hence, this thesis will use the GDPR as a guiding regulatory lens to design a DigI verification reference architecture.

1.2. Research Problem

Gartner (2016) classifies a digital ecosystem as: "an interdependent group of enterprises, people and/or things that share standardized digital platforms for a mutually beneficial purpose (such as commercial gain, innovation or common interest). Digital ecosystems enable you to interact with customers, partners, adjacent industries even your competition". Hadzic & Chang (2010) define a digital ecosystem “as the dynamic and synergetic complex of digital communities consisting of interconnected, interrelated, and interdependent digital species situated in a digital environment that interact as a functional unit and are linked together through actions, information, and transaction flows”. Digital ecosystems are a distributed and interdependent network of actors that interact and collaborate for value co-creation (Alam & Gill 2020; Gill 2013, 2015, 2017; Gill et al. 2021; Madhuri, Gill & Khan 2020).

The increased number of connections in digital ecosystems increases the need for DigI verification. Most of the information used for DigI verification is PII. The more the information in a digital ecosystem, the more valuable the digital ecosystem is for bad actors. Digitization must not put DigI and its verification at risk. Privacy attacks (such as WannaCry ransomeware (‘The WannaCry ransomware attack’ 2017), Dyn DDos (Egbo 2018) on multiple media companies, a major European telecom company, banks in India and Heathrow airport signify that digital ecosystems are continually at risk (Joshi 2017). Global privacy regulations as well as country-specific regulations provide the requirements to attaining privacy in a digital ecosystem. Nevertheless, guidance on the implementation of the regulatory requirements is still unclear. Henceforth, the key challenge is how to ensure regulatory compliance and the privacy of PII involved in DigI verification in a digital ecosystem? A digital ecosystem is a very broad concept which includes several complex components (Dong, Hussain & Chang 2007). Hence, this thesis focuses on the identity ecosystem as an instance of a digital ecosystem and DigI as an instance of PII. Therefore, the focus of this research is ensuring the privacy of DigI during its verification in an identity ecosystem based on the guidelines provided by regulations, particularly GDPR.

DigI verification has always been a vital element for service delivery in both the private and public sectors. Changing user requirements in the digitally transformed world emphasizes the need for new methods to verify that a person is whom they say they are (Wolfond 2017). All forms of identity are built on PII and therefore involve an innate probability of exploitation. However, digital forms of identity (i.e., DigI) hold much higher risk. They have a wider range and generate large amounts of information regarding people, their digital footprints, monetary details, associates, and supposedly political and religious beliefs (Dixon 2019). Verizon (2020) highlighted in their 2020 Data Investigation Report that credential theft and loss comprise approximately 80% of all breaches or attacks targeting sensitive online information. Securing the DigI verification process is vital for enabling transactions in online distributed digital ecosystems (Goode 2019; Lourinho, Kendzierskyj & Jahankhani 2021; Oh, Kim & Shin 2018).

1.2.1. Research Gaps

Traditional DigI verification methods and solutions have several limitations corresponding to DigI and its verification such as storage and access control for PII, privacy and security and regulatory compliance (Shehu, Pinto & Correia 2019). According to The European Union Blockchain Observatory & Forum report (Blockchain and digital identity 2019), the present DigI verification solutions are disjointed, unsecure and lack adaptability. Furthermore, most DigI verification solutions are either centralised (such as Okta (*Modern identity from cloud to ground | Okta* n.d.), and Jumio (*Jumio: End-to-End ID and Identity Verification Solutions* n.d.) or federated (Facebook, Google, Microsoft passport) in nature. These centralised and federative DigI solutions bring numerous problems in the realms of privacy, security, usability, trust, and compliance (L'Amrani et al. 2016). The DigI is controlled by a central authority that opens the door for many vulnerabilities. Decentralisation is a visible trend in the DigI verification process to tackle privacy issues (Dunphy, Garratt & Petitcolas 2018). DDigI verification increases the control of the identity

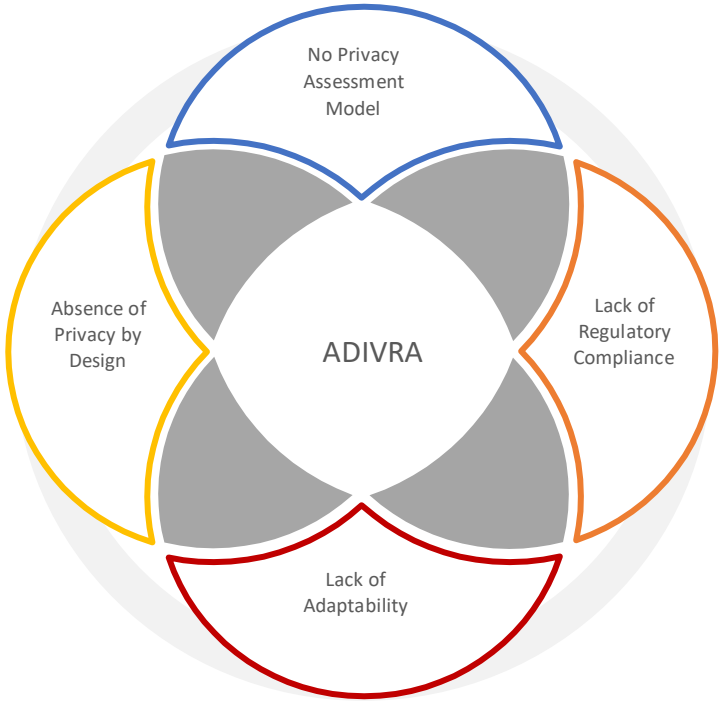


Figure 1.1. Research Gaps

owners over their DigIs. The core challenge with DDigI verification is that it increases the burden of managing and protecting PII for the identity owner. Moreover, the existing DDigI verification solutions do not fully comply with regulations (Takemiya & Vanieiev 2018). DigI verification solutions are operating in complex and heterogeneous environments as a result of varying regulatory requirements in country and internationally. Therefore, DigI verification solutions need to adapt to diverse and up to date regulatory frameworks while dealing concurrently with a variety of privacy risks and business needs. Moreover, the actors involved in digital ecosystems may come from different geographical locations and can be subject to different regulations and laws. Inability to adjust to evolving regulations in various jurisdictions could have significant effects. This may result in a large number of scams, identity theft and fraud for organization, along with complex procedures for end-users.

Many companies (such as Civic (*Identity Verification by Civic - Know-Your-Customer KYC for Business* n.d.), ShoCard (*Personal Identity Verification for COVID-19 Vaccinations and Test Results | Project COVID Freedom* n.d.), Evernym (Evernym 2020)) have developed proofs-of-concept and solutions for DDigI verification solutions, but they have not been thoroughly analyzed in light of changing regulations and increasing risks. In addition, the existing DigI verification solutions store and manage PII much like centralised DigI verification solutions. Furthermore, to design a regulatory compliant DigI verification solution, it is important to conduct a self-assessment of technologies, systems, procedures, and policies to ensure compliance with privacy and PII access requirements. One of the problems is that the theoretical foundation for technologies that can be used for DigI verification is meagre and not much research has been conducted on how different technologies (such as OCR, biometric, blockchain) can fit to enable privacy in the DigI verification. Technology adoption if not done correctly, can create unintended problems. It can increase privacy risks instead of mitigating them and increase costs and response time. Hence, it is essential to ascertain that the potential technology is appropriate for DigI verification. As a result of initial research, we found that there is no research-based criterion on which the viability of technology for DigI verification solutions can be assessed. The research gaps are:

RG1: There is a lack of a research-based privacy assessment model to conduct an assessment of technology, systems, procedures and policies in the DigI verification ecosystem.

RG2: There is a lack of a research-based privacy reference architecture for DigI verification that ensures the privacy of DigI by design.

RG3: There is a lack of a research-based privacy reference architecture for DigI verification that ensures compliance to regulatory requirements.

RG4: There is a lack of a research-based privacy reference architecture for DigI verification that adapts to changing business needs, privacy risks and the regulatory landscape.

Therefore, this research aims to address the important practical challenge and research gap of an adaptive DigI verification reference architecture for actors operating in the inherently complex and diverse regulatory environment of digital ecosystems.

1.3. Research Question, Aims and Objectives

Against the backdrop of the research problem detailed in previous section, the main research question (RQ) is:

RQ: ***How to ensure regulatory compliance and privacy of PII involved in DigI verification operations in digital ecosystem?***

To scope the main research question, the following sub-questions were devised:

RQ1: How to assist in the assessment of privacy risk to DigI verification in an identity ecosystem?

RQ2: How to design a privacy aware and regulatory compliant DigI verification reference architecture using blockchain technology to address the privacy risk to the DigI verification process in an identity ecosystem?

RQ3: How to ensure the adaptability of the design in response to changing risk, regulatory landscape, and business needs in the context of the DigI verification process in an identity ecosystem?

Table 1.1 Research Questions, Research Aims and Research Objectives

Broad Topic	Restricted Topic	Narrowed Topic	Research Question	Research Aim	Research Objective
Privacy Risks	Privacy Risks to PII in digital ecosystem.	Privacy risks to DigI verification in identity ecosystem.	How to assist in the assessment of privacy risk to DigI verification in an identity ecosystem?	To assess the risks associated with the DigI during DigI verification in an identity ecosystem.	Assess the risks associated with DigI verification in an identity ecosystem.
Privacy Solutions	Solution to reduce privacy risks to PII in a digital ecosystem.	Solutions to reduce privacy risks to DigI verification in an identity ecosystem.	How to assist in the assessment of privacy risk to DigI verification in an identity ecosystem?	To evaluate existing privacy measures taken to safeguard DigI verification in an identity ecosystem and identify the gaps.	Conduct a review of the existing DigI verification solutions and evaluate them to identify the gaps.
Compliance	Privacy Regulations	Blockchain-based regulatory compliant DigI verification platforms.	How to design a privacy aware and regulatory compliant DigI verification reference architecture using blockchain technology to address the privacy risk to DigI verification in an identity ecosystem?	To design a privacy reference architecture based on the principles of privacy by design and guidelines from regulations, leveraging blockchain technology that ensures the privacy of DigI verification in an identity ecosystem.	Design a privacy reference architecture for DigI verification in an identity ecosystem that is aligned with the principles of privacy by design and regulations.
Adaptability	Changing business needs, privacy risks and regulatory requirements	Adaptive DigI reference architecture.	How to ensure the adaptability of the design in response to changing risk, regulatory landscape, and business needs in the context of the DigI verification process in an identity ecosystem?	To identify the change requirements and evolve the DigI verification design.	Evolve and adapt the proposed architecture by monitoring and identifying change requirements.

To find answers to the RQ's, a literature review of the existing research and the literature on DigI, privacy, security, regulations and blockchain technology was conducted. It is intended that the

research findings will contribute to the development of a reference architecture where privacy is embedded into the design of the solution.

Hence, the aims of this research in the light of the above research questions are:

RA 1: To assess the risks associated with DigI during DigI verification in an identity ecosystem.

RA 2: To evaluate the existing privacy measures taken to safeguard DigI verification in an identity ecosystem and identify the gaps.

RA 3: To design a privacy reference architecture based on the principles of privacy by design and guidelines from regulations, leveraging blockchain technology that ensures the privacy of DigI verification in an identity ecosystem.

RA 4: To identify the change requirements and evolve the DigI verification design.

To achieve the aims, the study will pursue the following objectives:

RO 1: Assess the risks associated with DigI verification in an identity ecosystem (Aim 1)

RO 2: Conduct a review of the existing DigI verification solutions and evaluate them to identify the gaps (Aim 2)

RO 3: Design a privacy reference architecture for DigI verification in an identity ecosystem that is aligned with the principles of privacy by design and regulations (Aim 3)

RO 4: Evolve and adapt the proposed architecture by monitoring and identifying change requirements (Aim 4)

Table 1.1 sumarises the reseach questions and corresponding aims and objectives.

1.4. Significance and Scope

The research started with the broader topic of the privacy of PII involved in DigI verification in a digital ecosystem. As the research progressed, the focus was narrowed to privacy, regulatory compliance, and the adaptability of DigI verification in an identity ecosystem (see Figure 1.2). The scope of the study includes the design of a reference architecture to ensure privacy, regulatory compliance, and the adaptability of DigI verification in an identity ecosystem. The technical details like the cryptographic technique or the network architecture is beyond the scope of this research however, different encryption techniques can be applied as per the context. This research is conducted as an action design research (ADR)(Sein et al. 2011) project. The timeframe of the study spans three years and is not limited to any specific geographical coverage.

The following are the features of the study scope:

1. A DigI verification assessment model:
    a. to identify the privacy risks during DigI verification in an identity ecosystem

b. to identify the gaps in existing DigI verification solutions in an identity ecosystem

2. A design of a blockchain-based DigI verification reference architecture:
    a. to identify regulatory requirements
    b. to develop the multisource structure of DigI
    c. to design a DigI secure container for Privacy by Design
    d. to design a regulatory compliant DigI verification process model leveraging blockchain technology
3. Digital identity verification adaption model:
    a. To adjust and evolve the design with changing privacy risks, business needs and regulatory landscape.

This research will advance knowledge through the theoretical developments in DigI design principles, architecture models, knowledge representation, and adaptation while addressing practical issues around secure and adaptable DigI verification. A novel ADIVRA framework is developed that is technology-enabled and adaptive to withstand the scope of digital ecosystems. The ADIVRA framework is underpinned by DigI verification components and artefacts to empower industry to better understand and effectively exploit DigI and its innovations. The proposed framework will adopt a decentralised approach to secure a DigI verification solution without the need to permanently store PII. This research will also propose a conceptual innovation through new theoretical developments and an understanding of DigI verification using well-known

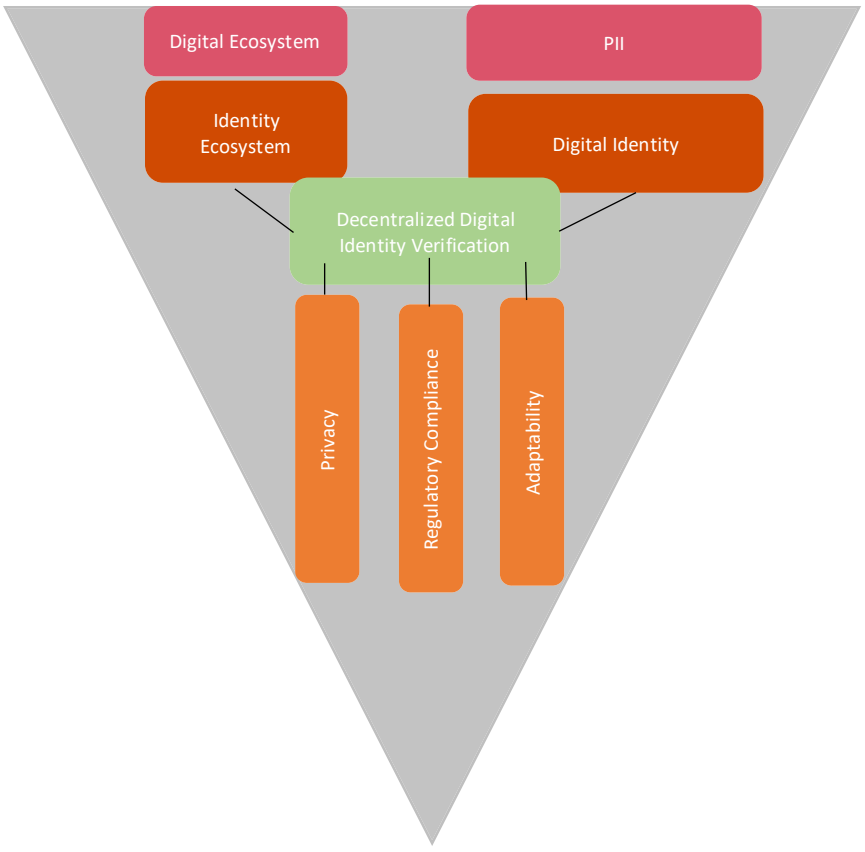


Figure 1.2. Research Scope

information systems theory generation abstraction and reflection techniques from ADR (Gregor, Müller & Seidel 2013).

1.5. Research Contributions and Limitations

This section summarises the key contributions of this research. This research proposes an ADIVRA framework (see Figure 1.3) for DigI verification. The current version of the ADIVRA incorporates ideas from recent research and several DigI verification methods and solutions. The components and artefacts of the ADIVRA framework will improve the digital innovation and DigI verification in an effective manner. The proposed framework is unique in its decentralized approach to privacy aware and regulatory-compliant DigI verification without storing PII. It is based on the combination of the identity management privacy assessment model (IdMPAM), PESTLE+ risk analysis model, information security audit maturity model (iSAM2), regulatory requirement model (RRM), compound digital identity (CDigI), digital identity verification process model (DigIVPM), information security envelope architecture model (iSEA), and digital identity verification adaptation model (DigIVAM). This research does not discuss the implementation details and network architecture of DigI verification solutions and is limited to the reference architecture only.

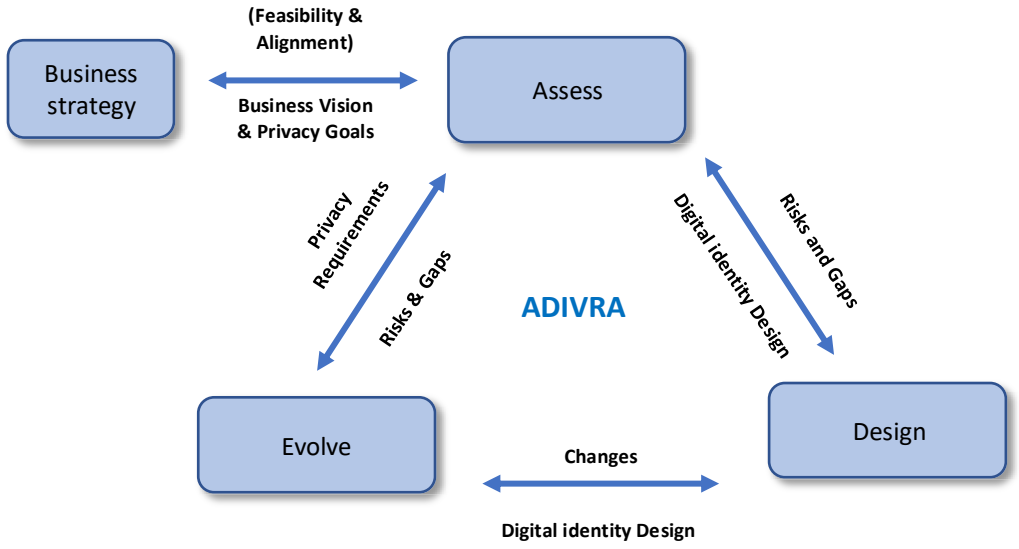


Figure 1.3. Adaptive Digital Identity Verification Reference Architecture Framework – High Level Contextual Diagram (reported in Anwar et al. 2021)

The main contribution of this research is an ADIVRA framework (see Figure 1.3) which fulfills the aforementioned gaps (see Figure 1.1). The ADIVRA framework is divided into three main components and a preliminary step in understanding the business strategy (see Chapter 4). Each of these components produces artefacts to fill the gaps identified in this research. The components of an ADIVRA framework are Assess, Design and Evolve.

1.6. Application and Users

This section briefly discusses the ADIVRA application and its users. The ADIVRA framework is intended to be used by security architects, DigI architects, regulators and law makers, researchers,

government agencies and identity owners. The reference architecture proposed in this research can be used as a blueprint by DigI architects and can capture different aspects of the DigI structure and secure the DigI verification process, especially from a privacy viewpoint. Additionally, this research provides insights on blockchain technology and its suitability for DigI verification. The reference architecture can help security architects in assessing the privacy capability of blockchain technology which will help security architects ascertain its appropriateness. An analysis of the existing solutions by different vendors will help DigI architects and government agencies in deciding what are the gaps in the current DigI verification solutions and how these gaps can be addressed. Furthermore, the discoveries also reveal the limitations of the legal frameworks and guidelines shielding privacy in DigI verification. Regulators and law makers can use ADIVRA to outline the additional requirements to be approved into regulations, consequently addressing the gaps in the DigI legal framework. Utilising ADIVRA, researchers can address the current inadequate understanding of complex DigI (such as CDigI), its verification, privacy, and regulatory compliance in the digital ecosystem. Identity owners can make informed decisions about the choice of a reliable DigI verification provider based on the insights highlighted in this research. The ADIVRA framework components and artefacts have been evaluated and verified by industry experts and the research community (see Chapter 5) and then have been updated based on their feedback.

1.7. Research Strategy

In this research, a well-known ADR method (Gill & Chew 2019; Sein et al. 2011) has been used to efficiently design an ADIVRA framework (Chapter 3). The reason behind using ADR is that in this context, we needed a research method that could facilitate the development of a solution which is theoretically grounded and also useable in practice as well. The first stage of ADR i.e., problem formulation was done by conducting a thorough literature review (Chapter 2). For this research, the literature is mostly derived from relevant research conducted in relevant fields such as privacy, PII, the digital ecosystem, DigI verification, blockchain, regulations and adaptability. This

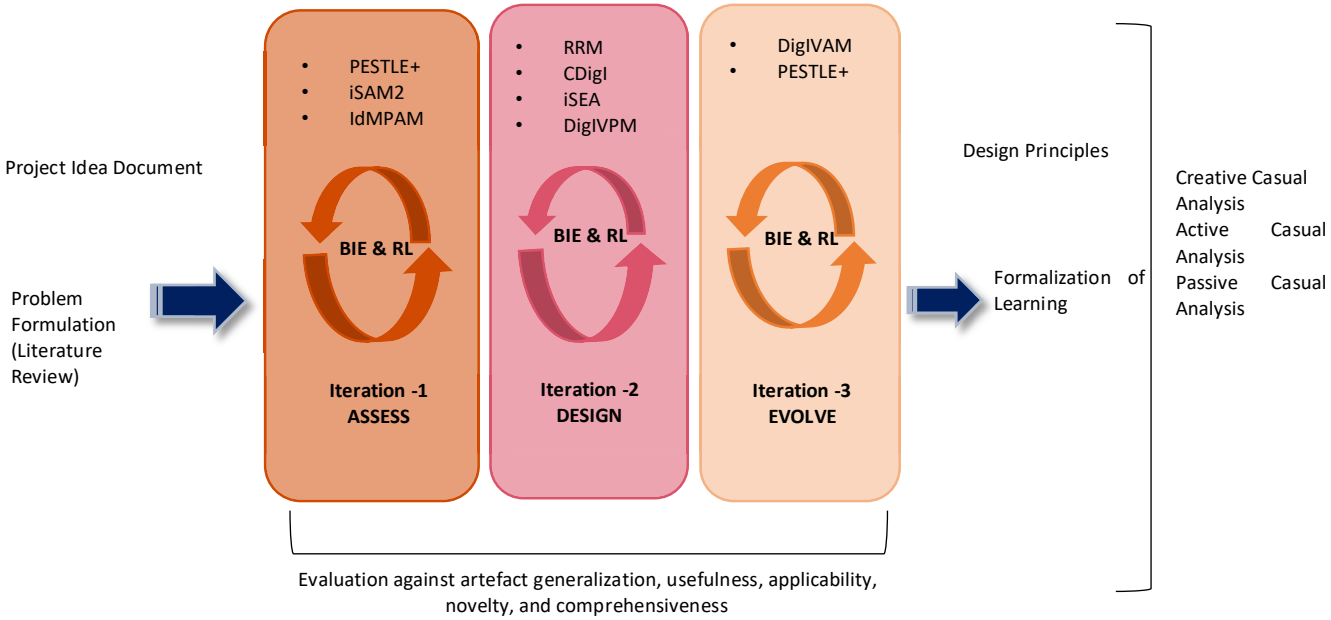


Figure 1.4. Research Strategy

research also actively involves the industry partner IDZ (coded name), which has similar needs. All the ADR stages are not strictly followed in top-to-bottom or waterfall ways; instead, they are more iterative and incremental (see Figure 1.4). Therefore, this ADR project was divided into three iterations (see Figure 1.4) to fit our context and the given conditions, and we adapted the build, intervene, and evaluate (Chapter 5) in accordance with the prospects appearing in the course of the research project. The first iteration includes the development of the assessment model (PESTLE+, *i*SAM2, IdMPAM) and finding the gaps in the existing solutions. The second iteration provides a blockchain-based DigI verification reference architecture with associated artefacts (RRM, CDigI, *i*SEA, DigIVPM) that fills in the gaps identified in the first iteration. The third iteration evolves the solution design to address the changing threat and regulatory landscape and evolving business needs (PESTLE+ and DigIVAM). The artefacts were built, intervened, and evaluated by thorough application as well as via feedback from industry experts through design and review workshops and an industry survey (Chapter 5) was conducted to evaluate the artefacts.

The evaluation of the artefacts produced by each component is done using Carvalho (2012) criteria. The artefacts were validated against the level of artefact generalization, usefulness, applicability, novelty, and comprehensiveness. Further, the design principles (Chapter 6) are extracted using the creative, passive, and active casual analysis techniques as mentioned by Gregor, Müller & Seidel (2013).

1.8. Thesis Outline

This thesis comprises six chapters.

This introductory chapter introduced the research topic, discussed the research context, and highlighted the research problem, research gaps, research questions, aims, objectives and scope. The research strategy is briefly described with the proposed solution and application and users.
Chapter two begins by explaining the concept of privacy and the terms that augment it. The relationship between privacy and PII is explored. This chapter builds the conceptual foundations by defining important concepts that are used in this thesis. It explains how other researchers have defined and built connections between these key concepts by conducting a thorough literature review. The chapter finishes by establishing definitions of the concepts that best fit with this research and their importance in filling the research gap.
Chapter three describes the research method adopted for this thesis.
Chapter four details the novel design of the ADIVRA that emerged from this ADR project. Each component of the ADIVRA framework is explained in detail.
Chapter five details the three cycles of build, intervene and evaluate. The chapter highlights how the research outcomes were refined based on early feedback to mirror the increasing awareness of the ensemble artefacts. The industry field survey results are statistically analyzed in this chapter.
Chapter six concludes with a discussion of the high-level design principles, research contributions, research limitations and also presents directions for future research.

The appendices contain the research data (link to CloudStor, the cloud storage recommended by the University of Technology Sydney [UTS]), publications, ethics approval and consent forms, online survey template, comment logs from design and review workshops, and evaluation results.

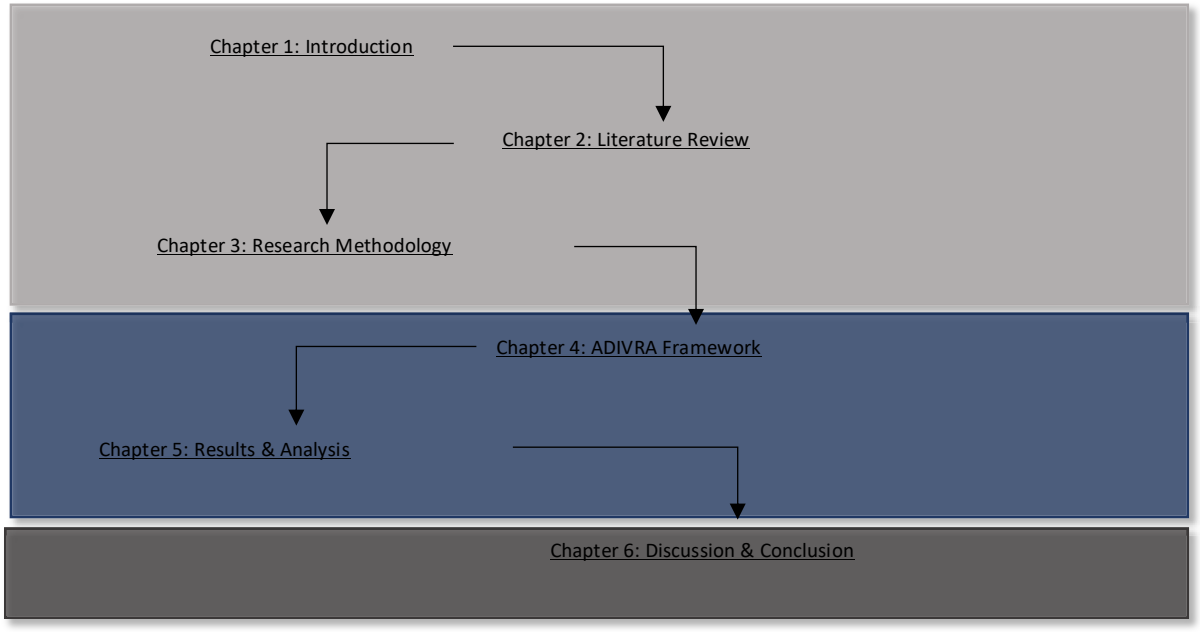


Figure 1.5. Thesis Outline

1.9. Summary

This chapter presented an introduction to the research conducted in the area of DigI verification. In this chapter, the research problem is stated by highlighting the gaps in the existing research. It further establishes the research questions and associated research aims and objectives. This research develops an ADIVRA framework to address the main research question: How to ensure regulatory compliance and the privacy of personally identifiable information involved in DigI verification in a digital ecosystem? The framework comprises three components: Assess, Design and Evolve. It is proposed that the ADIVRA framework presented in this research may fill the gaps identified in this research.

The ADIVRA framework will be discussed in detail in chapters 4-6. This chapter highlighted the main theoretical as well as practical contributions of this research and the methodological approach used to conduct this research. The next chapter discusses the literature review and the theoretical lens for this study.

Chapter 2 Literature Review

This chapter presents the existing work and literature on the research topic and reviews the advancement and limitations of the main subjects linked to the research. The purpose of this literature review is to summarize the existing knowledge around DigI verification and identify the gaps in the research. It outlines the insights and provides an overview of what the scholarly literature states on the topic in hand. The literature review helps in refining the problem formulation, establishing the conceptual foundations, choosing the kernel theories, showing research originality, and justifying the novelty. This chapter also presents the conceptual foundations within which this thesis is elaborated and introduces the main research concepts used to address the research questions. It builds the conceptual viewpoint which will be applied to parse the subject areas, ideas, constructs, and patterns. The chapter concludes with a summary.

2.1. Conceptual Foundation

The first step is to build conceptual foundations to understand the underpinning concepts related to this research (see Table 2.1). These concepts are defined to understand what they mean generally in the literature and to know which definition for each concept this research will focus on. In addition, it is important to know the relationship between these concepts in the context of this thesis (see Figure 2.1). The definition of the concepts used in this thesis is founded on several kernel theories. These theories are discussed in section 2.2. For this research, the concept of a digital ecosystem is defined based on adaptive enterprise architecture (EA) (Gill 2015) theory and privacy is defined as a combination of confidentiality, integrity, availability, and non-repudiation (Kumar & Bhatia 2020). In addition to privacy, we also focus on compliance for which GDPR is chosen as a guiding lens. The scope of this research is limited to DigI verification in an identity ecosystem. For the purpose of this research, the underlying technology for DigI verification will be blockchain.
Hence, to design a conceptual foundation for this research, we revisit the RQs and identify the key variables and relationships between these variables. The RQs and corresponding concepts are detailed in Table 2.1.

Table 2.1: Research Concepts

Research Question	Variables
How to ensure regulatory compliance and the privacy of PII involved in DigI verification operations in a digital ecosystem?	Privacy, PII, Compliance, Digital Ecosystem
How to assist in the assessment of the privacy risk to DigI verification in an identity ecosystem?	Privacy, DigI Verification, Identity Ecosystem
How to design a privacy aware and regulatory compliant DigI verification reference architecture using blockchain technology to address the privacy risk to the DigI verification process in an identity ecosystem?	Regulatory Compliance, Blockchain, Privacy, DigI Verification, Identity Ecosystem
How to ensure the adaptability of the design in response to the changing risk, regulatory landscape and business needs in the context of the DigI verification process in an identity ecosystem?	Adaptability, DigI Verification, Identity Ecosystem

After analyzing the RQs, eight concepts were identified: privacy, personally identifiable information, regulatory compliance, digital ecosystem, DigI, DigI verification, identity ecosystem, blockchain and adaptability. The relationships between these variables are shown in Figure 2.1.

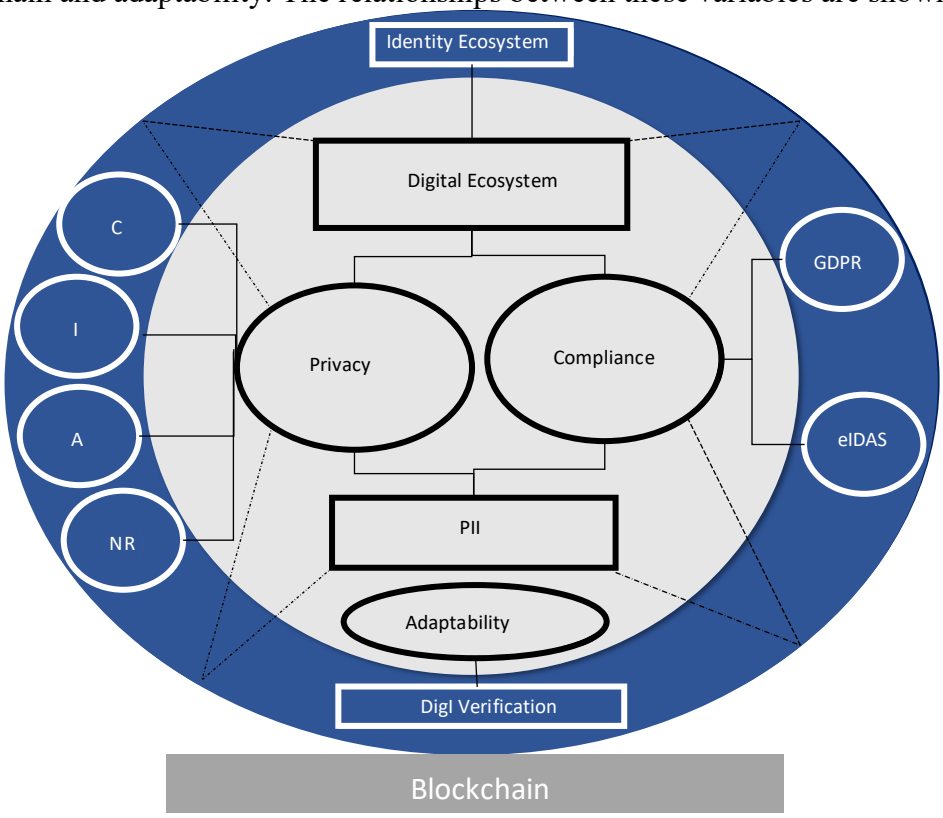


Figure 2.1. Conceptual Foundation

Section 2.2 details the literature review conducted in the aforementioned areas.

2.2. Literature Review

2.2.1 Digital Ecosystem

Digital ecosystems are always changing (Nischak & Hanelt 2019; Schmitz 1996). They mature and evolve as new entities enter the ecosystem (Um et al. 2016). Gartner (2016) defines the "digital ecosystem" as an *"interdependent group of actors sharing standardized digital platforms to achieve a mutually beneficial purpose."* Chronéer et al. (2017) addresses the collaboration challenges faced by key partners in the development of business-to-business digital platform ecosystems in the early phases. D'Angelo et al. (2011) define a digital ecosystem as: *"an ecosystem constructed out of so-called digital organisms that can foster the development of novel distributed services"*. The ways to create value by emerging digital technologies keep on changing in terms of their development and adoption. This signifies that there is no single type of 'ecosystem' (Valdez-De-Leon 2019a). Rather, there are multiple types of ecosystems depending on the size and kind of services they offer. There are smaller vs larger ecosystems, ecosystem of ecosystems, sub-ecosystems where they overlap, global ecosystems (Apple, AirBnB), as well as local ecosystems. Some operate in a role (To Good To Go), while others are market specific (Verifone and Klöckner). Valdez-De-Leon (2019) gives a description of a digital ecosystem as: *"those networks of interacting organization that are digitally connected and enabled by*

modularity, and that affect and are affected by each other's offerings". Recently, Jacobides, Sundararajan & Van Alstyne (2019) characterized digital ecosystems as *"interacting organizations that are digitally connected and enabled by modularity and are not managed by a hierarchical authority".* Iansiti & Levien (2004) suggest that a digital ecosystem gives all involved parties "a collective advantage over competing networks". In fact, research by McKinsey recommends that businesses that adopt an ecosystem approach have a higher profit rate compared to those who do not (Bughin, Catlin & Dietz 2019). Pranata, Skinner & Athauda (2011) examine the security procedures for a digital ecosystem. Seigneur (2005) demonstrates the state of security in digital business ecosystems. Valdez-De-Leon (2019b) presents a framework for developing a digital ecosystem. Each actor in the ecosystem profits by communicating inside the ecosystem and thereby is motivated to keep taking part (Van Alstyne & Parker 2017; Eisenmann, Parker & Alstyne 2007; Jacobides, Sundararajan & Van Alstyne 2019). As ecosystems are becoming more and more rooted and able to secure more of the accessible marketplaces, those companies outside of the ecosystem may find it difficult to keep up with the progress (Gawer 2009).
Even though digital ecosystems are widely discussed in the literature, usually there is a shortage of models or contexts that can help industry practitioners steer the digital ecosystem paradigm in practice. A digital ecosystem must be designed to deliver a strong and resilient structure while at the same time avoiding centralized control and a single point of failure (Boley & Chang 2007;

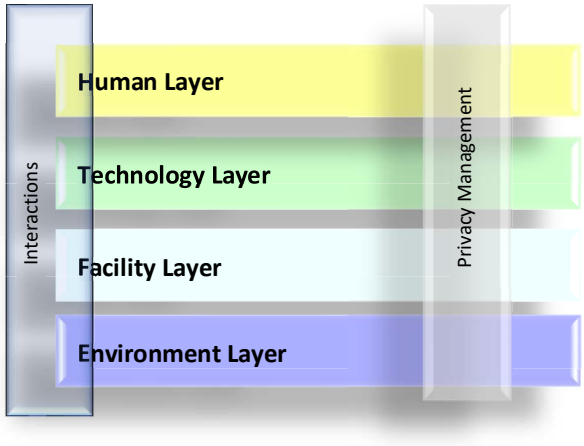


Figure 2.2. Digital Ecosystem adapted from (Gill 2015; Anwar & Gill 2019)

Kuperberg 2020a). A practice-oriented approach to the development of a digital ecosystem and associated policies that can bridge this divide is therefore essential. In addition, it appears that there is a close connection between companies that operate in different industry verticals. Therefore, there is a need to re-examine the digital ecosystem design in detail. It is also important to define digital footprints before developing a definition for digital ecosystems. A digital footprint is any online connection that a customer establishes with the business using digital channels. The digital ecosystem of a business is a mixture of all related digital footprints that work on important business information, the people who interact with them, and the business processes and technology that support them (Senyo, Liu & Effah 2019). This study aims at designing a reference architecture of an adaptive DigI verification ecosystem which is part of a broader digital ecosystem. To design such an identity ecosystem, the existing definitions of a digital ecosystem are not enough. Hence, a digital ecosystem is redefined to cover the end-to-end DigI verification lifecycle.

Table 2.2: Digital Ecosystem (based on Anwar and Gill 2019)

Architectural Design Areas								
DE Layers	***People (ppl)***	***Process (pro)***	***Capability (cap)***	***Performance (prfmnce)***	***Information (info)***	***Interface (int)***	***Service (svc)***	***Product (Prod)***
Human								
Business (Bus)	Bus:ppl	Bus:pro	Bus:cap	Bus:prfmnce	Bus:info	Bus:int	Bus:svc	Bus:Prod
Information (Info)	Info:ppl	Info:pro	Info:cap	Info:prfmnce	Info:info	Info:int	Info:svc	Info: Prod
Social (Soc)	Soc:ppl	Soc:ppl	Soc:cap	Soc:prfmnce	Soc:info	Soc:int	Soc:svc	Soc: Prod
Professional (Prof)	Prof:ppl	Prof:ppl	Prof:cap	Prof:prfmnce	Prof:info	Prof:int	Prof:svc	Prof: Prod
Technology								
Application (App)	App:ppl	App:Pro	App:cap	App:prfmnce	App:info	App:int	App:svc	App: Prod
Data(Data)	Data:ppl	Data:Pro	Data:cap	Data:prfmnce	Data:info	Data:int	Data:svc	Data: Prod
Platform (Pltfrm)	Pltfrm:ppl	Pltfrm:Pro	Pltfrm:cap	Pltfrm:prfmne	Pltfrm:info	Pltfrm:int	Pltfrm:svc	Pltfrm: Prod
Infrastructure (Infstrct)	Infstrct:ppl	Infstrct:Pro	Infstrct:cap	Infstrct:pfrmnce	Infstrct:info	Infstrct:int	Infstct:svc	Infstct:svc
Facility								
Spatial (Sptl)	Sptl:ppl	Sptl:pro	Sptl:cap	Sptl:prfmnce	Sptl:info	Sptl:int	Sptl:svc	Sptl: Prod
Energy (Enr)	Enr:ppl	Enr:pro	Enr:cap	Enr:prfmnce	Enr:info	Enr:int	Enr:svc	Enr: Prod
HVAC (HVAC)	HVAC:ppl	HVAC:pro	HVAC:cap	HVAC:prfmnce	HVAC:info	HVAC:int	HVAC:svc	HVAC: Prod
Ancillary (Anc)	Anc:ppl	Anc:pro	Anc:cap	Anc:prfmnce	Anc:info	Anc:int	Anc:svc	Anc: Prod
Environment								
Political	-	-	-	-	-	-	-	-
Economic	-	-	-	-	-	-	-	-
Social	-	-	-	-	-	-	-	-
Technological	-	-	-	-	-	-	-	-
Environmental	-	-	-	-	-	-	-	-
Legal	-	-	-	-	-	-	-	-

The definition used in this thesis is based on adaptive EA (Gill 2015) due to its higher relevance to the layers of a digital ecosystem. Adaptive EA is about vital "elements (concepts or properties) of integrated adaptive human (BIPS: business, information, professional, social), technology (ADPI: application, data, platform, infrastructure) and facility (SEHA: spatial, energy, HVAC, ancillary) system or ecosystem (value network of systems) in its secure environment (PESTLE: political, economic, sociological, technological, legal, and environment), relationships (type, strength), and the principles (adaptive design) and evolution" (Gill 2015). The adaptive EA has two key aspects: adaptive architecture design and practice. For the purpose of defining a digital ecosystem (Anwar, Gill & Beydoun 2019), we combine an adaptive EA design and practice in such a way that it covers the maximum possible concepts of an end-to-end digital ecosystem.
Therefore, a digital ecosystem is a group of **people (or organizations)** with a different set of **capabilities** that follow a **process** to work on **information** to deliver **products** and **services** which are accessed via an **interface** that accounts for digital ecosystem **performance**. These are the generic elements that make up the building blocks of a digital ecosystem. These generic elements can be embedded in different sub-layers of a digital ecosystem such as the business layer, information layer etc. Thus, human, technology, facility, and environment will be the top-level perspectives.

2.2.2. Privacy

It is necessary to highlight the historic development of the privacy concept to establish a definition of the privacy right, as well as to simplify the differing descriptions of privacy and which one this research will focus on. The Electronic Privacy Information Centre (EPIC) as well as various researchers such as Beresford & Stajano (2003); Jones et al. (2004) and Langheinrich (2001), categorized privacy into four groups: territorial privacy, bodily privacy, information privacy and communication privacy. This research will focus on information privacy.

With the advent of the World Wide Web, the notion of privacy has become much more vague (Renaud & Gálvez-Cruz 2010). The Internet space is constantly changing to give users new modes with which to communicate, share knowledge and interact with other people or businesses. Constant technological developments and its adoption on digital platforms result in the collection of confidential data on millions of people while safeguarding and supporting their privacy. The collection and centralized storage of sensitive personal information has increased over time with information owners having limited or no control over their information (Pimenidis 2010). This has created privacy awareness at the individual level. However, the concept of privacy is interpreted differently by different people. There are multiple definitions of privacy, each one focusing on different facets of privacy. However, agreeing on one definition of privacy is still an unsolved issue. Therefore, in this thesis, multiple aspects of privacy are explored to provide a foundation for privacy research.

Initial attempts at defining privacy started back in 1890, as proved by "The right to privacy" (Samuel D Warren & Brandeis 1890). Williams (1964) mentioned the concept of privacy as *"the right to be let alone",* like the contemporary concept of privacy (Nissenbaum 2018). Privacy is also defined as: *"the state or condition of being withdrawn from the society of others, or from public interest, seclusion"*(Graham 2019:2). This thesis also explores some industry definitions of privacy. According to Privacy International (Privacy International 2017), it is a basic human right, connected with human self-respect. The formal definition of privacy according to Privacy International is: "*The desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves"* (Smith 2004). The Great Britain Committee on Privacy (1990) contemplates privacy as a right with a specific emphasis on defense against infringement into someone's private life, activities, matters, their family matters, either directly by physical methods or by inferring indirect information. Any unlawful takeover of an individual's right, within a rational or physical boundary can represent a breach of an individual's privacy (Renaud & Gálvez-Cruz 2010). These descriptions come together to devise the notion of a boundary between an individual and the adjacent environment, concentrating on the demarcation of an individual's frontiers.

Given the scale of the Internet, it has generally been an unregulated entity, which is the most significant characteristic that has allowed the unwelcome free flow of information. In any online business, privacy is one of the major issues among many others (Chai & Pavlou 2002; Palvia 2009; Peng et al. 2010; Teo & Liu 2007). The reason for this is that information has become a valuable asset in the global economy, particularly in e-commerce (Azmi 2002) and the use of a customer's personal information is an important component in offering online services. This sensitive information utilized for online transactions is bundled into DigI and thus contains an innate probability of abuse. In fact, protecting the privacy of DigI is imperative and intricate. At the same time, this privacy protection is essential due to the pervasiveness of the technology-driven and

information-intensive environment. The type of information comprising DigI is significantly more vulnerable and susceptible to identity theft. It is not surprising that the concept of privacy has always been a central idea where identity information is involved. As governments and businesses across the globe implement new, DDigI solutions or modernize existing identity programs, there is a dire need for greater privacy practices and procedures around them. It is extremely important for businesses to know their privacy capability. To the best of our knowledge, there is no assessment tool or metric that organizations can use to measure their privacy capability. This

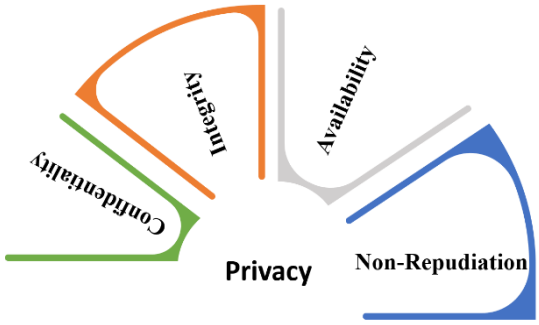


Figure 2.3. Privacy Principles

assessment is usually done through information privacy and compliance practices. Hence, information privacy represents a type of privacy that comprises a challenging section of regulations due to the fast growth of technology, especially after the success of the World Wide Web (Langheinrich 2001). The voluminous exchange of PII is the reason privacy breaches are a common event today, even from well recognized organizations (Adobe 2013, eBay 2014, LinkedIn 2016, Equifax 2019, Dubsmash 2018, Canva 2019). An approach based on the privacy by design (PbD) principle can address the issue of privacy. Therefore, this research focuses on embedding privacy into the design of DigI verification based on the PbD principle. PbD is a particular methodology of privacy, formed by the previous Privacy and Information Commissioner of Ontario, Canada, Dr Ann Cavoukian, in the 1990s (Cavoukian 2010).

Hence, the concept of privacy continued to develop over many years. There is still a lot of variation in the way this concept is interpreted. In this thesis, privacy is interpreted as the confidentiality, integrity, availability, and non-repudiation, as well as the establishment of an individual's frontiers. It is our objective in this research for privacy to be built-in to the design and architecture of DigI verification under four privacy paradigms: privacy as confidentiality, privacy as integrity, privacy as availability and privacy as non-repudiation.

2.2.3. Personally Identifiable Information (PII)

The idea of PII surfaced only in the last five decades and was bound to the advancement of the computer (Schwartz & Solove 2011). PII is any information about a person which is able to identify that individual. It is sometimes referred to as personal information or personal data. DigI verification is based on the PII that individuals share with an organization to prove their identity.

The definition of PII varies depending on the jurisdiction and usage. In the United States, the term "personally identifiable" was used for the first time in 2007 in a memorandum from the Executive Office of the President, Office of Management and Budget (OMB 2020). Afterwards, the definition of PII was made an important part of various standards such as the NIST *Guide to*

Protecting the Confidentiality of Personally Identifiable Information (NIST) (SP 800-122) (McCallister, Grance & Kent 2010). The OMB memorandum distinguishes PII as:
"Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

A term analogous to PII, personal data, is specified in the EU directive 95/46/EC (Directive 95/46/EC 1995), for the purposes of the directive:

"Article 2a: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"
In Australia, the Privacy Act 1988 (Australian Government *1988*) takes care of the end user's privacy by implementing the OECD Privacy Principles (Australian Government 1980) from the 1980s. The definition of personal information according to the Privacy Act 1988 (article 6(1)) is:
"Information or an opinion about an identified individual, or an individual who is reasonably identifiable."
Likewise, the HIPAA Privacy Rule (United States Government 2002) classifies PII in terms of personal specific health information:
"1) that identifies the individual; or 2) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."
Privacy regulations across the world describe PII in a much wider manner. The regulations also look at the potential of indirectly identifiable information and do not present a definitive inventory of informational characteristics that comprises PII. In addition to laws defining PII, researchers give their own interpretations on the definition of PII. According to Narayanan & Shmatikov (2008), information regarding online searches, surfing records, social connections, health records and so forth is PII. Schwartz & Solove (2011) gave the concept of PII 2.0, which treats "identified" and "identifiable" data differently. PII is specified by the Office of Australian Information Commissioner as facts such as birth date, driver's license, social security number, tax file number, or biometric data, that can be used separately or in combination with other records to recognize or advocate an individual's identity (OAIC 2017). It is important to point out that not all PII is crucial in terms of significance and sensitivity (Kuperberg 2020a; Matthews & Esterline 2010; Onik et al. 2019; Rana, Zaeem & Suzanne Barber 2018). As an example, an individual's social security number is unique. This uniqueness makes it vitally significant for their identity. In contrary, an individual's name is also categorized as PII however, it may be possible in most instances that several individuals have the same name. For a notion that is so prevalent throughout the judicial and technological debate on information privacy, defining PII is extremely challenging. In this research, the term PII refers to any direct or indirect information about an individual that comprises the DigI of individuals. This information (PII) can be used to identify an individual.

2.2.4. Privacy Challenges reported in (Anwar et al. 2021)

With the increasing amount of PII, data breaches are also increasing. Investigating and tackling privacy issues demands the analysis of their underlying cause (Phelps, Nowak & Ferrell 2000). Therefore, a systematic literature review (SLR) (Anwar et al. 2021) was conducted to synthesize and draw attention to the noteworthy privacy challenges of PII. We used the adaptive EA

framework for the digital ecosystem (Anwar, Gill & Beydoun 2019) (Fig. 3) as a theoretical framework to derive and code the categories used for structuring, analyzing, and synthesizing the results of this SLR. This approach is suitable for categorizing the results of this SLR as it provides adequate coverage of the privacy & security challenges. Moreover, a frequency analysis of each type was performed to pinpoint the strength and tendency of the research interest in that field.
For this SLR, 79 studies were carefully selected and reviewed. Each selected paper was analyzed and a score of 1–6 was assigned across each of the six criteria. The criteria included research context relevance, research aim, relevance to research question, quality of results, thorough and detailed discussion on results, and future directions. As a result, 21 overall challenges and 11 key privacy and security challenges relevant to PII in the digital ecosystem were identified. It is an arduous task to ensure appropriate levels of privacy and security of PII in a digital ecosystem. It requires appropriate government rules, laws, and policies to deal with security breaches and privacy violations. The detailed analysis of the studies highlights the following privacy-related challenges as presented in Table 2.3:

Table 2.3 Privacy and Security Challenges of PII identified in (Anwar et al. 2021)

Description	Frequency of occurrence in selected articles	Percentage
Inference	17	22%
Lack of consent	14	18%
Social misuse of knowledge	9	11%
Diverse data sources	13	17%
Multiple uses of data	8	10%
Storage and processing	2	3%
Technology gap	4	5%
Agreed data usage	3	4%
Unauthorized Access	6	8%
Lack of governance	11	14%
Data provenance	9	12%

One of the major privacy challenges encountered by a digital ecosystem is the validity of the inferences drawn from non-PII data. The mishmash of PII with non-PII data can lead to new results interpreted in such a way that can lead to the disclosure of an individual's identity without their knowledge and consent. It is possible to use standard data, which does not contain any personal information, to predict sensitive and personal facts about individuals such as bank details and sexual interests (Kshetri 2014). In the mid-90s, Latanya Sweeney, a PhD student at MIT, correctly identified patients by comparing and correlating anonymous health data with a voter database (BUTTLER 2017). A lack of consent is a big problem in terms of privacy. PII is often taken without the data owner's knowledge and is used to gain commercial benefits. It has been reported that iPhones and Android phones are sending an individual's location information to other vendors (Apple and Google) without the consent of the user (Kshetri 2014). In the context of PII,

"the concept of notice and consent underlying the data protection laws around the world is no longer suitable as it is often either too restrictive to unearth data's latent value or too empty to protect individuals' privacy" (Munir et al. 2015). Unwanted consequences are especially high for consumers who are not particularly familiar with technology or are poor and naive (Kshetri 2014). This leads to the social misuse of PII by more informed users. Multiple sources of information pose challenges and may affect people's privacy in digital ecosystems. PII such as health records, financial statements, and DigI information can be accessed via diverse sources that may result in trust alarms. Multiple users can misuse the data collected on an individual. The extent to which the data will be used cannot be controlled at the time of collection especially when no consent is taken (Brown et al. 2011). Data is not always necessarily used for beneficial purposes. Data owners do not have control over data on themselves and hence, they are uncertain about the possible use of this data (Brown et al. 2011). Finally, the infrastructure of a digital ecosystem is expected to uphold end-to-end security. This will ensure that no DigI theft or loss can happen throughout the DigI verification lifecycle. In addition to the need for appropriate technology, there is a need for a suitable governance framework as well. The absence of a suitable governance framework in a digital ecosystem can result in the deceptive analysis of PII and hence can cause high costs (Lafuente 2015). The absence of legal support for the application of data policies (Chauhan, Agarwal & Kar 2016) in relation to big data needs immediate research attention. Uncertain provenance is a bottleneck to privacy and security. Data provenance must be available and certified (Bertino 2014).

The most cited challenges reported in the existing literature are inference (22%), diverse data sources (17%) and a lack of consent (18%). There are no boundaries on data usage at the time of collection. In some cases, it is used for purposes other than the one for which it was originally collected (Brown et al. 2011). The least mentioned challenge in the context of privacy and security is storage and processing (3%), however although this may not represent the importance of this challenge, it indicates its importance in the selected studies.

The focus of this research is on those PII attributes that constitute the DigI of any individual. Hence, PII refers to identity attributes throughout this thesis. Often, identity thieves piece together a potential victim's PII. Safeguarding PII is vital due to its increasing usage for engineering privacy attacks, identity frauds and security incidents. This research will address the privacy challenges of PII in a digital ecosystem by ensuring confidentiality, integrity, availability, and non-repudiation.

2.2.5. Privacy Principles

Information privacy and security has been categorized in terms of "confidentiality, integrity, and availability" (mentioned as the CIA triad) principles for many years (Kumar & Bhatia 2020). In contrast to many foundational concepts in information privacy and security, the CIA triad does not appear to be a static concept; instead, it has emerged over a period of time. According to the Committee on National Security Systems (CNNS 2010), information privacy and security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability". ISO 7498-2 (ISO 1989) describes a basic security architecture and main security attributes, such as authorization and authentication, identity and access management, information integrity, information confidentiality, and nonrepudiation. The CIA triad is the foundation for information privacy which includes the three fundamental characteristics of privacy i.e., confidentiality, integrity, and availability (Chia 2012). When it comes to online transactions, non-

repudiation also becomes an important privacy principle to ensure the authenticity and integrity of online information (Pranata, Skinner & Athauda 2011). Aloraini & Hammoudeh (2017) present an analysis of the three important data security principles within the context of cloud computing, that is, confidentiality, integrity, and availability. In designing a privacy aware DigI reference architecture framework, privacy measures for the confidentiality, integrity, and availability of DigI and associated PII attributes are considered. Hence, the core privacy principles centered in this research include confidentiality, integrity, availability, and non- repudiation. In the context of DigI, these concepts are defined as follows:

Confidentiality: confirms that DigI information is never illegally accessed by the attacker. It ensures the prevention of the unnecessary disclosure of DigI information to unauthorized people or systems. It is a basic requirement to make sure that the privacy and security of DigI is taken care of. This can be achieved by the application of policies and regulations that can restrict access to sensitive information comprising DigI. To address the confidentiality risks, Raju & Sirajudeen (2014) proposed a solution that applies the Cramer–Shoup cryptosystem. Nevertheless, the proposed scheme is tested only with text messages and does not reflect additional file formats. To enhance an individual's control over their information, Jain & Kumar (2016) offered a solution to make sure only the information owner can access it. More recently, a strong data confidentiality scheme was suggested by Saroj et al. (2015) which is based on threshold cryptography. The advantage of this scheme is that it keeps the key management overheads to a minimum. On the other hand, system performance is compromised using many keys along with the extra effort to safeguard them. Nuñez, Agudo & Lopez (2015) introduced a model to ensure the confidentiality of the identity attributes while providing identity services at the same time. The underlying identity management protocol used for this model is SAML 2.0 along with the application of proxy re-encryption techniques. There is a need for a DigI verification solution that is capable of ensuring the confidentiality of DigI information without hindering usability.

Integrity: confirms that during the processing of DigI information, it is not modified or changed by the bad actors. The DigI verification solutions should ensure the highest level of integrity. This leads to an increased level of trust by the identity owners. Retaining integrity can be defined as a method with certain objectives (Mayfield et al. 1991; Pfleeger, Lawrence Pfleeger & Margulies 1997; Sandhu 1994):

a) blocking unauthorised access and modifications to DigI information
b) retaining external and internal uniformity.
c) stopping legitimate users from making illicit changes.

Hence, **integrity** refers to DigI information being legitimate and safe from intentional or accidental alteration or tampering (Balogh and Turčáni 2016). A lot of work (Fieremans et al. 2013; Ghogare, Gupta & Pawar 2021; Gupta, Vathana & Chahar 2020; Hakak et al. 2019; Yoon et al. 2013) has been done towards ensuring the integrity of sensitive information. Ruballo (2018) developed a desktop and web application for digital signatures to enhance data integrity and non-repudiation. Thomas & Meinel (2010) proposed a framework that includes the format and semantic enabling inclusion of a unique identity attribute into security tokens. These tokens are sent from the identity provider to a service provider attached to the attribute value itself. Their proposal adds value in terms of integrity, but they have not defined the mechanism of trust that will enable the real meaning of claim-based identity. Windley (2005) details an identity management architecture that can enhance the confidentiality, integrity, and non-repudiation of a DigI. For a DigI verification use case, we not only need integrity at the information storage level but throughout the lifecycle of DigI verification. This research aims to propose a reference architecture based on which a DigI

verification solution supporting DigI integrity throughout the verification lifecycle can be developed.

Availability: confirms access to DigI information at any time it is needed by the authorized users. It can be described as "ensuring that information and information processing resources both remain readily accessible to their authorized users" (Gill 2015). The concept of availability emphasizes that all the required data and information is always accessible by authorized users. The online availability of PII for DigI verification is not without risks. Hacks, breaches, and even full-blown identity thefts are still quite common. While privacy and security solutions often focus on blocking illicit and unlawful information access, it is just as important that efficient policies facilitate lawful and genuine access. Doherty, Anastasakis & Fulford (2011) state that by creating acceptable use policies, users can ensure the availability of their PII with privacy. To keep the data available under protection, some scholars (Garfinkel n.d.; Lee et al. 2018; Radhakrishnan, Kharrazi & Memon 2005) use data desensitization. Al-Anzi et al. (2014) built an architecture based on reliability, security, and availability for data storage. The Depsky framework was proposed by Bessani et al. (2013) that addresses the confidentiality and availability of data stored in multi-cloud environments. However, to ensure availability, it is paramount that users have control over the information collection methods and should know how their personal identity traits will be used for online validation. This research focuses on enhancing the availability of DigI information while giving maximum control in the hands of the identity owner.

Non-Repudiation: confirms that no one can deny the validity of information. Legally, non-repudiation indicates a person's intent to meet commitments to a contract. It refers to a service that delivers proof of the origin of information and the integrity of the information. In vocabulary and regulatory language, a repudiation is a disagreement to something as legitimate or genuine, for example, denial to repay a debt. Non-repudiation is translated into a way of ensuring that the legitimacy of anything cannot be repudiated or rejected. "Non-repudiation is a much-desired property in the digital world" (Czagan 2019). Wang & Yao (2019) provide a vehicle cloud platform based on remote identity authentication to ensure the confidentiality and non-repudiation of sensitive information. However, their solutions lack an ecosystem-based approach. A permissioned blockchain-based forensics framework to improve the authenticity, non-repudiation, and integrity characteristics for the information gathered was suggested by Le et al. (2019). In addition, they also proposed a cryptographic-based method to address the privacy challenges of identity. However, the framework has not been evaluated for reliability and performance. Sekhar & Sarvabhatla (2012) proposed a protocol offering a secure and privacy aware mobile payment that meets the non-repudiation of delivery, the non-repudiation of submitting an application, and the non-repudiation of a receipt in a digital ecosystem. However, the protocol is based on some assumptions (pre-registered customers, existing trust, pre-existing identity) that limits its applicability.

Table 2.4: Studies covering Privacy Principles

Study	Technology	Confidentiality	Integrity	Availability	Non-Repudiation
(Shaw 2000)	Steganography		✓		
(Windley 2005)	-	✓		✓	✓
(Radhakrishnan, Kharrazi & Memon 2005)	Steganography			✓	
(Thomas & Meinel 2010)	SAML 2.0		✓		
(Gomi 2011)			✓		
(Doherty, Anastasakis & Fulford 2011)	Acceptable Use Policy		✓		
(Sekhar & Sarvabhatla 2012)	Symmetric Key Cryptography		✓		✓
(Bessani et al. 2013)	Cloud of clouds	✓		✓	
(Nuñez, Agudo & Lopez 2015)	SAML 2.0	✓			
(Al-Anzi et al. 2014)	RAID 10			✓	
(Raji, Jazi & Miri 2015)	Peer-to-peer			✓	
(Ruballo 2018)	Digital Signature		✓		✓
(Le et al. 2019)	Blockchain		✓		✓
(Wang & Yao 2019)	Cloud	✓			✓

Table 2.4 highlights some of the recent research studies and the technologies used to address the confidentiality, integrity, availability, and non-repudiation challenges. Most of the aforementioned literature takes into account one or the other principle of privacy. Further, the literature is scarce with respect to a comprehensive and generalized solution that addresses all three privacy principles (CIA) and non-repudiation altogether. This research closes this gap by providing a DigI verification framework which attains all these principles of privacy. DigI and the broad set of PII used to prove the identity of individuals is intricately associated with security and privacy. Both privacy and security are focused on ensuring that PII is protected against unlawful access and use, although both need organizations to diligently gather and administer PII for lawful usage. For DigI verification that runs on processing PII, organizations cannot survive if customers do not trust them. To achieve the stated privacy values, it is imperative that all the available layers of the identity ecosystem are protected to ensure the privacy and security of DigI and the identity owners.

2.2.6. Identity Ecosystem

It is justified to affirm that each organization requires an ecosystem strategy (Valdez-De-Leon 2019b). With the varying approaches to DigI, it is easy to see how a single united online identity would prove to be evasive. In this context, an identity ecosystem can be created and retained by federal governments, educational institutions, financial institutions, employers, individuals, and groups of them, for different goals. The identity ecosystem, for all aims and objectives, embodies the collective endeavor of a broad range of stakeholders in setting up trustworthy identities on the web. As described in the National Strategy For Trusted Identities In Cyberspace (NSTIC 2011, p. 2),the identity ecosystem is *"an online environment where individuals and organizations can trust*

each other because they follow agreed-upon standards and processes to identify and authenticate their digital identities". Former chief identity architect at Microsoft, Kim Cameron (2005) wrote in his article, "The Laws of Identity" that a partnership between industry and academia has specified fundamental aspects of an identity ecosystem. It has generally been acknowledged as a standard and guideline for developing DigI solutions (Hansen, Pfitzmann & Steinbrecher 2008). Although traditional identity ecosystems are not disappearing, they are continually being modified and improved. Numerous identity ecosystems have now been created, while others are still evolving, each employing distinctive digital models and practices. These systems typically overlap and can diverge depending on the scale varying from global to micro-identity systems.
Different identity ecosystems exhibit different DigI verification models. Although DigI verification models have evolved enormously to address the challenges of identity theft and fraud, the risks associated with the traditional and latest objectives of DigI continue to exist and will differ depending on the specific technological or organizational background. There is a need for more adaptability in an identity ecosystem to address the ever-changing risk environments. Adaptive EA (Gill 2015) can gradually respond to the new information related issues as they involve the creation and usage of identity. Hence, the definition of an identity ecosystem used in this thesis is based on adaptive EA. Individuals and institutions equally require more in-depth insight into privacy-related risks, threats and subsequent repercussions as the scope and impact of identity-related crimes persist in growing. To address this demand, we present the identity ecosystem as a "human-centric (HUMAN) connected environment (ENVIRONMENT), a collection of organizational policies, technologies (TECHNOLOGY), processes and approved standards that securely (PRIVACY & SECURITY) enable communications (INTERACTION) ranging from unidentified to fully authenticated and from lesser to higher worth based on data stored in a secure data center (FACILITY)" (House & America 2011; Gill 2015).The main layers of an identity ecosystem are presented in Figure 2.2.

2.2.7. Digital Identity

PII is vital and the certain kinds of PII that are presented throughout DigI verification is precisely what hackers and identity thieves are searching for (Kuperberg 2020a; Matthews & Esterline 2010; Onik et al. 2019; Rana, Zaeem & Suzanne Barber 2018). DigI verification is playing an ever more pivotal role in an individual's life as an increasing number of daily interactions are moving online. The digital economy is growing fast (Kuperberg 2020a; Wu 2020). According to 2021statistics, 92.6% of users around the world bought products and availed themselves of services on the Internet (Johnson 2021). The United Nations assesses the worth of the digital economy to be as high as the world GDP (GSMA 2020). 'Am I who I am claiming to be?' is the query at the essence of DigI (Bouma 2018). There is no straightforward answer to this question due to the multidimensional and intricate nature of DigI (Meng & Agarwal 2007). To address this issue, identity owners try to prove their identity to entities intending to achieve a mutual understanding. DigI is often thought of as a subtopic of privacy (Windley 2005). It can relate to the account names and digital footprints that identity owners select and create online for multiple reasons, such as transacting with banks, buying products or availing services (Whitley & Hosein 2010).
DigI is the most talked about subject in the literature. Cameron (2005) identifies a digital subject as a *"person or thing represented or existing in the digital realm which is being described or dealt with"*. He describes a claim as an *"assertion of the truth of something, typically one which is disputed or in doubt"*. So, in simpler terms, a digital identity is a "*set of claims made by one digital*

subject about itself or another digital subject." Ben Ayed (2014, p.15) explains that "*identity is defined as a collection of data about subject that represent attributes, preferences, and traits, so in parallel, in the digital world a person's identity is typically referred to as their digital identity.*" Windley (2005, p.3) explains a digital identity as follows: "*A digital identity contains data that uniquely describes a person or thing but also contains information about the subject's relationships to other entities.*" A report written by PWC (2019, p.4) defines a digital identity as *"a set of digitally captured and stored attributes such as name, date of birth or gender coupled with credentials that are linked to a unique identifier to identify a person and thereby facilitate transactions in the digital world".*

Several authors in the early 20th century also highlighted the value of identity to specifically comprehend human behaviors and generally understand societies (Leary & Tangney 2011). In terms of the privacy debate, the concept of DigI turns out to be extremely significant, simply owing to the related risk of privacy breach and identity theft. However, examining privacy in the context of DigI is not a straightforward undertaking. This is due to the multidimensional nature of this notion (Brubaker & Cooper 2000). For example, DigI aids in explaining certain behavioral responses, irrespective of their origin (ethnic, social, racial, or general variations) (Moshman 2007; Baum 2008; Schwartz, Dunkel & Waterman 2009). It impacts an individual's preferences and choices (Kroger 2007). Identity also adds to the practical opinion of the powers individuals get from societal and public connections (Ellemers, Spears & Doosje 2002; Schildkraut 2007). The ambiguity of this idea has even led some authors like Baumeister (2011) to think that DigI "is not really a single topic at all, but rather an aggregate of loosely related subtopics". Furthermore, Cameron (2005) defines DigI with reference to two of its basic elements: subjects and claims. Therefore, DigI can be defined as the digital version of the facts known about a certain entity (Bertino, Paci & Shang 2009). The Global System for Mobile Communications states that in recent times, DigIs are increasingly becoming an integral part of an individual's daily life as they switch to a mobile world. These DigIs anticipate the manner in which individuals act, transact and do business. In the business community, utilizing the strength of DigIs is an essential component of conducting business, especially when it is about fulfilling different compliance and customer due diligence obligations (Kvitnitsky 2018). DigI is not a new concept, rather it has always existed in our routine lives. The hardest part is binding an individual to DigI, helping them to use their e-mail account, financial statements, and bank accounts. DigI architects are constantly struggling to create safer methods to introduce more people to this journey of digital transformation in an efficient manner (Brunetti et al. 2020; Heavin & Power 2018a, 2018b; Henriette, Feki & Boughzala 2016; Nambisan, Wright & Feldman 2019; Wolf, Semm & Erfurth 2018). Malik, Anwar & Shibli (2016) discussed in detail the current federated DigI verification and considerations such as trust acquisition and management, and the protection of an identity owner's privacy as the core components whilst adopting models of DigI verification. Zhang (2020) describes that DigIs allow acquaintances to connect with us, authorities to examine and evaluate us and media boards to monetize us. Bertino et al. (2010) argue that DigI information is privacy sensitive, hence it is imperative that appropriate privacy and security procedures be embraced for its defense.

A variety of aspects can compile a single DigI, each one with a different level of trustworthiness and consistency. Though the involvement of PII in DigI makes it a very sensitive concept for information privacy researchers, the concept of DigI used in this research is not only PII-based. DigI can comprise any non-PII attributes (such as comments and likes on social media, tweets on Twitter) that can link to PII and hence identify individuals. Tredinnick (2019) asserts that DigI is

established by individual profiles, ethnic investment, and data like videos on YouTube. From this, we infer that DigI is a combination of business information, social information, professional information, and information from identity documents.

2.2.8. Identity Theft

Identity theft or the illegal use of DigI has a similar impact on identity owners, organizations and government institutions (Tomison 2015). According to the results of the surveys carried out by the Australian Institute of Criminology, 20 percent of participants have had their DigI or underlying PII mishandled (Smith & Jorna 2018). As one of the rapidly increasing criminal activities globally, different people interpret identity in different ways. A few researchers (Priesnitz et al. 2021; Reyns 2013; Wei, Zhang & Hua 2019) have reasoned that an individual's identity which includes PII attributes such as biometric information cannot be stolen. On the other hands, some scholars (Smith & Lias 2005; Holt & Turner 2012; Schreft 2007) look at the challenge of identity theft as a superset for referring to the unlawful employment of identity attributes such as first name, last name, phone number, home address, or other identity documents issued by government institutions for the purpose of committing crimes. Numerous scholars (Copes & Vieraitis 2009; Brody & Kiehl 2010; Friedrichs 2019; Randa & Reyns 2020) classify identity theft as a "white-collar crime". Scholars do not reach an agreement on a generally accepted characterization of identity theft (LoPucki 2001; Koops & Leenes 2006; White & Fisher 2008; Biegelman 2009; Finklea 2010; Cheney 2011; Finch 2012)**.** Despite the difference in definitions, identity theft involves some common elements that can help in developing a common concept. Such elements are an individual's first name, last name, address, phone number, date of birth, attributes issued by government such as passport number, social security number, medicare card number, driver's license number, financial details, credit card numbers, professional information, and other highly sensitive PII. The FBI (FBI n.d.) defined identity theft as illegally acquiring someone's PII and employing it for committing theft or scam. Identity thefts challenge organizations to think differently about customer engagement.

The frequency and complexity of identity theft continues to increase. Regardless of this increase, not much work has been done on the identity theft response mechanisms and how victims can be assisted to recuperate. Any controls and procedures developed to address the problem do not take into account the requirements, needs or experience of sufferers (Marsh, Cochrane & Melville 2004). Neira & Capstone (2016) proposed security measures to avoid identity theft by analyzing what goes on inside a cybercriminal's mind. Although existing research has investigated the emotional implications of identity fraud, the precise structure of the response strategies, their legal status and technological support to implement a response system have not been adequately explored.

2.2.9. Models of DigI Verification

The overall architecture of DigI verification is comprised of an Identity Issuer (II), Identity Provider (IdP), a Service Provider (SP) and an Identity Owner (IO). Since the birth of the Internet, as stated by Christopher Allen (2016), a DigI verification model has been established across four stages: Centralized Identity, Federated Identity, User-Centric Identity, and now Self-Sovereign Identity.

a) Centralized DigI Verification Model

A centralized DigI verification model is where a single reliable IdP is in charge of the collection and provision of identity information. Typically situated in a secure realm, this model supports Single Sign On and sharing DigI with multiple SPs. However, the challenge of a single point of failure for the IdP exists (Bourass et al. 2014). If IdP is compromised, the whole DigI verification system will fail. Problems with giving the control of the DigI to centralized authorities are the same as in the physical world: identity owners are tied to a single entity who can refute their identity (Zwattendorfer, Zefferer & Stranacher 2014). Centralization removes the control of the DigI from the identity owner and gives the authority to the centralized entities (Allen 2016). The centralized architecture resembles existing document-based systems, in the sense that there still is a central body in control of all the DigI information as well as transactions over the network. Challenges such as privacy protection, identity fraud and access across distinct areas are very few constraints (Cao & Yang 2010). A more robust DigI verification model should let users recycle a DigI they created with one IdP with other websites and online services. Today, this is the dominating solution for managing online identities (Palvia 2009). However, there has been an increasing intent to return the command of the DigI to the identity owner's control for the last two decades (Allen 2016; European Union 2018).

b) Federated DigI Verification Model

Federated DigI verification supports the administrative control by multiple, federated authorities. Microsoft had long been planning to develop a federated identity and in 1999, they launched Microsoft Passport. This initiative allowed identity owners to create a DigI that could be used on multiple sites. Nonetheless, in the end, this was almost as centralized as before since it designated Microsoft as the centralized authority (Allen 2016). In response, Sun Microsystems, with the intention of eliminating central power, founded the Liberty Alliance (Liberty Alliance Project 2008). In this attempt to build an "authentic" federation, they ended up with an autocracy. The power of centralized authority was instead spread between many powerful entities (Cao & Yang 2010). Federated DigI verification made it possible for identity owners to go across multiple sites under the same scheme. Yet, every site continued to be a controlling authority (Allen 2016; Bourass et al. 2014). The IdP's tasks are scattered between quite a few IdPs, and in distinctly protected domains. This model requires a web of trust to be set up between the SPs and the IdPs to provide a single sign on to IOs associated with many IdPs and SPs.

Yet, in this model, the problem of centralized authority has not been resolved. The IOs still do not have the full ownership of their identity information, since they are stored in the IdP's database, and they can be revealed to a third party without their consent. Like a centralized model, the basic constraint of a federated DigI verification model is also the IdP playing as the central authority. There is no federation that can provide services to everybody around the world, and every federation is obliged to abide by the privacy procedures and guidelines its IdP can sustain. For instance, Facebook users are unable to utilize their DigI to log into their university account. Additionally, DigIs remain useable beyond the federation, therefore there is a level of client lock-in to a federation that remains in complete disproportion to the physical transferability of the DigI attributes individuals hold in their pockets to demonstrate they are who they claim to be in the physical world. Most crucial challenges of federated DigI verification are due to mishandling DigI information, DigI theft, and the lack of trust between IdPs and SPs.

c) User-Centric DigI Verification Model

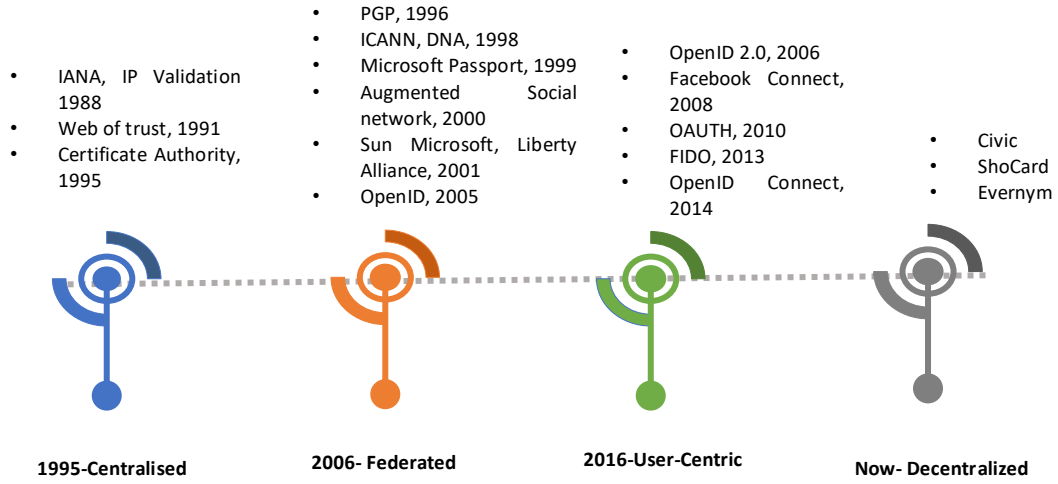


Figure 2.4. Timeline of Identity management Models

User-Centric DigI verification is where the IO has all the rights and power with no federation in between. The Augmented Social Network (ASN) group felt that : "every individual ought to have the right to control his or her own online identity" (Jordan, Hauser & Foster 2003a), that Microsoft's Passport and the Liberty Alliance did not attempt to achieve the same objectives because the "business-based initiatives" regard IOs as customers. ASN published a comprehensive white paper (Jordan, Hauser & Foster 2003b) in which they offered the construction of a "persistent online identity". This turned out to be the groundwork for a novel DigI (Allen 2016). With decentralization as the focus, The Identity Commons, a community that works for an open identity layer for the Internet, started improving the new work on DigI. In conjunction with the Identity Gang, the alliance of Identity Commons, they created the Internet Identity Workshop (IIW). The IIW's work supported several new methods for creating DigI such as OAuth and OpenID. Two principles that the User-Centric Identity methodologies usually focus on is user consent and interoperability, and these two principles can together give the opportunity for a user to decide to share an identity between multiple systems. The intent of the User-Centric Identity community was to offer identity owners full possession of their DigI. Nevertheless, still today User-Centric Identities' ownership is retained with the bodies who sign them up. According to Christohper Allen (2016), co-author of the TLS Security Standard, "being user-centric is not enough".

d) Self-Sovereign/ DDigI Verification Model

The next step of DigI verification demands IO's independence. This is the focus of the Self-Sovereign Identity (Allen 2016), which is an identity that the individual is in control of, without the need for trusted third parties (Tobin & Reed 2017). Self-Sovereign Identity, which is alternatively known as DDigI, is the focus of this research.

Table 2.5. DigI Verification Model Challenges

IDM Model	Characteristics	Technology	Privacy Protection	Best suited for	Challenge	Example
Centralized IdM	IdP controls user data, Centralized data is a honeypot for identity frauds, Controlled by a single entity.	ID/ Password MFA	Weak protection	To deliver a specific form of the fact and a thorough, precise, and consistent picture of non-confidential information among multiple users	Single point of failure, Centralized decision making, Surveillance.	Okta
Federated IdM	IdP's functions are distributed among several IdPs, Controlled by multiple entities.	SAML OAuth	Weak Protection	To deliver a specific form of the fact and a thorough, precise and consistent picture of information whilst letting users authenticate to a group of third parties, thus removing copyrighted logins	Lack of user control, Identities are not portable, User lock-in	Facebook, Google, Microsoft Passport
User Centric IdM	Users select IdP functions to aggregate the identity data, Individual or administrative control	OpenID Minimal Disclosure Tokens Minimum footprint technologies	Relatively better protection	To provide strict control of information flows by the user and data minimization	IdPs governance to use personal data	STROK PICOS Cardspace PRIMELife
Decentralized IdM	Portable and Reusable identity, Users control their identity information, Individual Control	Blockchain Cryptography Digital Signatures	Strong Protection	To integrate several IdPs and RPs, offering ease of use, user control and privacy in a digital world	Lack of standards, Lack of recommendations to address full user lifecycle, Data Permanence, in some cases centralized authority stores biometric data.	Civic, Evernym, IDKEEP, CULedger, ShoCard, ID2020

This DigI verification model, commonly known as DDigI verification and more specifically as self-sovereign identity, was non-existent until recently. In the past, the underlying technology for DigI entailed Internet-scale federated DigI procedures i.e., OpenID Connect and user centric information distribution procedures i.e., User-Managed Access (UMA) (Maler & Reed 2008). Numerous conferences on blockchain identity were organized at the 23rd Internet Identity Workshop in October 2016 (*iiw 2020 | iiw On-line Annual Assembly - July 15/25* n.d.). Subsequently, the U.S. Department of Homeland Security Science & Technology (United States 2003) initiated a Small Business Innovation Research (SBIR) grant topic, "The Applicability of Blockchain Technology to Privacy Respecting Identity Management" (Sbir.gov 2015). While interest in DDigI verification has increased over the last few years, the road to build this type of DigI is quite old. The methodology to develop blockchain-based DigI verification is influenced by the years of experience acquired. Considerable work is yet to be done to implement true decentralization in DigI verification and fill the existing gaps.

The first and most noticeable gap lies in standards regarding the design and development of blockchain-based DDigI verification. The basic elements of this technological enhancement are already defined, such as the Decentralized Identifier Data Model (Reed, Sporny & Allen 2019)

which were in draft phase in 2019. In November 2019, the Verifiable Credentials Data Model 1.0 specification (N. Otto, S. Lee, B. Sletten, D. Burnett, M. Sporny 2019) was issued in the form of W3C recommendation. The Rebooting the Web of Trust Conference, the W3C Credentials Community Group, the Hyperledger Project, the Decentralized Identity Foundation, and many other communities are trying to incubate standards for the interoperability and portability of SSI. However, detailed guidelines covering the entire DigI verification lifecycle are still missing. In addition, there is a need to develop proofs-of-concept and prototypes to address security and privacy concerns in DDigI verification solutions. Another grey area exists when it comes to the finer suggestions and the safest approaches to focus on the complete DigI verification lifecycle, covering the loss or theft of DigI documents, public and private keys, devices or blockchain wallets. Blockchain-based DigI verification solutions face the challenge of the immutability of DigI information, which could theoretically contradict privacy obligations like the GDPR's "right to be forgotten." The resolutions of all these concerns should not only be technical like not storing PII on-chain but statutory and regulatory as well. DigI verification solutions not only need to address existing concerns, but also future challenges that are yet to come.

2.2.10. Blockchain

Blockchain is an "immutable distributed ledger" that preserves the possession of digital assets in the form of transactions and blocks (Nakamoto 2008). The invention of blockchain technology by Satoshi Nakamoto (2008) heralded a new wave of innovation for individuals and companies able to see its huge potential. A blockchain network is made up of peers, each keeping an identical copy of the ledger data controlled through peer-to-peer (P2P) interactions. Unlike conventional decentralized P2P networks, in which each peer functions individually, in blockchain the decision is taken via a consensus between the peers. Blockchain is one of the key advancements in the digital era, where almost everything is digital or is digitally represented and associated (Aydar & Ayvaz 2019). This advanced blockchain technology can bring openness and trust to a digital ecosystem by designating a DigI to each stakeholder/node/entity, decentralizing data storage instead of centralizing, and automating the entire procedure with smart contracts. Thus, the idea of DDigI verification is a vital component and possibly the initial point of a blockchain network. Blockchain integrates trust in the network and hence can be a cornerstone for secure DigI verification solutions. As for DDigI verification, blockchain empowers IOs (Casino, Dasaklis & Patsakis 2019) to own their DigI by maintaining the sovereignty of their DigI, controlling access to their PII and disclosing minimum data along with certifying integrity and trust.
The basic architecture and design of blockchain technology offer features such as transparency, auditability, robustness, and security (Christidis & Devetsikiotis 2016; Greenspan 2016). Specific limitations such as performance, scalability of platforms, and regulatory compliance continue to persist (Fridgen et al. 2018). In spite of the limitations, the speed with which this technology is adopted, demonstrates its suitability for a variety of applications (Hileman & Rauchs 2018). There can be several use cases of blockchain technology instead of simply managing the Bitcoin business system (Di Battista et al. 2015; Casino et al. 2020). Blockchain-based DDigI and access control schemes can be employed to improve DigI verification solutions (Defranco et al. 2021). Similar arrangements have been applied in the past for storing information about products and provenance, DigI credentials, business attributes, and digital rights. Table 2.6 shows the projects which apply blockchain in the management of identity. Several researchers have emphasized that DDigI verification is the much-needed advancement of DigI verification, and it can be accomplished exclusively based on decentralized and distributed features of technology which blockchain holds

as its fundamental properties (Al-Zaben et al. 2019). Many proposed use cases of blockchain in DDigI verification (Civic, ShoCard, Uport, Evernym) focus on leveraging blockchain to manage PII that comprises DigI. Alketbi, Nasir & Talib (2018) listed numerous use cases and debated the technical benefits of blockchain, for example hashing, cryptography, digital signatures, smart contracts, and consensus mechanisms, augmenting DigI verification with transaction logs ensuring regulatory compliance. Jacobovitz (2016) talks about the recent trends and application of blockchain technology, emphasizing solutions and applications in DigI verification. A report by Deloitte detailed voting using blockchain-based DDigI verification. The Australian government also revealed its intention to organize digital voting through blockchain technology in an attempt to cut costs and increase the effectiveness of parliamentary elections (Pawczuk, Massey & Schatsky 2018).

Detailed discussions on DigI and centralized DigI verification solutions have concluded that DDigI verification solutions are critically needed for the provision of self-sovereign rights for IOs to own, control and reserve PII rather than becoming a target of identity crimes and data breaches (Kuperberg 2020a; Rivera et al. 2017). Blockchain has surfaced as a vital technology that might comply with these technical requirements to set up a system of self-sovereign DigI verification. This thesis uses blockchain technology for DDigI verification design and investigates the use and feasibility of blockchain as an underlying technology to guarantee the privacy, security and regulatory compliance of

Table 2.6: Blockchain based DigI Solutions

Project	Description
Bitnation	A governance program fueled by blockchain technology
e-Residency	Estonian smart card that can be used by residents to sign documents.
ConsenSys	Decentralized software facilities and products that run on the Ethereum blockchain
ID2020	A project to provide a legitimate DigI for each individual by 2020
Australia Post	AI driven DigI verification
Platform Identity Management Netherlands	An organization based in the Netherlands concentrating on identity management systems
ShoCard	An identity verification platform built on blockchain
Uport	A venture by ConsenSys3 aimed at identity management.
Ascribe GmbH	A project to build technical means for artists to facilitate the management of their identities.
I/O Digital	A blockchain-based identity management startup
BlockVerify	A startup company developing blockchain-based solutions
BlockAuth	Individual's identity administrator permitting users to present their identity attributes for verification.
UniqueID	A biometric-based identity and access management
Jolocom	A blockchain-based self-owned personal DigI
Cambridge Blockchain	A blockchain-based identity platform for the secure authentication of DigI documents, processing electronic signatures, and bookkeeping.
Cryptid	Eliminates the risk of fake identification by combining elements of identification and encryption.
CertCoin	A project undertaken by MIT student on NameCoin based 27 decentralized authentication system which holds a domain ledger and accompanying public keys.

DDigI verification, and the related issues concerning the confidentiality, integrity, availability, and non-repudiation of PII. The thesis proposes a reference architecture for DDigI based on identity documents, verifiable claims, unforgeable transaction logs, and enhanced user control, which are internationally operable and portable throughout the life of an identity owner.

2.2.11. DigI Verification

Information about DigI is gradually becoming an indispensable enabler of the modern digital world because it plays a major part in the communications between IOs, SPs, and any entity in between. On the other hand, due to its value for marketing and strategic advancement reasons or, merely, for selling to interested companies it is also becoming more advantageous for organizations managing DigI information (Kanyengo 2009; Roxana MOSTEANU & Faccia n.d.; Succar & Poirier 2020). DigI verification proves that the subject exists or is true or correct (Aiello, Lodha & Ostrovsky 1998; Aydar & Ayvaz 2019; Bertino et al. n.d.; Meng & Agarwal 2007). When DigI is verified using a digital means, it is referred to as DigI verification. Hence, DigI verification

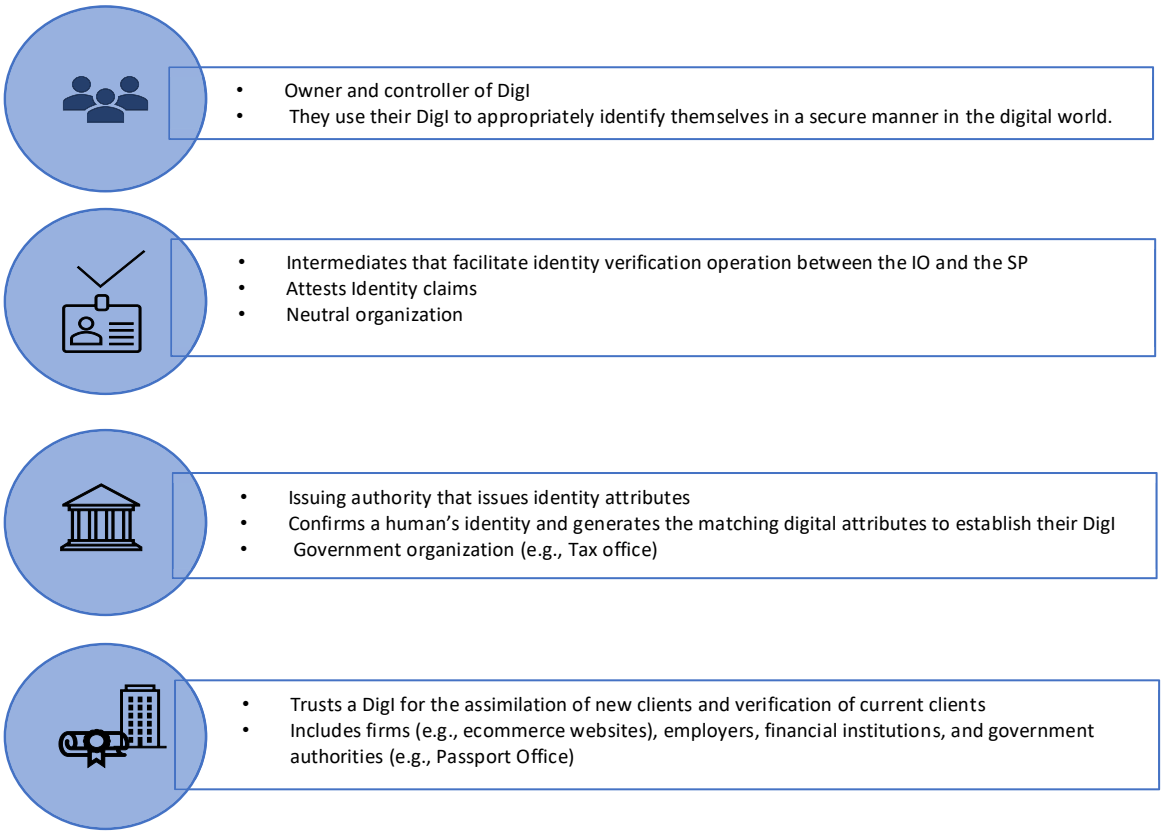


Figure 2.5. Digital Identity Verification Entities

is a practice which confirms an individual's distinguishing attributes and validates them as an actual person. Consequently, DigI verification continues to be a key challenge in the field of information privacy and security and covers multiple sub-fields, like user experience and reusability, authorization techniques, or trust and reputation administration (Dhamija & Dusseault 2008). Therefore, to increase the privacy and security safeguards, DigI needs secure handling at each stage of its life cycle. The life cycle of DigI differs with each DigI verification model. Research has many versions of the DigI lifecycle (Bertino, Paci & Shang 2009; Petullo & Solworth 2011). Figure 2.5 shows a simple view of a DDigI verification process that describes the flow of information between participants.

A typical DigI verification process involves four entities, as shown in Figure 2.5. The PII (such as authorities which issue driver's licenses and passports) issues identity attributes to IO (any person e.g., Alice, Bob). The IO presents their identity to an SP (such as banks, universities, employers)

to avail themselves of their services (such as opening a bank account). The SP verifies the identity attributes provided by the identity owner through IdP (such as Civic, uport). The way these participants interact with each other differs depending on the DigI verification model. Other participants can be involved as per the specific use case.
For DigI to fully utilize its capability, it is important that the underlying PII is strongly protected. DigI verification systems must ensure that DigI is not mistreated, and an individual's privacy is assured. In this thesis, we focus on a DDigI verification design for the privacy preserving verification of DigI, based on blockchain technology. The aim is to ensure that digital interactions are safer yet simpler, while privacy is protected. Hence, we adopt an ecosystem approach in the development of blockchain-based DDigI verification reference architecture.

2.2.12. Privacy Regulations

In the DigI verification realm, privacy provision is inevitable for safeguarding PII (Barth et al. 2019). With increasing digitization, DigI has gradually become a well-known concept, but still not completely understood. Many people are now aware that they have a DigI but its current and future legal landscape, its business purpose, and its impacts, are not properly realized. A number of regulations (Privacy Act 1988, GDPR, eIDAS, HIPPA, COPPA) have been devised and revised over the years to guarantee the privacy of citizens. The administration and continuing upkeep of the privacy requirements for DigI is very challenging due to a broad spectrum of interrelated but often dissimilar laws and regulations applicable to various kinds of information and areas (Holt & Malčić 2015). The law makers confront a lot of problems that arise while managing information that extends beyond the legal boundaries in the digital ecosystem (Kar et al. 2018; Sinha 2018). Jamieson et al. (2008, p.10) state that "the United States leads all countries in enacting identity theft laws from a national and state level". Nevertheless, as identity thieves are constantly finding new and more complex methods for accessing PII and committing identity crimes, regulations will also have to evolve. Data security breaches (Verizon 2020), such as the recent publicized storage losses of private data by many companies (Facebook, Google, LinkedIn), are rightfully calling into question how storage is protected. Government regulations such as eIDAS and GDPR, and international standards (ISO 27001, ISO 27701) which address the security and privacy of PII, are also spurring interest in storage security. Although many proofs of concept have been developed for a blockchain-based DigI verification solution, none of them discusses and ensures regulatory compliance in detail. Therefore, this thesis fills this gap by designing a DigI verification reference architecture that ensures GDPR compliance.
Many nations in the world including American, Asian, and European areas are following data protection obligations, for instance the extensively conversed UK Data Protection Act 1998 (DPA), Personal Information Protection Act of South Korea, the Freedom of Information Act 2000 (FIA) of United States, European GDPR, the Privacy Act 1988 in Australia, and Personal Data Protection Act (PDPA) in Malaysia to address data protection challenges. As detailed in a separate paper (Anwar, Gill & Beydoun 2018a), the GDPR sets out the procedures concerning the privacy of people in relation to the processing of PII and the requirements concerning the transfer of PII. GDPR has a broader scope that enables it to make sure that individuals and businesses comply with the law and safeguard their personal data (Anwar, Gill & Beydoun 2018a). The term personal data used in GDPR refers to PII, but it has a wider range. DigI consists of PII, hence, GDPR is pertinent for the topic of DigI verification. In addition, possibly the most significant EU regulation dealing specifically with identity is eIDAS. eIDAS is a set of standards for "electronic identification and trust services" for digital operations in the EU Single Market (Lyons, Courcelas

& Timsit 2019). eIDAS pertains to government-issued identity attributes and has a profound effect on the DDigI verification solutions, hence, it is worth a closer look. However, for the major part, the regulatory guidelines for this thesis are taken from GDPR.
In general, GDPR has a contradictory connection with blockchain technology and must be carefully considered when implementing a blockchain-based DigI verification solution. However, designing a blockchain-based DigI verification solution is a challenging task due to some inherent contradictions between the nature of blockchain and GDPR requirements. One such example is the "right to erasure". The phrases 'erasure' and 'erase' are mentioned many times in the official documentation of the GDPR (European Union 2018). It is contrary to the immutable nature of blockchain. This view is also underpinned in GDPR Art. 17 "right to be forgotten", nevertheless, 'erasure of data' has not been specified in the regulation. This gives the legal foundation for a rigorous translation of the phrase "erasure of data". Thus, even encrypting PII and destroying encryption keys will not be satisfactory as the "erasure of data". It should be noted that the existing blockchain-based DigI verification solutions do not provide in depth details of their GDPR compliance status. This represents a significant research gap and will be addressed in this thesis.

2.2.13. Adaptive Enterprise Architecture

An ecosystem tends to extend outside its original boundaries. It signifies that new market entry may not occur by individual efforts, but instead by adjusting the whole ecosystem that manages market existence, infrastructure, and reputation (Gawer & Cusumano 2014). One such example is Nokia, which lost its paramount status to new competitors who adopted an ecosystem approach. Recently, Apple secured market share from Spotify by harnessing its market strength in relation to operating systems, mobile devices, and application distribution after entering the music streaming business (Apple Store). This is applicable to identity ecosystems as well. It is important to note that identity attributes (such as marital status) can evolve over time (Wang & De Filippi 2020). Identity is not developed as a result of a one-off process, rather it is built progressively over a course of time and continually develops as an outcome of the interactions with the individual's environment (Eakin 2019). Therefore, DigI is ever changing and multidimensional. For this reason, each DigI verification solution should be constructed so that it is adequately adjustable, robust, and adaptable to respond to the ever-changing and intricate nature of DigI, privacy risks, business needs and legal compliance obligations. Additionally, the stringent regulatory obligations for information privacy, information exchange and data protection add to the complexity of managing and processing PII for DigI verification. In the EU, most recent legislation concerning privacy and data protection include the Payment Services Directive (PSD2) (European Commission 2016), which regulates how banks and retailers share consumer information to simplify payments, and the GDPR, which has strict controls around the collection and usage of customer data. In the United States, the California Consumer Privacy Act (CCPA) (State of California Department of Justice 2018), which is yet another comprehensive information privacy law, took effect in 2020. These regulations introduce the risk of strict consequences for non-compliance and indicate the seriousness of information privacy. This means that DigI and related verification operations need to adapt to the speed of increasing cyber threats and changing regulatory requirements and business needs.
In this information-saturated age, when complex regulations and varying privacy risks are to be faced simultaneously, an adaptive DigI verification solution must keep pace with the speed. To the best of our knowledge, there is no research-based adaptive and privacy aware DigI verification

architecture that ensures compliance with relevant regulations. This thesis presents a DigI verification reference architecture that can keep pace with this change to remain relevant and effective. Adaptive EA (Gill 2015) is used as a kernel theory to design such an architecture.

2.3 Research Gaps and Questions

The success of DigI verification solutions lies in finding a balance between usability against non-negotiable regulatory compliance, and privacy and security needs that arise from processing PII, whilst maintaining a high success rate in verifying an individual's DigI accurately to combat fraud. The literature review detailed in section 2.2 further identifies the research gaps highlighted in Figure 1.1.

Table 2.7 Research Gaps

DigI Verification Challenge	Research Gap	Research Question
Changing privacy risks	The ever-changing privacy risks are overlooked if not monitored and analyzed at regular intervals considering all possible environmental factors	RQ1 must address the challenge of assessing the environment for ever-changing privacy risks and threats.
Unknown privacy capability	The DigI verification solutions seldom conduct self-assessment to analyze their privacy capability and take necessary actions	RQ1 must provide a means to self-assess the privacy capability and work towards continual improvement
Emerging technologies	There are many technologies that can offer DigI verification however there is no metric which can assess the feasibility and suitability of technology in light of the regulations.	RQ1 must provide a metric that can assist in the assessment of the viability of technology for use in a DigI verification solution. RQ2 should provide a design based on the technology's viability for DigI verification
User control	The large majority of current blockchain-based DigI verification solutions either involve service providers giving IOs access to their own data and information that they ultimately control or involve third-party identity providers to manage their authenticators with the ability to use them on their behalf.	RQ2 must design a DigI identity verification architecture that puts maximum control in the hands of the identity owner.
The variety of identity documents	There are multiple sources of DigI information beside government-issued identity documents. Most DigI verification solutions today verify a limited number of identity documents excluding certain important identity information such as social identities and professional identities	RQ2 must address the issue of multidimensional DigI information by providing a DigI structure that covers all possible sources of identity
Repeated DigI verifications	DigI verification solutions provide reusable DigI by storing the IO's PII	RQ2 must address the challenge of reusability and put maximum control in the hands of IO at the same time
Rising identity thefts and frauds	Even after decentralization, identity theft and identity fraud are on the rise	RQ2 must provide a solution to minimize identity theft and fraud
Digital trust	It is hard to develop a web of trust between all the entities involved in DigI verification.	RQ2 should enable the development of a web of trust between involved parties
Synthetic identity	The social security number of one individual, date of birth of another individual, and an address of yet another individual may be used to successfully build a counterfeit or "synthetic" identity	RQ2's main aim is to address identity fraud such as synthetic identity
Compliance and user experience	In an effort to comply with stringent regulatory requirements, the existing solutions make the verification process complex, especially for users who are not experienced with technology use.	RQ2 must ensure compliance along with a seamless digital experience and a smooth and easy DigI verification process.
Lack of a structured process for updating and re-proofing identity attributes	Blockchain is immutable, so in the case of a change in identity attributes (such as	RQ2 must ensure the IO's right to erasure and rectification

	surname change after marriage) the DigI cannot be rectified	
Different DigIs used for specific limited context	DigIs keep on evolving. The existing DigI verification solutions cannot adapt to the speed of changing multidimensional DigI information	RQ2 must consider multidimensional DigI and adapt with changing DigI attributes
Changing privacy risks, regulatory requirements, and business needs	Most DigI verification of today are designed for one particular jurisdiction or organization and hence comply to a particular regulation. Organizations have to keep up with changing regulations and privacy risks.	RQ3 must address the challenges of changing regulatory requirements, business needs, and privacy risks
Lack of consent flexibility	The DigI verification solutions of today do not provide "Consent Revocation"	RQ2 aims to put maximum control in the hands of IOs for their DigI verification.
Online identity requires a lot of PII	Every time an IO needs to prove their identity, they need to share PII which might not be needed.	RQ2 must ensure data minimization
Privacy and security	Privacy controls are critical for any service that captures PII. Most DigI verification solutions store the IO's PII for DigI verification purposes. Even DigI verification stores PII in an encrypted, hashed or digitally signed form. This creates privacy and security vulnerabilities	RQ2 aims at embedding privacy into the design of DigI verification architecture
Huge cost	The lack of reusability and interoperability of multiple DigI verification solutions results in the re-verification of DigI every time IO needs to prove their identity. This incurs a huge cost.	RQ2 must ensure the reusability and interoperability of DigI with enhanced digital trust.
Centrally managed user data	The PII comprising DigI is managed directly or indirectly by a centralized authority	RQ2 aims to put maximum control in the hands of IOs for their DigI verification.
Large-scale data breaches and exponentially growing fines and regulatory areas.	With digitization, the amount of online data is increasing. Most of this online data is PII. The free-flowing PII results in the rise of data breaches and corresponding fines	RQ1 must assess the environmental risks in which DigI verification operates. RQ2 must design a DigI verification reference architecture that is able to provide privacy along with regulatory compliance. RQ3 enables the DigI verification design to adapt as per the changing business needs, regulatory requirements, and privacy risks

2.4. Research Novelty

Recent research has made progress in providing DigI verification, including ID2020 by Microsoft (*ID2020 | Digital Identity Alliance* n.d.), Secure Key by IBM (*SecureKey: Building Trusted Identity Networks* n.d.), ERC #752(*EIP-725: ERC-725 Smart Contract Based Account* n.d.) , Sovrin (Sovrin n.d.), Estonian Identity (*ID-card — e-Estonia* n.d.), and numerous others. In addition to the Estonian Identity, the underlying technology for most of these is blockchain, however, blockchain is not a surety for decentralization. The Estonian Identity is launched by the government; therefore, all related encryption keys are generated by them which, puts government in control of information, reducing the transparency and decentralization of DigI verification.

A similar example is the Ethereum proposal ERC #752 and #753 that proposes a generalized DigI management on the basis of claims. Although, the mechanism of creation and management of claims is properly explained, but negligible information is provided on how user is given the control and transparency over their information. Once users present a claim to SP during the verification, they have no control over their information afterwards. Therefore, when a SP verifies user's claim, users should have control over type and amount of PII presented in the verification process, duration of information exposure, and intended processing and usage of information included in their claims.

It is not clear that the existing blockchain-based DigI verification solutions (ShoCard, Civic, Evernym) are fully compliant with regulations such as GDPR. The literature (Ahmed et al. 2020; Heiss, Ulbricht & Eberhardt 2020; Kuperberg 2020b, 2020a; Poelman & Iqbal 2021; Tatar, Gokce & Nussbaum 2020) also

highlights certain areas where blockchain clashes with GDPR such as data destruction, data editing, and data controller requirements. Another vital dimension of GDPR for blockchain is the transfer of DigI and the associated PII across the border. In a public blockchain network, there is no control over the hosting and jurisdiction of the nodes. However, with a private and permissioned blockchain network, this challenge is addressed however a private blockchain might not offer true decentralization. In addition, all the aforementioned initiatives store an IO's PII in some form (encrypted or hashed).
This research begins to build the foundation of how a DigI verification reference architecture which is compliant to global regulatory requirements and supports decentralization needs without storing PII can be designed. Furthermore, the proposed architecture also addresses the adaptability challenges in response to changing risks, business needs and the regulatory landscape. These features may offer greater privacy and enhanced control to IO's.

2.5. Summary

This chapter has listed the important concepts used in this thesis, presented the relevant literature, and highlighted the gaps in the literature. The existing literature detailed in this chapter emphasizes that DigI is a critical asset that needs to be securely verified to avoid data breaches, lawsuits, or loss of business. The review of the current research on privacy, PII, regulatory compliance, the digital ecosystem, DigI, the identity ecosystem, blockchain, and adaptability, has resulted in the conclusion that there is significant need for a DigI verification reference architecture which ensures privacy, compliance with regulations, and provides decentralization and enhanced control to individuals for owning, accessing, and preserving their DigI instead of becoming a victim of data breaches and identity thefts. Moreover, this chapter highlighted the research novelty.
The next chapter will present the foundation for the ADR method adopted from Sein et al. (2011) to develop and evaluate the proposed ADIVRA framework.

Chapter 3: Action Design Research

This chapter presents the review of the potential research methodological options for this research. It discusses ADR as the most suitable methodology for this research. It presents the stages of ADR and selected kernel theories. The chapter then describes the research ethics before presenting the conclusion.

3.1 Background and Context

The research method explains how a researcher should go about finding a suitable approach to develop and evaluate an artefact (Guba & Lincoln 1994). The selection of a research method depends on several factors, including the nature of the research problem and its underlying objectives, the availability of resources and data, and the research traditions that are local to that institute or organization (Benbasat, Goldstein & Mead 1987).
There are several information system research methods from which to choose. However, the practice-oriented nature of this research indicates that a qualitative research method is the most appropriate choice for the research problem in hand. The characteristics of different possible qualitative research methods in information systems are reviewed, compared, and described below.

3.2. Review of the Research Methods

Research methods can be categorized in many ways. The most common distinction of research methods is qualitative and quantitative research methods. Qualitative research may be suitable for focusing on the description of the issue in detail and the formulation of a new theory. In this research, the issue is privacy and regulatory compliance in DigI verification, whereas a new theory will be generated in the shape of a new DigI verification reference architecture (ADIVRA). The most basic qualitative research includes the collection and use of qualitative data such as interviews, documents, observations, empirical case studies, visual text, and introspection, in order to understand and explain the issue. This section includes a review of some of the available qualitative research method choices for this research.

3.2.1. Grounded Theory

Grounded theory is defined as the method for "the discovery of theory from data systematically obtained from social research."(Glaser & Strauss 1967). Grounded theory enables researchers to devise theory from data, thoroughly acquired and examined via a comparative analysis. Grounded theory enables theory development during the course of the research project by systematically gathering and analyzing data (Fernandez, Lehmann & Underwood 2002). According to Martin & Turner (1986), grounded theory is "an inductive, theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data." The method is suitable for addressing the research problems for which the existing literature is sparse and for which theory building is required (Fernández 2004; Seidel & Urquhart 2016; Urquhart, Lehmann & Myers 2010).

In IS research, grounded theory methods are becoming more and more popular to conduct research in the fields of technology and sociotechnical actions in developing research fields (Urquhart &

Fernández 2006; Matavire & Brown 2013; Birks et al. 2013). This is mainly because the method is beneficial in creating context-based, process-based justifications and details of the research problem (Orlikowski 1993).

3.2.2. Case Study

The most commonly used research method in information systems is case study research (Alavi & Carlson 1995; Orlikowski & Baroudi 1991). This is a robust research method, especially when an in-depth review of the problem is needed. The case study research method is defined in many different ways, however Yin (2002) identifies the case study as an experimental investigation that explores an emerging research area inside its real-world context, particularly when the boundaries between a research area and context are not quite obvious.
The case study research method has a significant application record in the fields of social science, information systems and logistic research (Caplinskas & Vasilecas 2004; Orlikowski & Baroudi 1991; Toomer, Bowen & Gummesson 1993). It is appropriate for information systems research due to the fact that the purpose of this field is to conduct research on information systems in organizations and "interest has shifted to organizational rather than technical issues" (Benbasat, Goldstein & Mead 1987). Despite the recognition, the agreed applicability and acceptance of the case study research method in the context of IS research, a more fundamental criticism is its inability to provide a generalized conclusion (s) and also the known lack of statistical reliability and validity (Gummesson 2000).

3.2.3. Design Science Research

Design research and design science research are two different ways of addressing a research problem. Design research is more appropriate for only practice research (Österle et al. 2011), whereas design science research also includes scientific and theoretical contributions (Winter 2008). Here, this thesis refers to design science research as design research for simplicity purposes. The intention of this type of research is to generate knowledge for artefact design and create and evaluate artefacts to solve a real-world problem (Dresch, Lacerda & Antunes 2015). Due to its emphasis on problem-solving, the implementation of design science research can possibly lessen the current gap amongst theory and practice (Van Aken 2005; Romme 2003). It is widely adopted in IS research due to the balance it offers between research relevance and rigor (Benbasat, Goldstein & Mead 1987; Deng & Ji 2018; Hevner 2004). Therefore, IS research might benefit by the implementation of design science research (Arnott & Pervan 2008; Goes 2014). However, design science research does not require a collaborator or an industry partner who is interested in the research (Iivari & Venable 2009). The research problem in hand requires joint collaboration between researchers and industry, hence this method was not found suitable for this research.

3.2.4. Action Research

There are several definitions of action research, nevertheless Rapoport's definition is one of the most commonly cited (Rapoport 1970). Rapoport defines action research as follows: "Action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable

ethical framework". This description puts the focus on the collective challenges of action research and to potential ethical issues that occur by its application. It also clarifies that action research is intended to widen the range of understanding of the social science area (Clark 1972).
Action research has been acknowledged as an effective research method in areas like organizational development and education (Kemmis & McTaggart 1988). Action research intends to develop scientific knowledge while at the same time working to solve real-world problems (Collatto et al. 2018). Action research focuses on intervention by paying concurrent attention to the implementation in organizations and collaboration between researchers and the industry experts (Coghlan & Shani 2005; Coughlan & Coghlan 2002). In summary, action research has two main goals: intervention in industry and the generation of knowledge.

3.2.5. ADR

ADR, as described by Sein et al. (2011), "*is a research method for generating prescriptive design knowledge through building and evaluating ensemble IT artefacts in an organizational setting*". It has been designed to assist IS practitioners by implementing in practical circumstances, while also contributing to the body of knowledge (Rogerson & Scott 2014a). After the publication of ADR as a research methodology (Sein et al. 2011), a number of research initiatives (Hilpert et al. 2013; Huhtamäki 2016; Keijzer-Broers, Florez-Atehortua & De Reuver 2016; Lempinen, Rossi & Tuunainen 2012; Maccani, Donnellan & Helfert 2014; Mustafa & Sjöström 2013; Schacht & Mädche 2013; Haj-Bolouri, Bernhardsson & Rossi 2016) have commenced or switched to pursue ADR as their basic research approach. ADR embodies a variation of design research (Hevner 2004; March & Smith 1995; Vaishnavi, Kuechler & Petter n.d.) that realizes industry feedback early in the design and development of the artefact, stressing the building-intervention-evaluation iterations as a substitute to the stage-gate method, letting researchers in conjunction with industry practitioners to shape the research outcome throughout the research period. ADR is devised (Sein et al. 2011) and designated by the design researchers as a type of design research (Gregor & Hevner 2013; Iivari 2014), since it needs the research outcomes to find a solution to a specific real-world problem while addressing a class of problems via either specific artefacts (such as Keijzer-Broers, Florez-Atehortua & De Reuver 2016; Miah & Gammack n.d.; Rogerson & Scott 2014b) or refined design knowledge (such as Haj-Bolouri et al. 2017; Lempinen, Rossi & Tuunainen 2012; Mustafa & Sjöström 2013).
The ADR method was selected as the most suitable for the objectives defined in this research. What follows is a discussion of the rationale for choosing ADR as well as details of the ADR research method employed in this thesis.

3.2.6. Rationale for choosing ADR

The reasons for choosing the ADR method for this research are:

- **Firstly**, ADR appears suitable for the research problem in hand as it involves both incremental ADIVRA artefact development and evaluation and intervention.
- **Secondly**, ADR is effective for solving real-world problems through intervention and collaboration between researchers and practitioners (Sein et al. 2011). This helps in addressing any unforeseen effects of employing the artefact, benefiting both researchers from a theoretical perspective and practitioners from a practical standpoint.

- **Thirdly**, in the ADR method, the researcher is part of the team that enables the researcher to produce a useful outcome for the participating organization while at the same time satisfying academic criteria.
- **Finally**, ADR is not only practice-oriented but also theory ingrained to include academic rigor. It involves the development of novel artefact while getting feedback from the participating organization to inform the design of the artefact in reiterative cycles.

3.3. ADR Stages

The ADR method comprises four core stages that aim to connect practice with theory via incremental phases of investigation, engagement, and design-directed endeavors. The stages are (1) problem formulation; (2) building, intervention, and evaluation (BIE); (3) reflection and learning (RL), and (4) formalization of learning (FL). The ADR stages are not strictly followed top to bottom or in waterfall ways; instead, they are more iterative and incremental. Prior to problem formulation, a preliminary stage i.e., idea formulation enabled the development of this research project idea (see figure 3.1).

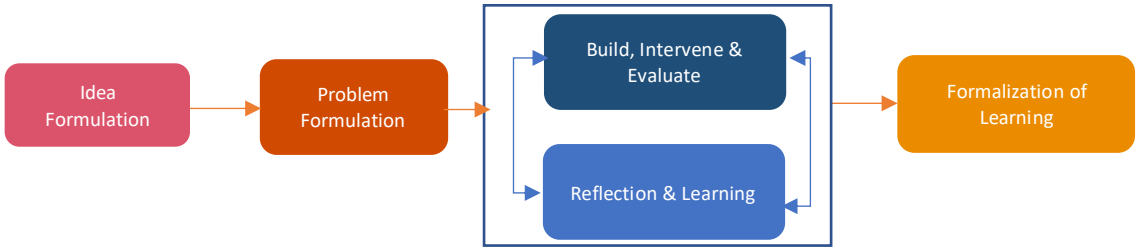


Figure 3.1 The stages of ADR adapted from Sein et al. (2011), Gill & Chew (2019) and Gregor et al. (2013)

The idea formulation stage is adopted from Gill & Chew (2019). The completion of the idea formulation stage then initiates the next stage of problem formulation. This marks the transition from idea to detailed problem formulation. Idea formulation and problem formulation are linear stages that were performed once at the beginning of this research to set the course of this research. Once the problem is formulated, the research transitions to integrated BIE and RL. The integrated BIE and RL stages are bidirectional, which are performed in cycles informing and shaping the design of the artefact through the feedback of the participants, whereas BIE focuses on the iterative development and evaluation of the proposed framework (ADIVRA) through the intervention and involvement of the participants and RL focuses on analyzing the feedback which was then used for the ongoing shaping of the proposed model. The ADIVRA components and artefacts were evaluated using Carvalho (2012) criteria as detailed in Table 3.1. The final increment of the ADIVRA marks the end of integrated BIE and RL stages and the project transitions to the final FL stage. FL is the last stage that focuses on consolidating the proposed model for generalization and reusability. It is important to note here that, to generalize the learning in the form of design principles, the extraction techniques proposed by Gregor, Müller & Seidel (2013) were integrated into the ADR.

Table 3.1 Evaluation Criteria

Criteria	Description	Evaluation Approach
Generalization	ADIVRA is general and is not attached to one context or situation.	Industry field survey (expert evaluation)
	ADIVRA can adapt to multiple circumstances and be applied with different technology stacks.	
	ADIVRA is instantiable and appropriate for a class of DigI verification conditions.	
Applicability	ADIVRA is applicable for the assessment of privacy risk to DigI verification in an identity ecosystem	Industry field survey (expert evaluation), design and review workshops
	ADIVRA is applicable for achieving privacy and compliance in DigI verification operations	
	ADIVRA is applicable for adapting to continuously changing privacy risks and regulatory obligations in DigI verification operations	
Novelty	ADIVRA provides new knowledge in the context of DigI verification.	Industry field survey (Expert Evaluation), logical argument (related work review and gap analysis)
Comprehensiveness	ADIVRA provides adequate coverage for assessment of privacy risk to DigI verification in an identity ecosystem	Industry field survey (expert evaluation), design and review workshops
	ADIVRA provides sufficient guidelines for designing a privacy aware and regulatory compliant DigI verification solution	
	ADIVRA provides ample support for eliciting change requirements in context of DigI verification operations.	
Usefulness	ADIVRA is useful for identity architects, regulators, and researchers	Industry field survey (expert evaluation), design and review workshops
	ADIVRA is a useful for filling the research gaps	

Further, for each ADR stage, Sein et al. (2011) additionally provided guiding principles that are described in Table 3.2 (and illustrated in Figure 3.6) along with their specific use in the context of this research project.

Table 3.2 Summary of the ADR Process in ADIVRA Development

Stages	Principles	Practices	Artefacts
Stage 0. Idea Formulation	Principle 1: Practice Inspired Research	Initial idea is powered by the literature review and further refined by IDZ's initiative to design an adaptive, privacy aware and regulatory compliant DigI verification solution. Conception via initial commitment and investigation Non-disclosure agreement development	Project idea document Non-disclosure agreement (NDA)
Stage 1. Problem Formulation	Principle 1: Practice Inspired Research	Business strategy analysis and project vision and scope description Project planning and budget allocation for the project Research contract	Research questions Research gaps Research problem Project vision, aims, objectives and scope. Goals, project plan, project contract Workstream structure
	Principle 2: Theory Ingrained Artefact	The development and design of the artefacts were informed by theories. The following main kernel theories have been recognized and examined to enlighten the practice-oriented research: ADR, Adaptive EA, ISO 27001, PESTLE risk analysis model, GDPR, Kim Cameron's Identity laws, TOGAF Coverage Analysis, Integrated Requirement Engineering, Attribute-Based Encryption (Carvalho 2012) (Gregor, Müller & Seidel 2013)	Kernel theories Evaluation criteria
Stage 2: BIE	Principle 3: Reciprocal Shaping	Challenges faced were addressed iteratively and initial design principles were devised in partnership with practitioners.	Industry field survey ADIVRA Alpha, Beta and Gamma Versions Framework review
	Principle 4: Mutually Influential Roles	The ADR team comprised university researchers and industry practitioners to ensure the inclusion of theoretical, technical, and practical perspectives.	Work stream structure
	Principle 5: Authentic and Concurrent Evaluation	ADIVRA was iteratively assessed by the ADR team and in the broader setting of experts at IDZ.	
Stage 3: Reflection and Learning	Principle 6: Guided Emergence	The overall nature of the assessment model was recognized, communicated, and discussed. Publications	ADIVRA showcases and demonstrations for feedback for reflection and learning. Work in progress academic papers
Stage 4: Formalization of Learning	Principle 7: Generalized Outcomes	Project retrospective Final review Handover and closure	ADIVRA design principles

3.3.1. Idea formulation

Based on the guidelines of (Gill & Chew 2019), idea formulation has been added as a preliminary step of the ADR method. The preliminary stage of ADR starts with a research idea that leads to the formal initiation of the research project. The initial research idea (RQ1) was proposed via the literature review (Chapter 2) which was also aligned with the industry research problem. This stage takes on the ADR practice-inspired research principle (Principle 1) and procedures (see Table 3.2). The real-world problem class (e.g., ensuring privacy and regulatory compliance of PII during DigI

verification) was in hand; however, there was a lack of publicly available theoretical knowledge and research-based solutions or artefacts at least at the time when this research was first initiated (i.e., a privacy aware and regulatory compliant DigI verification reference architecture). The decision was to build the ADIVRA as a reference architecture and use it to develop privacy aware and regulatory compliant DigI verification solutions. Therefore, at this stage, the key artefacts were a project idea document and the NDA.

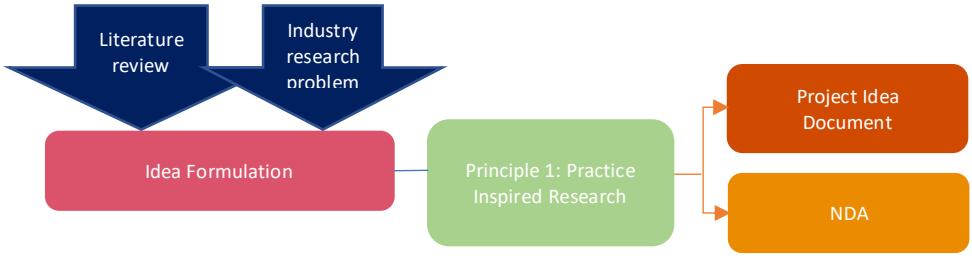


Figure 3.2 Idea Formulation

3.3.2. Problem Formulation

The problem was formulated by conducting a literature review in the field of study (theory-inspired research). This research also involved the industry research partner IDZ. Thus, the problem was also aligned with the industry partner's interest (practice-inspired research) which was demonstrated through research idea workshops (Appendix H). This stage is guided by the ADR principles of practice-inspired research and theory-ingrained artefacts. The practice-oriented research problem is identified, articulated, and scoped in order to start and run the research endeavours. The starting point for this research was the understanding that an individual's DigI information is becoming a critical asset that needs to be securely verified to avoid data breaches, lawsuits, or loss of business. The more specific problem statement is: How to ensure regulatory compliance and the privacy of PII involved in DigI verification operations in a digital ecosystem (problem class)? Thus, this research contributes to a class of problem surrounding the design of privacy aware DigI verification (privacy and compliance perspectives). Knowledge from this research (the proposed artefact) can be applied to a similar class of problems and an organizational context, which is an important consideration for research generalizability (Sien et al. 2011).
This stage resulted in the formulation of the research problem, research aims, objectives, initial project vision, scope and organizational goals that describe the above-stated research problem as an instance of a class of problems. This provided the basis for the development of the research plan, research contract, funding, roles, and responsibilities, and securing the industry partner's commitment for this research project. This stage also involves identifying some relevant kernel theories and literature that were used and reviewed by the ADR team to inform the problem and design of the theory ingrained artefacts (principle 2) for this project (see Table 3.2).

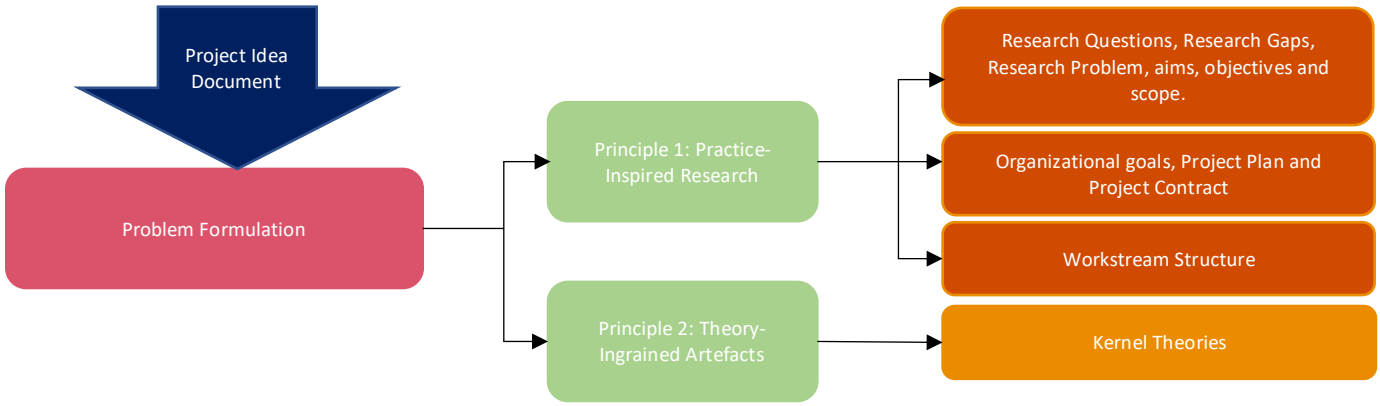


Figure 3.3 Problem Formulation

3.3.3. Build, Intervene and Evaluate

This stage was conducted by collaborating and co-working with participants in order to iteratively build, intervene and evaluate the ADIVRA. This stage focuses on the integrated and interactive BIE stages for the ADIVRA (principles 2 and 3). Throughout BIE, the ADIVRA artefacts are co-produced and evaluated (mutually influential roles) with stakeholders (appendix H, I and J). Building and evaluating each of the three BIE cycles was done through design and review workshops in alignment with the identified research problem and idea from stage 1. In addition, BIE is not a linear stage-gate model, thus artefact building and intervention are interlinked and evaluation is a progressive activity rather than a one-off post design evaluation activity (Peffers et al. n.d.). Thus, the alpha, beta, and gamma versions of ADIVRA were iteratively developed. The final version of ADIVRA was evaluated via an industry field survey. During the BIE stage, the ADIVRA framework was built (B) and intervened in the organizational setting (I). As the artefact is used in the organizational environment, it is continuously reviewed and polished (E). The various understandings presented by the ADR participants in relation to the development of the artefact made ADIVRA a more effective blend of theory and practice. In conclusion, this stage was primarily centered on incremental building, intervening, and evaluating the ADIVRA artefacts. The next stage discusses the RL and is performed in parallel with the BIE stage for continuous learning. The ADIVRA was developed in three iterations of BIE and RL to address the research gaps within the boundaries of the research scope.

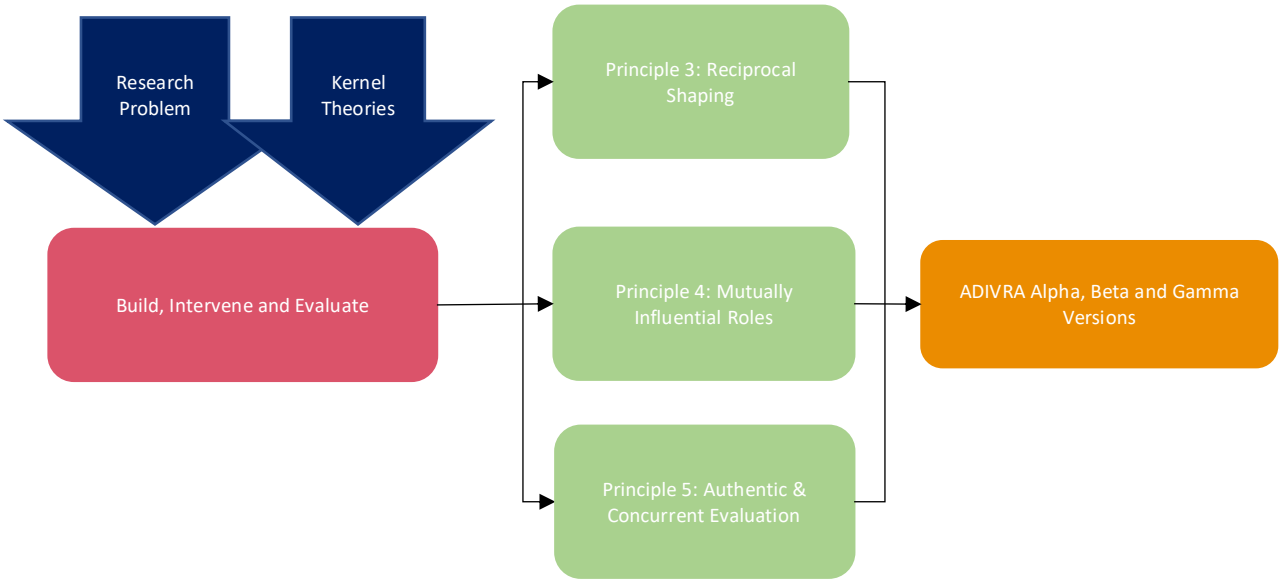


Figure 3.4 Build, Intervene and Evaluate

3.3.4. Reflection and Learning

This stage is directed by the principle of guided emergence, which requires the ADIVRA to be adaptive in response to its evaluation and the stakeholders' needs. This stage is conducted simultaneously with the BIE by continuously applying the learning derived during the process. RL learns and analyzes the results from the BIE stage regarding the problem articulated in the first stage. The output of this stage is the ADIVRA showcases and demonstrations for feedback for reflection and learning. This enables the ADIVRA to embody not only the initial design but also its continuing emergence via use in the industry partner's organizational context, the stakeholders' diverse viewpoints, and by the results of reliable and parallel evaluation to determine if the new ADIVRA is fit for its purpose (meets the criteria in Table 3.1 within the project scope boundaries). The ADIVRA design was adjusted which resulted in the new ADIVRA framework as we advanced through this feedback based continuous RL mechanism. The RL tasks are a) ongoing reflection of the design and re-design; and b) analyze the intervention results against the goals. The output of this stage are showcases and demonstrations and academic publications based on the learnings drawn from this stage.

3.3.4.1 ADIVRA Evaluation (BIE, RL)

The ADIVRA evaluation process comprises two steps: ongoing evaluation via design and review workshops and expert evaluation using an industry field survey. The initial evaluation of the proposed framework was done by means of design and review workshops in the industry partner's organizational setting (Chapter 5) during BIE and RL. The ADIVRA evolved as the framework components emerged in increments over a period of time. Finally, for the purpose of closure and final review, and also for the identification of future work, the empirical evaluation of the refined

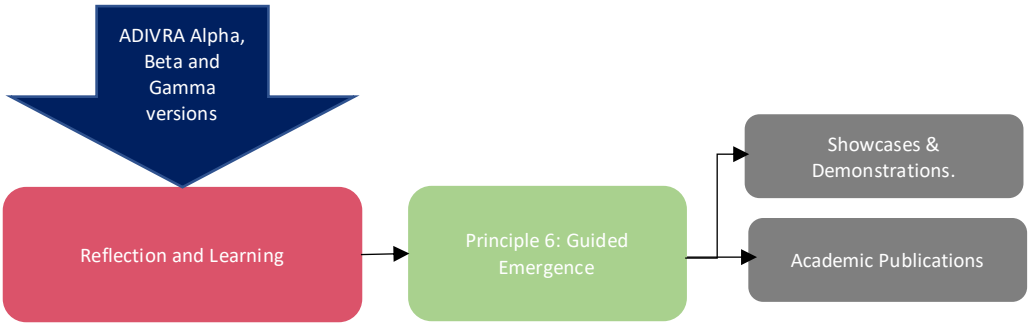


Figure 3.5 Reflection and Learning

framework (ADIVRA) has been conducted via the industry field survey involving thirty experienced experts from industry.

a) Design and Review Workshops

During the BIE and RL, researchers were persuaded to conduct continuous assessment in order to steer the course of the design and development of ADIVRA. The ADIVRA was continuously evaluated by intervention in the industry partner's organizational setting and conducting artefact design and review workshops, which involved the IT manager, business analyst, compliance manager, digital identity architect and privacy officer (see appendix H, I and J). The feedback obtained during the workshops was included in successive versions of the artefact until the adjustments and enhancements were hardened and only minimal alterations were noted during the design cycles. During the evaluation process, the participant's feedback, comments, and re-design decisions were documented (Appendix I) to keep track of progressive and cyclic upgrades to ADIVRA framework (Chapter 5), feedback and comments in log file. During the design and review workshops the target was to look at the artefact from applicability, comprehensive and usefulness perspective.

b) Industry Field Survey

Survey research is defined as "the collection of information from a sample of individuals through their responses to questions" (Check & Schutt 2011). The identified ADIVRA components were presented to experts (industry as well as researchers) to get their experience-based opinion via a questionnaire-based survey to facilitate further refinement and development. The final version of ADIVRA has been updated and improved based on the feedback received from the industry experts. The surveys conducted in this research use the ratings outlined in the Table 3.3. The ratings convert the respondents' qualitative answers to the survey questions into statistical data (quantitative ratings). The following rating table was used in the industry field survey.

Table 3.3 Survey Ratings

Score	Rating Col 2
5	Strongly Agree
4	Agree
3	Somewhat Agree
2	Disagree
1	Strongly Disagree
0	Not Sure/Not Applicable

The qualitative ratings were transformed into numerical data to help with the quantitative analysis of the surveys. The qualitative ratings in Table 3.3 are explained as follows:

- **Not Sure/Not Applicable:** The respondents are not sure about the declaration, or it is not applicable to their context.
- **Strongly disagree:** The respondents strongly disagree with the declaration.
- **Disagree:** The respondents disagree with the statement.
- **Somewhat Agree:** The respondents somewhat agree with the declaration.
- **Agree:** The respondents agree with the statement.
- **Strongly agree:** The respondents strongly agree with the declaration.

The surveys followed a commonly used structure (Hyndman 2008):

- **Planning a survey:** Outline the survey objectives (purpose, need, knowledge requirements).
- **Design the sampling procedure:** Identify the target respondents (ethical considerations are required).
- **Select a survey method:** Data collection plan (online method was used in this research).
- **Develop the questionnaire:** Industry survey questionnaires were developed by the researcher using artefact evaluation criteria (Carvalho 2012).
- **Conduct the survey:** Execute the survey effectively over a fixed period (July 2020 to Dec 2020).
- **Collect and analyze the data:** The surveys provide quantitative and qualitative data. The surveys data analysis comprises two steps:
    - Survey quantitative evaluation
    - Survey qualitative evaluation.

Survey Quantitative Evaluation: The data generated from the industry survey was categorical. The respondents in the survey contributed their responses to the survey questionnaires as qualitative ratings (see Table 3.3). This research used statistical formulas adapted from Bou Ghantous & Gill 2021, to make sense of the survey data (see Chapter 5). Statistical formulas are better suited to provide an analysis of a survey's numerical data. According to Hyndman (2008), "statistics is the study of making sense of data". The statistical equations utilized to analyze the survey responses are described in equations 3.1 – 3.3.

Equation 3.1: Somewhat Agree and Above Frequency

SAAF Formula
SAAF = Σ Frequency (Ratings >= 3) SAAF is the sum of all responses [Somewhat Agree (3) + Agree (4) + Strongly Agree (5)]

Equation 3.2: Somewhat Agree and Above Percentage

SAAP Formula
SAAP = Σ Percentage (Ratings >= 3) SAAP is the sum of all percentages of responses [Somewhat Agree (3) + Agree (4) + Strongly Agree (5)]

Equation 3.3: Chi^2 Formula

Chi^2 Statistical Formula
Chi^2 or $X^2 = \Sigma_{(O-E)^2/E}$ (O = frequency and E = expected value) E = Σ O/N (where O = frequency and N = total number of observations) The p-value decides if the null hypothesis H_0 is accepted or rejected based on an important value α = 0.01 (where p-value = the probability (or chance) of the collected data or a more extreme event happening under the assumption of the H_0.) α is the significance level. The value of α is selected as 0.01 as opposed to conventional 0.05 to reduce the area where H_0 can be rejected If p-value < α, then H_0 is rejected and H_1 is accepted, and there is a positive association among the test variables (ADIVRA Components) and the evaluation criteria mentioned in Table 3.1. [If p-value < 0.000^{β} ($^{\beta}$ is a small number), then p is mathematically adjusted to p < 0.001] **H_0 (null hypothesis):** test variables and the evaluation criteria are not associated **H_1 (alternative hypothesis):** there is positive association between the test variables and the evaluation criteria

Survey Qualitative Evaluation: The qualitative data collected in the industry survey were analyzed using the hypothesis confirmation general technique of analysis (Runeson & Höst 2009a). The hypotheses were the artefact evaluation criteria (Carvalho 2012) (see Table 3.2). Participants' feedback was cross-examined against the evaluation criteria by highlighting the occurrence of the criteria in the text (adapted from Bou Ghantous & Gill 2021). The industry feedback was organized into tables. The analysis tables include an explanation column about each item of feedback and a category column to identify the criteria in each item of feedback.

3.3.5. Formalisation of learning:

The fourth ADR stage includes the FL and is based on the principle of generalized outcomes. The objective of this stage is to formalize the learning for generalized outcomes. Therefore, this ADR project extracted broad design ideas and principles using the design principle extraction techniques by Gregor & Hevner (2013). Section 6.1 further explains the FL for generalized results in the form of implications and design principles, which is a major contribution of this research project both

from academia and industry standpoints. The project retrospective was conducted with IDZ stakeholders and UTX researchers to extract the design principles and formalize the overall learning. It is important to point out here that in addition to the proposed framework (ADIVRA), this research also provides the learnings for developing and executing other ADR projects in this vital field of privacy and compliance-driven identity ecosystems.

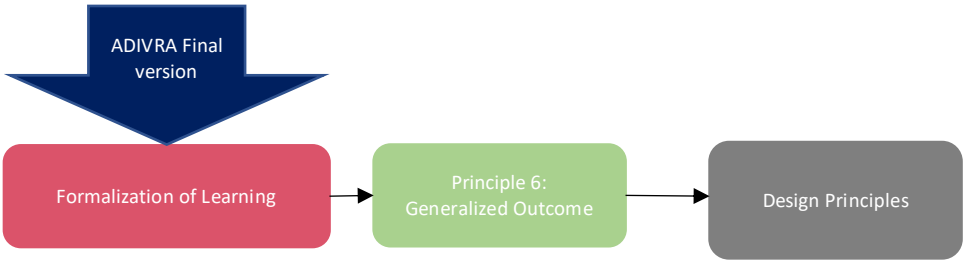


Figure 3.6 Formalization of Learning

3.4. Research Ethics

Formal approval was received from the UTS Research Ethics Committee in compliance with the research ethics policies of the University of Technology Sydney. The approval document can be found in Appendix A. The research did not raise any ethical issues. A formal consent letter (see Appendix B) was sent to each participant. The participants were free to withdraw from the research at any time and could contact the supervisor or the university. Additional forms that provided information about the online survey and the ADIVRA framework were also sent to willing participants, along with the consent form (see Appendix D). The objective of these forms was to provide detailed information about the project, the survey questionnaires, the anonymity of the data collection, and storage.

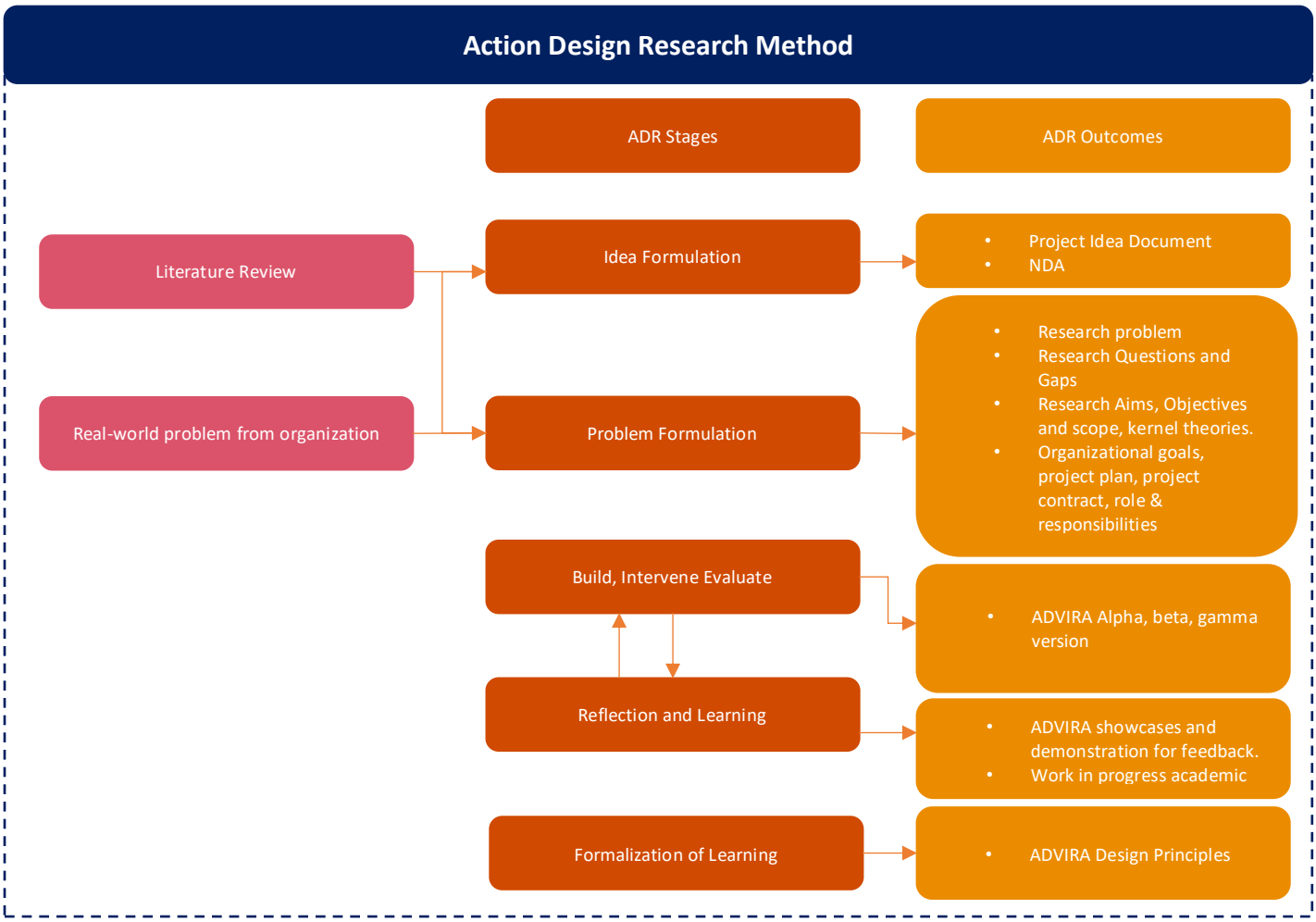


Figure 3.6. ADR Methodology

3.5. Summary

This research was conducted to develop a novel framework, the ADIVRA, for privacy aware and regulatory compliant DigI verification using an iterative ADR method. The ADR used in this thesis was established on guidelines published by Gill & Chew (2019) and Sein et al. (2011). This chapter presented the resources and architecture development process used to construct the ADIVRA, and it outlined the evaluation methods used to obtain experts' feedback. The evaluation was conducted by involving practitioners and experts from industry to acquire feedback regarding the generalization, applicability, novelty, relevance, and usefulness of the ADIVRA framework. The ADIVRA is presented in detail in Chapter 4.

Chapter 4: The ADIVRA Framework

This chapter presents the novel ADIVRA framework, which is the main contribution of this research. The ADIVRA framework is a practical solution to the research questions identified in Chapter 1. The ADIVRA framework was developed using the well-known ADR method (discussed in Chapter 3). In this chapter, the details of the reference architecture for designing a DigI verification solution are presented. The three main components (assess, design, and evolve) of the ADIVRA framework and their subsequent artefacts are discussed. The incremental development (alpha, beta, and gamma versions) and evaluation of the ADIVRA framework is detailed separately in Chapter 5 to avoid any possible confusion between the contribution and evaluation of this research. This chapter presents the final version of the ADIVRA framework.

4.1. The ADIVRA Overview

The ADIVRA framework provides new knowledge on developing the privacy aware DigI verification reference architecture and supporting solutions which comply to international privacy regulations (such as GDPR) and adapt to changing business needs, privacy risks, and the regulatory landscape via feedback loops. The ADIVRA is based on a decentralized model of identity verification using blockchain as an underlying technology. The new ADIVRA framework comprises three components; Assess, Design, and Evolve. The ADIVRA has a preliminary step for understanding business strategy and making the design decisions in alignment with the business vision.

4.1.1 ADIVRA Framework Components and Relationships

ADIVRA components are related to each other in a way that the output of one component may serve as the input of the other. A brief description of ADIVRA components, their artefacts, input, output, and kernel theories used for their development is presented in Table 4.1.

Table 4.1. ADIVRA Components, Artefacts, Input, Output and Kernel Theories

Component/Artefact	Description	Input	Output	Kernel Theory
Understanding Business Strategy	This preliminary step focuses on establishing the business context for ADIVRA. This involves reviewing the business vision, which provides the foundation for feasibility and alignment. Uncovering the privacy goals for the new framework shapes the DigI design, identifies the gaps, and streamlines the risks.	Feedback and alignment	Business vision and privacy goals	Strategic need analysis
Assess	The first component of ADIVRA is Assess. The assess component can encompass different aspects from reviewing information security processes and procedures to environment scanning and technology adoption.			
PESTLE+	A novel PESTLE+ risk analysis framework has been developed as part of the Assess component to identify the changing security and privacy risks in the DigI verification process. This component assesses the existing privacy capability of the DigI verification process according to the organization's business strategy and privacy goals and identifies the risks and gaps.	Business vision and privacy goals, DigI Design, Privacy Requirements	Risks and gaps	PESTLE risk analysis model
IdMPAM	An assessment model to assess the privacy capability of the DigI verification design. The IdMPAM assists in making	Business vision and privacy goals, DigI Design,	Risks and gaps, Feasibility and alignment	GDPR Kim Cameron Identity laws

	technology adoption decisions by assessing the viability of technology for DigI verification	Privacy Requirements		TOGAF Coverage Analysis
*i*SAM2	*i*SAM2 enables the assessment of the maturity of the information security audit process. The emphasis in this type of assessment is to ensure that privacy requirements are fulfilled, risks and gaps are identified, policies are in place and procedures are being followed along with revealing actions that may put organizational compliance at risk.	Business vision and privacy goals, DigI Design, Privacy Requirements	Maturity of information security audit process	ISO 27001
Design	The second component of the ADIVRA framework is Design. The starting point for the design component is the risks and gaps identified as a result of the previous component (Assess). The outputs of the Design component artefacts are assessed using artefacts of the Assess component. In addition, change requests from the Evolve component (using DigIVAM) are also adjusted.			
CDigI	CDigI is a multidimensional DigI structure to broaden the scope of DigI and enable the interoperable DigI verification process without costly and time-consuming reworks.	Risks and Gaps	Digital Identity Structure	Adaptive EA
*i*SEA	*i*SEA is an encryption-based architecture for a secure container to embed privacy into the DigI verification solution.	Risks and Gaps	Secure digital identity for privacy by design	Attribute Based Encryption
DigIVPM	DigIVPM is a DigI verification process model to securely verify the DigI information or credentials without storing the PII. This process can involve several parties such as identity owner, regulators, issuers, verifiers, and service providers operating within the global digital ecosystem.	Risks and Gaps, Change Requirements, Regulatory requirements	Digital identity behavior	Kim Cameron's Identity Laws GDPR
RRM	To ensure regulatory compliance, a regulatory requirement model is designed to develop a catalogue of regulatory requirements for the DigI verification process.	Risks and Gaps, Change Requirements	Regulatory Requirements	Integrated Requirement Engineering GDPR
Evolve	The third component of the ADIVRA framework is Evolve. This component utilizes the PESTLE+ risk analysis model from the Assess component in addition to DigIVAM.			
DigIVAM	To ensure adaptability, ADIVRA needs to continuously evolve as per business needs, changing privacy risks and the regulatory landscape. The Evolve component has DigIVAM which identifies the change requirements and feeds them back to the Design component for design adjustments.	Risks and gaps, DigI verification Design	Change Requirements	Change Management

4.1.2. ADIVRA Artefacts and Relationships

This final version of ADIVRA (gamma version) which was shaped through collaborative design cycles and evaluation interventions (see Chapter 5) is presented in this section. As detailed in the previous section, each component of ADIVRA has further artefacts that fill the research gaps and meets organizational needs. The first component, Assess, includes the development of the assessment model to enable the finding of the risks and gaps in potential technologies and existing privacy capability of systems, policies, and procedures. The second component, Design, provides a blueprint for a blockchain-based DigI verification solution that fills in the gaps identified by the Assess component. The third component Evolve focuses on continuously evolving the solution design to address the emerging threats, regulatory requirements, and business needs. The relationships between the artefacts of the ADIVRA components are depicted in Figure 4.1.

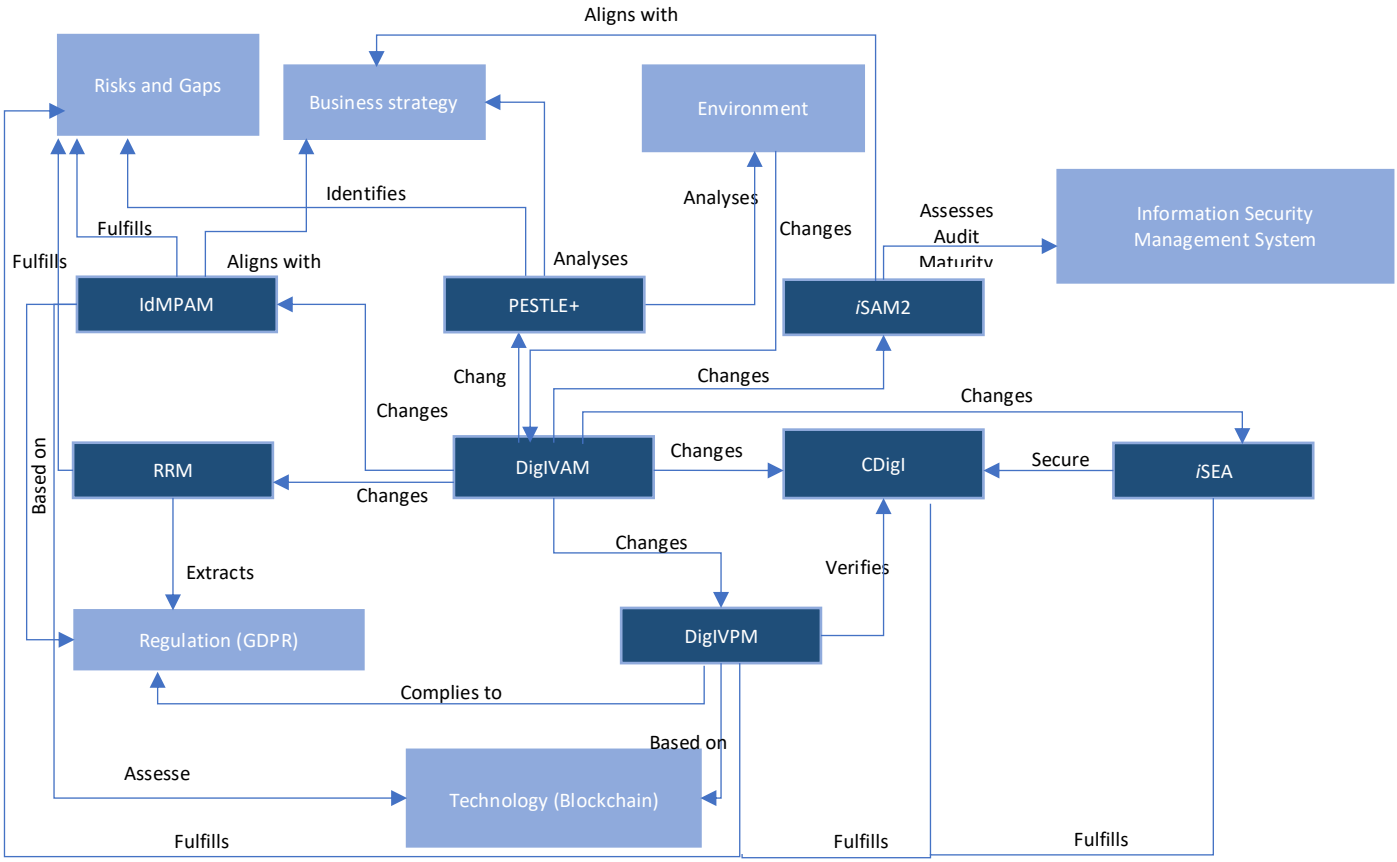


Figure 4.1. ADIVRA-Component Artefacts' relationships

4.2. Pre-liminary Stage: Understanding the Business Strategy

In this preliminary stage, the organization's business strategy is analyzed using the stakeholder strategic need analysis technique (Smith et al. n.d.) to understand the business vision and privacy goals (see Figure 4.2).

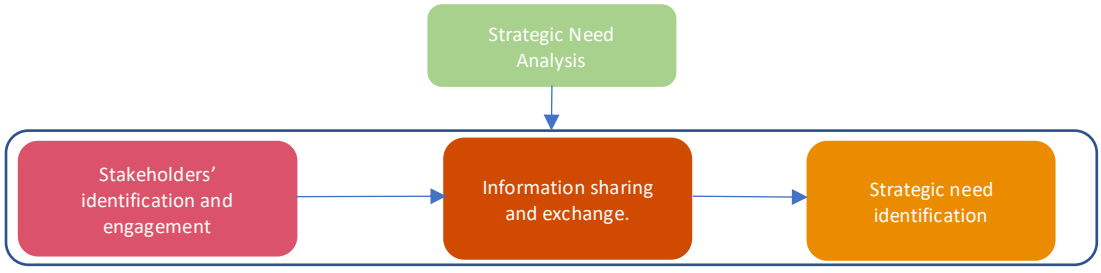


Figure 4.2. Strategic Need Analysis Process

The initial engagement session is a preliminary stage in the process conducted before the formal part of the strategic needs analysis begins. The aim of this engagement is to enlist stakeholders'

support and to make them aware of the details of the business strategy. This is followed by information sharing and exchange that presents the strategic needs analysis approach to all participants. The workshops are the major working and decision-making sessions following the information via business strategy workshops based on Haj-Bolouri, Bernhardsson & Rossi (2016). Stakeholders are actively involved in developing strategies and evaluating them within the organizational constraints. Stakeholders assemble at a series of business strategy workshops and meetings (see Appendix H) to explore their knowledge and views about potential strategies for the organization and devise realistic goals. This pre-design phase of ADIVRA involves all the stakeholders clearly establishing a basis for the design. This component is not limited to business vision or privacy goals; however, it may be extended to include other elements as required to support the need for framework component adaptability. However, in this research, the scope is limited to the business vision and privacy goals.

This preliminary step is very important for the business-outcome driven approach to privacy. Several workshops with stakeholders indicated that central to organizational privacy goals was confidentiality, integrity, availability, and non-repudiation. Furthermore, an important part of the business strategy is regulatory compliance and technology adoption decisions in addition to adaptability that is critical for today's competitive landscape. The business strategy may include any technology however in this research, the scope is limited to blockchain as this is an emerging technology for use in DigI verification. For regulatory requirements, GDPR is selected due its

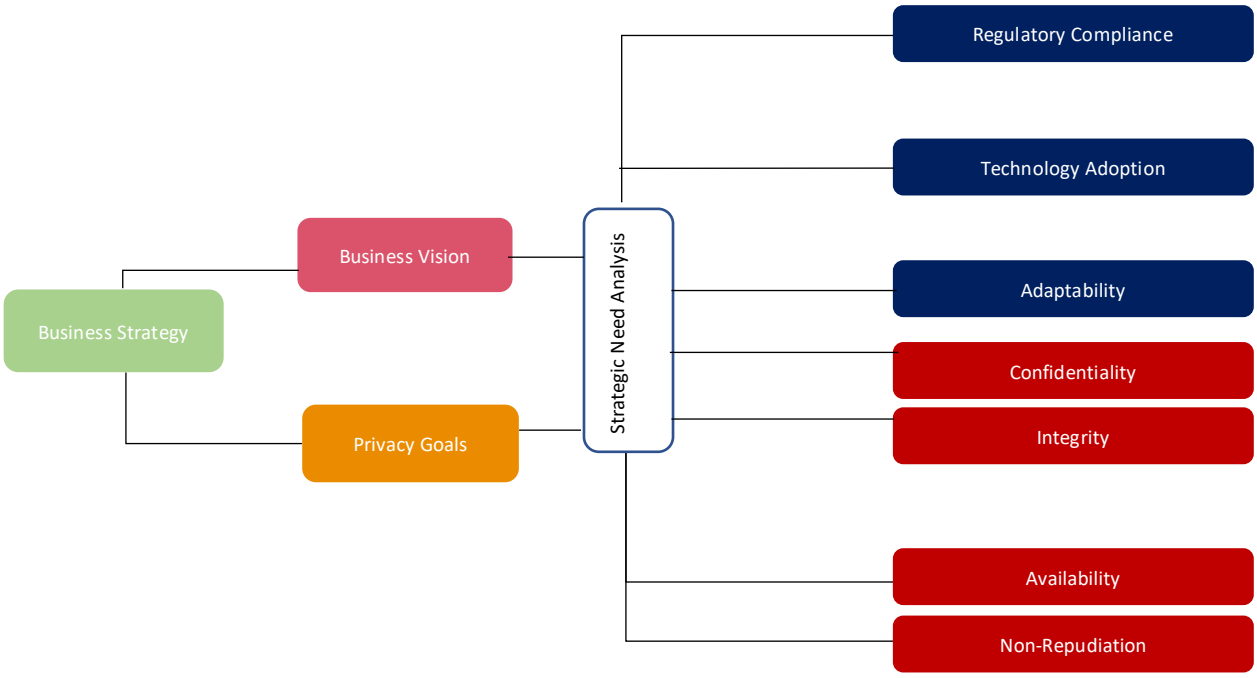


Figure 4.3. Business Vision and Privacy Goals

global relevance and broader scope. The choice of blockchain as an underlying technology and GDPR as a regulatory lens was also aligned with our industry partner's needs. To better align the target DigI verification solution with the business vision and privacy goals, ADIVRA has an assess component to assess the environment, check the feasibility of the technology and evaluate the existing privacy and security capability.

4.3. Assess Component

The assess component can encompass different aspects, from reviewing information security processes and procedures to environment scanning and technology adoption. The assess component of ADIVRA addresses RQ1 (see Chapter 1). The scope of the assess component is limited to analyzing the environment, evaluating the maturity of the information security internal audit process, and assessing the viability of technology in the light of regulatory requirements with the primary focus on risks and gaps analysis. It is not possible to discuss all the regulations thus, GDPR is chosen for the regulatory requirements as it is also aligned with the industry partner's needs and interests. Other factors such as cost-benefit analysis and technical details are beyond the scope of this research as discussed in research limitations.

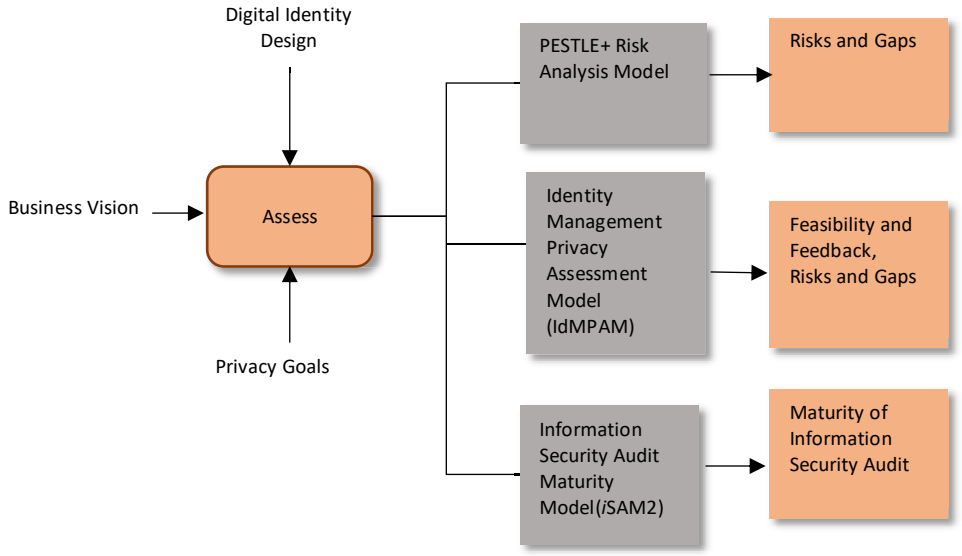


Figure 4.4. ADIVRA-ASSESS Component

4.3.1 PESTLE+ Model

There are multiple environmental vertices that will condition the ways DigI verification is conducted; therefore, the assessment of the environment is crucial to understand the potential developments and devise the business plan to be followed. A helpful way to achieve this objective is the PESTLE (Political, Economic, Social, Technological, Legal and Environmental) risk analysis model, which enables a comprehensive review of the problems that have the highest impact on the evolution of business endeavors or the project under development. Even though the current form of the PESTLE model offers a key understanding at the abstract level, for the assessment of the macro environment, it has certain gaps with respect to evaluation criteria and analysis. Firstly, the traditional PESTLE model does not include the health factor explicitly. Health is considered under other factors (e.g., social, legal), however this does not suffice the level of depth needed to identify health-related risks and threats. Considering the level and breadth of the risk analysis required to foresee and prepare for health crises, ADIVRA includes health as an additional factor in the risk analysis, and its impact on other factors (political, economic, social, technological, legal, and environmental) is also considered. Secondly, although the theoretical basis for PESTLE analysis proposes a comprehensive model (Oppenheim et al. 2019), this is not

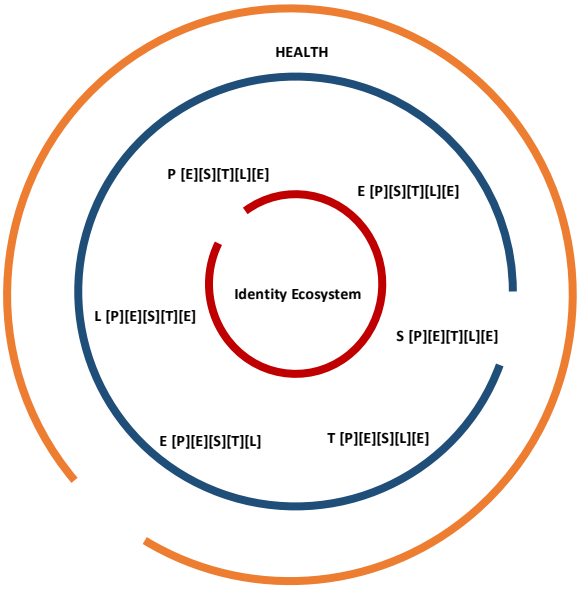


Figure 4.5. PESTLE+ Risk Analysis Model

mirrored in the evaluation criteria and measurement process. The factors included in the traditional PESTLE model are assessed and measured individually. This gap in the PESTLE model does not permit a thorough study of the macro environment in which DigI operates. In ADIVRA, the PESTLE model is extended by adding the health factor such that its impact on all other environmental factors is analyzed (see Figure 4.5). This risk analysis model is referred to as the PESTLE+ model and is part of the assess component of ADIVRA. The perspective taken into account for the development of the PESTLE+ model is the relationships and interdependencies between macro-environmental factors. The objective evaluation and assessment of each macro-environmental PESTLE factor is not reflective of the actual

situation. For instance, legal arrangements or economic conditions cannot be measured and evaluated independently of political circumstances. A political scenario can create socio-cultural and economic consequences. PESTLE+ analysis adopts a matrix-based analysis instead of linear analysis, which is built on the interconnections and dependencies of the factors (see Table 4.2). ADIVRA proposes that each macro environmental factor could be related to other factors.

The addition of the health factor may enable the PESTLE+ model to support decision-making by providing a broader analysis of the environmental factors. It may also help in conducting a multidimensional analysis of risks, uncertainties, and their impact on business. Table 4.2 details the interdependence of PESTLE+ environmental factors. All interdependencies from Table 4.2 might not apply to every organizational context. Businesses can choose and tailor the factors and interdependences applicable to their particular context.

Table 4.2. PESTLE+ Macro Environmental Factors

	P	**E**	**S**	**T**	**L**	**E**	**+**
	Political	*Economic*	*Social*	*Technological*	*Legal*	*Environmental*	**H**
Political	X	H(Political Economic)	H(Political Social)	H(Political Technological)	H(Political Legal)	H(Political Environmental)	**Health**
Economic	H (Economic Political)	X	H(Economic Social)	H(Economic Technological	H(Economic Legal)	H(Economic Environmental	
Social	H(Socio Political)	H(Socio Economic)	X	H(Socio Technical)	H(Socio Legal)	H(Socio Environmental)	
Technological	H(Techno Political)	H(Techno Economic)	H(Techno Social)	X	H(Techno Legal)	H(Techno Environmental)	
Legal	H(Legal Political)	H(Legal Economic)	H(Legal Social)	H(Legal Technological)	X	H(Legal Environmental)	
Environmental	H(Enviro Political)	H(Enviro Economic)	H(Enviro Social)	H(Enviro Technological)	H(Enviro Legal)	X	

4.3.2 Identity Management Privacy Assessment Model (IdMPAM)

One aspect of the assess component is to develop a model to assess the feasibility of technology (i.e., blockchain) for DigI verification. With the new data protection laws such as GDPR, there are stringent limitations on the collection, storage, and usage of PII comprising DigI. The failure to comply with regulatory mandates may result in heavy fines. Hence, it is essential to ascertain where the use of specific technology is appropriate for DigI verification. Therefore, prior to employing any technology for DigI verification, a careful assessment of the technology for preserving the privacy of PII must be conducted in light of global regulatory requirements such as GDPR. Traditional technology assessment and adoption models (e.g., Technology Acceptance Model (Venkatesh & Bala 2008) and the IS success model (DeLone & McLean 1992) are too generic in nature and do not seem to provide concrete criteria or principles in the emerging context of technologies, DigI verification, privacy and regulatory compliance. Hence, to assess the viability of a specific technology (i.e., blockchain for this research) for designing a privacy aware

and regulatory compliant DigI verification solution, IdMPAM was made part of the assess component of the ADIVRA framework. IdMPAM is specially developed in light of GDPR (European Union 2018) and Kim Cameron's Identity Laws (Cameron 2005). The reason for choosing GDPR is its broader coverage and global relevance (Anwar, Gill & Beydoun 2018b).
The IdMPAM consists of 4 broad categories and 16 consolidated underpinning assessment factors based on GDPR and Kim Cameron's Identity Laws (see Figure 4.6). The categories of the model are based on layers of the digital ecosystem (see Chapter 2) i.e., the data subject's right, data protection, technology, and a general category. The data subject corresponds to the Human layer of the digital ecosystem; data protection relates to Information; technology maps to the Technology layer and general covers the environment layer of the digital ecosystem. The assessment factors are chosen carefully to cover each layer of the digital ecosystem. A typical DigI verification solution processes the identity (data/information) of individuals (data subject/human) using relevant technology in a multifaceted environment (general). Figure 4.6 lists the categories and assessment criteria of IdMPAM. The IdMPAM can serve as a preliminary assessment metric to ascertain the viability of technology adoption for DigI verification.

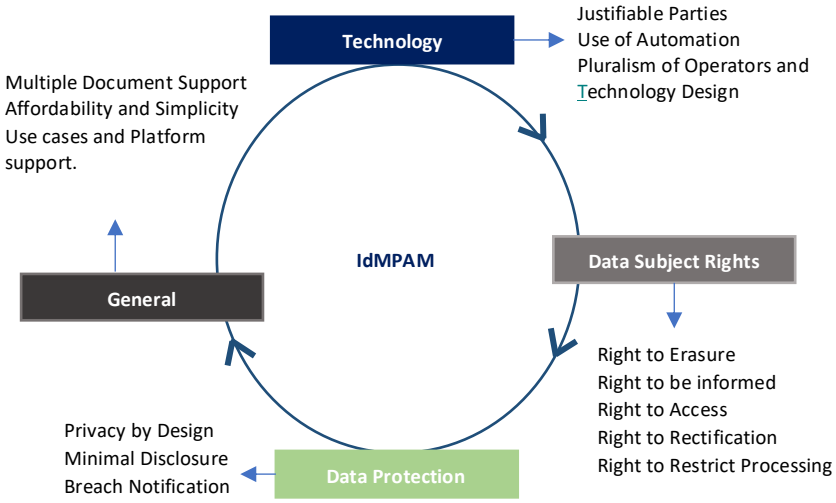


Figure 4.6. IdMPAM Evaluation Criteria

4.3.3 Information Security Audit Maturity Model (*i*SAM2)

The third and final artefact of the assess component is *i*SAM2, a maturity model that enables ADIVRA to assess the maturity of information security audit processes in an organization. During the stakeholder workshops and meetings, it was realized that before designing an adaptive DigI verification process model, it is important to assess the existing information security capability. One of the underlying challenges for organizations is the successful design and application of the information security audits to better understand their information security readiness. The central idea of this maturity model is to pinpoint a baseline for the improvement and extension of security audits in an organization. Once developed, this can be used to build consensus in iterations, prioritize security decisions, and monitor the operational progress. In this thesis, the foundations of *i*SAM2 are built on ISO 27001. The decision for selecting ISO 27001 is driven by the fact that

it is the most widely implemented standard as well as our industry partner's need and interest to be ISO 27001 certified. However, *i*SAM2 is not fixed to any specific standard and can be tailored as per the requirements. The levels of *i*SAM2, the set of activities for detailing the audit requirements and relevant evidence are presented in Table 4.3. The *i*SAM2 is divided into five maturity levels depending on the activities and rigor carried out during each stage of the internal audit (planning, fieldwork, and reporting). *i*SAM2 may help organizations in assessing the maturity of their information security audit procedures and identifies the gaps for further improvement.

Table 4.3. *i*SAM2 Levels and Requirements

Steps	Level 0: Initial	Level 1: Basic	Level 2: Compliance Focused	Level 3: Managed	Level 4: Optimized
Description	No stable audit process in place, missing audit scope and objectives, no validation of results or focus on quality	Moderate procedure in place but not totally reliable, effective reporting and documentation is lacking	Audit and processes are clearly defined, documented, and standardized	Audit procedures are extremely effective, including automated reports, constant surveillance, and clear correspondence	Continuous audit and surveillance processes in place, trusted data analytics with the ability to achieve a high level of excellence, vibrant approach to evolving practices
Planning	Unplanned Underfunded Understaffed	Critical Asset Identification Establish a targeted audit baseline. Ad-hoc/Case-by-case audit plan and scope Limited resources Lack of well-defined audit plan	Critical Asset Identification Outline Security objectives in line with the organization's compliance needs Well defined audit plan and scope Control-based security approach Approved budget Audit as per schedule	Visibility to top management Adequately positioned and resourced Involve subject matter expert.	Improvement objectives defined. Transparency to top management Sufficient budget and staff
Field Work	Lack of executive support Document reviews and interviews to solve a specific problem	Internal employee acts as an auditor Only critical assets are audited Employee interviews Document reviews	Develop a checklist according to objectives Employee interviews Collect evidence Check IT Logs Define threshold for critical audit observations Compare with prior audits.	Use of Computer Assisted Audit Technique (CAAT) Conduct security and vulnerability scans Risk Scoring Organizational Walk-through Analyze data supplier's security Workforce assessment	Multi-layered security and risk-based approach Integrated with IT Automated workflow Supervise the implementation level of audit suggestions by management and report the results to the audit committee.
Reporting	Lack of metrics for reporting	Audit report stating information security gaps Partially achieved goals	Internal audit report Management review meeting Management review meeting minutes Corrective and preventive action reporting	Audit report with corrective and preventive action plan Constant improvement plan Anticipated future requirements Updated security strategy Internal audit recommendations accepted by management. Feedback on the company's compliance framework.	Continual improvement Metrics to demonstrate success Full cyber-readiness framework Follow up

				The latest internal audit manual.	

4.4. Design Component

The design component artefacts fill the gaps and mitigate the risk identified using the assess component. The design component of ADIVRA addresses RQ2 (see Chapter 1). This component has four artefacts: RRM, CDigI, DigIVPM and *i*SEA. The scope of the design component is limited to RRM for regulatory requirements, CDigI for multidimensional DigI, iSEA for Secure DigI and privacy by design and DigIVPM for DigI behavior.

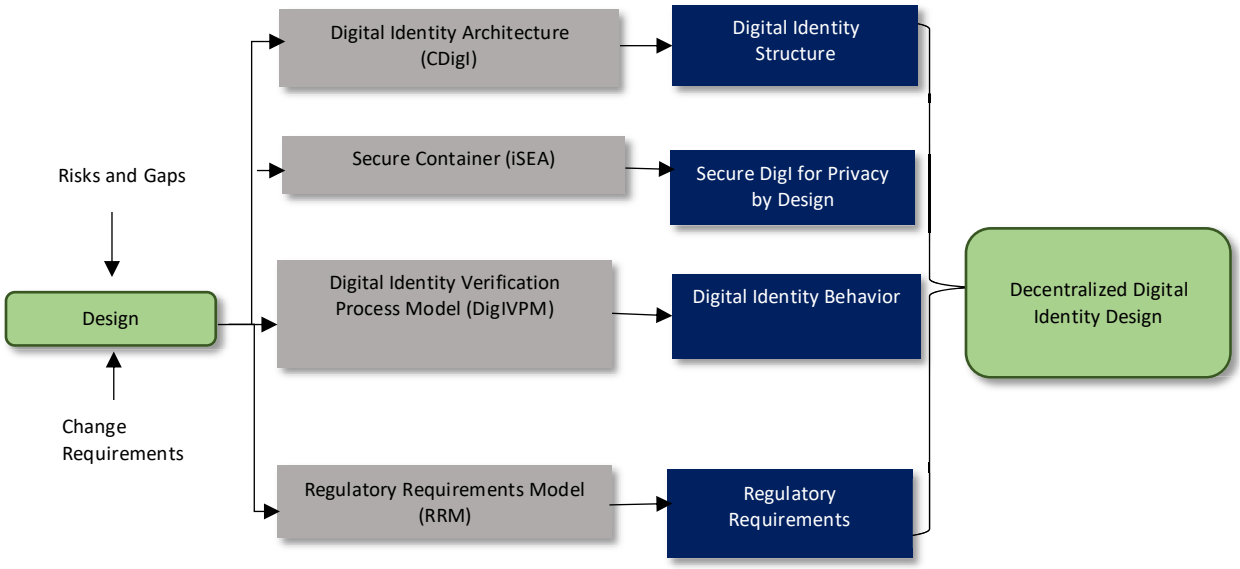


Figure 4.7. ADIVRA-DESIGN Component

4.4.1. Regulatory Requirements Model (RRM)

Considerable attention has been given to privacy requirements, particularly by system designers and users, but little attention has been given to DigI itself and relevant regulatory perspectives (Drljevic, Aranda & Stantchev 2020). There are many country-specific laws and standards (EU's National Identity Scheme, Trusted Digital Identity Framework, Australia) as well as international regulations (GDPR 2018, eIDAS 2014) that are applicable to DigI verification. However, the challenge is to determine and extract the regulatory requirements to design a regulatory compliant DigI verification solution. To fill this gap, ADIVRA proposes an RRM which is an artefact of the design component. RRM is developed using the integrated requirement engineering model as a kernel theory (Gill & Bunker 2014) as shown in Figure 4.8. The specific requirement engineering strategy might differ as per the individual organizational context, however, the five basic requirement engineering stages stay the same: "(1) elicitation, (2) analysis, (3) verification and validation, (4) documentation and (5) management" (Paetsch, Eberlein & Maurer 2003; Sommerville 2005). Figure 4.8 presents the alignment of the RRM with these five basic stages of the conventional requirement engineering process. Based on the integrated requirement engineering model (Gill & Bunker 2014), the first step of RRM requires the identification of

business processes as required by every entity involved in the DigI verification process. The regulatory articles (e.g., from eIDAS or GDPR) aligned with privacy goals are also extracted and analyzed in parallel. The mapping of business processes with entities involved in DigI verification and the selection of regulatory articles (eIDAS or GDPR) come under requirement elicitation and requirement analysis activities. The next step is the validation of selected articles and business processes. This step relates to requirement verification and validation from traditional requirement engineering activities. Finally, the requirements are recorded in the form of a backlog and managed using any tool for requirement documentation and management. The application and evaluation of RRM is detailed in Chapter 5.

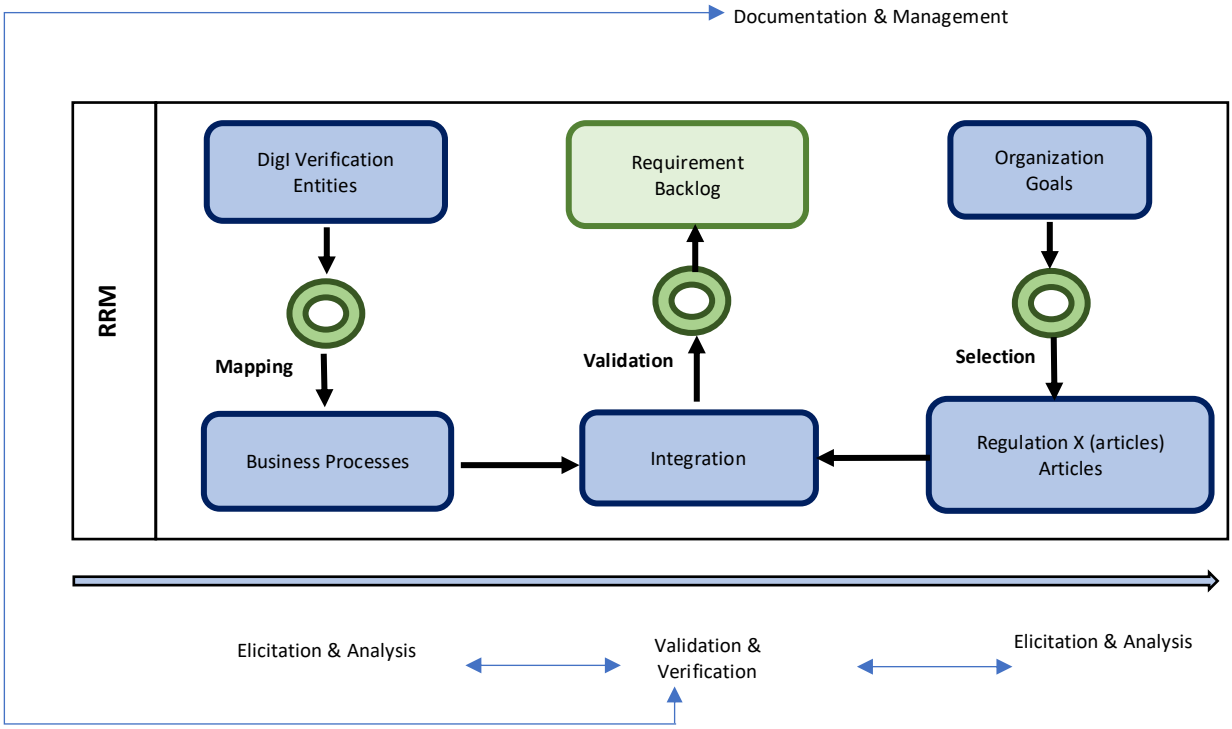


Figure 4.8. Regulatory Requirements Model

4.4.2. Compound Digital Identity (CDigI)

After extracting the regulatory requirements using RRM, it was observed that the one-dimensional view (for example DigI based on government-issued identity documents only) of DigI might not fulfill the regulatory obligations. Existing DigI verification solutions tend to overlook the fact that identity is not a singular concept. Rather, it is a complex and multi-dimensional (Buckingham 2008) concept encompassing different types of identities (e.g., biological, business, professional, social). A wider interpretation is that DigI may comprise information about people and their social, professional, or business communications and associations in electronic form. This information can be stored within government data centers and commercial databases or distributed on the Internet in the form of blogs, tweets, likes and comments on social networks. Whether it is a government, business, or individual transaction, the use of PII constituting DigI is an essential part of all online interactions. A DigI contains data that exclusively describes an individual alongside information about the individual's connections to other individuals and entities. Hence, DigI is

multidimensional (business, information, social and professional) and multisource (see Table 4.4). ADIVRA refers this type of DigI as CDigI. *CDigI can be defined as a combination of business, information, professional and social attributes that can identify humans, organizations, or devices according to the verification context.* One example of a verification context is travelling where passport information needs to be verified. Another verification context is employment where information on previous experience and qualifications is required. As CDigI is a combination of different attributes, it will serve both the aforementioned verification contexts.

Table 4.4. Compound Digital Identity

	Human	Organizations	Devices
Business Attributes	• Pay slips • Experience certificates • Designation	• Industry reputation • Business goals • Business strategy	• Deceive type • Business function • Device location
Information Attributes			
Natural Attributes	• Age • Height • DOB • Fingerprints • Facial recognition • Retina scan •	• Business domain • Business status	• Device name • Device ID • Warranty information
Acquired Attributes	• Health records • Marital status • Family name	• Business records • Legal records • Compliance certifications • Employee records	• Device owner • Usage record
Designated Attributes	• National identification No. • Phone number • Address • Passwords, security questions, tax ID • Academic degrees	• Identification numbers • Legal jurisdictions • Board of Directors • Roles and responsibilities	• Custodianship
Professional Attributes	• Job experience • LinkedIn Profiles • Employee ID	• Skills matrix	• Manufacturer
Social Attributes	• Social media profile and behaviour • Browsing history • Digital footprints • Online Interests	• Organizational culture	

4.4.3. Information Security Envelope Architecture (*i*SEA)

To ensure the privacy of the DigI, ADIVRA includes a secure container in the form of *i*SEA. The *i*SEA may provide the much-needed privacy for sensitive and confidential PII comprising CDigI. *i*SEA works by combining the strength of Attribute Based Encryption (ABE) (Sahai & Waters 2005) with authentication and authorization procedures to protect DigI information, at rest and in

transit. It seems to address the data protection requirements presented by state/federal privacy laws (extracted using RRM). The *i*SEA is divided into three key parts: authentication and authorization, CORE envelope, and logging and monitoring. An authentication and authorization module is implemented to verify individuals or applications willing to connect with *i*SEA. Once verified, *i*SEA returns a session ID for the verified user which is used for all communications. Once the session is established, the CORE is triggered for encrypting/decrypting sensitive information using key-policy attribute-based encryption (KP-ABE) defined by Goyal et al. (2006). The CORE is the part where KP-ABE is incorporated. To encrypt the DigI information, the encryption module requires the attributes of the service provider (the receiver of the DigI information), which are specified in the form of policy. The policy is defined by the identity owner utilizing the service provider's attributes. DigI information can only be accessed when the service provider possesses a certain set of attributes that satisfy the policy. The encryption module uses a set of attributes or credentials of the receivers to encrypt the DigI information. This provides security and fine-grained access control. The identity owners select the service provider before accessing their DigI information. The service provider will initially request DigI information. The identity owner may accept or reject the permission request. If the identity owner accepts the request, the service provider will receive a notification. The service provider can then access and verify the DigI information. Even though permission is granted by the identity owner, the service provider can access DigI information only when their attributes satisfy the policy. If the attributes are matched, DigI information can be decrypted. A logging and monitoring system maintains an audit trail. Each query to *i*SEA and response from iSEA passes across the audit module. Figure 4.9 shows a high-level contextual view of *i*SEA.

The iSEA workflow incorporates the following essential modules:

- Authentication and authorization
- CORE Envelope (Encryption Module, Decryption Module, ABE Engine, Privacy Module, SALT Engine)
- Logging and monitoring engine

The CORE envelope is further divided into five modules:

ABE Engine: The ABE engine is the central traffic controller that communicates with each module of *i*SEA. The ABE engine assigns the session ID to the end-user after authorization.

Privacy Module: This module takes as input the security parameter (SecP) and a list of attributes (U), such as bank manager, company CEO etc. from the ABE engine. The privacy module outputs a public key (pk) and master key (mk). The pk is fed into the encryption module to encrypt the DigI information and mk is fed into the SALT engine to generate SALT. Only the identity owner has access to SALT.

SALT Engine: The SALT engine takes as input the mk and a policy based on a set of selected attributes from U. Policy is a logical expression that combines several attributes through the AND and/or OR operator. The policy is defined by the identity owner. It outputs a SALT which is a secret key corresponding to the policy.

Encryption Module: The encryption module takes as input the pk, DigI information, and the set of attributes S selected by the identity owner from attributes list U. It outputs the encrypted DigI information associated with the set of attributes S in such a way that only the user whose SALT has policy that are satisfied by S can extract DigI information.

Decryption Module: The decryption module takes as input the encrypted DigI information containing attributes S, and SALT containing policy, and outputs the plain text if the set of attributes S meets the policy or null if decryption fails.

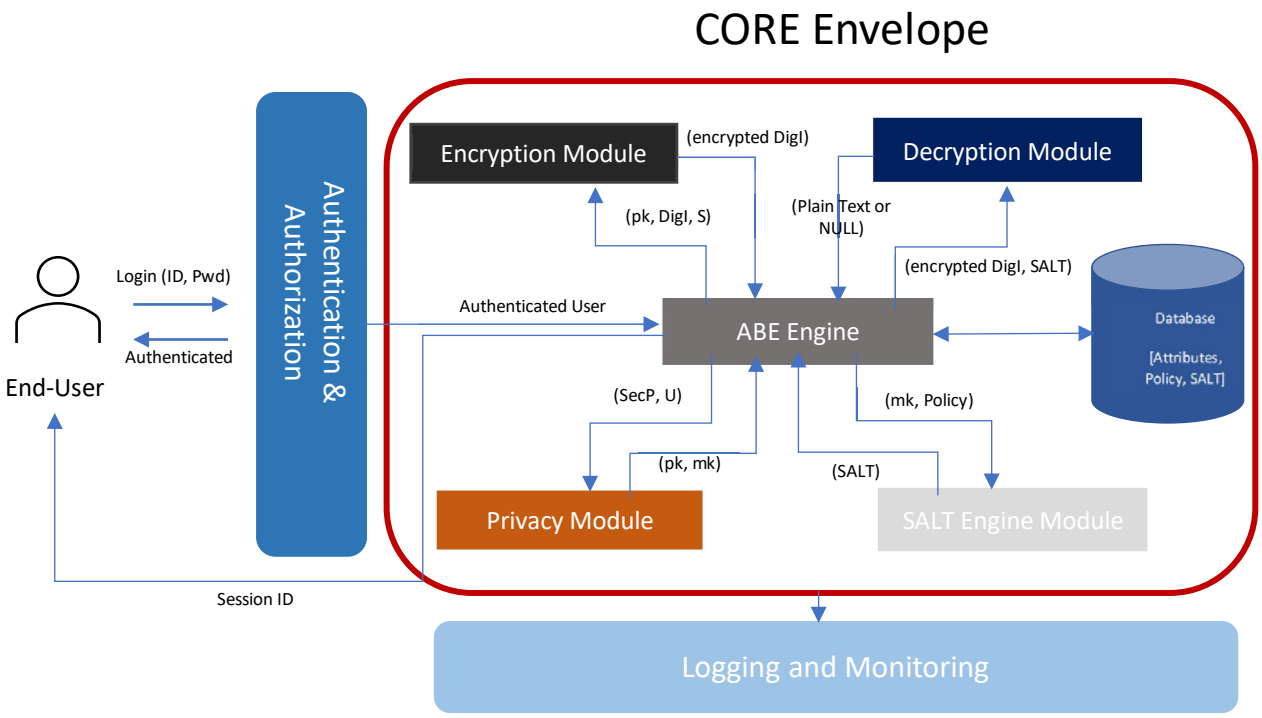


Figure 4.9. Information Security Envelope Architecture

4.4.4. Digital Identity Verification Process Model (DigIVPM)

The third artefact of the design component is DigIVPM, which is designed to securely verify DigI information. This model describes the entities, activities, (for both business-to-business (B2B) and business-to-customer (B2C) verification) and the DigI verification process without storing the PII. The DigIVPM is designed by keeping the CDigI architecture in mind. The DigIVPM is founded on a decentralized model of identity verification to meet privacy and compliance goals. The DigIVPM is designed by using blockchain as an enabling technology. Figure 4.10 presents a typical blockchain-based DigI verification process. DigIVPM is designed considering four main entities that interact with each other and with blockchain during the DigI verification process. The activities performed by each entity during the DigI verification process are detailed in Table 4.5. The DigI verification process can be initiated by the identity owner (B2C) or by the service provider (B2B). The ADIVRA DigIVPM considers both scenarios and provides a separate flow for each (see Figure 4.11). DigIVPM constructs the technology and regulations to deliver privacy, regulatory compliance, and adaptability, which is difficult to achieve with existing solutions.
DigIVPM is a blockchain-based DigI verification process where identity owners can have the ownership and control of their DigI. It provides DigI verification without storing PII. The identity owner has the power to choose to whom and when to disclose their PII. Identity providers can

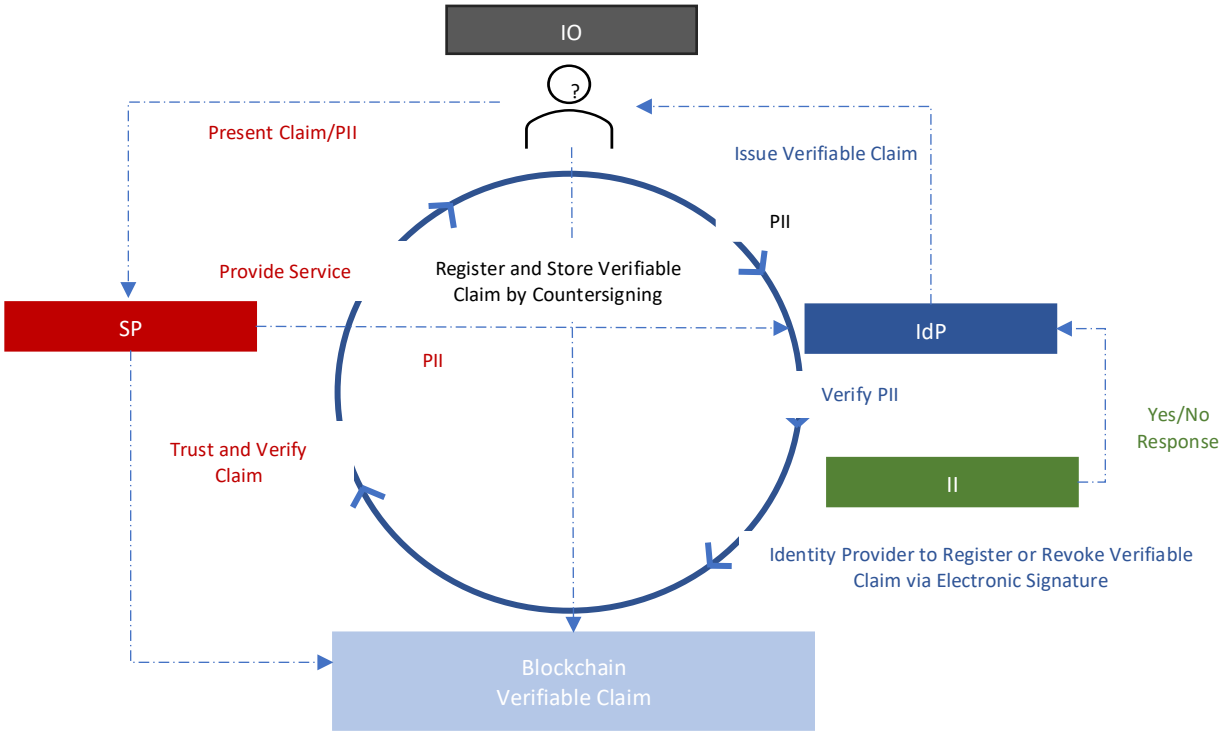


Figure 4.10. Decentralized Digital Identity Verification Life Cycle

verify the legitimacy of PII presented by the identity owner via blockchain without needing any centralized third-party's guarantee.

Table 4.5. Decentralized Digital Identity Verification Entities

Entity	Activities
IO	• Owner and controller of DigI • They use their DigI to identify themselves in a secure manner in the digital world. • Business people, information people, professional people and social people (e.g., Alice)
SP	• Trusts the verifiable claim for onboarding new customers and authenticating existing customers. • Includes businesses (e.g., online shops), employers, banks, universities and government agencies (e.g., tax offices)
IdP	• Intermediates that facilitate the DigI verification process between the service provider and the identity owner • Issues and attests verifiable claims. • Neutral organization (e.g., IDZ)
II	• Issuing authority that issues DigI credentials • Confirms the identity owner's physical identity and issues the corresponding identity attributes to ascertain their DigI. • Government agency (e.g., passport office)
Blockchain verifiable claim (VC)	• The digitally signed DigI certificate issued by the identity provider after verifying identity credential by identity issuer

The DigIVPM enables organizations and individuals to:

- securely verify the identity of an individual or an entity without storing PII

- reuse DigI
- exchange attested DigI among institutions while complying to GDPR

The fundamental architecture of DigIVPM is designed to enable two parties to build a web of trust via the autonomous authentication of PII, eliminating the need to trust each other or a centralized third party that holds the PII. This is achieved by enabling the identity owners or other involved entities to present their verifiable claims (VC) of DigI and the receiver to verify the information corresponding to the claims via blockchain. In DigIVPM, the identity owners do not need to provide any PII. They only need to provide proof of verification and assertation of their DigI by a reliable identity provider. The service provider might require some additional information that can be presented or verified if the identity owner wishes. The DigIVPM is designed to be integrated into the identity provider's mobile applications.

a) B2C DigIVPM

In the B2C model, the IOs install the mobile application into their phone. Using the mobile application, the IO creates a profile by uploading a picture of them holding the identity document (such as a passport). The IO's identity is first obtained either by a scanned driver's license, government ID, or passport or by biometric information, for example their fingerprints, iris-scan, facial matching, or liveness test. The PII extracted by IdP, (e.g., via Optical Character Recognition) from the identity document is split into separate name/value fields and verified by the identity issuer. The PII returns a yes/no response to the verification. If the verification is unsuccessful, the IO is asked to repeat the entire process. If the identity document is successfully verified by PII, the name/value fields are then attested by IdP, sealed in *i*SEA and maintained securely in the IO's device as well as in the IdP's data stores. This represents the IO's DigI. After this process, the IdP constructs the name/value fields in the form of one complete record. In the next step, the identity provider issues a VC against each record. The VC is digitally signed by the identity provider and identity owner and is placed on the blockchain in the IO's identity wallet. The IdP assigns a QR code to the IO against the identity wallet. In DigIVPM, the blockchain is used only as a medium to store evidence of the transaction and the confirmation of claims made by IO. DigI information in any form, encrypted or otherwise, is not stored on the blockchain. This is due to the fact that any PII on a public blockchain can be possibly stolen or tempered by cybercriminals. Even in an encrypted or hashed form, this sensitive PII is subject to theft or loss. In addition, any data on blockchain is immutable and once stored, cannot be erased, or altered. This can be problematic in the case of a change of circumstances. Hence, the blockchain serves as a repository of certifications and no PII is stored in any form on the blockchain.

b) B2B DigIVPM

In the B2B model, the service provider can initiate the identity verification process by presenting the IO's identity documents with their consent. The mechanics of the B2B model are very similar to the B2C model presented earlier. However, in this case, the SPs must acquire a pre-paid wallet where the verifiable claims of their customers (IO's) will go. In both cases, the IO will present a blockchain-based VC to the service provider via QR code scanning. Every time an IO's identity is

successfully verified by a service provider, an entry goes into the distributed ledger for that verification and the verifiable claim gets one star. The more stars, the more trusted the verifiable claim. This star-based system enables a web of trust to be built among multiple SPs and increases reusability. After a VC reaches a threshold of stars (e.g., 5 stars, 10 stars), the encrypted name/value DigI information stored in the IdPs data stores is deleted. Hence, the only store of PII comprising DigI is the IO's device. In the case of a change of circumstances (for example, the IO's marital status changes and their name changes too), the identity verification process is initiated from scratch by presenting the updated identity document.

When the QR code is scanned, a notification is sent to the IO detailing the type of information requested to be verified by the SP. The IO consents to share the requested information. The IdP gives a pointer to the IO's wallet where a verifiable claim is stored. The service provider may ask for further information which can be provided if the IOs give their consent. To keep the DigI up to date, a validity bracket is kept on the VC i.e., the VC expires after a certain period of time. After this bracket, the verification process is reinitiated, and updated claims are placed in the wallet.

The DigIVPM is intended to give IOs control over their DigI and its purpose and usage. The DigI can be verified over a secure channel across the named IdPs, and the results of the verification will be sent back to the SP or whoever requested the DigI verification in a secure manner without storing the PII. This approach seems to considerably minimize the compliance cost and enhance the interoperability, efficiency, privacy, security, and usability of DigI. Due to the need to maintain, for example, isolated expensive DigI verification and the management and support arrangements, support portals will be substantially lessened, thus enabling the personnel to concentrate more on service delivery rather than worrying about DigI verification.

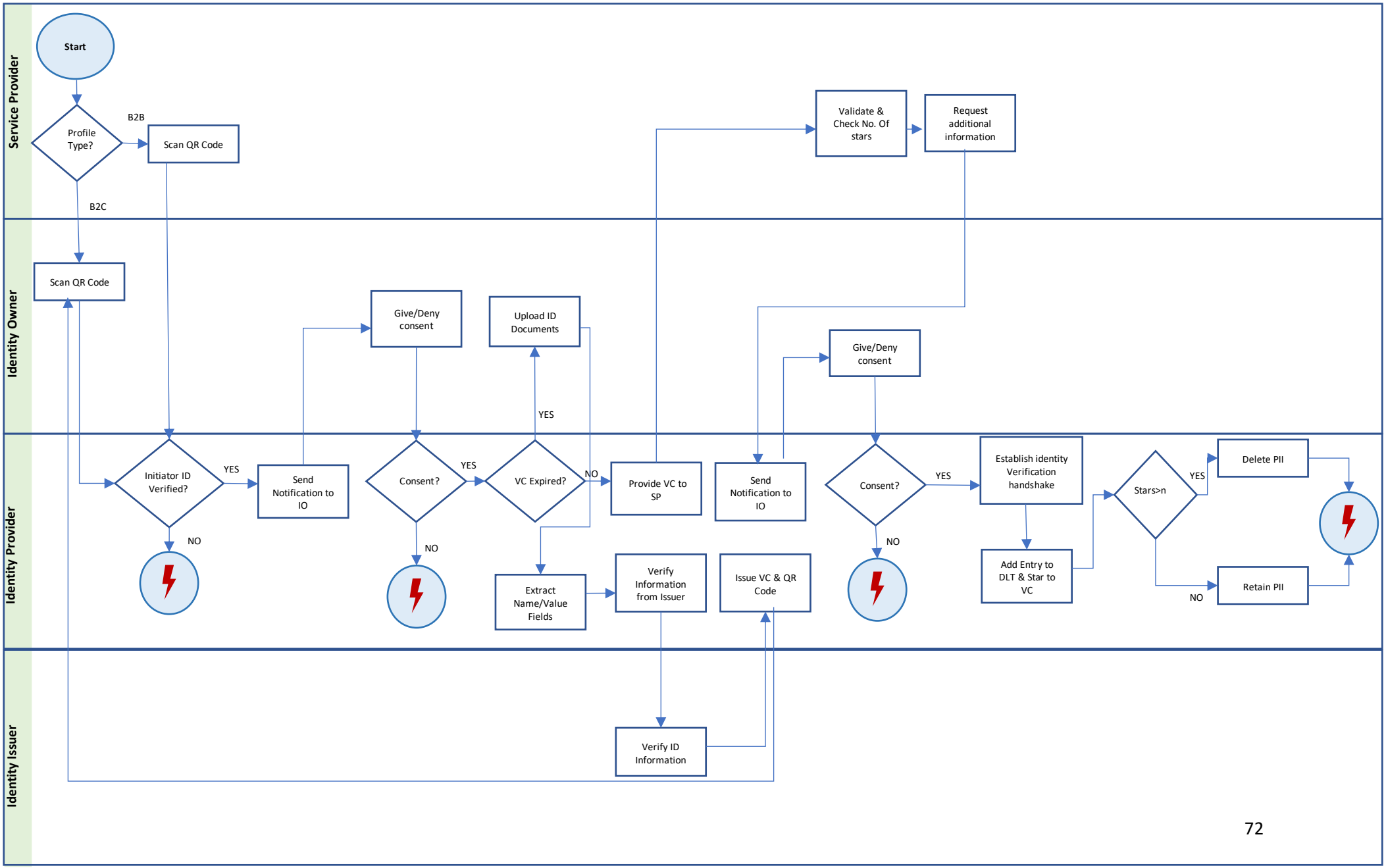


Figure 4.11. Digital Identity Verification Process Model

4.5. Evolve Component

The ADIVRA evolve component can help in discovering changes in regulatory requirements, privacy risks, or business strategy. The PESTLE+ risk analysis model (from the assess component) is used to identify the risks and gaps that serve as input to DigIVAM. The evolve component of ADIVRA addresses RQ3 (see Chapter 1). The objective of this component is to recognize changes and devise an action plan, which could be relevant to regulations, privacy risks and business strategy and feed these changes to other components such as assess and design. This will ensure adaptability in the proposed framework. There could be other types of changes which may be considered by this component. However, for the purpose and scope of this research, this component is limited to addressing regulatory requirements, privacy risks and business-need related changes.

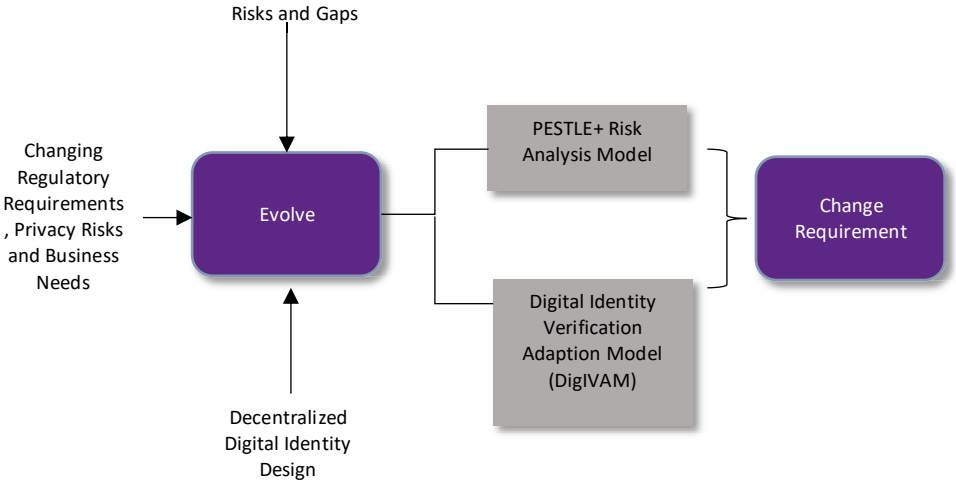


Figure 4.12. ADIVRA-EVOLVE Component

4.5.1 Digital Identity Verification Adaption Model (DigIVAM)

DigI underpins the functions of digital ecosystems and is key to enabling the transformation of service delivery. ADIVRA is not a static concept. It is designed keeping in mind the competitive landscape and understanding business needs in such a way that helps IdPs to make effective and timely strategic business decisions in the ever-changing digital ecosystem. Its privacy principles, the DigI structure, the verification process, and the compliance models need to adapt in response to changing business needs, regulatory requirements, emerging DigIs and evolving global digital ecosystem threats and opportunities.

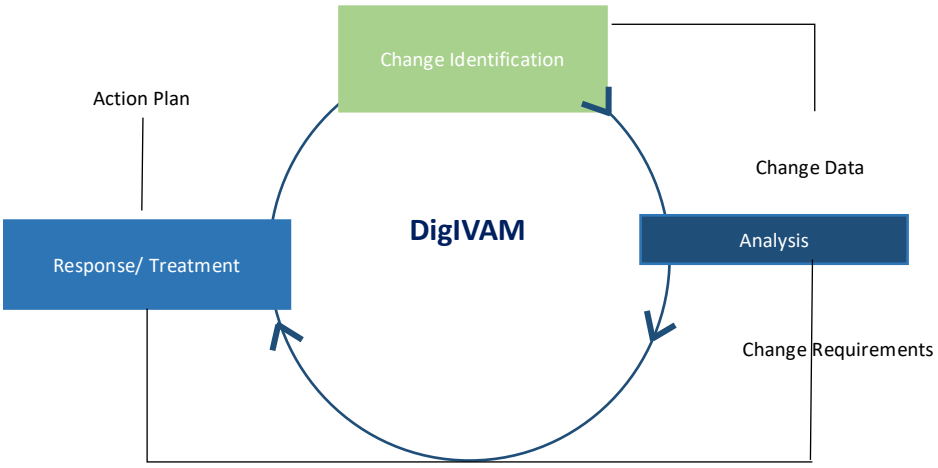


Figure 4.13. Digital Identity Verification Adaption Model

Once the change is identified, it is fed into DigIVAM manually. Human intervention in this process signifies a conventional way of linking specific requirements by human decision making and builds a foundation for analysis. Next, the change requirements are manually analyzed by a group of experts from each unit (business analyst, compliance manager, IT manager, privacy officer and digital identity architect). These analysis workshops help in symmetrically drawing relationships between requirement instances. This process extracts change requirements from classified change data, identifies what has changed in different areas (e.g., business strategy has changed, or regulation has changed, or some new privacy risk is introduced) and analyzes the change requirements by conducting risk analysis using the PESTLE+ model. Once the change requirements are driven from the data, the next step is the decision about adaptability that yields the action plan. This action plan includes the changes that will be realized in the DigI design to adjust. The DigIVAM is shown in Figure 4.13. Table 4.6 shows the activities at each step.

Table 4.6. Digital Identity Verification Adaption Model Activities

DigIVAM Stage	Activities	Description
Change Identification	Identify source, cause, and area of change.	Privacy risk Regulations Business Strategy
	Classify change.	Minor /Major
	Prioritize change.	Low/Medium/High
Analysis	Impact analysis of change	Low/Medium/High
	Risk management (PESTLE+ Analysis)	Risks associated with adapting to change
Response/Treatment	Action Plan	Change requirements backlog
	Implementation Plan	Timelines, effort estimation etc.

4.6. Summary

This chapter presented an overview of the overall ADIVRA and its components. Three components (Assess, Design, and Evolve) of ADIVRA are discussed in this chapter. Each component of ADIVRA has further artefacts which are also detailed in this chapter. This chapter presented the final version of ADIVRA. The details of the intermediate versions (alpha, beta, and gamma) and the reflections and learning are discussed in Chapter 5.

Chapter 5: Results and discussion

Chapter 4 presented the final version of the ADIVRA framework. The incremental development and evaluation of the ADIVRA framework was done using the well-known ADR method (see Chapter 3). This chapter discusses both the development of the framework, from the alpha to the gamma versions, and the evaluation. The evaluation is conducted in two ways. Firstly, this chapter discusses the design and review workshops that were conducted in the industry partner's organizational setting. Secondly, this chapter details the results of the industry field survey that was conducted with industry professionals from various organizations. The survey data are analyzed for the final evaluation of the ADIVRA framework. The generalization, applicability. novelty, usefulness, and comprehensiveness of the ADIVRA framework are evaluated based on the feedback collected from the design and review workshops and the industry field survey.

5.1. The ADVIRA Framework Evolution (alpha to gamma)

The ADIVRA framework progressed through the alpha, beta, and final gamma versions.

- Alpha (preliminary version)
- Beta (intermediary version)
- Gamma (final version)

Despite their traditional linear design and post-design evaluation, ADIVRA components were iteratively built and evaluated. The primary purpose of building and evaluating ADIVRA framework in iterations was to enable progressive emergence of the design (from alpha version to the final gamma version) as each component is progressed through BIE and RL iterations (ADR Principles 3, 4 and 5). The ADIVRA evaluation was conducted in a recursive way such that, within each BIE and RL iteration, the artefacts were evaluated via three design and review workshops. According to the ADR approach, continuous intervention into organizational setting and feedback workshops are conducted throughout the ADIVRA design process. Effective and ongoing comments (see Appendix I) from the relevant stakeholders facilitated the continuous refinement of the ADIVRA framework by reflecting on the design and redesigning the architecture along with analyzing the intervention results according to the stated criteria.

The design and review workshops were held as a part of the meetings among researchers, industry practitioners, and subject matter experts in DigI verification in IDZ's organizational setting. The industry practitioners were engaged in reviewing, analyzing, and giving their comments and feedback on the ADIVRA and its applicability, usefulness, and comprehensiveness (see Table 3.1) for DigI verification solutions. Throughout the interventions, architectural design decisions are made. New artefacts were added to fundamental ADIVRA framework as this feedback-based continuous reflection and learning mechanism progressed (ADR Principles 6). The RL activities like showcases, stakeholders' feedback workshops, retrospective and subsequent ongoing design refactoring improve the clarity and evolution of the ADIVRA framework and the development procedures.

To evaluate ADIVRA, the formative evaluation method is used. The evaluation of the alpha version in ADR is formative evaluation, "in which an artefact still under development is evaluated to determine areas for improvement and refinement" (Venable, Pries-Heje & Baskerville 2012).

The BIE and RL stage of the ADR are conducted in a non-linear way (see Figure 5.1). The final version of the ADIVRA is evaluated via industry field surveys.

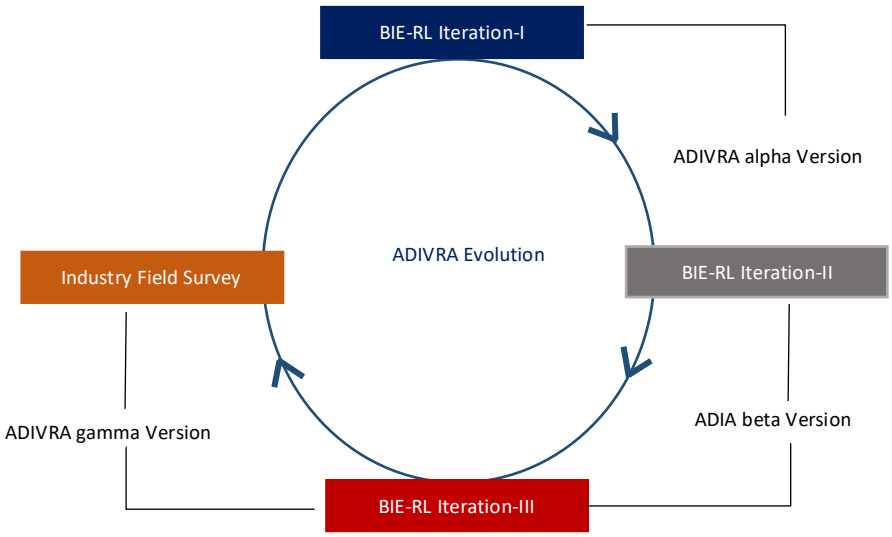


Figure 5.1. ADIVRA Evolution

5.2 BIE & RL Iteration-I (ADIVRA Alpha Version)

While creating the first (alpha) version of ADIVRA, the research team continuously worked on-site with the practitioners (the IDZ organizational setting). The first BIE iteration aims at the assess component of the ADIVRA framework. Three design and review workshops were held to design, review, and re-design the alpha and beta versions of the assess component (see Figure 5.2). IDZ employed blockchain technology and ensured GDPR (European Union 2018) compliance for their target DigI verification solution. The researchers presented the research problem and gaps

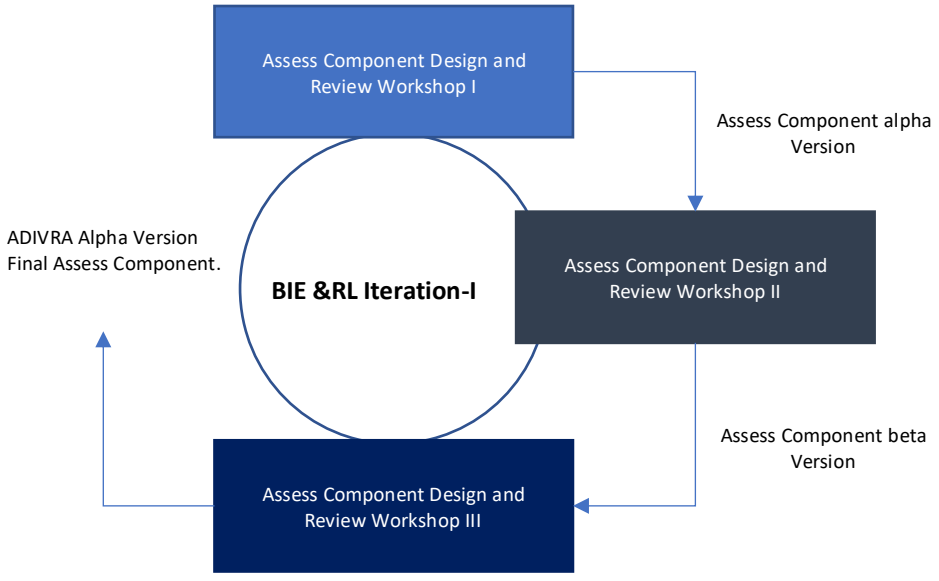


Figure 5.2. BIE & RL Iteration-I

identified by the literature review. The presentation ran for 30 minutes. After the presentation, the PhD researcher facilitated a brainstorming session to identify the alignment between IDZ's needs and the research problem for this research project. Table 5.1 details the first design workshop together with the workshop objectives, role and responsibilities and feedback and comments from the participants.

Table 5.1 Assess Component Design and Review Workshop I

Organization:	IDZ (coded name) is a leader in the eIDV (Electronic Identity Verification) industry with the capability to provide access to the widest, most in-depth, reliable, and independently sourced identity data throughout the APAC region.	
Workshop Objective	To make design decisions for ADIVRA assess component	
Workshop Facilitator	The researcher of this project is responsible for explaining the framework design, educating, and facilitating the framework design decisions, evaluation and documenting the feedback	
Workshop Participants	• IT Manager • Digital Identity Architect • Business Analyst • Privacy Officer • Compliance Manager	
Main Design/Evaluation Component	**Assess**	
Role/Responsibility	**Comment/Suggestion/Feedback**	**Interpretation**
Compliance Manager	*"The existing operation model for IDZ, whilst efficient and seamless for clients, must be improved with an enhanced offering to clients (and potentially individuals) in order to maintain and extend this status within the industry."*	IDZ's future DigI verification solution should be better than existing solutions in the eIDV field. To achieve this, it is important to assess the capability of existing solutions. This is aligned with RQ1.
IT Manager	*"IDZ is seeking to harness the potential of new global technology trends involving biometrics and blockchain. Incorporating these technologies into enhanced applications and efficient operations that its' clients can leverage will enable IDZ to continue as an industry leader and trusted identity verification partner."*	For IDZ's future DigI verification solution, blockchain should be used as an underlying technology. This is aligned with RQ1.
Privacy Officer	*"With all the interest in this technology, it is imperative to clearly understand blockchain and the privacy of DigI information considering regulations such as GDPR."*	To choose blockchain as an underlying technology for future DigI verification solution, it is important to assess the viability and suitability of technology for DigI verification. This is aligned with RQ1.
Digital Identity Architect	*"Before designing a blockchain-enabled privacy enhancing digital identity verification solution, it is important to identify the risks and gaps in the existing privacy capability of the organization."*	To enhance the privacy capability, IDZ needs to assess the existing privacy capability. This is aligned with RQ1.
Business Analyst	*"We would like to take these models further and offer capability to white label the IDZ platform and making the platform portable via an SDK to clients and potential verification partners."*	Increase user base by providing a reliable and secure DigI verification solution. This is aligned with RQ1.

The provision of privacy is one of the goals of IDZ because of the PII they process. Regardless of the claimed potential of using blockchain technology for the improvement of DigI and privacy, there is no research-based metric or model to assess its suitability for DigI verification (as highlighted in the research gaps). Hence, in this BIE cycle, the ADR team decided to build an assessment model to assess the viability of blockchain for DigI verification solutions. The model is named IdMPAM. During this workshop, the digital identity architect pointed out that before developing a model to assess blockchain's privacy capability in light of GDPR, it is important to identify the risks and gaps in the existing privacy capability of the organization. All the participants mutually decided to conduct PESTLE risk analysis for this purpose. However, at the time when

this research was conducted, the world was going through the corona virus pandemic, which posed unique risks for IDZ and its operational environment. As an example, the travel ban implemented by multiple countries forced many businesses to go online. As businesses in multiple jurisdictions, started more operations online, there was an increased need to verify DigI of individuals. This resulted in frequent transfer of information across borders therefore, increasing the risk of identity theft. Hence it was critical to assess the growing risks caused by corona virus pandemic and to prepare for any similar health related risks. Therefore, to suit the IDZ's practical context, PESTLE risk analysis cannot be applied as it is. Hence, it was decided to extend the PESTLE risk analysis model to provide a broader coverage of environmental factors. For this purpose, the PESTLE risk analysis model was extended by including the health factor to suit IDZ's context during the pandemic crisis. This risk analysis model was named PESTLE+. At the end of the design workshop, it was agreed to include PESTLE+ and IdMPAM into the assess component of the ADIVRA framework. The alpha versions of the PESTLE+ model and IdMPAM are shown in Figure 5.3a and 5.3b.

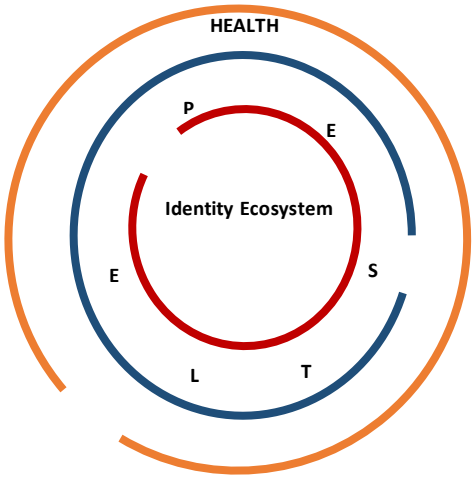


Figure 5.3a. PESTLE+ Model (alpha version)

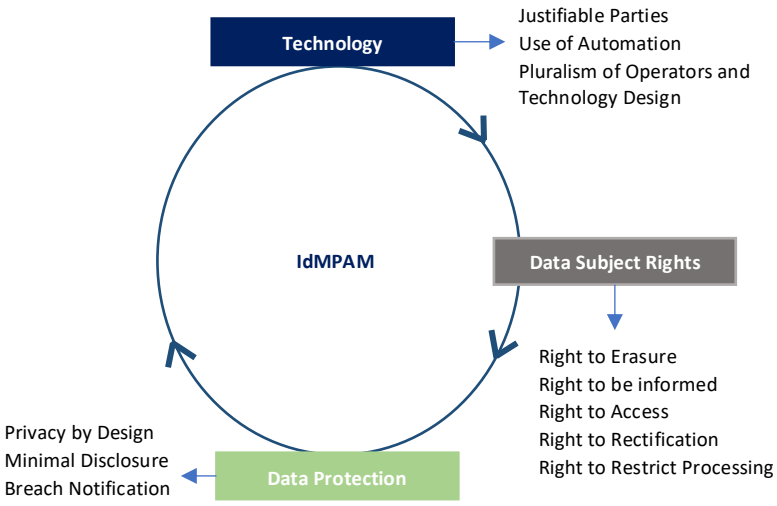


Figure 5.3b. IdMPAM Alpha version

After the alpha version of PESTLE+ (see Figure 5.3a) and IdMPAM (see Figure 5.3b), we constitute the alpha version of the assess component. A review workshop was conducted to obtain the participants' feedback on the assess component of ADIVRA. The alpha version was evaluated using the criteria detailed in Table 3.1. The demo and presentation of the alpha version ran for approximately 30 minutes. The workshop participants discussed the intervention results and guided the alpha version of both the artefacts. The privacy consideration was especially taken into account. After the demo and presentation, an evaluation session was organized with the participants (duration approximately 30 minutes). The participants provided qualitative feedback about the assess component in terms of its usefulness, applicability and comprehensive perspectives as detailed in Table 5.2. Feedback was captured during the design and review workshops.

Table 5.2 Assess Component Design and Review Workshop II

Role/Responsibility	Comment/Feedback/Suggestions	Artefact	ADIVRA Category	Interpretation
Privacy Officer	*"The level and depth of risk analysis required to foresee and prepare for pandemics like Corona Virus, requires health to be considered as a standalone factor in risk analysis, as well as its impact on other factors (political, economic, social, technological, legal and environmental) should also be taken into account."*	PESTLE+	Comprehensiveness	This feedback indicates that the PESTLE+ risk analysis model could be improved by making the macro-environmental factors interdependent
Compliance Manager	*"PESTLE+ is a good extension to the PESTLE model however, the factors included in the analysis are typically assessed and measured individually which may not cover everything."*	PESTLE+	Comprehensiveness	This feedback indicates that the PESTLE+ risk analysis model could be improved by making the macro-environmental factors interdependent
Business Analyst	*"The health factor treated as a sub factor in current PESTLE risk analysis model may not permit a thorough investigation of health-related risks. PESTLE+ fills this gap "*	PESTLE+	Usefulness Applicability	This feedback indicates that the PESTLE+ model is useful in any business context. It also indicates that it can be applied to contexts other than DigI verification.
Business Analyst	*"IdMPAM is straightforward and easy to understand"*	IdMPAM	Usefulness	This comment implies that the IdMPAM is simple and can be easily used.
Compliance Manager	*"Both the artefacts are good to assess the environment and technology from a privacy and compliance point of view. The fundamental challenge for IDZ is the effective design and correct implementation of privacy and security controls and the independent review of the security measures and performance using the internal audit function. This is missing from both artefacts"*	PESTLE+ IdMPAM	Applicability	This feedback indicates that both the PESTLE+ model and IdMPAM do not have much support for assessing the information security capability and maturity of the audit functions. This also indicates that we might need to add another artefact into the assess component of ADIVRA to cover this.
Privacy Officer	*"Although the conceptual foundation of the PESTLE+ analysis proposes a comprehensive approach, this is not mirrored in the evaluation criteria and measurement process."*	PESTLE+	Comprehensive Usefulness	This feedback indicates that PESTLE+ is a comprehensive model but there is a need to rethink the evaluation criteria.
IT Manager	*"The cost considerations have not been taken into account for IdMPAM which is very important for the feasibility of any solution and its adoption."*	IdMPAM	Applicability	This feedback indicates that we may need to add cost as an additional criterion in IdMPAM.
Digital Identity Architect	*"IdMPAM gives very easy to understand factors that can be applied to any organizational context. However, some important factors like ease of use, support for documents and use cases and affordability might be added as assessment criteria"*	IdMPAM	Usefulness Applicability	This feedback suggests the addition of more factors into the IdMPAM assessment criteria.

The assess component was updated according to the feedback received from the participants. New assessment criteria were added to IdMPAM and interdependence was added to the macro-environmental factors of PESTLE+. The IDZ's ISO 27001-based information security management system was also discussed during the review workshop. The compliance officer indicated that, in order for IDZ's information security management system to be able to guide the design of the assess component artefacts, it has to be efficient and effective. The fundamental challenge for IDZ was the effective design and correct implementation of privacy and security controls and the independent assessment of security procedures and their implementation, by the internal audit unit. During the workshop, it was mutually decided that there is a need to measure the effectiveness of the internal audit process. Hence, a third artefact was added to the assess component to measure the maturity of the internal audit process. This component is called *i*SAM2. The requirements and level of *i*SAM2 are detailed in Table 5.3. Hence the beta version of assess

includes the PESTLE+ beta version (see Figure 4.5), IdMPAM beta version (see Figure 4.6) and *i*SAM2 (see Table 5.3). The beta versions of the artefacts (i.e., IdMPAM, PESTLE+ and *i*SAM2) constitute the final version of the assess component and alpha version of ADIVRA (see Figure 5.4)

Table 5.3. *i*SAM2 Levels and stages

Stage	Level 0: Initial	Level 1: Basic	Level 2: Compliance Focused	Level 3: Managed	Level 4: Optimized
Description	No stable audit process in place, missing audit scope and objectives, no validation of results or focus on quality	Moderate procedure in place but not totally reliable, ineffective reporting and documentation is lacking	Audit methodology and processes are clearly defined, documented, and standardized	Audit procedures are extremely effective, including automated reports, constant surveillance, and clear correspondence	Continuous audit and surveillance processes in place, trusted data analytics with the ability to show high level of excellence, vibrant approach to evolving practices
Planning	Unplanned Underfunded Understaffed	Critical asset Identification Establish a targeted audit baseline Ad-hoc/case by case audit plan and scope Limited resources Lack of a well-defined audit plan	Critical asset identification Outline security objectives in line with the organization's compliance needs Well-defined audit plan and scope Control-based security approach Approved budget Audit as per schedule	Visibility to top management Adequately positioned and resourced Involves subject matter expert	Improvement objectives defined Transparency to top management Sufficient budget and staff
Field Work	Lack of executive support Document reviews and interviews to solve a specific problem	Internal employee acts as an auditor Only critical assets are audited Employee interviews Document reviews	Develop a checklist according to objectives Employee interviews Collect evidence Check IT logs Define threshold for critical audit observations Comparison to prior audits	Use of computer-assisted audit technique (CAAT) Conduct security and vulnerability scans Risk scoring organizational walk-through Analyse data supplier's security Workforce assessment	Multi-layered security and risk-based approach Integrated with IT Automated workflow Follow up on the implementation level of audit suggestions by management and report outcomes to the audit committee.
Reporting	Lack of metrics for reporting	Audit report stating information security gaps Partially achieved goals	Internal audit report Management review meeting Management review meeting minutes Corrective and preventive action reporting	Audit report with corrective and preventive action plan Constant improvement plan Anticipated future requirements Updated security strategy Internal audit recommendations accepted by management. Feedback on the organization control framework. An updated internal audit manual.	Continual improvement Metrics to demonstrate success Full cyber-readiness framework Follow up

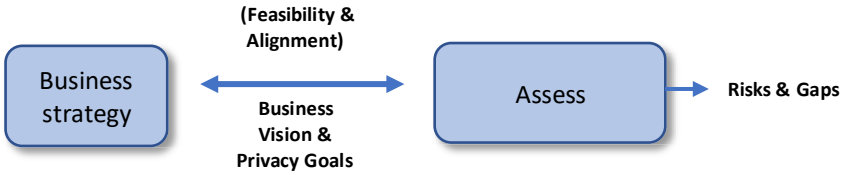


Figure 5.4. ADIVRA alpha version- High Level Contextual Diagram

The beta versions of the assess component artefacts were intervened (see Appendix J) into IDZ to evaluate them against the criteria specified in Table 3.1. The demo and presentation of the beta version ran for approximately 30 minutes. After the demo, the assess component was analyzed by applying it to IDZ's context. This lasted for 90 minutes. The PESTLE+ model was used to conduct a risk analysis to assess the pandemic preparedness of IDZ. IdMPAM was used to assess four DigI verification solutions. The third artefact of the assess component (*i*SAM2) was also evaluated by assessing the maturity level of the internal audit in IDZ. After the demo and presentation, an evaluation session was held with the participants (duration approximately 30 minutes). Table 5.4 details the feedback and comments of the participants from the third design and review workshop for the assess component. It was found that the ADIVRA assess component successfully achieved the desired outcome and needs no further changes. Hence, this is considered the final versions of the assess component and the alpha version of the ADIVRA framework.

Table 5.4 Assess Component Design and Review Workshop III

Role/Responsibility	Comment/Feedback/Suggestions	Artefact	ADIVRA Category	Interpretation
Business Analyst	*"Demo was easy to understand and well presented".*	PESTLE+	Usefulness	This feedback indicates that the assess component is useful and easy to understand
Compliance Manager	*"GDPR and Identity Laws are excellent choice to pick IdMPAM assessment criteria. "*	*IdMPAM*	Usefulness Comprehensiveness	This feedback indicates that the assess components are useful and comprehensive in covering the important aspects of DigI verification
Digital Identity Architect	*"ADIVRA "Assess" component is not specific to blockchain-based DigI verification solutions only. The application of IdMPAM for assessing a non-blockchain based DigI verification solution makes it broader and more generalizable"*	PESTLE+ IdMPAM *i*SAM2	Comprehensiveness Applicability Usefulness	This feedback indicates that the assess component is applicable to a class of problems.
Privacy Officer	*"I think the strength of the PESTLE+ model is the relationships and connections among the PESTLE macro-environmental factors. This enables PESTLE+ to be applicable in multiple organizational contexts."*	PESTLE+	Applicability Usefulness	This feedback indicates that the assess component is useful and applicable to multiple contexts
IT Manager	*"Independent evaluation and analysis of the individual macro-environmental PESTLE factor may not reflect the actual state of affairs. PESTLE+ addresses the issue of interdependence."*	PESTLE+	Usefulness Applicability	This feedback indicates that the assess component is useful and creates new knowledge

IT manager	*"The IdMPAM is an excellent reference for assessing the viability of blockchain for designing DigI verification solutions and brings to life the inherent need for such assessment models to ensure that such solutions are compatible with the changing regulatory landscape in regard to the appropriate use and handling of personally identifiable information (PII). There is no need for any further considerations until there is further research (and subsequent validation) into the best practices of an DigI verification."*	IdMPAM	Comprehensiveness	This feedback indicates that the assess component has sufficient breadth and depth to cover the end-to-end DigI verification lifecycle
Digital Identity Architect	*"The evolution and application of the proposed IdMPAM clarified what was initially a very daunting and complex prospect of understanding the current and potential use of blockchain in the DigI verification landscape. The assessment factors and design principles resolved the technology adoption aspects down to the business operational concepts that can be easily communicated and strategically discussed."*	IdMPAM	Usefulness	This feedback indicates that the assess component is useful in understanding the existing blurry interpretation of concepts related to DigI verification
Digital Identity Architect	*"The ADIVRA assess component will help organizations understand the true potential of any technology and align their privacy and compliance capability with the emerging technological trends"*	PESTLE+ IdMPAM *i*SAM2	Applicability Usefulness	This feedback indicates that the assess component is useful and applicable for understanding and adopting emerging technological trends
Business Analyst	*"The application of the assess component into IDZ's context successfully produced the desired outcomes"*	PESTLE+ IdMPAM *i*SAM2	Comprehensiveness	This feedback indicates that the assess component is complete in its totality of meeting the desired goals.

5.3 BIE & RL Iteration II (ADIVRA Beta Version)

In the second iteration of BIE, the main objective was to build, intervene and evaluate the design component of the ADIVRA. Similar to the assess component, three design and review workshops were held to build, intervene and evaluate the alpha and beta versions of the design component artefacts (see Figure 5.5). The researcher presented the research problem, risks and gaps identified by the literature review. The presentation ran for 30 minutes. After the presentation, a brainstorming session was held to identify the alignment between the IDZ's needs and the research problem for this research project. Table 5.5 details the first design and review workshop with the workshop objectives, roles and responsibilities and feedback and comments from the participants.

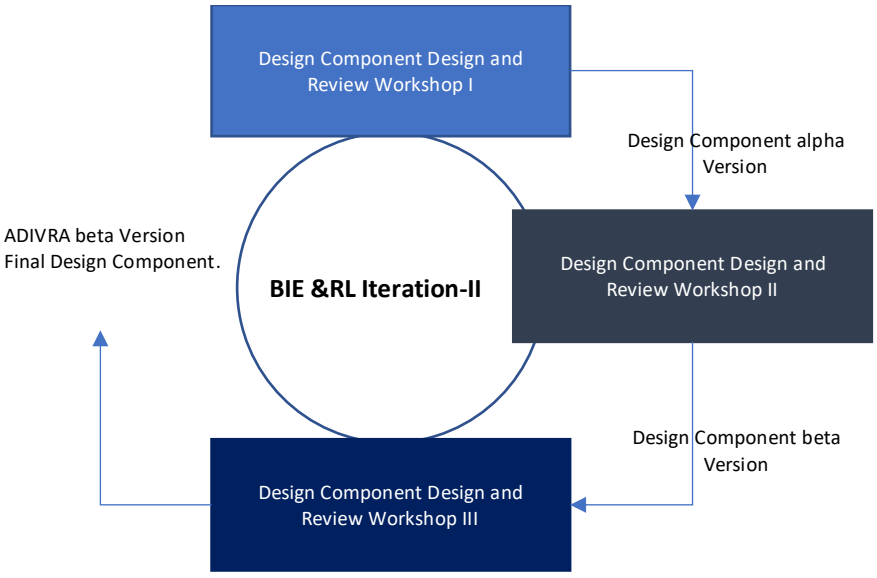


Figure 5.5. BIE & RL Iteration-II

Table 5.5 Design Component Design and Review Workshop I

Organization:	IDZ (coded name) is a leader in the eIDV (Electronic Identity Verification) industry with the capability to provide access to the widest, most in-depth, reliable, and independently sourced identity data throughout the APAC region.	
Workshop Objective	To make design decisions for the ADIVRA design component	
Workshop Facilitator	The researcher of this project is responsible for explaining the framework design, educating, and facilitating the framework design decisions, evaluation and documenting the feedback.	
Workshop Participants	• IT Manager • Digital Identity Architect • Business Analyst • Privacy Officer • Compliance Manager	
Main Design/Evaluation Component	**Design**	
Role/Responsibility	**Comment/Suggestion/Feedback**	**Interpretation**
Compliance Manager	*"The uncertainty around regulatory requirements and global information security standards are impeding the adoption of DigI verification solutions by end users. Therefore, the DigI verification solutions should be designed keeping regulations in mind".*	IDZ's future DigI verification solution should be more compliant with global regulations. This is aligned with RQ2.
Privacy Officer	*"The PII that constitutes the DigI needs to be secure. It will give IDZ's clients the confidence to use our DigI verification services without fears about privacy"*	IDZ's DigI verification solution should ensure the privacy of PII by giving control of PII to the identity owner. This is aligned with RQ2.
Business Analyst	*"How to optimise opportunities for IDZ to offer DigI verification with a unique point of difference through the use of biometrics and multi-factor authentication. A number of DigI verification providers offer various forms of biometric capabilities however many lack the data source availability that IDZ has. To maximise the potential of biometrics within the industry, by adding support for biometric authentication into IDZ's DigI verification solution, we can make it a secure and trustworthy solution for end users. This will also help us ensure compliance with regulatory requirements"*	For IDZ's future, the DigI verification solution should include support for biometrics. In addition, the DigI verification solutions should ensure privacy and regulatory compliance. This is aligned with RQ2.

Digital Identity Architect	*"We should look at incorporating blockchain technology into the DigI verification solution whereby IDZ clients can access previously verified individual's PII and documentation, whilst adhering to Know Your Customer, Anti-Money Laundering and other compliance regulations."*	For IDZ's future, the DigI verification solution should include support for biometrics. In addition, the DigI verification solutions should ensure privacy and regulatory compliance. This is aligned with RQ2.
IT manager	*"From a strategic business perspective, the implementation of regulatory compliant DigI verification solution employing blockchain as an underlying technology would position IDZ at the forefront of the industry, thereby enabling access to a wider range of data sources and suppliers as well as positioning as the preferred choice of DigI verification service provider. This will fulfill the decentralization needs in addition to providing a reusable digital identity to end users"*	IDZ's future DigI verification solution should be built on the decentralized model of identity verification. The DigI using this solution should be reusable. This is aligned with RQ2.

The design workshop concluded with the decision to build an ADIVRA design component which can fill the gaps identified in Chapter 2 in alignment with the industry partner's needs and interests (see Table 5.5). Hence, the alpha version of the design component includes RRM and DigIVPM, as shown in Figure 5.6a. The alpha versions of the design component artefacts (i.e., RRM and DigIVPM) are shown in Figures 5.6b and 5.6c.

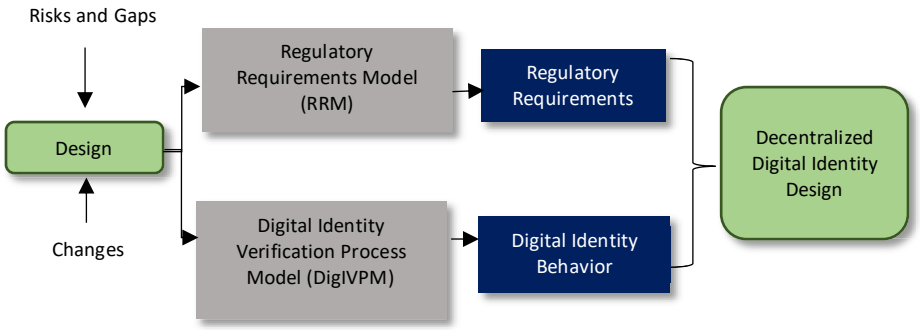


Figure 5.6a ADIVRA Design Component (alpha version)

The next step is to evaluate the alpha version through the design and review workshop. The alpha version was evaluated using the criteria detailed in Table 3.1. The demo and presentation of the alpha version ran for approximately 30 minutes. The workshop participants discussed the intervention results and guided the alpha version of the ADIVRA design component. Privacy and regulatory compliance were the focus of the ADIVRA design component. After the demo and presentation, an evaluation session was organized with the participants (duration approximately 30 minutes). The participants provided qualitative feedback about the design component from its usefulness, applicability and comprehensive perspectives as follows.

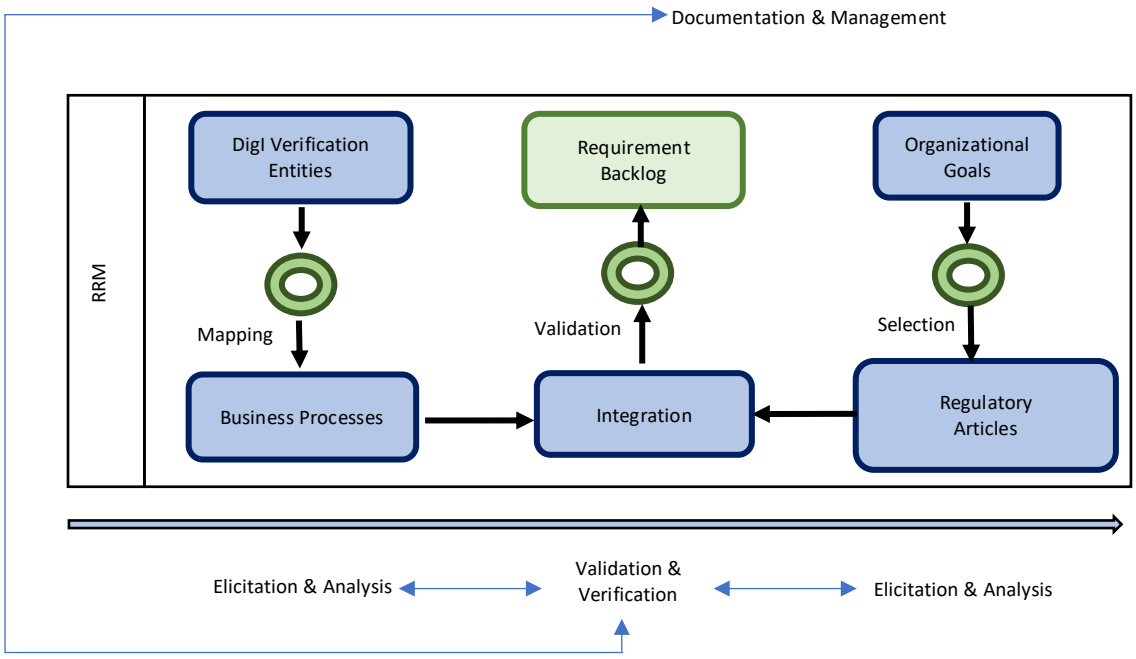


Figure 5.6b Regulatory Requirements Model (alpha version)

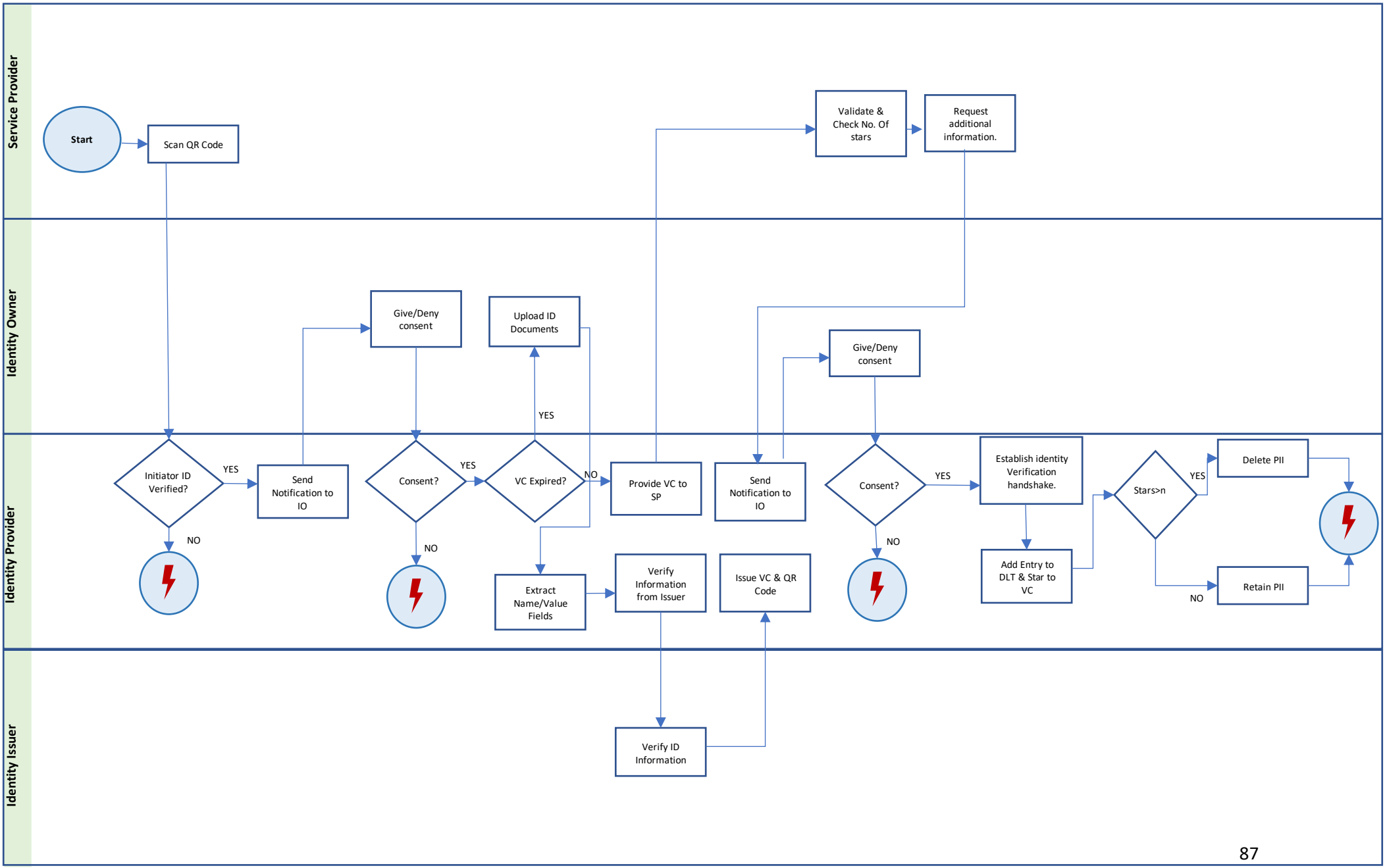


Figure 5.6c. Digital Identity Verification Process Model (alpha version)

Table 5.6 Design Component Design and Review Workshop II

Role/Responsibility	Comment/Feedback/Suggestions	Artefact	ADIVRA Category	Interpretation
IT Manager	*"DigIVPM provides a very useful and comprehensive reference architecture for decentralized and flexible DigI verification by providing support for various use cases in a wide range of environments. The process flow for the business to customer model will be useful"*		Usefulness	This feedback indicates that DigIVPM should include the process flow for the B2C model as well
Digital Identity Architect	*"The creation of VC is based on very typical documents i.e., passport, driver's license etc. However, I think the DigI structure should be such that it can support variable and personalized workflows without enduring expensive and time-consuming integrations and should include all facets of DigI"*		Comprehensiveness Applicability	This feedback indicates that the current structure of DigI might not cover all the facets of DigI. Hence, we may need to redefine the DigI structure
Compliance Manager	*"RRM is a very handy metric to extract relevant and applicable requirements from regulations. Also, DigIVPM provides a basis for a complete end-to-end decentralized verification. How will you ensure the security and privacy of the PII that will be temporarily stored in IdP's data stores"*		Usefulness Applicability	This feedback indicates the need to raise the privacy and security safeguards for PII comprising DigI. In addition, it mentions that RRM achieves its intended purpose i.e., extraction of regulatory requirements.
Business Analyst	*"The regulatory requirements-based DigIVPM is easy to understand and use. However, it works for the business-to-business model only. It will be great to add flow for the business-to-customer model as well"*		Comprehensiveness Usefulness	This feedback indicates that DigIVPM should include the process flow for B2C model as well
Privacy Officer	*"This architecture of DigI verification without storing PII is unique and useful from a privacy perspective"*		Applicability Usefulness	This feedback indicates that the ADIVRA design component is very useful because it provides the DigI verification architecture without storing PII.

To evaluate the RRM, the regulatory requirements for DigI were extracted from GDPR's and EU's electronic IDentification, Authentication and trust Services (eIDAS) regulation (European Union 2014) (See Appendix J). The extracted requirements were evaluated against Allen's principles of Self-Sovereign Identity. In addition, a scenario-based evaluation (Hevner et al. 2004) for RRM was conducted during the design and review workshop. The alpha version of RRM was found complete and fit for purpose. Hence, the alpha version of RRM was considered the final version. The alpha version of the DigIVPM was explained and demonstrated using a test case (see Appendix J). The overall interpretation of the evaluation was that all the participants believed that RRM is useful, comprehensive, and applicable. However, questions were raised on the comprehensiveness and applicability of DigIVPM. The alpha version of DigIVPM is designed for the B2B model only. It was suggested that DigIVPM should also include a workflow for the business-to-customer model. Hence, the newly emerged design of DigIVPM includes support for the business-to-customer model as well (see Figure 4.11).

An important conclusion from the participants' feedback was that the DigI is not a singular concept as it comes in different formats subject to different jurisdictions, regulations, and laws including the challenges of interoperability and compliance. Hence, a new artefact was added to the beta version of the design component i.e., CDigI (see Table 4.4). It was debated during the workshop that to fulfill the privacy and security obligations imposed by regulations and to safeguard the multi-faceted CDigI, something more than encryption was needed. Therefore, a fourth component

was added to the beta version of the design component which is information *i*SEA (see Figure 4.9). The beta version is the final version of the design component (see Figure 4.7). The details of final design component are in section 4.4.

Table 5.7 Design Component Design and Review Workshop III

Role/Responsibility	Comment/Feedback/Suggestions	Artefact	ADIVRA Category	Interpretation
Privacy Officer	*"A DigI verification solution based on the ADIVRA design can offer a verification process that is fast and simple. The OCR feature can pull the details from the ID and store them in the secure container. This gives our clients confidence in our services and for us, peace of mind in relation to the compliance perspective. The iSEA is a very good model to secure sensitive information that comprises DigI. The iSEA can be applied to other contexts as well as a standalone secure container."*	iSEA DigIVPM	Applicability Comprehensiveness	This feedback indicates that ADIVRA is applicable for DigI verification and can be applied to different contexts
Business Analyst	*"The architecture is easy and simple which end users need so they don't get confused or frustrated."*	CDigI RRM iSEA DigIVPM	Usefulness	This feedback indicates that ADIVRA is fit for purpose
Compliance Manager	*"Identity owner's control over their own information and DigI verification without storing PII are the two main strengths of this architecture. This takes a lot of compliance burden off our shoulders"*	DigIVPM	Comprehensiveness Usefulness	This feedback indicates that ADIVRA is useful and comprehensive for addressing compliance requirements and giving control to IO
Digital Identity Architect	*"The decentralized nature of CDigI allows the exchange of trustworthy documents regardless of the jurisdiction or context"*	CDigI	Applicability Usefulness	This feedback indicates that ADIVRA is useful and applicable to multiple jurisdictions
Compliance Manager	*"The regulatory requirements for DDigI solutions are mentioned in regulations but there is no definition of a structured approach to effectively extract and validate the requirements. RRM presented in this research provides a novel approach for integrating business processes to regulatory articles for regulatory compliant-DDigI."*	RRM	Applicability Usefulness	This feedback indicates that ADIVRA is useful and applicable in context of DDigI.
Compliance Manager	*"DigIVPM considerably reduces the manual review time and fraud risk. Every time the DigI information is accessed, the identity owner is notified which creates transparency and trust"*	DigIVPM	Applicability Usefulness	This feedback indicates that ADIVRA is a useful architecture
Digital Identity Architect	*"The validity threshold and star-based system are very good ways of keeping the DigI information up to date along with building a web of trust among verifiers"*	DigIVPM	Applicability Usefulness	This feedback indicates that ADIVRA is privacy aware DigI verification architecture
Digital Identity Architect	*"The VC enables the reusability and interoperability of DigI without repeating the tedious process of scanning and uploading the ID documents and verifying them"*	DigIVPM	Comprehensiveness Usefulness	This feedback indicates that ADIVRA is an efficient architecture in terms of reducing time and effort required for DigI verification
IT Manager	*"Every time the DigI is accessed, a log entry is maintained in DLT. This is a very good way of transaction monitoring and fulfilling our legal obligation of record keeping without including any form of PII into it"*	DigIVPM	Usefulness	This feedback indicates that logging and monitoring is a strong feature in ADIVRA design.
IT Manager	*"iSEA privacy and security is paramount"*	iSEA	Applicability usefulness	This feedback indicates that iSEA is fit for purpose and seems useful for providing a secure container for PII comprising DigI.
Business Analyst	*"Based on ADIVRA, identity ecosystems can be built that let identity owners and service*	CDigI RRM iSEA	Applicability Usefulness Comprehensiveness	This feedback indicates that overall, the framework is fit for purpose and seems to

	providers share DigI in a simple, secure and privacy-preserving way."	DigIVPM		provide an adequate foundation for privacy aware and regulatory compliant DigI verification solutions.

The beta version of the design component artefacts was intervened (see Appendix J) into IDZ to evaluate them against the criteria specified in Table 3.1. The demo and presentation of the beta version ran for approximately 30 minutes. After the demo, the design component was analyzed by applying it to IDZ's context. This lasted for 90 minutes. The CDigI was evaluated using a test case. The *i*SEA was evaluated by creating a sequence of DigI verification scenarios. The DigIVPM was evaluated using IdMPAM from the assess component. The CDigI, iSEA and DigIVPM were also analyzed against the regulatory requirements extracted using RRM. To check the generalization of DigIVPM, RRM was used to extract the regulatory requirements other than GDPR (i.e., eIDAS). After the demo and presentation, an evaluation session was organized with the participants (duration approximately 30 minutes). Table 5.7 details the feedback and comments of the participants from the third design and review workshop for the design component. It was found that the ADIVRA design component successfully achieved the desired outcome and needed no further changes. Hence, this is considered the final version of the design component. The addition of the design component resulted in a beta version of the ADIVRA framework (see Figure 5.7).

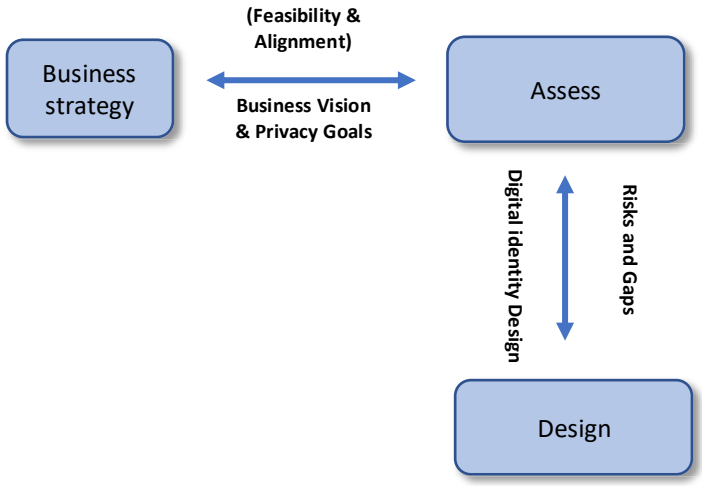


Figure 5.7. ADIVRA beta version- High Level Contextual Diagram

5.4 BIE & RL Iteration III (ADIVRA Gamma Version)

The last BIE cycle was conducted to build the evolve component. Three design and review workshops were held to design, review, and re-design the alpha and beta versions of the evolve component artefacts (see Figure 5.8). Adaptability was one of IDZ's initial design goals. The researchers presented the research problem and gaps identified by the literature review. The presentation ran for 30 minutes. After the presentation, a brainstorming session was organized to identify the alignment between the IDZ's needs and research problem for this research project. Table 5.8 details the first design workshop together with the workshop objectives, roles and responsibilities and feedback and comments from the participants.

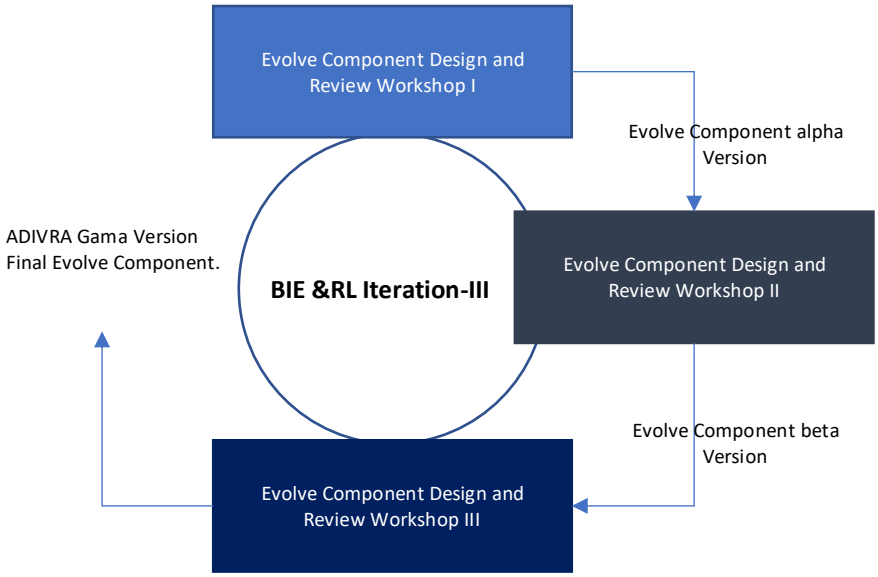


Figure 5.8. BIE & RL Iteration-III

Table 5.8 Evolve Component Design and Review Workshop I

Organization:	IDZ (coded name) is a leader in the eIDV (Electronic Identity Verification) industry with the capability to provide access to the widest, most in-depth, reliable, and independently sourced identity data throughout the APAC region.	
Workshop Objective	To make design decisions for the ADIVRA evolve component	
Workshop Facilitator	The researcher of this project is responsible for explaining the framework design, educating, and facilitating the framework design decisions, evaluation and documenting the feedback	
Workshop Participants	• IT Manager • Digital Identity Architect • Business Analyst • Privacy Officer • Compliance Manager	
Main Design/Evaluation Component	**Evolve**	
Role/Responsibility	**Comment/Suggestion/Feedback**	**Interpretation**
Compliance Manager	*"DigI verification process includes the processing of PII. It is very important to maintain compliance with every changing regulatory requirement. It is very important to match the pace of regulatory requirements."*	This comment indicates that DigI verification solutions should be able to detect and contain changes in regulatory requirements. This aligns with RQ3.

Privacy Officer	*"With a faster pace of innovation and rapidly evolving privacy threats, risks and vulnerabilities that impact the protection of DigI information, change is required continuously for the compliance operating model, privacy capabilities and technology"*	This comment indicates that DigI verification solutions should be able to detect and adjust as per changing privacy risks. This aligns with RQ3
Business Analyst	*"Staying competitive in the DigI verification business, poses a continual need for DigI solutions to adapt to change"*	This comment indicates that with new competitors entering the market, business needs are likely to change continuously. Hence, the architecture of DigI verification solutions should be able to adapt to changing business needs. This aligns with RQ3
Digital Identity Architect	*"Increasing digital transformation is changing the methods of DigI verification. New technologies are introduced and hence new methods. DigI verification solutions should be able to identify the changing trends in the DigI verification space and adapt to these changes as early as possible"*	This comment indicates the DigI verification solutions should adapt to changing technological advancements. This aligns with RQ3
IT Manager	*"The borders between organizations and governments will become more and more blurry as individuals adopt multiple roles in different contexts. DigI verification solutions need to evolve."*	This comment indicates that DigI verification solutions should be adaptive. This aligns with RQ3

The participants' feedback indicated that there are three main change verticals that may require the ADIVRA design to adjust i.e., business strategy, regulatory requirements, and emerging privacy risks. Hence, the ADIVRA evolve component was built to identify the change and adjust the design in light of these changes. Identifying the change requires the analysis of the environment in which DigI verification operates. Hence, the ADIVRA evolve component has one artefact i.e., DigIVAM. The participants suggested that the PESTLE+ model is re-used from the assess component to identify the risks and gaps in design. The risks and gaps are then analyzed by the stakeholders to create a change requirement backlog. This may help stakeholders to understand how to adjust the design component to fulfill the identified gaps and mitigate the risks. The change requirements are again analyzed using the PESTLE+ model to ensure they are aligned with the business and privacy goals. The alpha version of DigIVAM model is shown in Figure 5.9.

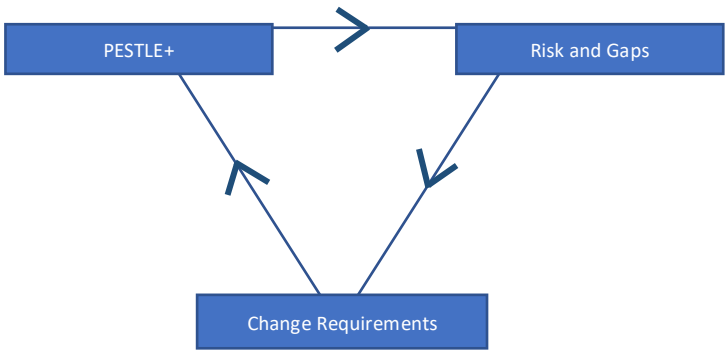


Figure 5.9. Digital Identity Verification Adaption Model (alpha Version)

The next step is to evaluate the alpha version of DigIVAM through the design and review workshop. The alpha version was evaluated using the criteria detailed in Table 3.1. The demo and

presentation of the alpha version ran for approximately 30 minutes. The workshop participants discussed the intervention results (see Appendix J) and guided the alpha version of the ADIVRA evolve component. After the demo and presentation, an evaluation session was organized with the participants (duration approximately 30 minutes). The participants provided qualitative feedback about the evolve component from its usefulness, applicability and comprehensiveness perspectives as detailed in Table 5.9.

Table 5.9 Evolve Component Design and Review Workshop II

Role/Responsibility	Comment/Feedback/Suggestions	Artefact	ADIVRA Category	Interpretation
Business Analyst Privacy Officer IT Manager	*"Identifying the change requirements requires a lot of effort and time."*	DigIVAM	Usefulness Applicability	This feedback indicates that identifying and addressing changes using DigIVAM is a time-consuming process.
Compliance Manager	*"There is no boundary between the identification of change requirements and analysis of change requirements. What marks the transition from one level to the next? The existing version of DigIVAM is not applicable in many situations and may not be able to cover all important facets"*	DigIVAM	Usefulness Applicability	This feedback indicates that there should be a more structured and well-defined process for change adaption.
Digital Identity Architect	*"A more structured approach will save a lot of time and effort, if for instance, we can classify the change i.e., if it's a regulatory requirement change or a privacy risk-related change or a change in business needs. In this way, only the SMEs and people with relevant skills and knowledge will work on the change for better adjustment. It will save time for all the other people who can invest their time during the implementation plan"*	DigIVAM	Usefulness Applicability Comprehensiveness	This feedback indicates that in order to effectively utilize the knowledge and skills of all the resources, it is important to divide the DigIVAM into stages.

IDZ is currently ISO 27001 compliant, but the IDZ management wants to enhance their privacy safeguards by implementing ISO 27701. The privacy and compliance manager suggested that DigIVAM should be tested to detect the changing requirements between ISO 27001 and ISO 27701. To address this change, the DigIVAM was implemented in the practical setting of IDZ in a series of workshops. At the end of the workshop, it was concluded that although the PESTLE+ model successfully identified the changes, it was a time-consuming process that required going back and forth between the two standard documentations and identify the changes. Three workshop sessions were dedicated to identifying the risks and gaps only. Next, two workshops were conducted to elicit the change requirements from the risks and gaps. The workshop participants collectively suggested that it was not feasible to spend too much time at one stage before moving to the other. A more structured and planned approach with a defined set of activities towards adapting the change, was needed. Hence, the set of activities to be performed at each stage of DigIVAM was defined and added (see Figure 4.13). The beta version of DigIVAM was again applied to identify and predict the changes between the requirements of ISO 27001 and ISO 27701. Appendix J shows the details of this intervention. It was concluded that DigIVAM is fit for purpose and useful for adapting changes in regulation, business needs and privacy risks.

Table 5.10 Evolve Component Design and Review Workshop III

Role/Responsibility	Comment/Feedback/Suggestions	Artefact	ADIVRA Category	Interpretation
Digital Identity Architect	*"DigIVAM is a useful tool to identify and understand the need and impact of change in the DigI operating environment"*	DigIVAM	Usefulness	DigIVAM is a useful for adapting change.
Compliance Manager	*"This model is not limited to regulatory, privacy risk or business-related change. Following the steps of DigIVAM, change in any area can be identified and addressed"*	DigIVAM	Comprehensiveness	DigIVAM is comprehensive.
Privacy Officer	*"The stepwise approach adopted in DigIVAM can help in reducing the disruptive aspects and risks associated with change in the end-to-end identity ecosystem"*	DigIVAM	Usefulness Applicability Comprehensiveness	DigIVAM is useful for managing change. It is not specific to only one aspect of identity ecosystem
IT Manager	*"The change backlog created while following the steps of DigIVAM creates an opportunity towards the development and documentation of best practices that can be useful for others"*	DigIVAM	Usefulness	DigIVAM is comprehensive proves that not only addresses change but development of best practices in DigI verification domain
Business Analyst	*"The ADIVRA evolve component helps in assessing the impact of change before it is actually implemented. This creates a blueprint of what new solutions might look like and what other units might get impacted"*	DigIVAM	Comprehensiveness Applicability	DigIVAM is helpful in addressing change as well as anticipating change-related impacts.
Digital Identity Architect	*"The probability of unsuccessful change might be reduced by following the steps of DigIVAM"*	DigIVAM	Applicability Usefulness	DigIVAM is helpful in identifying which change to implement and which not to.

The finalization of DigIVAM completed the gamma version of ADIVRA. The gamma version is

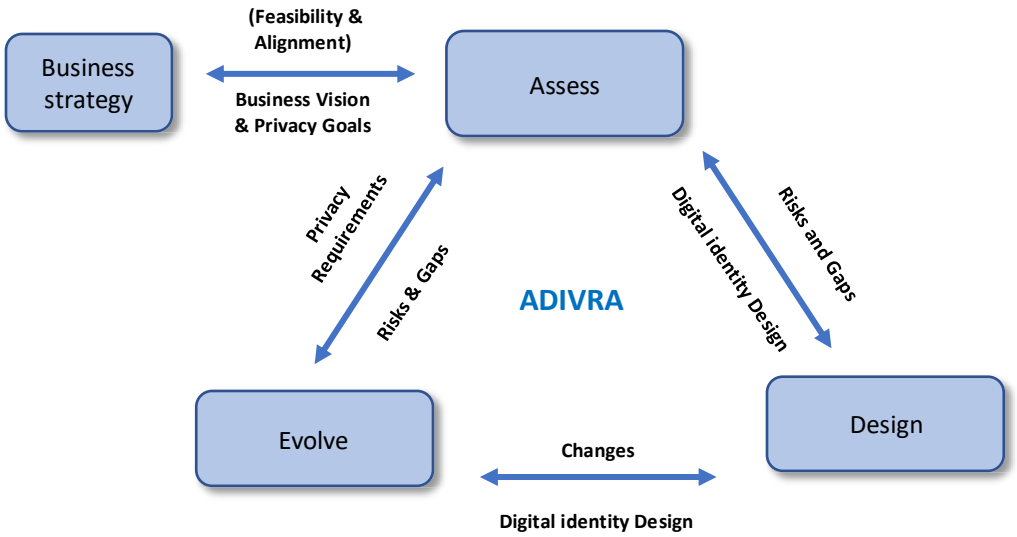


Figure 5.10. ADIVRA gamma version- High Level Contextual Diagram

the final version of ADIVRA (see Figure 5.10). The next step is the evaluation of ADIVRA through the industry field survey.

5.5 Industry Field Survey

After completing the gamma version, ADIVRA was evaluated through an industry field survey. The evaluation of ADIVRA was based on the needs identified by the organization's context. ADIVRA was evaluated in terms of generalization, applicability, novelty, comprehensiveness, usefulness, and other relevant quality attributes (see Table 3.1). The industry field survey is the final evaluation conducted in this research. The survey is a collection of specified information offered to specialized and specific populations (Runeson & Höst 2009b; Sjøberg et al. 2005). The survey was provided online to a group of local and global experts in DigI verification industry. It was constructed using a common survey design procedure as follows (Hyndman 2008).

a) Survey Planning

The aim was to obtain experts' feedback and opinions about the ADIVRA final version (gamma version). The survey plan was to obtain qualitative and quantitative data from the participants. The survey data analysis supports the view that the ADIVRA meets the evaluation criteria (see Table 3.1).

b) Design the Sampling Procedure

The survey (Link) was provided to participants and experts in the DigI verification industry who specialize in the field of DigI, privacy and security, regulatory compliance, and blockchain. The participants came from a group of companies located in Australia, the US, UK, India, and Pakistan. The participants were initially contacted via LinkedIn using the formal invitation letter approved by the UTS ethics approval **UTS HREC REF NO. ETH-182772** (see Appendix A, Appendix B and Appendix C). The informed consent sheet referred to the motivation and scope of this research, reasons for the selected individuals to participate in the survey, and the risks, privacy considerations, advantages, and rights of participants. In accordance with the ethics approval outlined in Appendix A, no personal information was collected about the participants. The survey was given to the participants after they replied to the survey invitation letter (see Appendix C) and consented to participate in the survey and receive the survey form (see Appendix B). The original survey data were stored on CloudStor (see Appendix E). The participants' information is given in Table 5.11, including information on their area of expertise and years of experience in a related field. The minimum experience in the industry was three years. The participants' years of experience, as shown in Table 5.11, ranged from 3 to 23 years, indicating. that the participants may provide abundant feedback and comments based on their years of experience and their expertise in DigI verification.

Table 5.11 Industry Field Survey Participants

Participant	Area of Expertise	Experience
1	Risk and Compliance	5 years
2	Information Security and Audit	6.5 years
3	Digital Trust and Compliance	20 years
4	Revenue	12 years
5	Digital Identity Architect	22 years
6	Operational Technology Assurance and Risk Management.	17 years
7	Decentralized & Trustworthy AI for IoT	9 years
8	Technology Analyst	19 years
9	IT Security Research Services	17 years
10	Biometrics and Digital Identity	23 years
11	Director Identity and Access Management	19 years
12	Identity and Access Management Architect/Security Architect	7 years
13	Identity Support Specialist	9 years
14	Blockchain based digital wallet	22 years
15	Cyber Security and Digital Trust	9 years
16	Digital Identity	5 years
17	Digital Identity	4 years
18	Authenticated trusted digital security, identity and communications.	20 years
19	Digital Identity Innovation	7 years
20	Blockchain	11 years
21	Digital Identity	21 years
22	Compliance	13 years
23	Privacy, Security and Compliance	6 years
24	GDPR	3 years
25	Digital Identity, Open Banking, Digital Architecture	8 years
26	Identity and Security	9 years
27	Digital Identity and API security	7 years
28	Law and Regulations	19 years
29	Cybersecurity	7 years
30	Risk Management	5years

c) Survey Method Selection

The ADIVRA framework was evaluated using a field survey (Link) (see Appendix D) that was provided to experts from DigI industry. The participants were contacted via LinkedIn (see Table 5.11). The survey was opened in August 2020 and closed in December 2020. A total of 30 participants completed the survey online.

d) Questionnaire Development

The survey comprised nine questionnaire sets (see Appendix D):
Q1 set: ADIVRA assess component questionnaire set (5 questions)
Q2 set: ADIVRA design component questionnaire set (7 questions)
Q3 set: ADIVRA evolve component questionnaire set (6 questions)
Q4 set: ADIVRA overall evaluation (9 questions)
Q5 set: ADIVRA feedback (1 question)
Q6 set: ADIVRA useful aspects (1 question)
Q7 set: ADIVRA suggested improvement (1 question)
Q8 set: ADIVRA overall comments and ratings (2 questions).

e) Collection and Analysis of Data

The survey questionnaire sets generated two types of data:

- Quantitative data: rating data or categorical data transformed into ordinal data (participants' ratings in sets Q1, Q2, Q3, Q4, Q8)
- Qualitative data (participants' feedback in sets Q5, Q6, Q7, Q8)

The survey evaluation comprised two main steps:

- Survey data collection
- Survey data analysis.

5.5.1 Survey Data Collection

The survey collection process presents the procedure used in the data collection. The collected data from the survey can be categorized into two types: quantitative and qualitative.

The quantitative data sources are the ratings collected from the survey questionnaire sets Q1, Q2, Q3, Q4, and Q8 (see Appendix D).

The qualitative data sources are the feedback collected from the survey questionnaire sets Q5, Q6, Q7, and Q8 (see Appendix D).
The collected data were organized into groups according to the questionnaire related to the survey evaluation criteria (see Table 3.2). The questionnaire was organized as follows.

a) ADIVRA Individual Components Questionnaire Group Set (Q1 to Q3)

The ADIVRA survey questionnaires (sets Q1–Q3) are organized into Tables 5.12 to 5.15. The questions in these sets offer the survey participants the option to evaluate ADIVRA components against the criteria in Table 3.1. The questionnaires are grouped as follows:

Table 5.12: ADIVRA Assess Component Questions Group

Question	Description	Category
Q1	Is the assess [PESTLE+] component able to assess the risks and gaps in other similar DigI verification contexts?	Generalization
Q2	Can the assess [IdMPAM] component be used to assess the GDPR privacy compliance of blockchain-based DigI solutions?	Applicability
Q3	Can the assess [iSAM2] component be used to assess the maturity level of information security internal audit?	Applicability
Q4	Does the assess component produce new knowledge in the context of the DigI ecosystem?	Novelty
Q5	Are the assess component artefacts [PESTLE+, IdMPAM, iSAM2] sufficient for the context?	Comprehensiveness

Table 5.13: ADIVRA Design Component Questions Group

Question	Description	Category
Q1	Is the design component able to design the DigI architecture in other DigI verification contexts?	Generalization
Q2	Does the digital identity structure [CDigI] defined in the design component cover all possible identity attributes?	Applicability
Q3	Can the secure digital identity container [iSEA] be used to safeguard the digital identity information?	Applicability
Q4	Does the BC-based DigI identity verification process model [DigIVPM] include all steps necessary to conduct electronic identity verification?	Applicability
Q5	Can the design component effectively elicit regulatory requirements for DigI?	Applicability
Q6	Does the design component produce new knowledge for designing a secure DigI ecosystem?	Novelty
Q7	Are the design component artefacts [CDigI, iSEA, DigIVPM, RRM] sufficient for conducting secure electronic identity verification?	Comprehensiveness

Table 5.14: ADIVRA Evolve Component Questions Group

Question	Description	Category
Q1	Is the evolve component able to adapt to changes in other similar DigI contexts?	Generalization
Q2	Is the evolve component able to adapt to changes in business strategy?	Applicability
Q3	Is the evolve component able to adapt to changes in the regulatory landscape?	Applicability
Q4	Is the evolve component able to adapt to changes in changing privacy risks?	Applicability
Q5	Does the evolve component produce new knowledge for adapting to changes in the DigI ecosystem?	Novelty
Q6	Are the evolve component artefacts (PESTLE+, DigIVAM) able for elicit change requirements in the context of the DigI ecosystem?	Comprehensiveness

b) ADIVRA Overall Questionnaire Group Set (Q4 to Q8)

The ADIVRA survey questionnaires (sets Q4–Q8) are organized into one group. The questions in these sets offer the survey participants the option to evaluate the overall ADIVRA framework against the criteria in Table 3.1. The qualitative data collected from these questionnaire sets were analyzed to determine the relationship between the participants' quotes and comments and the ADIVRA components represented by the evaluation criteria in Table 3.1. This process aimed to make sense of the qualitative data and correlate the participants' feedback with the framework. The qualitative data collected from sets Q4–Q8 provide overall ratings that aim to determine the usefulness and applicability of the ADIVRA based on the participants' ratings.

Table 5.15: Overall ADIVRA Framework Questions Group

Question	Description	Category
Q1	Is the architecture of the framework (ADIVRA) suitable for other similar DigI contexts?	Generalization
Q2	Does the framework (ADIVRA) address the issue of privacy in the DigI ecosystem?	Applicability
Q3	Does the framework (ADIVRA) address the issue of GDPR compliance in the DigI ecosystem?	Applicability
Q4	Does the framework (ADIVRA) address the issue of adaptability to the changing risks and regulations in the DigI ecosystem?	Applicability
Q5	Does the architecture of the framework (ADIVRA) produce new knowledge in the context of the DigI ecosystem?	Novelty
Q6	Does the architecture of the framework (ADIVRA) provide sufficient coverage for all necessary elements of a DigI ecosystem? If not please make suggestions for improvements below in number 7.	Comprehensiveness
Q7	Is ADIVRA useful for identity architects?	Usefulness
Q8	Is ADIVRA useful for regulators?	Usefulness
Q9	Is ADIVRA useful for researchers?	Usefulness

5.5.2 Survey Data Analysis

The survey evaluation process comprises two phases:

- Survey quantitative evaluation: The participants' ratings were transformed from categorical data to ordinal data (numerical) using the survey ratings in Table 3.3. The ordinal data were used in statistical formulas to evaluate the survey results (see Equations 3.1 to 3.3).

- Survey qualitative evaluation: The participants' feedback was analyzed using the hypothesis confirmation general technique of analysis (Runeson & Höst 2009b). The hypotheses are the artefact evaluation criteria (Carvalho 2012) (see Table 3.1). The participants' feedback was cross-examined against the evaluation criteria by highlighting and interpreting the occurrences of these criteria in the text. The industry feedback is organised in tables (see table 5.24 to table 5.28)

5.5.2.1 Survey Quantitative Evaluation

The quantitative evaluation process comprises two sections:

1. Individual ADIVRA components evaluation based on the data collected from sets Q1–Q3.

2. Overall ADIVRA framework evaluation based on the responses from participants collected in set Q4.

a) Individual ADIVRA Component Evaluation

The individual ADIVRA components evaluation has six steps (based on sets Q1–Q3). The survey data are located on CloudStor (Link). The individual evaluation process is as follows:

- Gather and map the survey rating into tables named **SR[X]**.
- Group the ordinal data from the rating tables into category rating tables named **CR[X]** on the basis of questions in the questionnaire.
- Plot the **SR [X]** tables into a bar graph representation of the data labelled **BG[X]**.
- Calculate the SAAP and SAAF statistical values for all **SR[X]** tables and calculate goodness-of-fit Chi^2 for all **CR[X]** (see Equation 3.1-3.3). The aim is to determine whether the ADIVRA components meet the evaluation criteria positively (see Table 3.1):
    - SAAF determines the frequency of participants somewhat agreeing or strongly agreeing that the ADIVRA components meet the evaluation criteria positively.
    - SAAP determines the percentage of participants somewhat agreeing or strongly agreeing that the ADIVRA components meet the evaluation criteria positively.
    - Goodness-of-fit Chi2, and p-value for each of the **CT[Index]** tables.

    H0 (null hypothesis)*: The ADIVRA components and the evaluation criteria are not associated*.
    H1 (alternative hypothesis)*: There is positive association between ADIVRA components and the evaluation criteria.*
    If p-value < α, then H0 is rejected and H1 is accepted, and the ADIVRA components meet the evaluation criteria positively (Generalization, Applicability, Novelty, Comprehensiveness, Usefulness).
    [If p-value < 0.000^{β} (β is a small number), then p is mathematically adjusted to p < 0.001].

i) Assess Component

Table 5.16: Assess Component Survey Rating SR1

	Q1	Q2	Q3	Q4	Q5	Rows Total	Percentage %
Strongly Agree	17	16	14	17	16	80	53.33%
Agree	6	8	11	7	9	41	27.33%
Somewhat Agree	3	4	3	6	3	19	12.66%
Disagree	0	0	1	0	0	1	0.66%
Strongly Disagree	1	0	0	0	1	2	1.33%
Not Sure/Not Applicable	3	2	1	0	1	7	4.66%
Column Total	30	30	30	30	30	150	100.00%

SAAF = 140
SAAP = 93.33%

Table 5.17: Assess Component Category Rating CR1

Evaluation Criteria								
	Generalization		Applicability (Q2, Q3)		Novelty		Comprehensiveness	
N=6 E= Σ O/N	**O**	**E**	**O**	**E**	**O**	**E**	**O**	**E**
Strongly Agree	**17**	**5**	**30**	**10**	**17**	**5**	**16**	**5**
Agree	**6**	**5**	**19**	**10**	**7**	**5**	**9**	**5**
Somewhat Agree	**3**	**5**	**7**	**10**	**6**	**5**	**3**	**5**
Disagree	**0**	**5**	**1**	**10**	**0**	**5**	**0**	**5**
Strongly Disagree	**1**	**5**	**0**	**10**	**0**	**5**	**1**	**5**
Not Sure/Not Applicable	**3**	**5**	**3**	**10**	**0**	**5**	**1**	**5**
H0 is rejected for p < 0.01	**Chi^2= 38.8**	**P<0.00001**	**Chi^2= 72.0**	**P<0.00001**	**Chi^2= 44.8**	**P<0.00001**	**Chi^2= 39.6**	**P<0.00001**

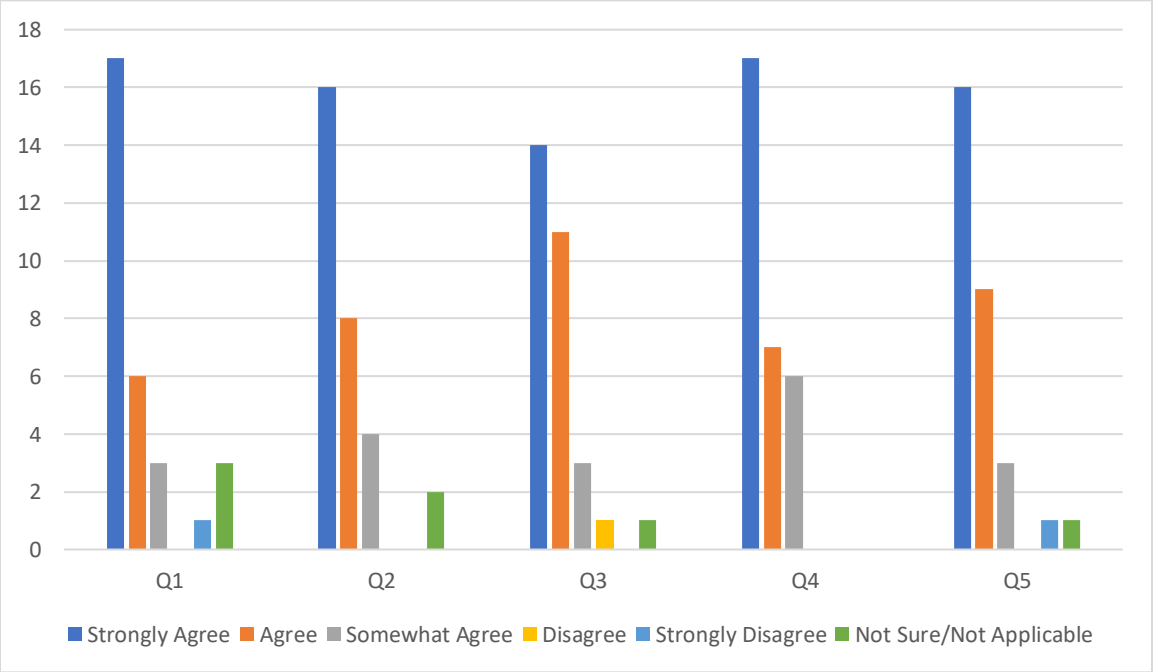


Figure 5.11. Assess Component Data Graph (BG1)

Analysis

The ordinal data in Table 5.16 (SR1) and Table 5.17 (CR1) yielded important statistical values based on the responses. The assess component evaluation results can be translated as below:
SAAF = 140 out of 150 response indicates (table 5.16) that most of the participants agree that the assess component meets the evaluation criteria positively.

SAAP = 93.33% suggests that a large percentage of participants agree that the assess component meets the evaluation criteria positively.

The p-value for the test variables:

- Generalization p-value is set at 0.00001 < α=0.01. This indicated that H_0 is rejected, H_1 is accepted, and there is a statistically significant relationship between the ADIVRA assess component and the generalization evaluation criteria.
- Applicability p-value is set at 0.00001 < α=0.01. This indicates that H_0 is rejected, H_1 is accepted, and there is a statistically significant relationship between the ADIVRA assess component and the applicability evaluation criteria.
- Novelty p-value is set at 0.00001 < α=0.01. This indicates that H_0 is rejected, H_1 is accepted, and there is a statistically significant relationship between the ADIVRA assess component and the novelty evaluation criteria.
- Comprehensiveness p-value is set at 0.00001 < α=0.01. This indicates that H_0 is rejected, H_1 is accepted, and there is a statistically significant relationship between the ADIVRA assess component and the comprehensiveness evaluation criteria.

The statistical values indicate that the participants consider that the ADIVRA assess component is appropriate and a vital design as well as it addresses the practical needs. Figure 5.11 shows the frequency of the participants' responses to add more graphic details to the results.

ii) Design Component

Table 5.18: Design Component Survey Rating SR2

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Rows Total	Percentage %
Strongly Agree	19	18	19	22	21	20	17	136	64.76%
Agree	7	8	8	5	4	5	9	46	21.90%
Somewhat Agree	3	4	1	3	4	5	4	24	11.42%
Disagree	0	0	0	0	0	0	0	0	0%
Strongly Disagree	0	0	1	0	1	0	0	2	0.95%
Not Sure/Not Applicable	1	0	1	0	0	0	0	2	0.95%
Column Total	30	30	30	30	30	30	30	210	100.00%

SAAF = 206
SAAP = 98.09%

Table 5.19: Design Component Category Rating CR2

Evaluation Criteria								
	Generalization Q1		Applicability (Q2, Q3, Q4, Q5)		Novelty Q6		Comprehensiveness Q7	
N=6 E= Σ O/N	O	E	O	E	O	E	O	E
Strongly Agree	19	5	80	20	20	5	17	5
Agree	7	5	25	20	5	5	9	5

Somewhat Agree	**3**	**5**	**12**	**20**	**5**	**5**	**4**	**5**
Disagree	**0**	**5**	**0**	**20**	**0**	**5**	**0**	**5**
Strongly Disagree	**0**	**5**	**2**	**20**	**0**	**5**	**0**	**5**
Not Sure/Not Applicable	**1**	**5**	**1**	**20**	**0**	**5**	**0**	**5**
H0 is rejected for p < 0.01	**Chi^2=54**	**P<0.0001**	**Chi^2= 238.7**	**P<0.0001**	**Chi^2=60**	**P<0.0001**	**Chi^2=4 7.2**	**P<0.0001**

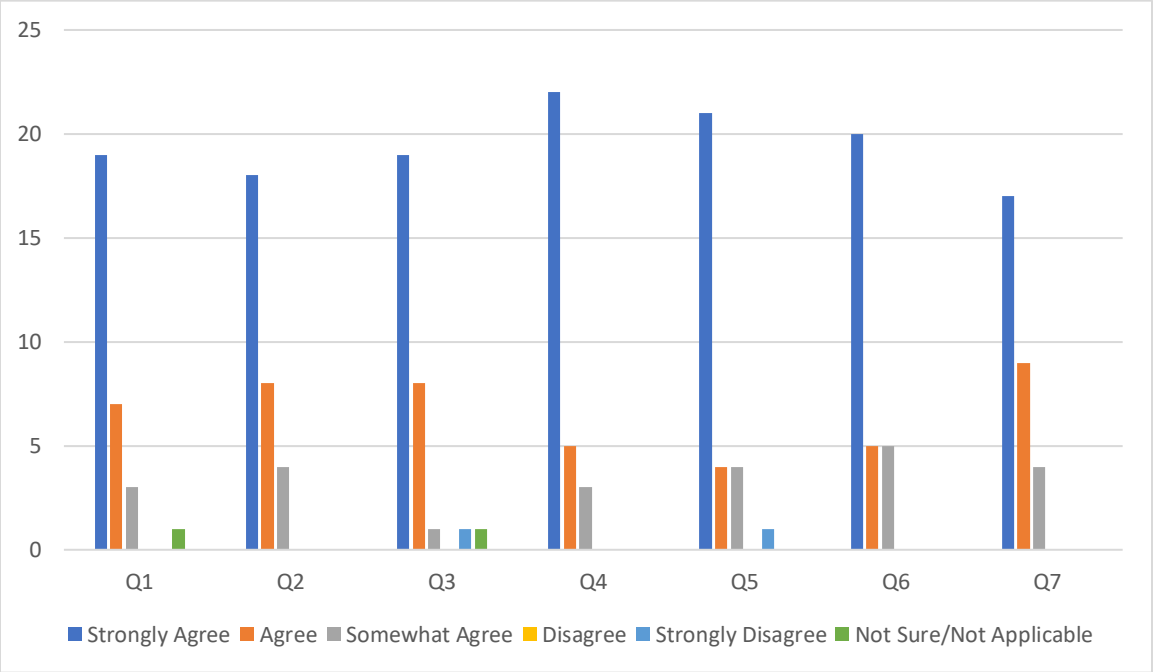


Figure 5.12. Design Component Data Graph (BG2)

Analysis

The ordinal data in Table 5.18 (SR2) and Table 5.19 (CR2) produced basic statistical values based on the responses. The design component evaluation results can be translated as below:
SAAF = 204 out of 210 responses suggest that a large proportion of participants agree that the design component fulfills the evaluation criteria positively.

SAAP = 98.09% indicates that a large proportion of participants agree that the design component fulfills the evaluation criteria positively.

The p-value for the test variables:

- Generalization p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA design component and the generalization evaluation criteria.
- Applicability p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA design component and the applicability evaluation criteria.

- Novelty p-value is set at 0.0001 < α=0.01. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA design component and the novelty evaluation criteria.
- Comprehensiveness p-value is set at 0.0001 < α=0.01. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA design component and the comprehensiveness evaluation criteria.

The statistical values indicate that the participants consider that the ADIVRA design component is appropriate and a vital design as well as it addresses the practical needs. Figure 5.12 shows the frequency of the participants' responses to add more graphic details to the results.

iii) Evolve Component

Table 5.20: Evolve Component Survey Rating SR3

	Q1	Q2	Q3	Q4	Q5	Q6	Rows Total	Percentage %
Strongly Agree	19	20	20	18	12	14	103	57.22%
Agree	4	4	6	5	11	10	40	22.22%
Somewhat Agree	5	5	4	5	3	3	25	13.88%
Disagree	2	0	0	0	1	1	4	2.22%
Strongly Disagree	0	0	0	1	2	2	5	2.77%
Not Sure/Not Applicable	0	1	0	1	1	0	3	1.66%
Column Total	30	30	30	30	30	30	180	100.00%

SAAF = 168
SAAP = 93.33%

Table 5.21: Evolve Component Category Rating CR3

	Evaluation Criteria							
	Generalization Q1		Applicability (Q2, Q3, Q4)		Novelty Q5		Comprehensiveness Q6	
N=6 E= Σ O/N	O	E	O	E	O	E	O	E
Strongly Agree	19	5	58	15	12	5	14	5
Agree	4	5	15	15	11	5	10	5
Somewhat Agree	5	5	14	15	3	5	3	5
Disagree	2	5	0	15	1	5	1	5
Strongly Disagree	0	5	1	15	2	5	2	5
Not Sure/Not Applicable	0	5	2	15	1	5	0	5
H0 is rejected for p < 0.01	Chi^2=51.2	P<0.0001	Chi^2= 162.67	P<0.0001	Chi^2=26	P<0.0001	Chi^2=32	P<0.0001

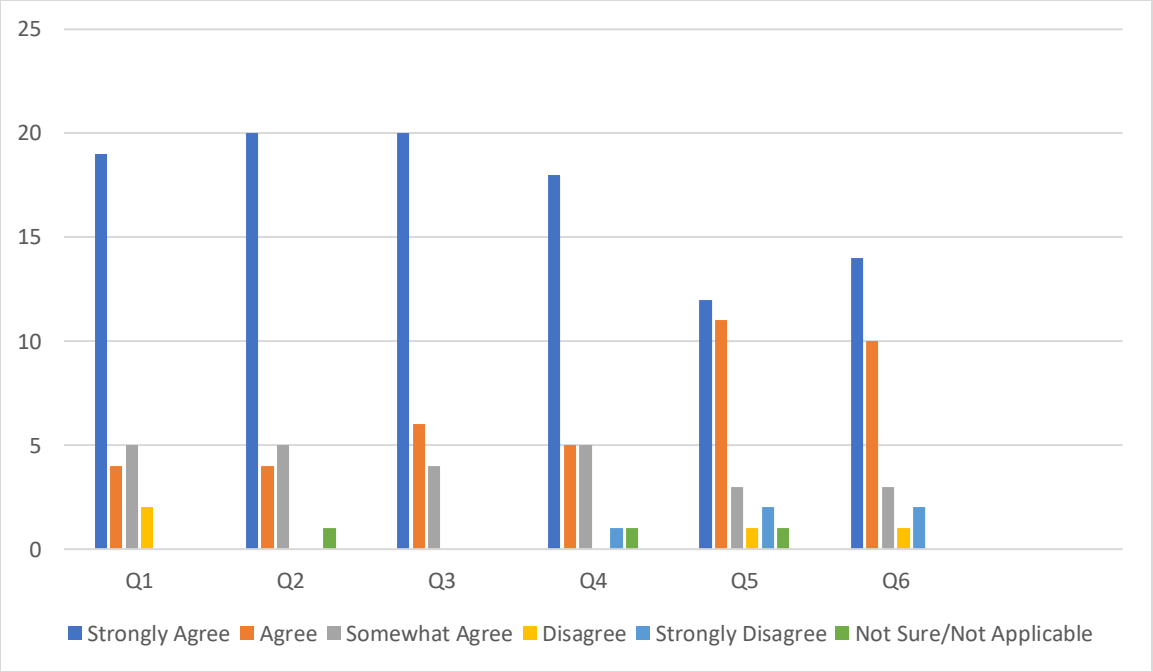


Figure 5.13. Evolve Component Data Graph (BG3)

Analysis

The ordinal data in Table 5.20 (SR3) and Table 5.21(CR3) produced basic statistical values based on the responses. The evolve component evaluation results can be translated as below:

SAAF = 168 out of 180 responses suggest that a large proportion of participants agree that the evolve component fulfills the evaluation criteria positively.

SAAP = 93.33% suggest that a high percentage of participants agree that the evolve component fulfills the evaluation criteria positively.

The p-value for the test variables:

- Generalization p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA evolve component and the generalization evaluation criteria.
- Applicability p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA evolve component and the applicability evaluation criteria.
- Novelty p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA evolve component and the novelty evaluation criteria.
- Comprehensiveness p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA evolve component and the comprehensiveness evaluation criteria.

The statistical values indicate that the participants consider the ADIVRA evolve component is appropriate and a vital design as well as it addresses the practical needs. Figure 5.13 shows the frequency of the participants' responses to add more graphic details to the results.

b) Overall ADIVRA Framework Evaluation

Table 5.22: Overall ADIVRA Framework Survey Rating SR4

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Rows Total	Percentage %
Strongly Agree	21	20	21	17	18	16	22	20	23	178	65.92%
Agree	6	9	6	7	10	9	5	8	5	65	24.07%
Somewhat Agree	3	1	1	3	1	3	3	2	2	19	7.03%
Disagree	0	0	0	0	0	0	0	0	0	0	0%
Strongly Disagree	0	0	0	0	1	1	0	0	0	2	0.74%
Not Sure/Not Applicable	0	0	2	3	0	1	0	0	0	6	2.22%
Column Total	30	30	30	30	30	30	30	30	30	270	100.00%

SAAF = 262
SAAP = 97.03%

Table 5.23: Overall ADIVRA Framework Category Rating CR4

	Evaluation Criteria									
	Generalization Q1		Applicability (Q2, Q3, Q4)		Novelty Q5		Comprehensiveness Q6		Usefulness (Q7, Q8, Q9)	
N=6 E= Σ O/N	O	E	O	E	O	E	O	E	O	E
Strongly Agree	21	5	58	15	18	5	16	5	65	15
Agree	6	5	22	15	10	5	9	5	18	15
Somewhat Agree	3	5	5	15	1	5	3	5	7	15
Disagree	0	5	0	15	0	5	0	5	0	15
Strongly Disagree	0	5	0	15	1	5	1	5	0	15
Not Sure/Not Applicable	0	5	5	15	0	5	1	5	0	15
H0 is rejected for p < 0.01	Chi^2=67.2	P<0.0001	Chi^2= 169.87	P<0.0001	Chi^2=55.2	P<0.0001	Chi^2=39.6	P<0.0001	Chi^2=216.53	P<0.0001

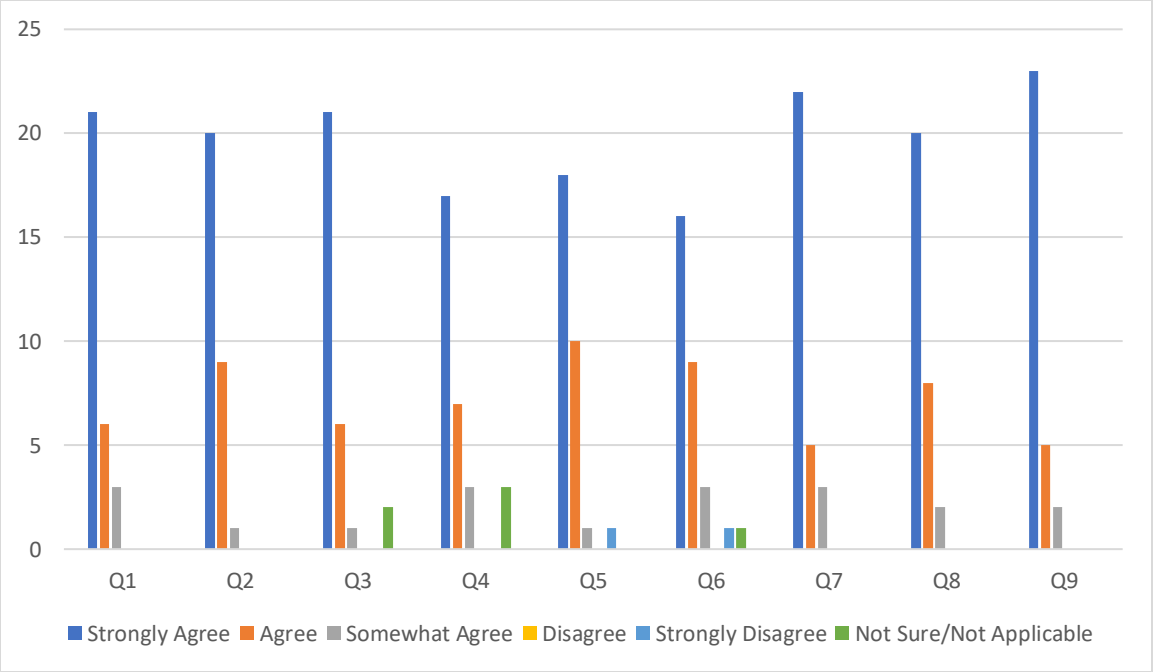


Figure 5.14. Overall ADIVRA Framework Data Graph (BG4)

Analysis

The ordinal data in Table 5.22 (SR4) and Table 5.23 (CR4) produced basic statistical values based on the responses. The ADIVRA framework evaluation results can be translated as below:
SAAF = 262 out of 270 responses suggest that large portion of participants agree the ADIVRA framework fulfills the evaluation criteria positively.

SAAP = 97.03% suggest that a high percentage of participants agree that the ADIVRA framework fulfills the evaluation criteria positively.

The p-value for the test variables:

- Generalization p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA framework and the generalization evaluation criteria.
- Applicability p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA framework and the applicability evaluation criteria.
- Novelty p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA framework and the novelty evaluation criteria.
- Comprehensiveness p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is statistically significant relationship between the ADIVRA framework and the comprehensiveness evaluation criteria.
- Usefulness p-value is set at $0.0001 < \alpha=0.01$. This indicates that H0 is rejected, H1 is accepted, and there is a statistically significant relationship between the ADIVRA framework and the usefulness evaluation criteria.

The statistical values indicate that the participants consider the ADIVRA framework appropriate and an important architecture and that it addresses the practical requirements. Figure 5.14 shows the frequency of the participants' responses to add more graphic details to the results.

5.5.2.2 Survey Qualitative Evaluation

This section provides the qualitative evaluation of the survey feedback and comments from the participants, regarding the ADIVRA framework. The survey qualitative evaluation is based on the participants' feedback provided on the ADIVRA framework and the components in the questionnaire sets (Q5–Q8).
The qualitative evaluation process comprises two sections:

- ADIVRA usefulness aspects evaluation [Q6 set] and three questions from overall ADIVRA framework usefulness (for identity architects, regulators, researchers) evaluation [Q4 set)
- ADIVRA overall feedback, comments, and ratings [Q5 and Q8 set].

ADIVRA-suggested improvements [Q7 set] are used in Chapter 6 to determine future research based on the participants' suggestions in this question.

a) ADIVRA Usefulness Evaluation

This section evaluates the participants' responses on ADIVRA usefulness for identity architects in industry, regulators, law makers and researchers. The evaluation process is as below:

- Gather and map the feedback on the ADIVRA useful aspects into Table 5.24.
- Analyse Table 5.24 responses on the basis of occurrences of the criteria (see Table 3.1) in the feedback using the cross-examination technique.
- Identify the ADIVRA component to which the responses refer.
- Calculate the percentages for each component that determine the most useful ADIVRA component.
- Collect and map the usefulness rating as numerical data in Table 5.25, labelled CR5.
- Plot Table 5.25 (CR5) data into a bar graph in Figure 5.15, labelled BG5.
- Calculate the statistical values SAAF and SAAP from Table 5.25 (CR5) data (see Equation 3.1-3.2):
- SAAP determines the frequency of participants that consider the ADIVRA useful for identity architects, regulators, and researchers (see Equation 3.2).
- SAAF determines the percentage of participants that consider the ADIVRA useful for identity architects, regulators, and researchers (see Equation 3.1).
- Calculate the goodness-of-fit Chi2 and p-value for each test variable (identity architects, regulators, researchers) at a critical value $\alpha = 0.01$ (see Equation 3.3).

If $p < \alpha$, then the null hypothesis H_0 is rejected and H_1 is accepted.
H_0: The test variables are not associated.
H_1: The ADIVRA framework meets the evaluation criteria positively (usefulness for identity architects, regulators, researchers).

Table 5.24: ADIVRA Usefulness Results

No.	Participant's Comment (What aspects are useful or valuable about ADIVRA?)	Category	Component		
			Assess	Design	Evolve
1	The design and evolve components are the strength of this project.	Applicability		☑	☑
2	I found IdMPAM and the entire design component very useful	Usefulness	☑	☑	
3	The IdMPAM, CDigI and iSEA	Usefulness	☑	☑	
4	Assess and design	Applicability Usefulness	☑	☑	
5	The design component is very strong and valuable	Usefulness Applicability		☑	
6	Artefacts (EG, PESTLE+, Evolve Component, etc).	Usefulness Applicability	☑		☑
7	Design component	Applicability Usefulness		☑	
8	I found the assess component very useful. Also, the concept of compound digital identity	Applicability Usefulness	☑	☑	
9	All three components and the fact that everything is linked back and aligned to strategy	Applicability Usefulness Comprehensiveness	☑	☑	☑
10	I think DigIVPM is very robust and comprehensive	Comprehensiveness Usefulness Generalization		☑	
11	Strong privacy and GDPR compliance aspects	Applicability Usefulness	☑	☑	☑
12	Very useful	Usefulness	☑	☑	☑
13	The RRM and CDigI	Applicability Usefulness		☑	
14	Information security envelope architecture	Usefulness		☑	
15	Design component is very useful	Usefulness		☑	
16	The attribute-based encryption is a very strong addition to the platform and increases security and privacy standards.	Applicability Usefulness		☑	
17	Design component/iSEA	Usefulness		☑	

18	The assess and design components	Usefulness	☑	☑	
19	The structured approach of the evolve component	Usefulness Applicability			☑
20	ADIVRA framework and artefacts	Usefulness Applicability Comprehensiveness	☑	☑	☑
		Total	10	18	7
		Percentage	50.00%	90.00%	35.00%

Table 5.24 shows that 18/30 participants responded to Q6 set of the survey questionnaire which was about the useful aspects of ADIVRA. 50% found the assess components the most useful (RQ1), 90% found the design components the most useful (RQ2) and 35% found the evolve components the most useful (RQ3). Hence, the ADIVRA framework is useful in addressing the research gaps and research questions. The usefulness of the ADIVRA components for identity architects, lawmakers and researchers is further analyzed in Table 5.25.

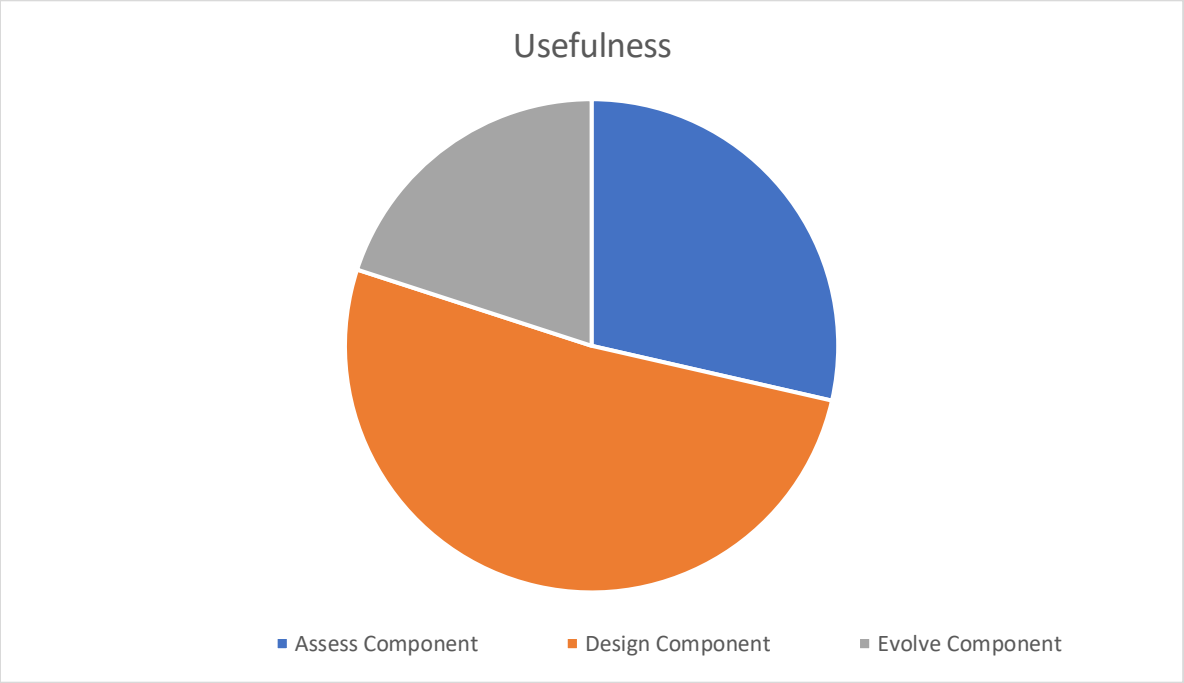


Figure 5.15. ADIVRA Component Usefulness (BG5)

Table 5.25: ADIVRA Usefulness Ratings (CR5)

ADIVRA Usefulness	Identity Architects		Regulators		Researchers		Total	Percentage %
N=6 E= Σ O/N	O	E	O	E	O	E		
Strongly Agree	23	5	20	5	24	5	67	74.44%
Agree	4	5	8	5	4	5	16	17.77%
Somewhat Agree	3	5	2	5	2	5	7	7.77%

Disagree	0	5	0	5	0	5	0	0%
Strongly Disagree	0	5	0	5	0	5	0	0%
Not Sure/Not Applicable	0	5	0	5	0	5	0	0%
H0 is rejected for p < 0.01	**Chi^2=80.8**	**P<0.0001**	**Chi^2=63.6**	**P<0.0001**	**Chi^2=89.2**	**P<0.0001**	90	100%

Analysis

The ADIVRA framework usefulness results can be translated as below:
SAAF = 90 out of 90 responses imply that all of the survey participants agree that the ADIVRA framework meets the usefulness criteria positively.

SAAP = 100% indicates that a high percentage of participants agree that the ADIVRA framework meets the usefulness criteria positively.

The p-value for the test variables:

- Identity architects p-value is set at 0.0001 < α=0.001. H0 is rejected, H1 is accepted, and the ADIVRA components meet the evaluation criteria positively (usefulness for identity architects).
- Regulators p-value is set at 0.0001 < α=0.001. H0 is rejected, H1 is accepted, and the ADIVRA components meet the evaluation criteria positively (usefulness for regulators).
- Researchers p-value is set at 0.0001 < α=0.001. H0 is rejected, H1 is accepted, and the ADIVRA components meet the evaluation criteria positively (usefulness for the researchers).

The statistical values imply that the participants consider the ADIVRA framework useful for identity architects, regulators, and researchers. Figure 5.15 shows the frequency of the participants' responses to add more graphic details to the results.

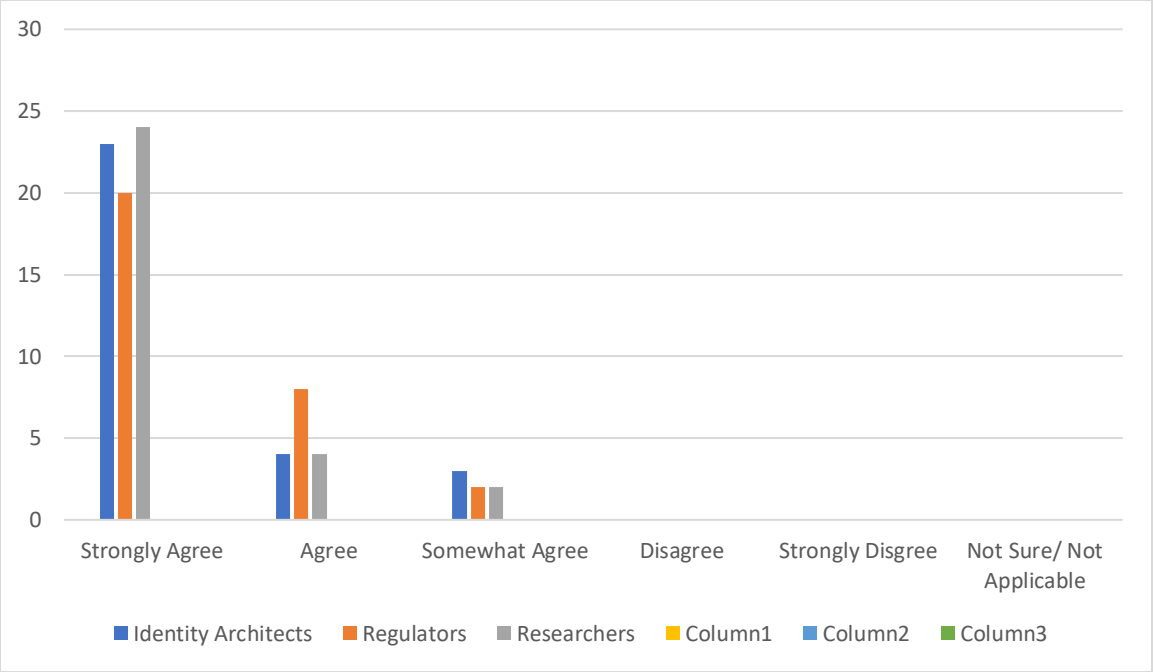


Figure 5.16. Overall ADIVRA Framework Usefulness Rating (BG6)

b) ADIVRA Overall Feedback, Comments and Rating

This section evaluates the overall feedback of the survey participants and rating on the ADIVRA framework. The evaluation process is as below:

- Gather and map the participants' comments and feedback about the ADIVRA into Table 5.26.
- Analyse the comments and feedback in Table 5.26 on the basis of the frequency criteria occurrences in the text (see Table 3.1) using the cross-examination technique
- Tag comments/feedback into positive aspects (PA), neutral comments (NC) and suggestions and improvements (SI).
- Calculate the percentage of the comment/feedback tag (see table 5.27).
- Collect the ADIVRA overall ratings and map them as numerical data in Table 5.28, labelled CR6.
- Plot Table 5.28 (CR6) data into a bar graph representation in Figure 5.16, labelled BG6.
- Calculate the statistical value for rating 3 and above percentage from Table 5.28 (CR6) data
    - 3 and above percentage indicates the frequency of survey participants who are happy with the ADIVRA overall.

Table 5.26: ADIVRA Feedback/Comments and Response

No	Participants' Feedback/Overall Comments	Category	Weight
1	This research addresses the pressing problem of privacy by enabling businesses, system designers, regulators, and other stakeholders to follow a general framework for reliable privacy preserving decentralized digital products.	Usefulness Generalization Comprehensiveness	PA
2	The iSAM2 can be improved by making it more generalized.	Generalization	S&I
3	The digital identity design can be improved by addressing the blockchain's inherent problem of scale	Applicability	S&I
4	Addition of analytics to the design and evolve component	Applicability Comprehensiveness Novelty	S&I
5	The validation of regulatory requirements extracted using RRM can be made stronger by making a validation criterion that is inclusive of international regulations and digital identity principles	Generalization Novelty Applicability Comprehensiveness	S&I
6	The real time monitoring of changes in risks, threats, regulations and business competitors needs AI and machine learning to be embedded into the reference architecture	Novelty Comprehensiveness Applicability	S&I
7	Attaching automated tools like RRM a requirement management tools can be integrated to adopt an integrated approach to cross-domain product development	Applicability Novelty	NC
8	Addition of biometric/liveness/voice recognition increases privacy and security	Applicability	PA
9	Improving performance and response time	Applicability Comprehensiveness	S&I
10	The framework is really complete and helpful in covering many aspects of the identity verification process	Comprehensiveness Applicability	PA
11	ADIVRA can be made more comprehensive and useful for regulators and law makers by considering regulations from multiple jurisdictions	Comprehensiveness Usefulness	PA
12	ADIVRA design component is really good	Usefulness	PA
13	None		NC
14	I would like to rate it between 4 and 4.25.	Generalization Applicability Novelty Comprehensiveness Usefulness	PA
15	I like the design component, also the gaps identified in the previous research are addressed in the proposed framework. I was more interested to see the technical implementation or proof of concept of the approach which could be very useful to assess the overall framework. In general, I think ADIVRA is a great contribution that could be helpful for researchers in the future.	Usefulness Comprehensiveness Applicability	PA
16	An end-to-end application of the entire framework in one organization would be very helpful for its future use and extension	Applicability Generalization	PA
17	I found a lot of potential in iSEA. I would like to see a POC.	Usefulness Applicability Novelty	PA
18	This research has considered the maximum aspects of digital identity verification. It is a very structured and comprehensive approach	Comprehensiveness Applicability	PA
19	Would like to see MVC.	Applicability	NC
20	Overall, the framework is very strong and covers the maximum concepts of the digital identity verification lifecycle	Comprehensiveness	PA
21	A demonstration of the assess component application to other regulations for example the Australian Privacy Act 1988 and any other standard for example ISO 27701 would be helpful.	Generalization Applicability	NC
22	The framework has great potential and can be used by government as well as private organizations	Generalization Applicability Usefulness	PA

23	My only comment is on performance and response time. With so much happening in this kind of framework, what impact will it have on performance and how quickly will the response be sent out to end users.	Applicability Usefulness	NC
24	A complete and comprehensive digital identity verification platform	Comprehensiveness Applicability	PA
25	Addition of multiple regulations as well as analytics will make ADIVRA more comprehensive and useful	Comprehensiveness Applicability Generalization	NC
26	Adding some analytics to the evolve component will be very good	Usefulness Novelty	NC

Table 5.27: ADIVRA Feedback/Comments Weight Frequency

Weight	Total	Percentage
PA	13	50%
NC	8	30.76%
S&I	5	19.23%
Total	26	100%

Tables 5.26 and 5.27 show that 50% of the participants gave positive comments/ feedback on the ADIVRA framework, 30.76% of the comments/feedback were neutral and 19.23% suggested potential areas of improvements for the ADIVRA framework components.

Table 5.28: ADIVRA Framework Overall Rating (CR6)

On a scale of 1 to 5 (5 being highest). Please provide an overall rating for the ADIVRA framework		
Rating	**Frequency**	**Percentage**
5	15	50%
4	11	36.66%
3	4	13.33%
2	0	0%
1	0	0%
Total	30	100%

Analysis

The ordinal data in Table 5.28 (CR6) produced a statistical value based on the participants' responses. Overall, the ADIVRA Q8 set showed that:

- 3 and above rating percentage = 100%, indicating that all the participants agree that the ADIVRA framework components meet the evaluation criteria (see Chapter 3, Table 3.1).

5.6 Summary

This chapter presented the iterative development, evaluation, and refinement of the ADIVRA framework. The ADIVRA framework was developed in three iterations of BIE and RL. The evaluation comprised two steps: review and feedback workshops and an industry field survey. The data collected from the evaluation iterations was reviewed to determine the relevance and importance of the ADIVRA and whether it covered the research aims and objectives. The intermediate versions of ADIVRA are described and how the design emerged via continuous feedback. The design principles, research implications, limitations and key contributions are discussed in Chapter 6.

Chapter 6: Discussion and Conclusion

This chapter outlines the design principles that were extracted during this research. This final chapter summarizes the research implications in section 6.3. The contributions and publications are listed in section 6.4. The ADIVRA limitations and future work are discussed in section 6.5, based on the feedback from the evaluation. Finally, section 6.6 provides the conclusion and summary.

6.1 ADIVRA Design Principles

This is the last stage of the ADR method, that draws on the principle of generalized outcomes (ADR Principle 7). In this last stage of the ADR method, FL, we proceeded to consolidate the discoveries during the course of this research with the knowledge base with the aim of developing design principles. The key steps in the FL stage are to conceptualize the knowledge into ideas for a class of similar problems, communicate the results and evaluation with industry experts, extract the results as design principles, and express the knowledge obtained in the context of kernel theories and formalize the outcomes for communication (Gregor, Müller & Seidel 2013; Sein et al. 2011). This research contributes to research community alongside practice by developing not only a novel ADIVRA framework, but additionally the fourteen design principles for adaptive, privacy aware and regulatory compliant DigI verification.

Table 6.1 describes a set of design principles that were extracted by using the creative, passive, and active casual analysis techniques as mentioned by Gregor, Müller & Seidel (2013). The creative causal analysis permits the fundamental design idea and its purpose and scope to be determined, e.g., the purpose of ADIVRA was to ensure regulatory compliance and privacy of PII involved in DigI verification in the digital ecosystem i.e., privacy by design, interoperability, and reusability. Passive casual analysis allows principles of form to be found by analysing the way different material attributes create explicit affordances in a particular user context, e.g., enhanced user control, minimal disclosure and breach notification are principles of form. Active casual analysis is used to extract principles of function by detailing the significance brought about by cautious acts and involvements, e.g., simplicity, affordability, and multiple platform support. Table 6.1 describes the extraction of design principles.

Table 6.1. Extraction of design principles

Principle	Purpose & Scope	Principle of Form	Principle of Function	Creative Casual Analysis	Active Casual Analysis	Passive Casual Analysis
Reusability	x			x		
Ecosystem Approach	x			x		
Digital Identity Life Cycle management	x			x		
Multi-dimensional digital identity		x				x
Interoperability			x		x	
Adaptability		x				x
Compliance	x			x		
Privacy by Design	x			x		

Simplicity			x		x	
Affordability			x		x	
Multiple Document support			x		x	
Enhanced user control		x				x
Minimal Disclosure/Data Minimization		x				x
Breach Notification		x				x

This research aims to design a reference architecture for the DigI verification solution where privacy is embedded into the design of the solution as required by the regulations. Hence, the principles of purpose and scope are:

1. Reusability
2. Ecosystem Approach
3. Digital Identity Lifecycle Management
4. Privacy by Design
5. Compliance

The principles of purpose and scope are obtained using creative casual analysis. Creative casual analysis refers to the situation where mental activity creates the change: that is, a designer envisioned a reusable and privacy aware DigI verification solution and was then able to put these ideas into a real-world design. The design principles stemming from creative casual analysis (reusability, ecosystem approach, DigI lifecycle and privacy by design) are the basis of innovation that differentiates ADIVRA from the others.

However, the designer of blockchain-based DigI verification solutions may need some central design principles. These principles are core to the conceptualization and requirements of what it means to be an adaptive DigI verification solution that is privacy aware and regulatory-compliant:

6. multi-domain digital identity
7. adaptability
8. enhanced User Control
9. minimal disclosure
10. breach notification

The above principles for DigI verification solutions are classified as principles of form. The principles of form (enhanced user control, minimal disclosure, and breach notification) are extracted by passive causal analysis which refers to characteristics that are contextual in nature**.** For instance, the DigI verification solution could be web-based or a mobile application, fully automated or have a data controller, hence these are all contextual features.

Additional principles can also be extracted by assessing existing DigI verification solutions and their use in different organizational contexts. For instance, in order for a DigI verification solution to be practical and useful for identity owners, it should have:

11. multiple document support
12. simplicity
13. affordability
14. interoperability

The above four principles are principles of function, which are extracted using active casual analysis. The design principles extracted from this research can be used to inform the design of a

privacy aware and regulatory-compliant DigI verification solution. Table 6.2 details the challenges that each design principle aims to address along with the guiding statements.

Table 6.2. Key design principles

DigI verification Challenges	Design Principle	Description: Guiding statement and recommendation
Compliance visibility: who has access to what?	Enhanced user control	DigI verification solutions must offer users details about the purpose of personal data collection, retention periods for PII, and the possible use and sharing of information. We call this privacy information
Friction of transacting digitally	Ecosystem approach	An ecosystem approach should be taken, and a healthy ecosystem adapts to maintain confidence and trust.
Lack of a structured process for updating and re-proofing identity attributes	Digital identity life cycle management	The whole digital identity ecosystem and its components must be considered – identity issuers (government, non-government and social); identity providers; service providers; identity owners; regulators.
Different DigIs used for specific limited context	Multi-dimensional digital identity, Interoperability	All domains must be considered – the individual, business, and "things" – and the adaptive philosophy means that other evolving domains and concepts become part of the framework over time.
Changing privacy risks, regulatory requirements, and business needs	Adaptability	The design of a DigI verification solution must evolve and adapt to drive innovation. The role and emergence of solutions must be encompassed in terms of governance, risk, and business. Adaptive DigI verification framework will be privacy enhancing.
Lack of consent flexibility	Enhanced user control	The data user can restrict the use of their personal data. No information can be processed without the data subjects' consent.
Online Identity requires a lot of PII	Minimal disclosure/Data minimization	Take realistic and logical steps to restrict the use, disclosure and any or all requests for PII to the bare minimum, which is essential to achieve the intended purpose.
Time-consuming DigI verification	Reusability, Multi-dimensional digital identity	A widespread identity system must emphasize and encourage the inter-working of various identities provided by different identity providers.
Privacy and Security	Privacy by Design	DigI verification solutions should be based on embedding privacy into the design and function of the IT unit, business practices, network, and infrastructure.
Regulatory requirements and complexity	Simplicity	DigI verification solutions should be simple and easy to use for onboarding customers.
Huge cost	Affordability	Increasing competitive pressures demand that DigI verification solutions should be affordable from A cost perspective.
Centrally managed user data	Enhanced user control	Thorough user controlled DigI verification solutions take a unique attitude, as they employ privacy by design principles and enhance identity owners' privacy by placing more control into their hands.
The single security feature can be forged	Multiple document support	Always check more than one security feature e.g., passport, driving license.

Large scale data breaches and exponentially growing fines and regulatory areas.	Breach notification	Identity owners should be informed when their PII is compromised. Breach notification prepares the identity owner for any possible identity theft which can happen as a result of a breach.

6.2 Research Implications

The proposed ADIVRA framework in this research addresses some important RQs such as how privacy risks can be assessed, how a privacy aware and regulatory compliant DigI verification solution should be designed and how this solution can adapt to changing regulations, privacy risks and business needs. In particular, ADIVRA focuses on privacy by design, GDPR compliance and meeting business goals. In this section, the implications for practice and research of ADIVRA are discussed.

6.2.1. Implications for Practice

This research aims to address the privacy, security, compliance, and adaptability concerns by developing a new blockchain-enabled DigI verification reference architecture framework by conducting innovative industry-based research. In this sense, the practical implications of research are listed below.

- The result of this research can help in addressing the current inadequate understanding of complex DigI, its verification, compliance, and adaptation in the distributed digital ecosystem.
- The ADIVRA framework can help industry practitioners in developing an integrated software technology-enabled adaptive architecture framework for secure DigI verification without storing the PII.
- The ADIVRA framework can help in developing meta-level learning about the potential to reduce DigI verification cost and information privacy risks.
- The ADIVRA framework seems to provide the multifaceted structure of DigI by looking at multiple attributes or personas of IOs (human, organizations, devices) depending on various use cases.
- The regulatory requirements for DigI verification solutions are mentioned in regulations but there is no definition of a structured approach to effectively extract and validate the requirements. The ADIVRA framework presented in this research offers a novel approach for integrating business processes to regulatory articles for regulatory compliant DigI verification.
- The comprehensive requirements backlog based on interoperable globally relevant regulations can help DigI architects to develop a regulatory compliant DigI architecture without having to read lengthy and time-consuming regulation documents.
- The ADIVRA framework can also be used by law makers. It draws their attention to establishing more actionable and enforceable regulatory requirements that will facilitate the co-existence of technology and regulation. As an example, blockchain's inherent immutability and transparency conflicts with the right to be forgotten and minimal disclosure principles. Hence, there is a need to rethink the regulatory requirements for a more practicable solution.
- The ADIVRA framework was developed by adopting a principle-driven approach. As a result, this ADR process produced a set of fundamental design principles for designing an

adaptive, privacy aware and regulatory-compliant DigI verification solution. The ADIVRA design principles are generic and thus can be adapted to different organizational contexts and operational details.

6.2.2. Implications for Research

This research, being investigative and informative in nature, presents a number of prospects for future studies in terms of theory development as well as idea validation. Additional work is required to enhance and further explain the new discoveries made in this research.

- ADIVRA may provide a research-based practical framework for DigI verification.
- The addition of the idea formulation stage adopted from Gill & Chew (2019), as well as the integration of design principle extraction techniques by Gregor, Müller & Seidel (2013) extends the ADR proposed by Sein et al. (2011). This implies that ADR may need tailoring and integration to address the problem class and context in hand. Thus, the ADR method need to be adaptive. This may require further research in developing the ADR method patterns for different problem classes and contexts.
- This research identified a number of design principles (see Section 6.1) which were extracted using creative, passive and active analysis techniques (Gregor, Müller & Seidel 2013). The design principles extracted from this research can be embraced by other organizations to design adaptive DigI verification solutions and a similar class of problems. Further, these principles can be used to inform the development of new DigI verification theories and frameworks. Moreover, these design principles were mirrored on the same class of problems, along with the one under discussion.
- From an academic perspective, this research contributes in many different ways, to the body of knowledge of three evolving fields: adaptability, regulatory compliance, and privacy. It provides a framework for developing ecosystem privacy as a separate discipline /subject that can be a part of the curriculum.

6.3 Key Contributions and Publications

The ADIVRA framework outlined in Chapter 4 was evaluated and tested as discussed in Chapter 5. Two types of testing and evaluation were used to determine the validity and relevance of the framework in the industry. Key publications contributed to the construction of the ADIVRA framework. The conference publications were peer-reviewed by key international researchers and experts. This section presents the key contributions of the research (see Table 6.3):

Table 6.3. Publications

No.	Contribution	Reference	Description
1	Journal	Title: 'A Secure Big Data Ecosystem: Systematic Literature Review and Future Directions' Authors: Anwar, M.J., Gill, A.Q., Hussain, F.K. and Muhammad, I. Journal homepage: https://jwcn-eurasipjournals.springeropen.com/	Springer

2	Conference	Anwar, M., Gill, A. & Beydoun,G. (2018). *A review of Australian information privacy laws and standards for secure digital ecosystems.* ACIS 2018 available at: http://www.acis2018.org/wp-content/uploads/2018/11/ACIS2018_paper_78.pdf	ACIS, 2018
3	Conference	Anwar, M., Gill, A. (2018). *A review of information privacy laws and standards for secure digital ecosystems.* CBI 2019 available at: https://ieeexplore.ieee.org/document/8807801	CBI, 2019
4	Conference	Anwar, M., Gill, A. & Beydoun,G. (2019). *Using Adaptive Enterprise Architecture Framework for Defining the Adaptable Identity Ecosystem Architecture.* ACIS 2019	ACIS, 2019
5	Conference	Anwar, M., Gill, A. (2020). *Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model.* ACIS 2020	ACIS, 2020
6	Journal (In Review)	Title: 'Decentralized Digital Identity Requirements Model: Regulatory Perspective' Authors: Anwar, M.J., Gill, A.Q., Fitzgibbon, A.D. and Gull,I. Journal homepage: https://www.journals.elsevier.com/computers-and-security	Elsevier
7	Journal (In Review)	Title: 'A Privacy Assessment Model for GDPR Compliant Blockchain enabled Identity Management: An Action Design Research' Authors: Anwar, M.J. and Gill, A.Q. and Fitzgibbon, A.D. Journal homepage: https://www.journals.elsevier.com/information-and-management	Elsevier
8	Journal (Accepted)	Title: 'Using PESTLE+ Analysis to Assess Pandemic Preparedness of Identity Ecosystems.' Authors: Anwar, M.J., Gill, A.Q., Fitzgibbon, A.D. and Gull, I. Journal homepage: https://onlinelibrary.wiley.com/journal/24756725	Security and Privacy Journal
9	Journal (In Review)	Title: 'Using ArchiMate for Modelling the Secure Digital Identity Ecosystem Architecture' Authors: Anwar, M.J. and Gill, A.Q., Fitzgibbon, A.D. and Gull, I. Journal homepage: https://www.journals.elsevier.com/computers-and-security	Elsevier

10	Journal (In Draft)	Title: 'Information Security Audit Maturity Model: An Action Design Research' Authors: Anwar, M.J., Gill, A.Q., Fitzgibbon, A.D and Ross, J. Journal homepage:	Springer
11	Magazine Paper (In Draft)	Title: 'Unlocking Digital Identity Verification Architecture' Authors: Anwar, M.J., Gill, A.Q., Fitzgibbon, A.D and Ross, J. Magazine homepage: https://www.computer.org/csdl/magazine/it	IEEE Computer Society
12	Journal (Planned)	Title: 'An Attribute Based Encryption Based Information Security Envelope Architecture' Authors: Anwar, M.J., Gill, A.Q., Fitzgibbon, A.D and Ross, J. Journal homepage:	
13	Journal (Planned)	Title: 'Adaptive Digital Identity Verification Architecture: An Action Design Research' Authors: Anwar, M.J., Gill, A.Q., Fitzgibbon, A.D and Gull, I. Journal homepage:	
14	Journal (Planned)	Title: 'Digital Identity Adaption Model' Authors: Anwar, M.J., Gill, A.Q. and Fitzgibbon, A.D Journal homepage:	

6.4 Limitations and Future Work

IS research can be conducted using a variety of strategies and a wide range of settings (Banker & Kauffman 2004; Benbasat & Weber 1996). In addition, there can be no ideal strategy since different approaches have relative advantages and disadvantages (Dennis & Valacich 2001). The ADIVRA framework in this thesis has been evaluated via design and review workshops (see Chapter 5) and assessed by experts using survey questionnaires. The incremental versions of the

framework have also been peer reviewed at renowned conferences (Anwar & Gill 2020, 2019; M. Anwar, Gill & Beydoun 2019; Anwar, Gill & Beydoun 2018b). Despite the aforementioned research contributions, the current version of the ADIVRA framework has a few limitations that can lead the path to future work:

- The first limitation is the time constraint of the PhD program, which limited the researcher's ability to stay longer in the field to investigate further issues, especially in light of the fact that the research covered a project that has not been fully implemented yet. It would be interesting to conduct a longitudinal study to analyze how these issues change over time with usability.
- Secondly, this study's potential methodological limitation is related to the industry field survey recruitment method and the sample used. The participants of this study were mainly recruited via LinkedIn and the survey remained open for 6 months. Therefore, this might be a threat to the external evaluation of the ADIVRA framework. However, the responses are imperative and there can be repetition in the type of responses. Future research can further strengthen the current findings by using 15+ participants in addition to the already evaluated work.
- The scope of the study is limited to the DigI verification reference architecture only. The study does not focus on the cryptographic details and network structure required for carrying out DigI verification.
- Any pre-verification and post-verification considerations are beyond the scope of this study. For example, the study did not highlight the initial trust establishment between SPs and IdPs. IOs may have pre-existing trust with a SP and may interact for the first time with an IdP or vice versa when they use a DigI verification solution for the first time. Therefore, trusting beliefs in IdPs in this study were not measured based on all possible relationships with IdPs with whom the identity may have familiarity and experience. Future research could therefore consider the further differentiation of IO's trusting beliefs of IdPs as well as comparing this between familiar versus unfamiliar providers, which could enhance the understanding of trusting beliefs in the DigI verification process.
- Future work may embed analytics into the ADIVRA framework to enhance the change prediction

6.5. Conclusion and Summary

This thesis presented the ADIVRA framework that appears to provide a practical solution for the problem of privacy and regulatory compliance in the DigI verification process. The ADIVRA was developed iteratively using a well-known ADR method. The ADIVRA framework is intended for use by researchers and practitioners (identity architects, business analysts and information security and compliance teams) as a practical guide for assessing risks and identifying gaps, designing, and developing a privacy aware and regulatory compliant DigI verification solution and adapting the design with changing privacy risks, regulatory requirements, and business needs. The ADIVRA framework offers three important components, assess, design, and evolve, which could be used in any organizational context. Moreover, this research also suggests empirically grounded design principles to sustain the usefulness of the ADIVRA framework, based on FL in the three ADR iterations. The implications of the research findings stated in this thesis are twofold, for the research community and for practice. The ADR methodology and architecture components presented in this thesis could be used and extended by industry practitioners and researchers as suitable for their individual setting. Since this research is limited at the architecture and theoretical analysis level, an effective future direction is to implement a DigI verification solution based on the reference architecture and then investigate its full potential in a practical scenario. It is important to note that the use of blockchain technology for DigI verification is still in its early stages. Hence, prospective research could also be the development of proof of concept for DigI verification, employing the latest trends in blockchain technology for DigI verification to comply with the regulatory requirements and to strengthen the privacy and security of PII. The ADIVRA framework will be further extended based on future learning, research, and experience.

Bibliography

Adeyemo Kingsley, A. 2012, 'Frauds in Nigerian banks: Nature, deep-seated causes, aftermaths and probable remedies', *Mediterranean Journal of Social Sciences*, vol. 3, no. 2, pp. 279–89, viewed 17 April 2021, <https://www.academia.edu/download/30172283/mjss_vol_3_no_2_may_2012.pdf#page=279>.

Ahmed, J., Yildirim, S., Nowostaki, M., Ramachandra, R., Elezaj, O. & Abomohara, M. 2020, 'GDPR compliant consent driven data protection in online social networks: A blockchain-based approach', *Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020*, Institute of Electrical and Electronics Engineers Inc., pp. 307–12.

Aiello, W., Lodha, S. & Ostrovsky, R. 1998, 'Fast digital identity revocation', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1462, Springer Verlag, pp. 137–52.

Van Aken, J.E. 2005, 'Management research as a design science: Articulating the research products of mode 2 knowledge production in management', *British Journal of Management*, vol. 16, no. 1, pp. 19–36, viewed 2 May 2021, <https://www.researchgate.net/publication/254021036>.

Al-Anzi, F.S., Salman, A.A., Jacob, N.K. & Soni, J. 2014, 'Towards robust, scalable and secure network storage in Cloud Computing', *2014 4th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2014*, pp. 51–5, viewed 25 April 2021, <https://ieeexplore.ieee.org/abstract/document/6821656/>.

Al-Zaben, N., Onik, M.M.H., Yang, J., Lee, N.Y. & Kim, C.S. 2019, 'General Data Protection Regulation Complied Blockchain Architecture for Personally

Identifiable Information Management', *Proceedings - 2018 International Conference on Computing, Electronics and Communications Engineering, iCCECE 2018*, Institute of Electrical and Electronics Engineers Inc., pp. 77–82.

Alam, L. & Gill, A. 2020, 'A Social Engagement Framework for the Government Ecosystem: Insights from Australian Government Facebook Pages', *ICIS 2020 Proceedings*, viewed 17 April 2021, <https://aisel.aisnet.org/icis2020/digitization_in_cities/digitization_in_cities/8>.

Alavi, M. & Carlson, P. 1995, 'A review of mis research and disciplinary development', *Journal of Management Information Systems*, pp. 45–62.

Alketbi, A., Nasir, Q. & Talib, M.A. 2018, 'Blockchain for government services-Use cases, security benefits and challenges', *2018 15th Learning and Technology Conference, L and T 2018*, Institute of Electrical and Electronics Engineers Inc., pp. 112–9.

Allen, C. 2016, 'The Path to Self-Sovereign Identity', *Life With Alacrity*, viewed 25 April 2021, <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html>.

Aloraini, A. & Hammoudeh, M. 2017, 'A survey on data confidentiality and privacy in cloud computing', *Cam-bridge, United Kingdom. ACM Reference*, vol. Part F130522, viewed 25 April 2021, <https://dl.acm.org/doi/abs/10.1145/3102304.3102314>.

Van Alstyne, M. & Parker, G. 2017, 'Platform Business: From Resources to Relationships', *NIM Marketing Intelligence Review*, vol. 9, no. 1, pp. 24–9.

Anwar, M. & Gill, A. 2020, 'Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model', *ACIS 2020 Proceedings*, viewed 18 April 2021, <https://aisel.aisnet.org/acis2020/20>.

Anwar, M., Gill, A. & Beydoun, G. 2019, 'Using Adaptive Enterprise Architecture Framework for Defining the Adaptable Identity Ecosystem Architecture', *ACIS 2019 Proceedings*, viewed 18 April 2021, <https://aisel.aisnet.org/acis2019/94>.

Anwar, M.J. & Gill, A.Q. 2019, 'A review of the seven modelling approaches for digital ecosystem architecture', *Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019*, vol. 1, Institute of Electrical and Electronics Engineers Inc., pp. 94–103.

Anwar, M.J., Gill, A.Q. & Beydoun, G. 2018a, 'A review of information privacy laws and standards for secure digital ecosystems', *ACIS 2018 - 29th Australasian Conference on Information Systems*, viewed 16 November 2020, <https://opus.lib.uts.edu.au/handle/10453/130132>.

Anwar, M.J., Gill, A.Q. & Beydoun, G. 2018b, 'A review of information privacy laws and standards for secure digital ecosystems', *ACIS 2018 - 29th Australasian Conference on Information Systems*, viewed 18 April 2021, <https://opus.lib.uts.edu.au/handle/10453/130132>.

Anwar, M.J., Gill, A.Q. & Beydoun, G. 2019, 'Using Adaptive Enterprise Architecture Framework for Defining the Adaptable Identity Ecosystem Architecture', *Australasian Conference on Information Systems 2019*, pp. 890–900, viewed 26 April 2021, <https://aisel.aisnet.org/acis2019/94/>.

Anwar, M.J., Gill, A.Q., Hussain, F.K. & Imran, M. 2021, 'Secure big data ecosystem architecture: challenges and solutions', *Eurasip Journal on Wireless Communications and Networking*, Springer Science and Business Media Deutschland GmbH, pp. 1–30, viewed 4 July 2021, <https://doi.org/10.1186/s13638-021-01996-2>.

Arnott, D. & Pervan, G. 2008, 'Eight key issues for the decision support systems discipline', *Decision Support Systems*, vol. 44, no. 3, pp. 657–72, viewed 2

May 2021, <www.elsevier.com/locate/dss>.

AUSTRAC 2020, *How to comply with KYC requirements during the COVID-19 pandemic | AUSTRAC*, viewed 18 November 2020, <https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/kyc-requirements-covid-19>.

Australian Government 1980, *OECD Privacy Guidelines - OECD*, viewed 26 April 2021, <https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>.

Privacy Act 1988 1988 (Attorney-General's Department).

Avison, D. & Wood-Harper, T. 1990, *MULTIVIEW: An Exploration in Information Systems Development*, Blackwell Scientific Publications, Oxford.

Aydar, M. & Ayvaz, S. 2019, 'Towards a blockchain based digital identity verification, record attestation and record sharing system', *arXiv*, arXiv.

Ben Ayed, G. 2011, 'Digital identity metadata scheme: A technical approach to reduce digital identity risks', *Proceedings - 25th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2011*, pp. 607–12.

Ben Ayed, G. 2014, *Digital Identity Management*, pp. 57–95.

Azmi, I.M. 2002, 'E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill', *International Review of Law, Computers & Technology*, vol. 16, no. 3, pp. 317–30, viewed 26 April 2021, <http://www.bileta.ac.uk/02papers/madieha.html>.

Banker, R.D. & Kauffman, R.J. 2004, 'The Evolution of Research on Information Systems: A Fiftieth-Year Survey of the Literature in Management Science', *Management Science*, INFORMS Inst.for Operations Res.and the Management Sciences, pp. 281–98, viewed 16 November 2020, <https://pubsonline.informs.org/doi/abs/10.1287/mnsc.1040.0206>.

Barth, S., de Jong, M.D.T., Junger, M., Hartel, P.H. & Roppelt, J.C. 2019, 'Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources', *Telematics and Informatics*, vol. 41, pp. 55–69.

Bartolomeu, P.C., Vieira, E., Hosseini, S.M. & Ferreira, J. 2019, 'Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT', *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, vol. 2019-Septe, Institute of Electrical and Electronics Engineers Inc., pp. 1173–80.

Di Battista, G., Donato, · V Di, Patrignani, · M, Pizzonia, M., Roselli, · V, Tamassia, · R, Pham, V., Donato, V. Di, Vu, O., Valentino, P. & Donato Background, D. 2015, *BitConeView: Visualization of Flows in the Bitcoin Transaction Graph Chicago · U.S.A Background on Bitcoin Bitcoin anonymity BitConeView: Requirements BitConeView: key concepts and metaphors Experiments Evaluation Conclusions and ongoing work*.

Baum, S. 2008, *The psychology of genocide: Perpetrators, bystanders, and rescuers.*, viewed 25 April 2021, <https://psycnet.apa.org/record/2008-11028-000>.

Baumeister, T. 2011, 'Adapting PKI for the smart grid', *2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011*, pp. 249–54, viewed 25 April 2021, <https://www.researchgate.net/publication/254012118>.

Benbasat, I., Goldstein, D.K. & Mead, M. 1987, 'The case research strategy in studies of information systems', *MIS Quarterly: Management Information Systems*, vol. 11, no. 3, pp. 369–86, viewed 23 April 2021, <https://www.jstor.org/stable/248684>.

Benbasat, I. & Weber, R. 1996, 'Research Commentary: Rethinking "Diversity" in

Information Systems Research', *Information Systems Research*, INFORMS Inst.for Operations Res.and the Management Sciences, pp. 389–99, viewed 16 November 2020, <https://pubsonline.informs.org/doi/abs/10.1287/isre.7.4.389>.

Beresford, A.R. & Stajano, F. 2003, 'Location privacy in pervasive computing', *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55.

Berghel, H. 2012, 'Identity theft and financial fraud: Some strangeness in the proportions', *Computer*, vol. 45, no. 1, pp. 86–9.

Bertino, E. 2014, 'Data security - Challenges and research opportunities', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8425 LNCS, Springer Verlag, pp. 9–13, viewed 26 February 2021, <https://link.springer.com/chapter/10.1007/978-3-319-06811-4_2>.

Bertino, E., Lafayette, W., Paci, F., Shang, N. & Ferrini, R. n.d., 'Privacy-preserving Digital Identity Management for Cloud Computing', *Identity*, pp. 1–7, viewed 5 May 2021, <https://www.academia.edu/download/48857081/DataEngBullMarch09CloudComputing.pdf#page=23>.

Bertino, E., Martino, L.D., Paci, F. & Squicciarini, A.C. 2010, *Security for web services and service-oriented architectures*, *Security for Web Services and Service-Oriented Architectures*, viewed 25 April 2021, <https://books.google.com.au/books?hl=en&lr=&id=RYBKAAAAQBAJ&oi=fnd&pg=PP7&dq=Bertino+et+al.+(2009)++digital+identity&ots=wT-7OZ4ouL&sig=SbvqRIJjzeClKpzS3DmxjwEsnFA>.

Bertino, E., Paci, F. & Shang, N. 2009, 'Digital identity protection - concepts and issues', *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*.

Bessani, A., Correia, M., Quaresma, B., Andre, F. & Sousa, P. 2013, 'DepSky: Dependable and secure storage in a cloud-of-clouds', *ACM Transactions on Storage*, vol. 9.

Biegelman, M.T. 2009, 'Identity Theft Handbook: Detection, Prevention, and Security', *Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki*, viewed 25 April 2021, <https://books.google.com.au/books?hl=en&lr=&id=TzJZXIoo4tIC&oi=fnd&pg=PA15&dq=Biegelman,+2009&ots=u7QzS-AyZu&sig=bBUgHvp0VVIx9kyYFZgDjhi-dBY>.

Birks, D.F., Fernandez, W., Levina, N. & Nasirin, S. 2013, 'Grounded theory method in information systems research: Its nature, diversity and opportunities', *European Journal of Information Systems*, Palgrave Macmillan Ltd., pp. 1–8, viewed 23 April 2021, <https://www.tandfonline.com/action/journalInformation?journalCode=tjis20>.

Blockchain and digital identity 2019.

Boley, H. & Chang, E. 2007, 'Digital ecosystems: Principles and semantics', *Proceedings of the 2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference, DEST 2007*, pp. 398–403.

Bou Ghantous, G. & Gill, A.Q. 2021, 'Evaluating the DevOps Reference Architecture for Multi-cloud IoT-Applications', *SN Computer Science*, vol. 2, no. 2, p. 123, viewed 5 July 2021, <https://doi.org/10.1007/s42979-021-00519-6>.

Bouma, T. 2018, 'Digital Identity: A Chain of Claims', *Medium*, viewed 5 May 2021, <https://trbouma.medium.com/digital-identity-a-chain-of-claims-70fee8519d3d>.

Bourass, I., Afifi, N., Belhadaoui, H., Ouzzif, M. & Hilali, R.F. 2014, 'Towards a

new model of management and securing digital identities', *International Conference on Next Generation Networks and Services, NGNS*, pp. 308–12, viewed 25 April 2021, <https://ieeexplore.ieee.org/abstract/document/6990269/>.

Brody, R.G. & Kiehl, K.A. 2010, 'From white-collar crime to red-collar crime', *Journal of Financial Crime*, vol. 17, no. 3, pp. 351–64.

Brown, B., Bughin, J., Chui, M., Dobbs, R., Hung Byers, A., Manyika, J. & Roxburgh, C. 2011, *Big data: The next frontier for innovation, competition, and productivity*, *McKinsey Global Institute*, viewed 25 April 2021, <https://catalog.lib.kyushu-u.ac.jp/ja/recordID/3144682/>.

Brubaker, R. & Cooper, F. 2000, *Beyond 'Identity'*, *Source: Theory and Society*, viewed 25 April 2021, <https://www.jstor.org/stable/3108478>.

Brunetti, F., Matt, D.T., Bonfanti, A., De Longhi, A., Pedrini, G. & Orzes, G. 2020, 'Digital transformation challenges: strategies emerging from a multi-stakeholder approach', *TQM Journal*, vol. 32, no. 4, pp. 697–724.

Buckingham, D. 2008, 'Introducing Identity', *Youth, Identity, and Digital Media*.

Buckingham, R.A., Hirschheim, R.A., Land, F.F. & Tully, C.J. 1987, 'Information Systems Education: Recommendations and Implementation', *British Computer Society Monographs In Informatics*, pp. 204–214, viewed 3 April 2021, <https://dl.acm.org/doi/abs/10.5555/19600>.

Bughin, J., Catlin, T. & Dietz, M. 2019, *The right digital-platform strategy*.

Cameron, K. 2005, 'The Laws of Identity', *Microsoft Corp*, no. May, pp. 8–11, viewed 25 April 2021, <www.identityblog.com>.

Cao, Y. & Yang, L. 2010, 'A survey of Identity Management technology', *Proceedings 2010 IEEE International Conference on Information Theory and Information Security, ICITIS 2010*, pp. 287–93, viewed 25 April 2021, <https://www.researchgate.net/publication/224212196>.

Caplinskas, A. & Vasilecas, O. 2004, 'Information systems research methodologies and models', *Citeseer*, p. 1, viewed 23 April 2021, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.9245&rep=rep1&type=pdf>.

Carvalho, J.Á. 2012, 'VALIDATION CRITERIA FOR THE OUTCOMES OF DESIGN RESEARCH', *IT Artefact Design & Workpractice Intervention*, Barcelona, viewed 18 April 2021, <http://repositorium.sdum.uminho.pt/handle/1822/21713>.

Casino, F., Dasaklis, T.K. & Patsakis, C. 2019, 'A systematic literature review of blockchain-based applications: Current status, classification and open issues', *Telematics and Informatics*, Elsevier Ltd, pp. 55–81.

Casino, F., Kanakaris, V., Dasaklis, T.K., Moschuris, S., Stachtiaris, S., Pagoni, M. & Rachaniotis, N.P. 2020, 'Blockchain-based food supply chain traceability: a case study in the dairy sector', *International Journal of Production Research*, pp. 1–13, viewed 24 April 2021, <https://www.tandfonline.com/doi/abs/10.1080/00207543.2020.1789238>.

Castillo, M. del 2018, 'Big Blockchain: The 50 Largest Public Companies Exploring Blockchain', *Forbes*, 3 July, viewed 16 November 2020, <https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/big-blockchain-the-50-largest-public-companies-exploring-blockchain/?sh=5581a1d22b5b>.

Cavoukian, A. 2010, 'The 7 Foundational Principles', *Identity in the Information Society*, vol. 3, no. 2, pp. 1–12, viewed 26 April 2021, <www.privacybydesign.ca>.

Chai, L. & Pavlou, P. 2002, 'Customer relationship management. com: a cross-cultural empirical investigation of electronic commerce', *AMCIS 2002 Proceedings*, p. 70, viewed 26 April 2021, <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1429&context=amcis2002

>.

Chauhan, S., Agarwal, N. & Kar, A.K. 2016, 'Addressing big data challenges in smart cities: a systematic literature review', *Info*, Emerald Group Publishing Ltd., pp. 73–90.

Check, J. & Schutt, R.K. 2011, *Research Methods in Education*, SAGE Publications (CA).

Cheney, J.S. 2011, 'Identity Theft: Do Definitions Still Matter?', *SSRN Electronic Journal*, viewed 25 April 2021, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=815684>.

Chia Terry 2012, 'Confidentiality, Integrity, Availability: The three components of the CIA Triad « Stack Exchange Security Blog', *Blogoverflow.Com*, viewed 25 April 2021, <https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/>.

Christidis, K. & Devetsikiotis, M. 2016, 'Blockchains and Smart Contracts for the Internet of Things', *IEEE Access*, pp. 2292–303, viewed 25 April 2021, <https://ieeexplore.ieee.org/abstract/document/7467408/>.

Chronéer, D., Johansson, J., Nilsson, M. & Runardotter, M. 2017, 'Digital Platform Ecosystems – From information transactions to collaboration impact', *9th ISPIM Innovation Conference: Composing the Innovation Symphony,* vol. 25, pp. 18–21, viewed 24 April 2021, <www.ispim.org.>.

Clark, A.W. 1972, 'Sanction: A Critical Element in Action Research', *The Journal of Applied Behavioral Science*, vol. 8, no. 6, pp. 713–31.

CNNS 2010, 'National Information Assurance (IA) glossary', *The National Security Systems Instruction*, Committee on National Security Systems, p. 103, viewed 25 April 2021, <https://www.hsdl.org/?abstract&did=>.

Coghlan, D. & Shani, A.B. 2005, 'Roles, politics, and ethics in action research design', *Systemic Practice and Action Research*, pp. 533–46, viewed 2 May

2021, <https://link.springer.com/content/pdf/10.1007/s11213-005-9465-3.pdf>.

Collatto, D.C., Dresch, A., Lacerda, D.P. & Bentz, I.G. 2018, 'Is Action Design Research Indeed Necessary? Analysis and Synergies Between Action Research and Design Science Research', *Systemic Practice and Action Research*, vol. 31, no. 3, pp. 239–67.

Copes, H. & Vieraitis, L.M. 2009, 'Understanding identity theft: Offenders' accounts of their lives and crimes', *Criminal Justice Review*, vol. 34, no. 3, pp. 329–49, viewed 25 April 2021, <http://cjr.sagepub.com/cgi/content/abstract/34/3/329>.

Coughlan, P. & Coghlan, D. 2002, 'Action research for operations management', *International Journal of Operations & Production Management*, vol. 22, no. 2, pp. 144–3577, viewed 2 May 2021, <http://www.emeraldinsight.com/0144-3577.htm>.

Czagan, D. 2019, *Non-Repudiation and Digital Signature [Updated 2018] - Infosec Resources*, viewed 25 April 2021, <https://resources.infosecinstitute.com/topic/non-repudiation-digital-signature/>.

D'Angelo, G., Ferretti, S., Ghini, V. & Panzieri, F. 2011, 'Mobile computing in digital ecosystems: Design issues and challenges', *IWCMC 2011 - 7th International Wireless Communications and Mobile Computing Conference*, pp. 2127–32.

Defranco, J.F., Ferraiolo, D.F., Kuhn, R. & Roberts, J. 2021, 'A Trusted Federated System to Share Granular Data among Disparate Database Resources', *Computer*, vol. 54, no. 3, pp. 55–62.

DeLone, W.H. & McLean, E.R. 1992, 'Information systems success: The quest for the dependent variable', *Information Systems Research*, vol. 3, no. 1, pp. 60–

95, viewed 15 February 2021, <https://pubsonline.informs.org/doi/abs/10.1287/isre.3.1.60>.

Deng, Q. & Ji, S. 2018, 'A Review of Design Science Research in Information Systems: Concept, Process, Outcome, and Evaluation', *Pacific Asia Journal of the Association for Information Systems*, pp. 1–36.

Dennis, A.R. & Valacich, J.S. 2001, 'Conducting Experimental Research in Information Systems', *Communications of the Association for Information Systems*, vol. 7, p. 5, viewed 16 November 2020, <https://aisel.aisnet.org/cais/vol7/iss1/5>.

Der, U., Jähnichen, S. & Sürmeli, J. 2017, 'Self-sovereign Identity $-$ Opportunities and Challenges for the Digital Revolution', *arXiv*, viewed 16 November 2020, <http://arxiv.org/abs/1712.01767>.

Dhamija, R. & Dusseault, L. 2008, 'The seven flaws of identity management: Usability and security challenges', *IEEE Security and Privacy*, vol. 6, no. 2, pp. 24–9, viewed 24 April 2021, <https://ieeexplore.ieee.org/abstract/document/4489846/>.

Dhillon, G. & Backhouse, J. 2001, 'Current directions in IS security research: towards socio-organizational perspectives', *Information Systems Journal*, vol. 11, no. 2, pp. 127–53, viewed 16 November 2020, <https://onlinelibrary.wiley.com/doi/full/10.1046/j.1365-2575.2001.00099.x>.

Dixon, P. 2019, *Digital Identity Ecosystems The Context for Modern Identity*.

Doherty, N.F., Anastasakis, L. & Fulford, H. 2011, 'Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy', *International Journal of Information Management*, vol. 31, no. 3, pp. 201–9, viewed 25 April 2021, <https://www.sciencedirect.com/science/article/pii/S0268401210000873>.

Dong, H., Hussain, F.K. & Chang, E. 2007, 'An Integrative view of the concept of

Digital Ecosystem', *3rd International Conference on Networking and Services,ICNS 2007*.

Dresch, A., Lacerda, D.P. & Antunes, J.A.V. 2015, 'Design Science Research', *Design Science Research*, Springer International Publishing, pp. 67–102.

Drljevic, N., Aranda, D.A. & Stantchev, V. 2020, 'Perspectives on risks and standards that affect the requirements engineering of blockchain technology', *Computer Standards and Interfaces*, vol. 69.

Dunphy, P., Garratt, L. & Petitcolas, F. 2018, 'Decentralizing Digital Identity: Open Challenges for Distributed Ledgers', *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*, Institute of Electrical and Electronics Engineers Inc., pp. 75–8.

Eakin, P.J. 2019, *How Our Lives Become Stories*, Cornell University Press.

Egbo, S. 2018, *The 2016 Dyn DDOS Cyber Attack Analysis: The Attack that Broke the Internet for a Day*, p. 44, viewed 5 May 2021, <https://dl.acm.org/doi/book/10.5555/3279152>.

EIP-725: ERC-725 Smart Contract Based Account n.d., viewed 6 May 2021, <https://eips.ethereum.org/EIPS/eip-725>.

Eisenmann, T., Parker, G. & Van Alstyne, M. 2007, *Platform Networks-Core Concepts Executive Summary Paper 232*, viewed 26 April 2021, <http://digital.mit.edu>.

Ellemers, N., Spears, R. & Doosje, B. 2002, 'Self and social identity', *Annual Review of Psychology*, vol. 53, pp. 161–86, viewed 25 April 2021, <https://psycnet.apa.org/record/2004-00232-000>.

Erramilli, V. 2012, 'The tussle around online privacy', *IEEE Internet Computing*, vol. 16, no. 4, pp. 69–71.

European Commission 2016, 'Payment services (PSD 2) - Directive (EU) 2015/2366 | European Commission', *Europa.eu*, viewed 24 April 2021,

<https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en>.

European Union 2014, 'eIDAS - The Ecosystem', *EU Regulation 910/2014*, viewed 18 April 2021, <https://www.eid.as/>.

European Union 2018, 'General Data Protection Regulation (GDPR) – Official Legal Text', *General Data Protection Regulation*, pp. 1–99, viewed 17 April 2021, <https://gdpr-info.eu/>.

Evernym 2020, *Evernym | The Self-Sovereign Identity Company*, viewed 5 May 2021, <https://www.evernym.com/>.

FATF 2020, *Guidance on Digital ID*.

FBI n.d., *Identity Theft — FBI*, viewed 4 July 2021, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/identity-theft>.

Fernandez, W., Lehmann, H. & Underwood, A. 2002, 'Rigor and Relevance in Studies of IS Innovation: A Grounded Theory Methodology Approach', *ECIS 2002 Proceedings*, viewed 23 April 2021, <https://aisel.aisnet.org/ecis2002/134>.

Fernández, W.D. 2004, 'The grounded theory method and case study data in IS research : issues and design', *Information Systems Foundations: Constructing and Criticising Workshop at The Australian National University2*, no. July 16-17, pp. 43–59, viewed 23 April 2021, <https://www.academia.edu/download/8151849/part-ch05.pdf>.

Fieremans, E., Benitez, A., Jensen, J.H., Falangola, M.F., Tabesh, A., Deardorff, R.L., Spampinato, M.V.S., Babb, J.S., Novikov, D.S., Ferris, S.H. & Helpern, J.A. 2013, 'Novel white matter tract integrity metrics sensitive to Alzheimer disease progression', *American Journal of Neuroradiology*, vol. 34, no. 11, pp. 2105–12, viewed 25 April 2021, <http://dx.doi.org/10.3174/ajnr.A3553>.

Finch, E. 2012, 'What a tangled web we weave: Identity theft and the internet',

Dot.cons: Crime, Deviance and Identity on the Internet, pp. 86–104, viewed 25 April 2021, <www.isbs.com>.

Finklea, K. 2010, *Identity theft: Trends and issues*, viewed 25 April 2021, <https://books.google.com.au/books?hl=en&lr=&id=eM7xRWjJoEUC&oi=fnd&pg=PA1&dq=Finklea,+2010+identity+theft&ots=Gzshkn6rsk&sig=nKqjHQKiCdK7MhOIblmdJC6icC4>.

French, M. 2019, 'Management's Next Frontier - The Digital Ecosystem', *People Love Technology*, viewed <https://www.subscribe-hr.com.au/blog/managements-next-frontier-the-digital-ecosystem>.

Fridgen, G., Guggenmos, F., Lockl, J. & Rieger, A. 2018, 'Challenges and Opportunities of Blockchain-based Platformization of Digital Identities in the Public Sector', *Twenty-Sixth European Conference on Information Systems*.

Friedrichs, D.O. 2019, 'White Collar Crime', *The Handbook of White-Collar Crime*, Wiley, pp. 16–31, viewed 25 April 2021, <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118775004.ch2>.

Garfinkel, S.L. n.d., 'De-Identification of Personal Information', *nvlpubs.nist.gov*, viewed 25 April 2021, <http://dx.doi.org/10.6028/NIST.IR.8053>.

Gartner 2016, *Ecosystems Drive Digital Growth - Smarter With Gartner*, viewed 17 April 2021, <https://www.gartner.com/smarterwithgartner/ecosystems-drive-digital-growth/>.

Gavison, R. 1980, 'Privacy and the Limits of Law', *The Yale Law Journal*, vol. 89, no. 3, p. 421.

Gawer, A. 2009, 'Platforms, markets and innovation: An introduction', *Platforms, Markets and Innovation*, Edward Elgar Publishing, pp. 1–16, viewed 26 April 2021, <https://ideas.repec.org/h/elg/eechap/13257_1.html>.

Gawer, A. & Cusumano, M.A. 2014, 'Industry Platforms and Ecosystem Innovation', *Journal of Product Innovation Management*, vol. 31, no. 3, pp.

417–33, viewed 24 April 2021, <http://doi.wiley.com/10.1111/jpim.12105>.

Ghogare, S., Gupta, D. & Pawar, A. 2021, 'Durable Implementation of Multi-cloud Storage with Assured Integrity for Sensitive Information', *Lecture Notes in Networks and Systems*, vol. 154, Springer Science and Business Media Deutschland GmbH, pp. 793–802.

Gill, A. 2013, 'Towards the Development of an Adaptive Enterprise Service System Model', *AMCIS 2013 Proceedings*, viewed 17 April 2021, <https://aisel.aisnet.org/amcis2013/IntelligentSystems/GeneralPresentations/3>.

Gill, A.Q. 2015, *Adaptive Cloud Enterprise Architecture*, *World Scientic Publishing Co. Pte. Ltd.*Intelligent Information Systems, vol. 4, WORLD SCIENTIFIC, viewed 16 November 2020, <https://www.worldscientific.com/worldscibooks/10.1142/9363>.

Gill, A.Q. 2017, 'Applying agility and living service systems thinking to enterprise architecture', *Decision Management: Concepts, Methodologies, Tools, and Applications*, vol. 1–4, IGI Global, pp. 487–502.

Gill, A.Q., Beydoun, G., Niazi, M. & Khan, H.U. 2021, 'Adaptive architecture and principles for securing the iot systems', *Advances in Intelligent Systems and Computing*, vol. 1195 AISC, Springer, pp. 173–82, viewed 17 April 2021, <https://link.springer.com/chapter/10.1007/978-3-030-50399-4_17>.

Gill, A.Q. & Bunker, D. 2014, 'SaaS requirements engineering for agile development', *Cloud Technology: Concepts, Methodologies, Tools, and Applications*, vol. 2, IGI Global, pp. 660–88, viewed 18 April 2021, <https://opus.lib.uts.edu.au/handle/10453/27483>.

Gill, A.Q. & Chew, E. 2019, 'Configuration information system architecture: Insights from applied action design research', *Information and Management*, vol. 56, no. 4, pp. 507–25.

Glaser, B.G. & Strauss, A.L. 1967, *Discovery of grounded theory: Strategies for qualitative research*, *Discovery of Grounded Theory: Strategies for Qualitative Research*, Aldine Publishing Co, Chicago.

Goes, P.B. 2014, 'Big Data and IS Research [Editor's Comments]', *MIS Quarterly*, vol. 38, no. 3, pp. iii–viii, viewed 2 May 2021, <https://www.jstor.org/stable/26634980>.

Gomi, H. 2011, 'An authentication trust metric for federated identity management systems', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6710 LNCS, pp. 116–31.

Goode, A. 2019, 'Digital identity: solving the problem of trust', *Biometric Technology Today*, vol. 2019, no. 10, pp. 5–8.

Goyal, V., Pandey, O., Sahai, A. & Waters, B. 2006, 'Attribute-based encryption for fine-grained access control of encrypted data', *Proceedings of the ACM Conference on Computer and Communications Security*, ACM Press, New York, New York, USA, pp. 89–98, viewed 16 November 2020, <http://dl.acm.org/citation.cfm?doid=1180405.1180418>.

Graham, I. 2019, *Putting Privacy in Context -- An overview of Current Technologies and the Concept of Privacy*, viewed 26 April 2021, <http://www.iangraham.org/talks/privacy/privacy.html>.

Great Britain. Committee on Privacy . 1990, *Report of the Committee on Privacy and related matters /*, H.M.S.O., London :

Greenspan, G. 2016, 'Understanding zero knowledge blockchains | MultiChain', *Private Blockchains*, viewed 25 April 2021, <https://www.multichain.com/blog/2016/11/understanding-zero-knowledge-blockchains/>.

Gregor, S. & Hevner, A.R. 2013, 'Positioning and presenting design science

research for maximum impact', *MIS Quarterly: Management Information Systems*, pp. 337–55, viewed 24 April 2021, <https://www.jstor.org/stable/43825912>.

Gregor, S., Müller, O. & Seidel, S. 2013, *Association for Information Systems AIS Electronic Library (AISeL) ECIS 2013 Completed Research ECIS 2013 Proceedings Reflection, Abstraction And Theorizing In Design And Development Research Recommended Citation REFLECTION, ABSTRACTION, AND THEORIZING IN*, *Abstraction And Theorizing In Design And Development Research*, viewed 16 November 2020, <http://aisel.aisnet.org/ecis2013_cr/74>.

GSMA 2020, *The Mobile Economy - Asia Pacific*, viewed 25 April 2021, <https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/06/GSMA_MobileEconomy_2020_AsiaPacific.pdf>.

Guba, E.G. & Lincoln, Y.S. 1994, 'Competing paradigms in qualitative research', *Handbook of qualitative research*, vol. 2, Sage, pp. 105–17, viewed 23 April 2021, <http://create.alt.ed.nyu.edu/courses/3311/reading/10-guba_lincoln_94.pdf>.

Gummesson, E. 2000, *Qualitative methods in management research*, viewed 23 April 2021, <https://books.google.com.au/books?hl=en&lr=&id=aBEqkxhd58YC&oi=fnd&pg=PR7&dq=Gummesson+2000+Qualitative+methods+in+management+research&ots=k1suuvu5rQ&sig=1YYkj4FSUNvqUy2XYhH6WOiqf_I>.

Gupta, R., Vathana, D. & Chahar, H. 2020, 'Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage', *International Journal of Advanced Science and Technology*, vol. 29, no. 6, pp. 2697–704, viewed 25 April 2021, <https://ieeexplore.ieee.org/abstract/document/8395433/>.

Gürses, F.S. 2010, 'Multilateral Privacy Requirements Analysis in Online Social Network Services', *Engineering*, no. May, p. 312, viewed 16 November 2020, <https://lirias.kuleuven.be/1655414>.

Hadzic, M. & Chang, E. 2010, 'Application of digital ecosystem design methodology within the health domain', *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, vol. 40, pp. 779–88.

Haj-Bolouri, A., Bernhardsson, L. & Rossi, M. 2016, 'PADRE: A method for participatory action design research', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9661 LNCS, Springer Verlag, pp. 19–36, viewed 18 April 2021, <https://link.springer.com/chapter/10.1007/978-3-319-39294-3_2>.

Haj-Bolouri, A., Purao, S.;, Rossi, M.; & Bernhardsson, L.; 2017, *Action Design Research as a Method-in-Use: Problems and Opportunities*, *cora.ucc.ie*, viewed 18 May 2020, <http://desrist2017.kit.edu/>.

Hakak, S., Kamsin, A., Tayan, O., Idris, M.Y.I. & Gilkar, G.A. 2019, 'Approaches for preserving content integrity of sensitive online Arabic content: A survey and research challenges', *Information Processing and Management*, vol. 56, no. 2, pp. 367–80, viewed 25 April 2021, <https://www.sciencedirect.com/science/article/pii/S0306457316305118>.

Hansen, M., Pfitzmann, A. & Steinbrecher, S. 2008, 'Identity management throughout one's whole life', *Information Security Technical Report*, vol. 13, no. 2, pp. 83–94, viewed 25 April 2021, <https://www.sciencedirect.com/science/article/pii/S1363412708000198>.

Heavin, C. & Power, D.J. 2018a, 'Challenges for digital transformation–towards a conceptual decision support guide for managers', *Journal of Decision Systems*, vol. 27, pp. 38–45, viewed 25 April 2021,

<https://orsociety.tandfonline.com/doi/abs/10.1080/12460125.2018.1468697>.

Heavin, C. & Power, D.J. 2018b, 'Challenges for digital transformation–towards a conceptual decision support guide for managers', *Journal of Decision Systems*, vol. 27, pp. 38–45.

Heiss, J., Ulbricht, M.R. & Eberhardt, J. 2020, 'Put Your Money Where Your Mouth Is - Towards Blockchain-based Consent Violation Detection', *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020*, Institute of Electrical and Electronics Engineers Inc.

Henriette, E., Feki, M. & Boughzala, I. 2016, *Association for Information Systems AIS Electronic Library (AISeL) Digital Transformation Challenges Recommended Citation*, *Digital Transformation Challenges*, viewed 25 April 2021, <http://aisel.aisnet.org/mcis2016http://aisel.aisnet.org/mcis2016/33>.

Hevner, A. 2004, *Design Science in Information Systems Research*, *JSTOR*, viewed 24 April 2021, <https://www.researchgate.net/publication/201168946>.

Hevner, A.R., March, S.T., Park, J. & Ram, S. 2004, 'Design science in information systems research', *MIS Quarterly: Management Information Systems*, vol. 28, no. 1, pp. 75–105.

Hileman, G. & Rauchs, M. 2018, '2017 Global Blockchain Benchmarking Study', *SSRN Electronic Journal*.

Hilpert, H., Beckers, C., Kolbe, L.M. & Schumann, M. 2013, 'Green IS for GHG emission reporting on product-level? An action design research project in the meat industry', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7939 LNCS, pp. 324–39.

Holt & Malčić 2015, 'The Privacy Ecosystem: Regulating Digital Identity in the United States and European Union', *Journal of Information Policy*, vol. 5, p.

155.

Holt, T.J. & Turner, M.G. 2012, 'Examining Risks and Protective Factors of On-Line Identity Theft', *Deviant Behavior*, vol. 33, no. 4, pp. 308–23.

House, W. & America, U.S. of 2011, 'National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy', *ncjrs.gov*, viewed 25 April 2021, <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=256928>.

Hu, F., Hu, J., Wang, W. & Wang, Y. 2014, 'Design identity system based on product identity and its case studies', *2013 IEEE-Tsinghua International Design Management Symposium: Design-Driven Business Innovation, TIDMS 2013 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., pp. 192–9.

Huhtamäki, J. 2016, 'Visualizing co-authorship networks for actionable insights Visualizing Co-authorship Networks for Actionable Insights: Action Design Research Experiment', *dl.acm.org*, pp. 208–15, viewed 24 April 2021, <https://doi.org/10.1145/2994310.2994340>.

Huo, Y., Meng, C., Li, R. & Jing, T. 2020, 'An overview of privacy preserving schemes for industrial Internet of Things', *China Communications*, vol. 17, no. 10, pp. 1–18.

Hyndman, R.J. 2008, 'Quantitative business research methods', *Department of Econometrics and Business Statistics,Monash University, Melbourne, Vic*.

Iansiti, M. & Levien, R. 2004, 'Strategy as Ecology', *Harvard Business Review*, vol. 82, no. 3, pp. 68–81, viewed 24 April 2021, <https://europepmc.org/article/med/15029791>.

ID-card — e-Estonia n.d., viewed 6 May 2021, <https://e-estonia.com/solutions/e-identity/id-card/>.

ID2020 | Digital Identity Alliance n.d., viewed 6 May 2021, <https://id2020.org/>.

Identity Verification by Civic - Know-Your-Customer KYC for Business n.d., viewed 5 May 2021, <https://www.civic.com/>.

Iivari, J. 2014, 'ISSUES AND OPINION Distinguishing and contrasting two strategies for design science research', *European Journal of Information Systems*, vol. 24, no. 1, pp. 107–15, viewed 24 April 2021, <www.palgrave-journals.com/ejis/>.

Iivari, J. & Venable, J. 2009, 'Action research and design science research - Seemingly similar but decisively dissimilar', *ECIS 2009 Proceedings*, viewed 2 May 2021, <https://aisel.aisnet.org/ecis2009/73>.

iiw 2020 | iiw On-line Annual Assembly - July 15/25 n.d., viewed 25 April 2021, <https://iiw2020.online/>.

ISO 1989, *ISO 7498-2:1989(en), Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*, viewed 25 April 2021, <https://www.iso.org/standard/14256.html>.

ISO 2015, *ISO - ISO/IEC 27001 — Information security management*, viewed 17 April 2021, <https://www.iso.org/isoiec-27001-information-security.html>.

Jacobides, M.G., Sundararajan, A. & Van Alstyne, M.W. 2019, 'Platforms and Ecosystems: Enabling the Digital Economy', *World Economic Forum Briefing Paper*, no. February, pp. 13–8, viewed 24 April 2021, <www.weforum.org>.

Jacobovitz, O. 2016, 'Blockchain for identity management', *Technical Report*, no. 1, pp. 1–19, viewed 24 April 2021, <https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf>.

Jain, A. & Kumar, R. 2016, 'Confidentiality enhanced security model for cloud environment', *ACM International Conference Proceeding Series*, vol. 04-05-March-2016, Association for Computing Machinery, New York, New York, USA, pp. 1–6, viewed 25 April 2021, <http://dl.acm.org/citation.cfm?doid=2905055.2905199>.

Jamieson, R., Land, L., Stephens, G. & Winchester, D. 2008, 'Identity crime: the need for an appropriate government strategy', *Forum on Public Policy: A Journal of the Oxford Round Table*, viewed 24 April 2021, <https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=1556763X&v=2.1&it=r&id=GALE%7CA197721349&sid=googleScholar&linkaccess=fulltext>.

Johnson, J. 2021, *Worldwide digital population as of January 2021*, viewed 25 April 2021, <https://www.statista.com/statistics/617136/digital-population-worldwide/>.

Jones, P., Clarke-Hill, C., Comfort, D., Hillier, D. & Shears, P. 2004, 'Radio frequency identification in retailing and privacy and public policy issues', *Management Research News*, vol. 27, no. 8–9, pp. 46–56.

Jordan, K., Hauser, J. & Foster, S. 2003a, 'The augmented social network: Building identity and trust into the next-generation internet', *First Monday*, vol. 8, no. 8.

Jordan, K., Hauser, J. & Foster, S. 2003b, 'The augmented social network: Building identity and trust into the next-generation internet', *First Monday*, vol. 8, no. 8, viewed 25 April 2021, <http://firstmonday.org/ojs/index.php/fm/article/view/1068>.

Joshi, H. 2017, *Security and Privacy in the Digital World*, Deloitte, viewed 17 April 2021, <https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/security-and-privacy-noexp.pdf>.

Jumio: End-to-End ID and Identity Verification Solutions n.d., viewed 5 May 2021, <https://www.jumio.com/>.

Kanyengo, C.W. 2009, 'Managing digital information resources in Africa: Preserving the integrity of scholarship', *International Information and Library Review*, vol. 41, no. 1, pp. 34–43.

Kar, S., Chakravorty, B., Sinha, S. & Gupta, M.P. 2018, 'Analysis of Stakeholders Within IoT Ecosystem', *Digital India*, Springer, Cham, pp. 251–76, viewed 24 April 2021, <https://link.springer.com/chapter/10.1007/978-3-319-78378-9_15>.

Keijzer-Broers, W., Florez-Atehortua, L. & De Reuver, M. 2016, 'Prototyping a health and wellbeing platform: An action design research approach', *Proceedings of the Annual Hawaii International Conference on System Sciences*, vol. 2016-March, HICSS, pp. 3462–71, viewed 24 April 2021, <https://ieeexplore.ieee.org/abstract/document/7427616/>.

Kemmis, S. & McTaggart, R. 1988, *The Action research planner*, 3rd edn, Waurn Ponds, Vic., Melbourne.

Koops, B.-J. & Leenes, R. 2006, 'Identity theft, identity fraud and/or identity-related crime', *Datenschutz und Datensicherheit - DuD*, vol. 30, no. 9, pp. 553–6, viewed 25 April 2021, <https://www.researchgate.net/publication/257703479>.

Kroger, J. 2007, 'Why is identity achievement so elusive?', *Identity*, vol. 7, pp. 331–48.

Kshetri, N. 2014, 'Big datas impact on privacy, security and consumer welfare', *Telecommunications Policy*, vol. 38, no. 11, pp. 1134–45.

Kshetri, N. 2017, 'Can Blockchain Strengthen the Internet of Things?', *IT Professional*, vol. 19, no. 4, pp. 68–72.

Kumar, R. & Bhatia, M.P.S. 2020, 'A systematic review of the security in cloud computing: Data integrity, confidentiality and availability', *2020 IEEE International Conference on Computing, Power and Communication Technologies, GUCON 2020*, Institute of Electrical and Electronics Engineers Inc., pp. 334–7.

Kuperberg, M. 2020a, 'Towards Enabling Deletion in Append-Only Blockchains

to Support Data Growth Management and GDPR Compliance', *Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020*, pp. 393–400, viewed 26 April 2021, <http://arxiv.org/abs/0712.4102>.

Kuperberg, M. 2020b, 'Towards Enabling Deletion in Append-Only Blockchains to Support Data Growth Management and GDPR Compliance', *Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020*, Institute of Electrical and Electronics Engineers Inc., pp. 393–400.

Kvitnitsky, A. 2018, 'GSMA | Digital Identity: Crucial for the Success of Today's Mobile-First World - Identity', *GSMA*, viewed 25 April 2021, <https://www.gsma.com/identity/digital-identity-crucial-for-the-success-of-todays-mobile-first-world>.

L'Amrani, H., Berroukech, B.E., El Bouzekri El Idrissi, Y. & Ajhoun, R. 2016, 'Identity management systems: Laws of identity for models7 evaluation', *Colloquium in Information Science and Technology, CIST*, vol. 0, Institute of Electrical and Electronics Engineers Inc., pp. 736–40.

Lafuente, G. 2015, 'The big data security challenge', *Network security*, vol. 2015, no. 1, pp. 12–4.

Langheinrich, M. 2001, 'Privacy by design - Principles of privacy-aware ubiquitous systems', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2201, Springer Verlag, pp. 273–91.

Le, D.P., Meng, H., Su, L., Yeo, S.L. & Thing, V. 2019, 'BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy', *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, vol. 2018-Octob, pp. 2372–7, viewed 25 April 2021, <https://www.researchgate.net/publication/331847470>.

Leary, M. & Tangney, J. 2011, *Handbook of self and identity*, viewed 25 April

2021, <https://books.google.com.au/books?hl=en&lr=&id=VukSQuVMQy0C&oi=fnd&pg=PP1&dq=Leary+and+Tangney+2012&ots=L1K-jDgsdB&sig=NmUY4d_Br4_i4U2yomfdxFlcQhY>.

Lee, D., Park, N., Kim, G. & Jin, S. 2018, 'De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment', *Peer-to-Peer Networking and Applications*, vol. 11, no. 6, pp. 1299–308.

Lempinen, H., Rossi, M. & Tuunainen, V.K. 2012, 'Design principles for inter-organizational systems development - Case Hansel', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7286 LNCS, pp. 52–65.

Li, C. & Palanisamy, B. 2019, 'Privacy in Internet of Things: From Principles to Technologies', *IEEE Internet of Things Journal*, Institute of Electrical and Electronics Engineers Inc., pp. 488–505.

Liberty Alliance Project 2008, *Home - Liberty Alliance*, viewed 25 April 2021, <http://www.projectliberty.org/>.

LoPucki, L.M. 2001, 'Human Identification Theory and the Identity Theft Problem', *Texas Law Review*, vol. 80, no. 1, viewed 25 April 2021, <https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tlr80&section=12>.

Lourinho, L., Kendzierskyj, S. & Jahankhani, H. 2021, 'Securing the digital witness identity using blockchain and zero-knowledge proofs', *Strategy, Leadership, and AI in the Cyber Ecosystem*, Elsevier, pp. 159–94.

Lyons, T., Courcelas, L. & Timsit, K. 2019, *Thematic Report 1 Blockchain and digital identity BLOCKCHAIN AND DIGITAL IDENTIT Y An initiative of the*.

Maccani, G., Donnellan, B. & Helfert, M. 2014, 'Action design research in

practice: The case of Smart Cities', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8463 LNCS, Springer Verlag, pp. 132–47.

Madhuri, M., Gill, A.Q. & Khan, H.U. 2020, 'IoT-enabled smart child safety digital system architecture', *Proceedings - 14th IEEE International Conference on Semantic Computing, ICSC 2020*, Institute of Electrical and Electronics Engineers Inc., pp. 166–9.

Maler, E. & Reed, D. 2008, *The Venn of Identity: Options and Issues in Federated Identity Management*, *IEEE Security & Privacy*, viewed 25 April 2021, <www.computer.org/security/>.

Malik, A.A., Anwar, H. & Shibli, M.A. 2016, 'Federated Identity Management (FIM): Challenges and opportunities', *Proceedings - 2015 Conference on Information Assurance and Cyber Security, CIACS 2015*, pp. 75–82, viewed 25 April 2021, <https://ieeexplore.ieee.org/abstract/document/7395570/>.

March, S.T. & Smith, G.F. 1995, *Design and natural science research on information technology*, *Decision Support Systems*, viewed 24 April 2021, <https://www.sciencedirect.com/science/article/pii/0167923694000412>.

Marsh, I., Cochrane, J. & Melville, G. 2004, *Criminal justice: An introduction to philosophies, theories and practice*, *Criminal Justice: An Introduction to Philosophies, Theories and Practice*, viewed 25 April 2021, <https://books.google.com.au/books?hl=en&lr=&id=Awsv2mPabl4C&oi=fnd&pg=PR7&dq=Marsh+I,+Cochrane+J+%26+Melville+G+2004.+Criminal+justice:+An+introduction+to+philosophies,+theories+and+practice.+London:+Routledge&ots=T46zimDbVi&sig=_o-0AtqqHdjrMDhuG6qcq5hBoe>.

Martin, P.Y. & Turner, B.A. 1986, 'Grounded Theory and Organizational Research', *The Journal of Applied Behavioral Science*, vol. 22, no. 2, pp. 141–57.

Matavire, R. & Brown, I. 2013, 'Profiling grounded theory approaches in information systems research', *European Journal of Information Systems*, vol. 22, no. 1, pp. 119–29.

Matthews, B.W. & Esterline, A. 2010, 'Personally identifiable information: Identifying unprotected PII using file-indexing search tools and quantitative analysis', *Conference Proceedings - IEEE SOUTHEASTCON*, pp. 360–2.

Mayfield, T., Roskos, J.E., Welke, S.R. & Boone, J.M. 1991, *Integrity in Automated Information Systems*, viewed 25 April 2021, <https://apps.dtic.mil/sti/citations/ADA253990>.

McCallister, E., Grance, T. & Kent, K. 2010, 'Guide to protecting the confidentiality of personally identifiable information (PII)', *Special Publication 800-122 Guide*, pp. 1–59.

Meng, M. & Agarwal, R. 2007, 'Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities', *Information Systems Research*, vol. 18, no. 1, pp. 42–67.

Miah, S.J. & Gammack, J.G. n.d., *ENSEMBLE ARTIFACT DESIGN FOR CONTEXT SENSITIVE DECISION SUPPORT*, *Australasian Journal of Information Systems*, viewed 24 April 2021, <http://journal.acs.org.au/index.php/ajis/article/view/898>.

Modern identity from cloud to ground | Okta n.d., viewed 5 May 2021, <https://www.okta.com/discover/okta-for-worlds-largest-organizations/?utm_campaign=search_google_apac_anz_ao_it_branded-okta_exact&utm_medium=cpc&utm_source=google&utm_term=okta&utm_page=%7Burl%7D&gclid=Cj0KCQjw4cOEBhDMARIsAA3XDRjJ_VBKZR3NsREYZyfo81uG0p49qzH1IeWQbz0OpKxi3V4518yxMgMaAj8iEALw_wcB>.

Moshman, D. 2007, 'Social identity and its discontents', *Journal of Applied*

Developmental Psychology, vol. 28, no. 2, pp. 184–7, viewed 25 April 2021, <https://digitalcommons.unl.edu/edpsychpapers>.

Mukta, R., Martens, J., Paik, H.Y., Lu, Q. & Kanhere, S.S. 2020, 'Blockchain-based verifiable credential sharing with selective disclosure', *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, Institute of Electrical and Electronics Engineers Inc., pp. 959–66.

Munir, A.B., Hajar, S., Yasin, M. & Muhammad-Sukki, F. 2015, 'Big Data Big Challenges to Privacy and Data Protection Developing "National Human Rights Action Plan" View project Blockchain Based Regulatory Framewrok View project', *International Scholarly and Scientific Research & Innovation*, p. 9, viewed 28 February 2021, <https://www.researchgate.net/publication/273441105>.

Mustafa, M.I. & Sjöström, J. 2013, 'Design principles for research data export: Lessons learned in e-Health design research', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7939 LNCS, pp. 34–49.

N. Otto, S. Lee, B. Sletten, D. Burnett, M. Sporny, and K.E. 2019, 'Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web', *W3C Recommendation 19 November 2019*, viewed 25 April 2021, <https://uidl.naswa.org/handle/20.500.11941/3138_Verifiable-Credentials-Data-Model>.

Naik, N. & Jenkins, P. 2020, 'Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems', *ISSE 2020 - 6th IEEE International Symposium on Systems Engineering, Proceedings*, Institute of Electrical and Electronics Engineers Inc.

Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, viewed 17 April 2021, <www.bitcoin.org>.

Nambisan, S., Wright, M. & Feldman, M. 2019, 'The digital transformation of innovation and entrepreneurship: Progress, challenges and key themestechnological-forecasting-and-social-change/call-for-papers/the-entrepreneurial-university-as-driver-for-economic-growth View project Innovation, intellectual property and technology management in biotechnology and talent mobility View project The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes', *Research Policy*, vol. 48, p. 103773, viewed 25 April 2021, <https://www.sciencedirect.com/science/article/pii/S0048733319300812>.

Narayanan, A. & Shmatikov, V. 2008, 'Robust de-anonymization of large sparse datasets', *Proceedings - IEEE Symposium on Security and Privacy*, pp. 111–25.

Neira, R.E. & Capstone, A. 2016, *IDENTITY THEFT: INSIDE THE MIND OF A CYBERCRIMINAL*, viewed 25 April 2021, <https://search.proquest.com/openview/912fc0d5c5c4fd6424c93f40e1b5c70c/1?pq-origsite=gscholar&cbl=18750&diss=y>.

Nischak, F. & Hanelt, A. 2019, 'Ecosystem change in the era of digital innovation - A longitudinal analysis and visualization of the automotive ecosystem', *40th International Conference on Information Systems, ICIS 2019*, viewed 3 April 2021, <https://www.researchgate.net/profile/Fabian_Nischak/publication/336304756_Ecosystem_Change_in_the_Era_of_Digital_Innovation_-_A_Longitudinal_Analysis_and_Visualization_of_the_Automotive_Ecosystem/links/5d9ae94aa6fdccfd0e7f06d5/Ecosystem-Change-in-the-Era->.

NSTIC 2011, 'National Strategy for Trusted Identities in Cyberspace', *Online*, p.

25, viewed 25 April 2021, <https://iiw.idcommons.net/images/c/c8/NSTIC_Fact_Sheet.pdf>.

Nuñez, D., Agudo, I. & Lopez, J. 2015, 'Privacy-preserving Identity Management as a Service', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8937, Springer Verlag, pp. 114–25.

OAIC 2017, *What is personal information?*, viewed 26 April 2021, <https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/>.

Oh, H., Kim, J. & Shin, J.S. 2018, 'Forward-secure ID based digital signature scheme with forward-secure private key generator', *Information Sciences*, vol. 454–455, pp. 96–109.

OMB 2020, 'Office of Management and Budget | The White House', *The White House*, viewed 26 April 2021, <https://www.whitehouse.gov/omb/>.

Onik, M.M.H., Al-Zaben, N., Yang, J., Lee, N.Y. & Kim, C.S. 2019, 'Risk Identification of Personally Identifiable Information from Collective Mobile App Data', *Proceedings - 2018 International Conference on Computing, Electronics and Communications Engineering, iCCECE 2018*, Institute of Electrical and Electronics Engineers Inc., pp. 71–6.

Oppenheim, B., Gallivan, M., Madhav, N.K., Brown, N., Serhiyenko, V., Wolfe, N.D. & Ayscue, P. 2019, 'Assessing global preparedness for the next pandemic: Development and application of an Epidemic Preparedness Index', *BMJ Global Health*, vol. 4, no. 1, p. 1157, viewed 16 November 2020, <http://gh.bmj.com/>.

Orlikowski, W.J. 1993, 'CASE tools as organizational change: Investigating incremental and radical changes in systems development', *MIS Quarterly: Management Information Systems*, vol. 17, no. 3, pp. 309–40.

Orlikowski, W.J. & Baroudi, J.J. 1991, 'Studying information technology in organizations: Research approaches and assumptions', *Information Systems Research*, vol. 2, no. 1, pp. 1–28.

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A. & Sinz, E.J. 2011, 'Memorandum on design-oriented information systems research', *European Journal of Information Systems*, Palgrave Macmillan Ltd., pp. 7–10, viewed 2 May 2021, <https://orsociety.tandfonline.com/doi/abs/10.1057/ejis.2010.55>.

Othman, A. & Callahan, J. 2018, 'The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity', *Proceedings of the International Joint Conference on Neural Networks*, vol. 2018-July, Institute of Electrical and Electronics Engineers Inc.

Paetsch, F., Eberlein, A. & Maurer, F. 2003, 'Requirements engineering and agile software development', *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*, vol. 2003-Janua, IEEE Computer Society, pp. 308–13.

Palvia, P. 2009, 'The role of trust in e-commerce relational exchange: A unified model', *Information and Management*, vol. 46, no. 4, pp. 213–20, viewed 26 April 2021, <http://www.elsevier.com>.

Pawczuk, L., Massey, R. & Schatsky, D. 2018, *Breaking blockchain open*, *Nippon Ronen Igakkai Zasshi. Japanese Journal of Geriatrics*, viewed 24 April 2021, <https://www2.deloitte.com/uk/en/pages/innovation/articles/global-blockchain-survey-2018.html>.

Peffers, K., Tuunanen, T., Rothenberger, M.A. & Chatterjee, S. n.d., *A Design Science Research Methodology for Information Systems Research*, *Journal of Management Information Systems*, viewed 11 April 2021, <http://www.tuunanen.fi.>.

Peng, Y., Chen, W., Chang, J.M. & Guan, Y. 2010, 'Secure online banking on untrusted computers', *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 720–2.

Personal Identity Verification for COVID-19 Vaccinations and Test Results | Project COVID Freedom n.d., viewed 5 May 2021, <https://www.shocard.com/>.

PETER BUTTLER 2017, '10 CHALLENGES TO BIG DATA SECURITY AND PRIVACY', *Dataconomy*, viewed 26 February 2020, <https://dataconomy.com/2017/07/10-challenges-big-data-security-privacy/>.

Petullo, W.M. & Solworth, J.A. 2011, 'Digital identity security architecture in Ethos', *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 23–30.

Pfleeger, C.P., Lawrence Pfleeger, S. & Margulies, J. 1997, *Security in Computing* , 5th edn.

Phelps, J., Nowak, G. & Ferrell, E. 2000, 'Privacy Concerns and Consumer Willingness to Provide Personal Information', *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 27–41, viewed 26 April 2021, <http://journals.sagepub.com/doi/10.1509/jppm.19.1.27.16941>.

Phiri, J. & Agbinya, J.I. 2006, 'Modelling and information fusion in digital identity management systems', *Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies,ICN/ICONS/MCL'06*, vol. 2006, pp. 181–6, viewed 17 April 2021, <https://www.researchgate.net/publication/224633733>.

Pilton, C., Faily, S. & Henriksen-Bulmer, J. 2021, 'Evaluating privacy - determining user privacy expectations on the web', *Computers and Security*, vol. 105.

Pimenidis, E. 2010, 'Digital identity management', *Handbook of Electronic Security and Digital Forensics*, World Scientific Publishing Co., pp. 279–94.

Poelman, M. & Iqbal, S. 2021, 'Investigating the compliance of the GDPR: Processing personal data on a blockchain', *2021 IEEE 5th International Conference on Cryptography, Security and Privacy, CSP 2021*, Institute of Electrical and Electronics Engineers Inc., pp. 38–44.

Pranata, I., Skinner, G. & Athauda, R. 2011, 'A distributed mechanism for secure collaboration in Digital Ecosystems', *Proceedings of the International Conference on Management of Emergent Digital EcoSystems, MEDES'11*, pp. 33–9.

Priesnitz, J., Rathgeb, C., Buchmann, N., Busch, C. & Margraf, M. 2021, 'An overview of touchless 2D fingerprint recognition', *Eurasip Journal on Image and Video Processing*, Springer Science and Business Media Deutschland GmbH.

Privacy International 2017, *What Is Privacy?*, viewed 26 April 2021, <https://privacyinternational.org/explainer/56/what-privacy>.

Prosser, W.L. 1960, 'Privacy', *California Law Review*, vol. 48, no. 3, p. 383, viewed 17 April 2021, <https://www.jstor.org/stable/3478805?origin=crossref>.

PWC 2019, *Digital identity- Your key to unlock digital transformation*, *Digital Identity*, viewed 25 April 2021, <https://www.pwc.ch/en/publications/2019/digital-identity-whitepaper-web.pdf>.

Radhakrishnan, R., Kharrazi, M. & Memon, N. 2005, 'Data Masking: A New Approach for Steganography?', *Journal of VLSI Signal Processing*, vol. 41, no. 3 SPEC. ISS., pp. 293–303, viewed 25 April 2021, <https://link.springer.com/article/10.1007/s11265-005-4153-1>.

Raji, F., Jazi, M.D. & Miri, A. 2015, 'PESCA: A peer-to-peer social network architecture with privacy-enabled social communication and data availability', *IET Information Security*, vol. 9, no. 1, pp. 73–80.

Raju, S. & Sirajudeen, Y.M. 2014, 'Data security in cloud computing using cramer - Shoup cryptosystem', *Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014*, pp. 343–6, viewed 25 April 2021, <https://www.researchgate.net/publication/271207703>.

Rana, R., Zaeem, R.N. & Suzanne Barber, K. 2018, 'US-Centric vs. International Personally Identifiable Information: A Comparison Using the UT CID Identity Ecosystem', *Proceedings - International Carnahan Conference on Security Technology*, vol. 2018-October, Institute of Electrical and Electronics Engineers Inc.

Randa, R. & Reyns, B.W. 2020, 'The Physical and Emotional Toll of Identity Theft Victimization: A Situational and Demographic Analysis of the National Crime Victimization Survey', *Deviant Behavior*, vol. 41, no. 10, pp. 1290–304.

Rapoport, R.N. 1970, 'Three Dilemmas in Action Research:With Special Reference to the Tavistock Experience', *Human Relations*, vol. 23, no. 6, pp. 499–513.

Reed, D., Sporny, M. & Allen, C. 2019, 'Decentralized Identifiers (DIDs) v1.0', *W3C*, no. November, pp. 1–56, viewed 25 April 2021, <https://www.w3.org/TR/2019/WD-did-core-20191107/>.

Renaud, K. & Gálvez-Cruz, D. 2010, 'Privacy: Aspects, definitions and a multi-faceted privacy preservation approach', *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*.

Reyns, B.W. 2013, 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses', *Journal*

of Research in Crime and Delinquency, vol. 50, no. 2, pp. 216–38.

Rivera, R., Robledo, J.G., Larios, V.M. & Avalos, J.M. 2017, 'How digital identity on blockchain can contribute in a smart city environment', *2017 International Smart Cities Conference, ISC2 2017*, Institute of Electrical and Electronics Engineers Inc.

Rogerson, C. & Scott, E. 2014a, 'Motivating an action design research approach to implementing online training in an organisational context', *Interactive Technology and Smart Education*, vol. 11, no. 1, pp. 15–31.

Rogerson, C. & Scott, E. 2014b, 'Motivating an action design research approach to implementing online training in an organisational context', *Interactive Technology and Smart Education*, vol. 11, no. 1, pp. 15–31.

Romme, A.G.L. 2003, 'Making a Difference: Organization as Design', *Organization Science*, vol. 14, no. 5, pp. 558–73.

Roxana MOSTEANU, N. & Faccia, A. n.d., 'Digital Systems and New Challenges of Financial Management – FinTech, XBRL, Blockchain and Cryptocurrencies', *Journal of Management Systems-Quality Access to success*, vol. 21, no. 174, pp. 159–66, viewed 24 April 2021, <https://dx.doi.org/>.

Ruballo, Á.H.Z. 2018, 'Application for digital signature and generation of certificates using the Bouncy Castle API considering digital signature law in El Salvador', *Proceedings of the 2018 IEEE 38th Central America and Panama Convention, CONCAPAN 2018*, viewed 25 April 2021, <https://ieeexplore.ieee.org/abstract/document/8596612/>.

Runeson, P. & Höst, M. 2009a, 'Guidelines for conducting and reporting case study research in software engineering', *Empirical Software Engineering*, vol. 14, no. 2, pp. 131–64, viewed 24 April 2021, <https://link.springer.com/article/10.1007/s10664-008-9102-8>.

Runeson, P. & Höst, M. 2009b, 'Guidelines for conducting and reporting case

study research in software engineering', *Empirical Software Engineering*, vol. 14, no. 2, pp. 131–64, viewed 16 November 2020, <https://link.springer.com/article/10.1007/s10664-008-9102-8>.

Sahai, A. & Waters, B. 2005, 'Fuzzy identity-based encryption', *Lecture Notes in Computer Science*, vol. 3494, Springer Verlag, pp. 457–73, viewed 16 November 2020, <https://link.springer.com/chapter/10.1007/11426639_27>.

Sandhu, R.S. 1994, *On five definitions of data integrity*, *IFIP Transactions A: Computer Science and Technology*, viewed 25 April 2021, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.53.903&rep=rep1&type=pdf>.

Saroj, S.K., Chauhan, S.K., Sharma, A.K. & Vats, S. 2015, 'Threshold cryptography based data security in cloud computing', *Proceedings - 2015 IEEE International Conference on Computational Intelligence and Communication Technology, CICT 2015*, Institute of Electrical and Electronics Engineers Inc., pp. 202–7.

Sbir.gov 2015, *Applicability of Blockchain Technology to Privacy Respecting Identity Management | SBIR.gov*, viewed 25 April 2021, <https://www.sbir.gov/sbirsearch/detail/867797>.

Schacht, S. & Mädche, A. 2013, 'How to prevent reinventing the wheel? - Design principles for project knowledge management systems', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7939 LNCS, pp. 1–17, viewed 24 April 2021, <https://www.researchgate.net/publication/262255730>.

Schildkraut, D.J. 2007, 'Defining American identity in the twenty-first century: How much "there" is there?', *Journal of Politics*, vol. 69, no. 3, pp. 597–615.

Schmitz, J.A. 1996, 'The Role Played by Public Enterprises: How Much Does It Differ Across Countries?', *Quarterly Review*, vol. 20, no. 2.

Schreft, S. 2007, 'Risks of Identity Theft: Can the Market Protect the Payment System?', *Economic Review Federal Reserve Bank of Kansas City*, vol. 92, no. 4, p. 5, viewed 25 April 2021, <www.KansasCityFed.org.>.

Schwartz, P.M. & Solove, D.J. 2011, 'The PII problem: Privacy and a new concept of personally identifiable information', *New York University Law Review*, vol. 86, no. 6, pp. 1814–94, viewed 26 April 2021, <http://www.gallup.com/poll/145337/>.

Schwartz, S.J., Dunkel, C.S. & Waterman, A.S. 2009, 'Terrorism: An Identity Theory Perspective Venezuelan Migrants View project Multisite School-Based Evaluation of a Brief Screener for Underage Drinking View project', *Taylor & Francis*, vol. 32, no. 6, pp. 537–59, viewed 25 April 2021, <https://www.researchgate.net/publication/225029149>.

SecureKey: Building Trusted Identity Networks n.d., viewed 6 May 2021, <https://securekey.com/>.

Seidel, S. & Urquhart, C. 2016, 'On emergence and forcing in information systems grounded theory studies: The case of strauss and corbin', *Enacting Research Methods in Information Systems: Volume 1*, Springer International Publishing, pp. 157–209, viewed 23 April 2021, <https://link.springer.com/chapter/10.1007/978-3-319-29266-3_8>.

Seigneur, J.M. 2005, 'Demonstration of security through collaboration in the digital business ecosystem', *Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005*, vol. 2005, IEEE Computer Society, pp. 108–9.

Sein, M.K., Henfridsson, O., Purao, S., Rossi, M. & Lindgren, R. 2011, 'Action design research', *MIS Quarterly: Management Information Systems*, vol. 35, no. 1, pp. 37–56.

Sekhar, V.C. & Sarvabhatla, M. 2012, 'Secure lightweight mobile payment

protocol using symmetric key techniques', *2012 International Conference on Computer Communication and Informatics, ICCCI 2012*, viewed 25 April 2021, <https://ieeexplore.ieee.org/abstract/document/6158876/>.

Senyo, P.K., Liu, K. & Effah, J. 2019, 'Digital business ecosystem: Literature review and a framework for future research', *International Journal of Information Management*, pp. 52–64, viewed 26 April 2021, <https://doi.org/10.1016/j.ijinfomgt.2019.01.002>.

Shaw, G. 2000, 'Digital document integrity', *IEE Colloquium (Digest)*, pp. 95–8, viewed 25 April 2021, <https://digital-library.theiet.org/content/conferences/10.1049/ic_20000223>.

Shehu, A.S., Pinto, A. & Correia, M.E. 2019, 'Privacy preservation and mandate representation in identity management systems', *Iberian Conference on Information Systems and Technologies, CISTI*, vol. 2019-June, IEEE Computer Society.

Sinha, G. 2018, 'Governance, risk and compliance: 2018 trends and predictions | ITProPortal', *ITProPortal*, viewed 24 April 2021, <https://www.itproportal.com/features/governance-risk-and-compliance-2018-trends-and-predictions/>.

Sjøberg, D.I.K., Hannay, J.E., Hansen, O., Kampenes, V.B., Karahasanović, A., Liborg, N.K. & Rekdal, A.C. 2005, 'A survey of controlled experiments in software engineering', *IEEE Transactions on Software Engineering*, vol. 31, no. 9, pp. 733–53.

Smith, A.D. & Lias, A.R. 2005, 'Identity Theft and E-Fraud as Critical CRM Concerns', *International Journal of Enterprise Information Systems (IJEIS)*, vol. 1, no. 2, pp. 17–36, viewed 25 April 2021, <https://www.igi-global.com/article/identity-theft-fraud-critical-crm/2079>.

SMITH, J., WYATT, R., JACKSON, N. & KENLEY, R. n.d., 'STRATEGIC

NEEDS ANALYSIS: TWO CASE STUDIES IN PROJECT INITIATION', *researchgate.net*, viewed 16 November 2020, <https://www.researchgate.net/profile/Russell_Kenley/publication/235956069_Strategic_needs_analysis_-_two_case_studies_in_project_initiation/links/00b495184936fb052f000000/Strategic-needs-analysis-two-case-studies-in-project-initiation>.

Smith, R.E. 2004, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, viewed 26 April 2021, <https://www.amazon.com/Ben-Franklins-Web-Site-Curiosity/dp/0930072146>.

Smith, R.G. & Jorna, P. 2018, *Counting the costs of identity crime and misuse in Australia, 2015–16, Statistical Bulletin no. 15*, *AIC bulletins*, viewed 25 April 2021, <https://www.aic.gov.au/sites/default/files/2020-05/sb15_counting_the_costs_of_identity_crime_and_misuse_in_australia_2015-16.pdf>.

Sommerville, I. 2005, 'Integrated requirements engineering: A tutorial', *IEEE Software*, vol. 22, no. 1, pp. 16–23.

Sovrin n.d., *Home - Sovrin*, viewed 6 May 2021, <https://sovrin.org/>.

State of California Department of Justice 2018, 'California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General', *State of California Department of Justice*, viewed 24 April 2021, <https://oag.ca.gov/privacy/ccpa>.

States, U. 2003, *Science and Technology for Army Homeland Security*, *Science and Technology for Army Homeland Security*, viewed 25 April 2021, <https://www.dhs.gov/science-and-technology>.

Succar, B. & Poirier, E. 2020, 'Lifecycle information transformation and exchange for delivering and managing digital and physical assets', *Automation in Construction*, vol. 112, p. 103090.

Takemiya, M. & Vanieiev, B. 2018, 'Sora Identity: Secure, Digital Identity on the Blockchain', *Proceedings - International Computer Software and Applications Conference*, vol. 2, IEEE Computer Society, pp. 582–7.

Tatar, U., Gokce, Y. & Nussbaum, B. 2020, 'Law versus technology: Blockchain, GDPR, and tough tradeoffs', *Computer Law and Security Review*, vol. 38, viewed 11 April 2021, <https://www.sciencedirect.com/science/article/pii/S0267364920300595>.

Teo, T.S.H. & Liu, J. 2007, 'Consumer trust in e-commerce in the United States, Singapore and China', *Omega*, vol. 35, no. 1, pp. 22–38, viewed 26 April 2021, <https://www.sciencedirect.com/science/article/pii/S0305048305000356>.

'The WannaCry ransomware attack' 2017, *Strategic Comments*, vol. 23, no. 4, pp. vii–ix, viewed 5 May 2021, <https://www.tandfonline.com/doi/abs/10.1080/13567888.2017.1335101>.

Thomas, I. & Meinel, C. 2010, 'An identity provider to manage reliable digital identities for SOA and the web', *ACM International Conference Proceeding Series*, pp. 26–36.

Tobin, A. & Reed, D. 2017, 'The Inevitable Rise of Self-Sovereign Identity', *Sovrin.org*, vol. 29, no. September 2016, p. 10, viewed 25 April 2021, <https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>.

Tomison, A. 2015, 'Trends and Issues in Crime and Criminal Justice: Foreword', *Trends and Issues in Crime and Criminal Justice*, p. 1.

Toomer, E., Bowen, K. & Gummesson, E. 1993, 'Qualitative Methods in Management Research.', *The Journal of the Operational Research Society*, vol. 44, no. 7, p. 735, viewed 23 April 2021, <https://books.google.com.au/books?hl=en&lr=&id=aBEqkxhd58YC&oi=fnd

&pg=PR7&dq=Gummesson+2000+Qualitative+methods+in+management+research&ots=k1suuvu2jU&sig=EKssTRwbthvbMTAUZZYmzwTzn70>.

Tredinnick, L. 2019, 'Cryptocurrencies and the blockchain', *Business Information Review*, SAGE Publications Ltd, pp. 39–44.

Um, S., Yoo, Y., Kulathinal, R. & Henfridsson, O. 2016, *THE COEVOLUTION OF DIGITAL ECOSYSTEMS*.

United States Government 2002, 'Privacy | HHS.gov', *HHS.gov*, viewed 26 April 2021, <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>.

Urquhart, C. & Fernández, W. 2006, 'Grounded theory method: The researcher as blank slate and other myths', *ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems*, pp. 457–64, viewed 23 April 2021, <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1152&context=icis2006>.

Urquhart, C., Lehmann, H. & Myers, M.D. 2010, 'Putting the "theory" back into grounded theory: Guidelines for grounded theory studies in information systems', *Information Systems Journal*, vol. 20, no. 4, pp. 357–81.

Vaishnavi, V., Kuechler, B. & Petter, S. n.d., *DESIGN SCIENCE RESEARCH IN INFORMATION SYSTEMS*.

Valdez-De-Leon, O. 2019a, 'How to Develop a Digital Ecosystem – a Practical Framework', *Technology Innovation Management Review*, vol. 9, no. 8, pp. 43–54, viewed 24 April 2021, <https://www.timreview.ca/article/1260>.

Valdez-De-Leon, O. 2019b, 'How to Develop a Digital Ecosystem – a Practical Framework', *Technology Innovation Management Review*, vol. 9, no. 8, pp. 43–54, viewed 25 April 2021, <https://www.timreview.ca/article/1260>.

Venable, J., Pries-Heje, J. & Baskerville, R. 2012, 'A comprehensive framework for evaluation in design science research', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes*

in Bioinformatics), vol. 7286 LNCS, Springer, Berlin, Heidelberg, pp. 423–38, viewed 18 April 2021, <https://link.springer.com/chapter/10.1007/978-3-642-29863-9_31>.

Venkatesh, V. & Bala, H. 2008, 'Technology Acceptance Model 3 and a Research Agenda on Interventions', *Decision Sciences*, vol. 39, no. 2, pp. 273–315, viewed 8 March 2021, <http://doi.wiley.com/10.1111/j.1540-5915.2008.00192.x>.

Verizon 2020, *2020 Data Breach Investigations Report*, viewed 17 April 2021, <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>.

Wang, F. & De Filippi, P. 2020, 'Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion', *Frontiers in Blockchain*, vol. 2.

Wang, S. & Yao, N. 2019, 'A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs', *Wireless Networks*, vol. 25, no. 3, pp. 1099–115.

Warren, Samuel D. & Brandeis, L.D. 1890, 'The Right to Privacy', *Harvard Law Review*, vol. 4, no. 5, p. 193, viewed 16 November 2020, <https://www.jstor.org/stable/1321160?origin=crossref>.

Warren, Samuel D & Brandeis, L.D. 1890, *The Right to Privacy*, *Harvard Law Review*, viewed 30 April 2020, <https://www.jstor.org/stable/1321160>.

Wei, W., Zhang, L. & Hua, N. 2019, 'Error management in service security breaches', *Journal of Services Marketing*, vol. 31, no. 7, pp. 783–97.

Westin, A.F. 1967, *Privacy And Freedom*, Ig Publishing.

White, M.D. & Fisher, C. 2008, 'Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts', *Criminal Justice Policy Review*, vol. 19, no. 1, pp. 3–24, viewed 25 April 2021,

<http://www.sagepub.com/journalsPermissions.nav>.

Whitley, E.A. & Hosein, G. 2010, 'Global Identity Policies and Technology: Do we Understand the Question?', *Global Policy*, vol. 1, no. 2, pp. 209–15, viewed 25 April 2021, <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1758-5899.2010.00028.x>.

Williams, C.A.J. 1964, 'The Right to be Let Alone', *University of Florida Law Review*, vol. 17, viewed 26 April 2021, <https://heinonline.org/HOL/Page?handle=hein.journals/uflr17&id=611&div=&collection=>.

Windley, P.J. 2005, *Digital Identity: Unmasking identity management architecture (IMA)*, *O'Reilly Media, Inc.*, viewed 25 April 2021, <https://books.google.com.au/books?hl=en&lr=&id=o8mHSbDHgPsC&oi=fnd&pg=PT5&dq=P.+J.+Windley,+Digital+Identity:+Unmasking+identity+management+architecture+(IMA).+%22+O%27Reilly+Media,+Inc.%22,+2008.&ots=UTgwjdvK7u&sig=Rr1YkTjcPEE3JL0zMeqVPoSZd_A>.

Winter, R. 2008, 'Design science research in Europe', *orsociety.tandfonline.com*, vol. 17, no. 5, pp. 470–5, viewed 2 May 2021, <www.palgrave-journals.com/ejis>.

Wolf, M., Semm, A. & Erfurth, C. 2018, 'Digital transformation in companies – challenges and success factors', *Communications in Computer and Information Science*, vol. 863, Springer Verlag, pp. 178–93.

Wolfond, G. 2017, *Technology Innovation Management Review*.

Wu, Y. 2020, 'Research on digital economy promoting high quality development of regional economy under the background of internet', *Proceedings - 2020 International Conference on E-Commerce and Internet Technology, ECIT 2020*, Institute of Electrical and Electronics Engineers Inc., pp. 225–7.

Yin, R.K. 2002, *Case study research : design and methods*, 3rd edn, SAGE

Publications, Newbury Park.

Yoon, M., Jang, M., Kim, H. Il & Chang, J.W. 2013, 'A new sensitive data aggregation scheme for protecting data integrity in wireless sensor network', *Lecture Notes in Electrical Engineering*, vol. 240 LNEE, pp. 277–84, viewed 25 April 2021, <https://ieeexplore.ieee.org/abstract/document/5578283/>.

Zhang, C. 2020, 'Right-wing populism with Chinese characteristics? Identity, otherness and global imaginaries in debating world politics online', *European Journal of International Relations*, vol. 2020, no. 1, pp. 88–115, viewed 25 April 2021, <https://doi.org/10.1177/1354066119850253>.

Zwattendorfer, B., Zefferer, T. & Stranacher, K. 2014, 'An overview of cloud identity management-models', *WEBIST 2014 - Proceedings of the 10th International Conference on Web Information Systems and Technologies*, vol. 1, pp. 82–92, viewed 25 April 2021, <http://saml.xml.org>.

Appendices

The appendices contain the information required to evaluate the framework. They also contain the published research papers and industry workshops.

Appendix A: Ethical Approval

From: research.ethics@uts.edu.au
Mon 07/13/2020
To: Memoona J. Anwar; Asif Gill

Dear Applicant

Re: ETH20-5009 - "Adaptive Digital Identity Verification Reference Architecture Framework"

Your local research office has reviewed your application and agreed that it now meets the requirements of the National Statement on Ethical Conduct in Human Research (2007) and has been approved on that basis. You are therefore authorized to commence activities as outlined in your application, subject to any conditions detailed in this document.
You are reminded that this letter constitutes ethics approval only. This research project must also be undertaken in accordance with all UTS policies and guidelines including the Research Management Policy.

Your approval number is UTS HREC REF NO. ETH20-5009

Approval will be for a period of five (5) years from the date of this correspondence subject to the submission of annual progress reports.
The following standard conditions apply to your approval:

- Your approval number must be included in all participant material and advertisements.
- Any advertisements on Staff Connect without an approval number will be removed.
- The Principal Investigator will immediately report anything that might warrant review of ethical approval of the project to the Ethics Secretariat (Research.Ethics@uts.edu.au).
- The Principal Investigator will notify the UTS HREC of any event that requires a modification to the protocol or other project documents and submit any required amendments prior to implementation. Instructions on how to submit an amendment application can be found here.
- The Principal Investigator will promptly report adverse events to the Ethics Secretariat. An adverse event is any event (anticipated or otherwise) that has a negative impact on participants, researchers or the reputation of the University. Adverse events can also include privacy breaches, loss of data and damage to property.
- The Principal Investigator will report to the UTS HREC annually and notify the HREC when the project is completed at all sites.

- The Principal Investigator will notify the UTS HREC of any plan to extend the duration of the project past the approval period listed above through the progress report.
- The Principal Investigator will obtain any additional approvals or authorisations as required (e.g., from other ethics committees, collaborating institutions, supporting organizations).
- The Principal Investigator will notify the UTS HREC of his or her inability to continue as Principal Investigator including the name of and contact information for a replacement.

This research must be undertaken in compliance with the Australian Code for the Responsible Conduct of Research and National Statement on Ethical Conduct in Human Research.

You should consider this your official letter of approval.

If you have any queries about this approval, or require any amendments to your approval in future, please do not hesitate to contact your local research office or the Ethics Secretariat.

Ref: 12a

Appendix B: Consent Form

PARTICIPANT INFORMATION SHEET

Adaptive Digital Identity Verification Reference Architecture Framework

WHO IS DOING THE RESEARCH?

My name is *Memoona Javeria Anwar,* and I am a PhD student in Information Systems at UTS. My supervisor is Dr. Asif Q Gill.

WHAT IS THIS RESEARCH ABOUT?

The aim of the research is to design an Adaptive Digital Identity Verification Reference Architecture (ADIVRA) that ensures privacy of identity information and adapts as per business needs, changing risks and regulatory landscape.

FUNDING

This research is supported by the Australian Government Research Training Program Scholarship for higher education and research students.

WHY HAVE I BEEN ASKED?

You have been invited to participate in this study because of your distinguished experience in Information Security/ Digital Identity field and understanding of blockchain, privacy regulations and identity ecosystem. Your contact details were obtained from LinkedIn and/or by Supervisors' Industry Contacts as he is actively engaged with the industry on similar projects.

IF I SAY YES, WHAT WILL IT INVOLVE?

If you decide to participate, I will invite you to kindly participate in the evaluation of my research outcome using the method of structured interviews.

The interview can be online or face to face depending on the availability and includes:

- A detailed description of the research project.
- A list of publications about the research project.
- A set of questionnaires designed to evaluate and rate the research outcome artefact (ADIVRA Framework)

I will ask you to:

- Read the project description PDF and refer to the publications' list for further information.
- Answer online questionnaire and rating survey questions in the online form.

Further information:

- The survey questionnaire may require 30 to 60 mins.
- No travelling or payments are required.
- The form is sent to you by email. The surveys will be conducted online. Upon completion the data will be sent back to me.
- The data will not include any information that may identify you in any way. No personal data will be collected; the data collected via survey is technical and completely anonymous.
- The data will be stored in UTS systems as per UTS research data management policy on the UTS Recommended cloud storage CloudStor https://cloudstor.aarnet.edu.au/. Only my supervisor and I have access to data via UTS secure login to CloudStor.
- The collected technical/anonymous data will be used for publications of conference papers, journal papers and the research thesis.

ARE THERE ANY RISKS/INCONVENIENCE?

There is no risk, (low category) because it only involves online survey and interview. It is only a technical and architecture content. Therefore, it is highly unlikely for any risk to occur.

DO I HAVE TO SAY YES?

Participation in this study is voluntary. It is completely up to you whether or not you decide to take part.

WHAT WILL HAPPEN IF I SAY NO?

If you decide not to participate, it will not affect your relationship with the researchers or the University of Technology Sydney. If you wish to withdraw from the study once it has started, you can do so at any time without having to give a reason, by contacting the researcher (Memoona Javeria Anwar, email: memoona.j.anwar@student.uts.edu).

If you withdraw from the study, you can do so at any time, the participation in this study is voluntary. However, it may not be possible to withdraw your response-data from the study results. Your response-data collected from the online survey will not contain any personal information about you. The collected data is technical and anonymous.

CONFIDENTIALITY

By signing the consent form, you consent to the research team collecting and using online survey anonymous response-data for the research project. All this information will be treated confidentially. The data will be stored in UTS systems as per UTS research data management policy. Only my supervisor and I have access to data via UTS secure login.

The anonymous data collected from your response to the online survey form will not identify you in any way and will only be used for the purpose of this research project (thesis) and paper publications (conferences and journals).

WHAT IF I HAVE CONCERNS OR A COMPLAINT?

If you have concerns about the research that you think I or my supervisor can help you with, please feel free to contact us on [Memoona Javeria Anwar (researcher):
memoona.j.anwar@student.uts.edu
Dr. Asif Q. Gill (supervisor): Asif.Gill@uts.edu.au]

You will be given a copy of this form to keep.

NOTE:
This study has been approved by the University of Technology Sydney Human Research Ethics Committee [UTS HREC]. If you have any concerns or complaints about any aspect of the conduct of this research, please contact the Ethics Secretariat on ph.: +61 2 9514 2478 or email: Research.Ethics@uts.edu.au] and quote the UTS HREC reference number. Any matter raised will be treated confidentially, investigated and you will be informed of the outcome.

CONSENT FORM

Adaptive Digital Identity Verification Reference Architecture
(UTS HREC REF NO. ETH-182772)

I _____ agree to participate in the research project ADIVRA for secure identity ecosystem **[UTS HREC REF NO. ETH-182772]** being conducted by Memoona Javeria Anwar (Email: memoona.j.anwar@student.uts.edu, researcher at the School of Software, University of Technology Sydney, Ultimo NSW 2007, Australia). I understand that funding for this research has been provided by Australian Government Research Training Scholarship.
I have read the Participant Information Sheet, or someone has read it to me in a language that I understand.

I understand the purposes, procedures and risks of the research as described in the Participant Information Sheet.

I have had an opportunity to ask questions and I am satisfied with the answers I have received.

I freely agree to participate in this research project as described and understand that I am free to withdraw at any time without affecting my relationship with the researchers or the University of Technology Sydney.

I understand that I will be given a signed copy of this document to keep.

I agree to:
☐ Receive the online google survey form by email
☐ Participate in the interview
☐ The collection of anonymous data from my response

I agree that the research data gathered from this project may be published in a form that:
☐ Does not identify me in any way
☐ May be used for future research purposes

I am aware that I can contact *Ms. Memoona Javeria Anwar* if I have any concerns about the research.

_____ ____/____/____
Name and Signature [participant] Date

_____Memoona J. Anwar_____ __01__/08____/2020__
Name and Signature [researcher] Date

Appendix C: Survey Invitation Letter

Adaptive Digital Identity Verification Reference Architecture (ADIVRA)
(UTS HREC REF NO. ETH-182772)

My name is Memoona Javeria Anwar, and I am a PhD student in Information Systems at the University of Technology, Sydney.

I am conducting research in the area of privacy for digital identity and developed an adaptive digital identity verification reference architecture based on Blockchain and would welcome your assistance. To evaluate the design and applicability of reference architecture, I would like to request you to take part in my research, review the reference architecture and provide your feedback via an online google survey form. The research review and evaluation will involve an online google survey form and will not take more than 60-90 minutes of your time. I kindly request you to participate in this research because of your expertise in the field of information security and digital identity.

This research is supported by the Australian Government Research Training Program Scholarship for higher education and research students.

I am looking forward to hearing from you. I would be glad to provide more information if required. Further, you may also contact UTS Graduate Research School and/or my supervisor Dr Asif Q Gill (School of Software, University of Technology Sydney; Ultimo NSW 2007; Australia Asif.Gill@uts.edu.au).

You are under no obligation to participate in this research. In case you chose to participate and help us evaluate the research output artefact, your contribution will be anonymous. No personal information about yourself will be collected or retained.

If you chose to participate in the online survey, your responses will be stored in UTS secure storage systems. Only my supervisor and I can access the collected survey data. The survey data will be used for academic analysis and publications.

Yours sincerely,

Memoona Javeria Anwar
School of Software
University of Technology Sydney
Ultimo NSW 2007, Australia
memoona.j.anwar@student.uts.edu

NOTE:

This study has been approved by the University of Technology, Sydney Human Research Ethics Committee. If you have any complaints or reservations about any aspect of your participation in this research which you cannot resolve with the researcher, you may contact the Ethics Committee through the Research Ethics Officer (ph: +61 2 9514 2478 Research.Ethics@uts.edu.au) and quote the UTS HREC reference number. Any complaint you make will be treated in confidence and investigated fully and you will be informed of the outcome.

Appendix D: Online Industry Survey Questionnaire

The following is a sample of the online Google survey that has been used to record the participants' responses. The survey participants are industry experts in the fields of privacy, digital identity verification, blockchain, compliance and regulations.

To access the online survey, please follow: https://forms.gle/jkuz2yeJMdb2rp256

Start Survey

Adaptive Digital Identity Verification Reference Architecture (ADIVRA) Evaluation

Please submit feedback regarding the ADIVRA framework

Introduction

The ADIVRA is designed to provide a reference architecture for blockchain-based decentralized digital identity by embedding privacy into the design of the solution. It has three main components; assess, design, and evolve. The starting point for the development of this framework is the organization's business needs and strategy, specifically in terms of privacy. This reference architecture also aims to ensure global regulatory compliance and adapt with changing business needs, privacy risks and regulatory landscape. Each component has artefacts which help in carrying out the activities for that component.

ADIVRA Framework Description

1- Research Project Outline https://youtu.be/8N5U0bgbGNk
2- Assess Component https://youtu.be/7K09ixQpJvQ
3- Design Component https://youtu.be/0wHxDHwlKwQ
4- Evolve Component https://youtu.be/U0MrGa7RHNE

Survey Rating Factors

Qualitative Rating	Quantitative Rating
Strongly Agree	5
Agree	4
Somewhat Agree	3
Disagree	2
Strongly Disagree	1
Not Sure/Not Applicable	0

Q1 Set: ADIVRA Assess Component Questions

The first component of ADIVRA is Assess. The assess component can encompass different aspects from reviewing information security processes and procedures to environment scanning and technology adoption. A novel PESTLE+ risk analysis framework has been developed as part of the Assess component to identify the changing security and privacy risks in the DigI verification process. This component assesses the existing privacy capability of the DigI verification process

according to the organization's business strategy and privacy goals and identifies the risks and gaps. An assessment model to assess the privacy capability of the DigI verification design. The IdMPAM assists in making technology adoption decisions by assessing the viability of technology for DigI verification. iSAM2 enables the assessment of the maturity of the information security audit process. The emphasis in this type of assessment is to ensure that privacy requirements are fulfilled, risks and gaps are identified, policies are in place and procedures are being followed along with revealing actions that may put organizational compliance at risk.

	Strongly Agree	Agree	Somewhat Agree	Disagree	Strongly Disagree	Not Sure/Not Applicable
Is the assess [PESTLE+] component able to assess the risks and gaps in other similar DigI verification contexts?	O	O	O	O	O	O
Can the assess [IdMPAM] component be used to assess the GDPR privacy compliance of blockchain-based DigI solutions?	O	O	O	O	O	O
Can the assess [iSAM2] component be used to assess the maturity level of information security internal audit?	O	O	O	O	O	O
Does the assess component produce new knowledge in the context of the DigI ecosystem?	O	O	O	O	O	O
Are the assess component artefacts [PESTLE+, IdMPAM, iSAM2] sufficient for the context?	O	O	O	O	O	O

Q2 Set: ADIVRA Design Component Questions

The second component of the ADIVRA framework is Design. The starting point for the design component is the risks and gaps identified as a result of the previous component (Assess). The outputs of the Design component artefacts are assessed using artefacts of the Assess component. In addition, change requests from the Evolve component (using DigIVAM) are also adjusted. CDigI is a multidimensional DigI structure to broaden the scope of DigI and enable the interoperable DigI verification process without costly and time-consuming reworks. iSEA is an encryption-based architecture for a secure container to embed privacy into the DigI verification solution. DigIVPM is a DigI verification process model to securely verify the DigI information or credentials without storing the PII. This process can involve several parties such as identity owner, regulators, issuers, verifiers, and service providers operating within the global digital ecosystem. To ensure regulatory compliance, a regulatory requirement model is designed to develop a catalogue of regulatory requirements for the DigI verification process.

	Strongly Agree	Agree	Somewhat Agree	Disagree	Strongly Disagree	Not Sure/Not Applicable
Is the design component able to design the DigI architecture in other DigI verification contexts?	O	O	O	O	O	O
Does the digital identity structure [CDigI] defined in the design component cover all possible identity attributes?	O	O	O	O	O	O
Can the secure digital identity container [iSEA] be used to safeguard the DigI information?	O	O	O	O	O	O

Does the BC-based DigI verification process model [DigIPM] include all steps necessary to conduct electronic identity verification?	O	O	O	O	O	O
Can the design component effectively elicit regulatory requirements for DigI?	O	O	O	O	O	O
Does the design component produce new knowledge for designing a secure DigI ecosystem?	O	O	O	O	O	O
Are the design component artefacts [CDigI, iSEA, DigIPM, RRM] sufficient for conducting secure electronic identity verification?	O	O	O	O	O	O

Q3 Set: ADIVRA Evolve Component Questions

The third component of the ADIVRA framework is Evolve. This component utilizes the PESTLE+ risk analysis model from the Assess component in addition to DigIVAM. To ensure adaptability, ADIVRA needs to continuously evolve as per business needs, changing privacy risks and the regulatory landscape. The Evolve component has DigIVAM which identifies the change requirements and feeds them back to the Design component for design adjustments.

	Strongly Agree	**Agree**	**Somewhat Agree**	**Disagree**	**Strongly Disagree**	**Not Sure/Not Applicable**
Is the evolve component able to adapt to changes in other similar DigI contexts?	O	O	O	O	O	O
Is the evolve component able to adapt to changes in business strategy?	O	O	O	O	O	O
Is the evolve component able to adapt to changes in the regulatory landscape?	O	O	O	O	O	O
Is the evolve component able to adapt to changes in privacy risks?	O	O	O	O	O	O
Does the evolve component produce new knowledge for adapting to changes in the DigI ecosystem?	O	O	O	O	O	O
Are the evolve component artefacts (PESTLE+, DigIVAM) sufficient for eliciting change requirements in the context of the DigI ecosystem?	O	O	O	O	O	O
Is the evolve component able to adapt to changes in other similar DigI contexts?	O	O	O	O	O	O

Q4 Set: Overall ADIVRA Framework Questions

The ADIVRA framework describes the components of an adaptive, privacy aware and regulatory compliant digital identity reference architecture framework and their relationships. This framework shows that an adaptive digital identity framework can be used to address the changing business needs, privacy risks and regulatory landscape.

	Strongly Agree	**Agree**	**Somewhat Agree**	**Disagree**	**Strongly Disagree**	**Not Sure/Not Applicable**
Is the architecture of the framework (ADIVRA) suitable for other similar DigI contexts?	O	O	O	O	O	O
Does the framework (ADIVRA) address the issue of privacy in the DigI ecosystem?	O	O	O	O	O	O

Does the framework (ADIVRA) address the issue of GDPR compliance in the DigI ecosystem?	O	O	O	O	O	O
Does the framework (ADIVRA) address the issue of adaptability to changing risks and regulations in the DigI ecosystem?	O	O	O	O	O	O
Does the architecture of the framework (ADIVRA) produce new knowledge in the context of the DigI ecosystem?	O	O	O	O	O	O
Does the architecture of the framework (ADIVRA) provide sufficient coverage for all the necessary elements of a DigI ecosystem? If not please make suggestions for improvements below in number 7.	O	O	O	O	O	O
Is ADIVRA useful for identity architects?	O	O	O	O	O	O
Is ADIVRA useful for regulators?	O	O	O	O	O	O
Is ADIVRA useful for researchers?	O	O	O	O	O	O

Q5 Set: ADIVRA Feedback

Q: What is your feedback on the ADIVRA framework
Your Answer……

Q6 Set: ADIVRA Usefulness

Q: What aspects about ADIVRA are useful or valuable?
Your Answer……..

Q7 Set: ADIVRA Suggested Improvement feedback

Q: What improvements would you suggest to the ADIVRA framework?
Your Answer……..

Q8 Set: ADIVRA Overall Comments and Ratings

	Strongly Agree	**Agree**	**Somewhat Agree**	**Disagree**	**Strongly Disagree**	**Not Sure/Not Applicable**
On a scale of 1 to 5 (5 being highest), provide an overall rating for the ADIVRA framework?	O	O	O	O	O	O

Q9 Comments ……..
……..
……
…..

Appendix E: Industry Field Survey Data

This section contains the source of the data used in the evaluation in this thesis. The data have been stored on CloudStor, the UTS-recommended cloud storage service. Only the thesis author (Memoona Javeria Anwar) and the principal supervisor (Dr Asif Q. Gill) have access to the data files on CloudStor. The empirical original data files are organised as follows:

- Industry Survey:
  https://forms.gle/A6pCputFKBPDzS4A9

- Industry survey files:

  https://cloudstor.aarnet.edu.au/plus/s/oKUUduaiggHlXya

- ADIVRA Presentation Slides (Used in industry field Survey):
  https://youtu.be/8N5U0bgbGNk
  https://youtu.be/7K09ixQpJvQ
  https://youtu.be/0wHxDHwlKwQ
  https://youtu.be/U0MrGa7RHNE

- Ethical approval letter, invitation letters, PIS form:
  shttps://cloudstor.aarnet.edu.au/plus/s/DiXQqNOv2qFkXWV

Note: The author's LinkedIn page has been used to communicate with professionals from the IT industry and offer the industry field survey to the participants using the survey invitation letter (see Appendix C).

Appendix F: Research Papers

Publication-1
Anwar, M.J., Gill, A.Q., Hussain, F.K. et al. Secure big data ecosystem architecture: challenges and solutions. J Wireless Com Network 2021, 130 (2021).

https://doi.org/10.1186/s13638-021-01996-2

Publication-2
Anwar, M.J., Gill, A.Q., Fitzgibbon, A.D. et al. PESTLE+ RISK ANALYSIS MODEL TO ASSESS PANDEMIC PREPAREDNESS OF DIGITAL ECOSYSTEMS, Security and Privacy Journal 2021, DOI: 10.1002/spy2.187

Publication-3
Anwar, M., Gill, A., and Beydoun, G. 2018. "A review of information privacy laws and standards for secure digital ecosystems", in ACIS, 2018, Sydney, Australia.

http://www.acis2018.org/wp-content/uploads/2018/11/ACIS2018_paper_78.pdf

Publication-4
M. J. Anwar and A. Q. Gill, "A Review of the Seven Modelling Approaches for Digital Ecosystem Architecture," 2019 IEEE 21st Conference on Business Informatics (CBI), Moscow, Russia, 2019, pp. 94-103, doi: 10.1109/CBI.2019.00018.

https://ieeexplore.ieee.org/document/8807801

Publication-5
M. Anwar, A. Gill, and G. Beydoun, "Using Adaptive Enterprise Architecture Frame-work for Defining the Adaptable Identity Ecosystem Architecture," 2019.
https://acis2019.io/pdfs/ACIS2019_PaperFIN_176.pdf

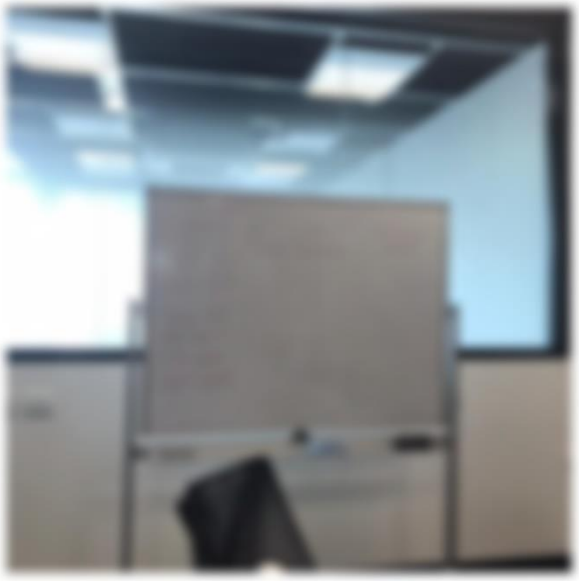
Publication-6
M. Anwar and A. Gill, " Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model," 2020.

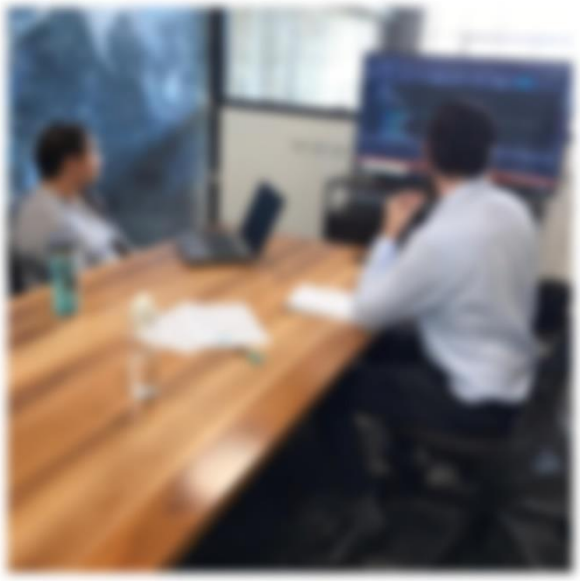
https://www.datazoo.com/wp-content/uploads/ISO27701-and-GDPR-Gaps-and-Overlaps.pdf

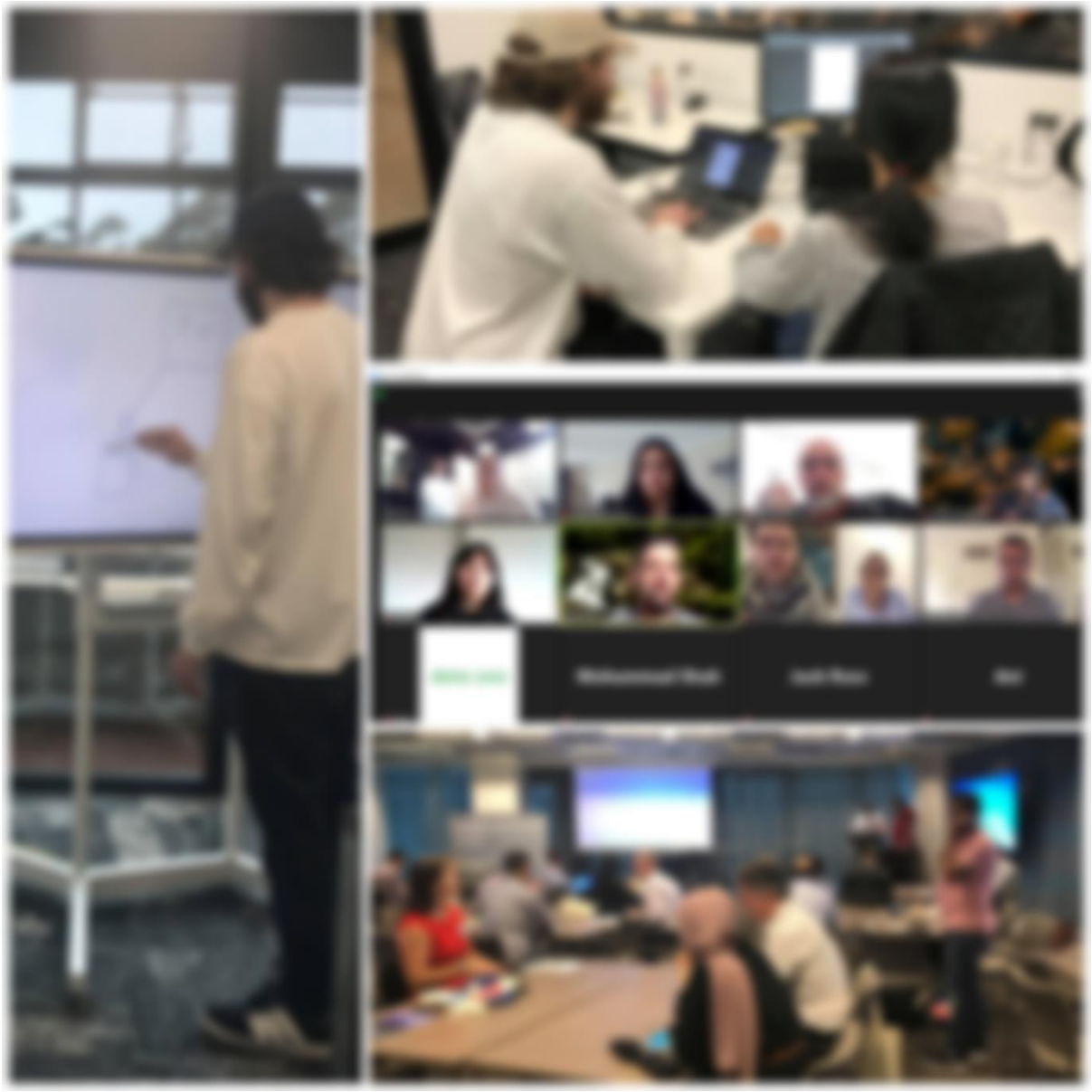
Appendix G: Non-Disclosure Agreement

[The actual NDA is not attached due to privacy concerns]

Appendix H: Feedback Workshops and Meetings







Appendix I: Design and Review Workshops comments Log

Workshop ID	**Assess Workshop-I**
Role	**Comment/Feedback**
Business Analyst	*"The existing operation model for IDZ, whilst efficient and seamless for clients, must be improved with an enhanced offering to clients (and potentially individuals) in order to maintain and extend this status within the industry."*
IT Manager	*"IDZ is seeking to harness the potential of new global technology trends involving biometrics and Blockchain. Incorporating these technologies into enhanced applications and efficient operations that its' clients can leverage will enable Data Zoo to continue as an industry leader and trusted identity verification partner."*
Privacy Officer	*"With all the interest in this technology, it is imperative to clearly understand blockchain and the privacy of DigI information considering regulations such as GDPR."*
Digital Identity Architect	*"Before designing a blockchain-enabled privacy enhancing digital identity verification solution, it is important to identify the risks and gaps in existing privacy capability of the organization."*
Business Analyst	*"We would like to take these models further and offer capability to whitelabel the IDZ platform and making the platform portable via an SDK to clients and potential verification partners."*
Workshop ID	**Assess Workshop-II**
Privacy Officer	*"The level and depth of risk analysis required to foresee and prepare for pandemics like Corona Virus, requires health to be considered as a standalone factor in risk analysis, as well as its impact on other factors (political, economic, social, technological, legal and environmental) should also be taken into account."*
Compliance Manager	*"PESTLE+ is a good extension to PESTLE model however, the factors included in analysis are typically assessed and measured individually which may not cover everything."*
Business Analyst	*"The health factor treated as a sub factor in current PESTLE risk analysis model may not permit a thorough investigation of health-related risks. PESTLE+ fill this gap "*
Business Analyst	*"IdMPAM is straight forward and easy to understand"*
Compliance Manager	*"Both the artefacts are good to assess the environment and technology from privacy and compliance point of view. The fundamental challenge for IDZ is the effective designing and correct implementation of privacy and security controls and independent review of security measures and performance by the internal audit function. This is missing from both artefacts"*
Privacy Officer	*"Although the conceptual foundation of PESTLE+ analysis proposes a comprehensive approach, this is not mirrored in the evaluation criteria and measurement process."*
IT Manager	*"The cost considerations have not been taken into account for IdMPAM which is very important for the feasibility of any solution and their adoption."*
Digital Identity Architect	*"IdMPAM gives a very easy to understand factors that can be applied to any organizational context. However, some important factors like ease of use, support for documents and use cases and affordability might be added as assessment criteria"*
Workshop ID	**Assess Workshop-III**
Business Analyst	*"Demo was easy to understand and well presented".*
Compliance Manager	*"GDPR and Identity Laws are excellent choice to pick IdMPAM assessment criteria. "*
Digital Identity Architect	*"ADIVRA "Assess" component is not specific to blockchain based DigI verification solutions only. The application of IdMPAM for assessing a non-blockchain based DigI verification solution makes it broader and generalizable"*

Privacy Officer	*"I think the strength of PESTLE+ model is the relationships and connections among PESTLE macro-environmental factors. This enables PESTLE+ to be applicable in multiple organizational contexts."*
IT Manager	*"Independent evaluation and analysis of individual macro environmental PESTLE factor may not reflect the actual state of affairs. PESTLE+ addresses the issue of interdependence."*
IT manager	*"The IdMPAM is an excellent reference for assessing the viability of blockchain for designing DigI verification solutions and brings to life the inherent need for such assessment models to ensure that such solutions are compatible with the changing regulatory landscape in regards to the appropriate use and handling of Personally Identifiable Information (PII). There is no need for any further considerations until there is further research (and subsequent validation) into the best practices of an DigI verification."*
Digital Identity Architect	*"The evolution and application of the proposed IdMPAM clarified what was initially a very daunting and complex prospect of understanding the current and potential use of blockchain in the DigI verification landscape. The assessment factors and design principles resolved the technology adoption aspects down to business operational concepts that can be easily communicated and strategically discussed."*
Digital Identity Architect	*"ADIVRA Assess component will help organizations in understanding true potential of any technology and align their privacy and compliance capability with the emerging technological trends"*
Business Analyst	*"The application of "Assess" component into IDZ's context successfully produced the desired outcomes"*
Workshop ID	**Design Workshop-I**
Compliance Manager	*"The uncertainty around regulatory requirements and global information security standards are impeding the adoption of DigI verification solutions by end users. Therefore, the DigI verification solutions should be designed keeping regulations in mind"*
Privacy Officer	*"The PII that constitutes the DigI needs to be secure. It will give IDZ's clients the confidence to use our DigI verification services without fears about privacy"*
Business Analyst	*"How to optimize opportunities for IDZ to offer DigI verification with unique point of difference through the use of biometrics and multi-factor authentication. A number of DigI verification providers offer various forms of biometric capability however many lack the data source availability as IDZ has. To maximize the potential of biometrics within the industry. By adding support for biometric authentication into IDZ's DigI verification solution, we can make it a secure and trustworthy solution for end users. This will also help us ensure compliance with regulatory requirements"*
Digital Identity Architect	*"We should look at incorporating blockchain technology into the DigI verification solution whereby IDZ clients can access previously verified individual's PII and documentation, whilst adhering to Know You Customer, Anti Money Laundering and other compliance regulations."*
IT manager	*"From a strategic business perspective, the implementation of a regulatory compliant DigI verification solution employing blockchain as an underlying technology would position IDZ at the forefront of the industry, thereby enabling access to a wider range of data sources and suppliers as well as positioning as the preferred choice of DigI verification service provider. This will fulfill the decentralization needs in addition to providing reusable digital identity to end users"*
Workshop ID	**Design Workshop-II**
IT Manager	*"DigIVPM provides a very useful and comprehensive reference architecture for decentralized, and flexible DigI verification by providing support for various use cases in a wide range of environments. The process flow for business to customer model will be useful"*
Digital Identity Architect	*"The creation of VC is based on very typical documents i.e., passport, driver's license etc. However, I think DigI structure should be such that it can support variable and personalized workflows without enduring expensive and time-consuming integrations and should include all facets of DigI"*
Compliance Manager	*"RRM is a very handy metric to extract relevant and applicable requirements from regulations. Also, DigIVPM provides a basis for a complete end to end decentralized verification. How will you ensure the security and privacy of the PII that will be temporarily stored in IdP's data stores"*

Business Analyst	*"The regulatory requirements based DigIVPM is easy to understand and use. However, it works for the business-to-business model only. It will be great to add flow for the business-to-customer model as well"*
Privacy Officer	*"This architecture of DigI verification without storing PII gives is unique and useful from privacy perspective"*
Workshop ID	**Design Workshop-III**
Privacy Officer	*"A DigI verification solution based on ADIVRA design can offer a verification process that is fast and simple. The OCR feature can pull the details from the ID and store in secure container. This gives our clients confidence in our services and peace of mind to us from a compliance perspective. The iSEA is a very good model to secure sensitive information that comprises DigI. The iSEA can be applied to other contexts as well as a standalone secure container."*
Business Analyst	*"The architecture is easy and simple which end users need so they don't get confused or frustrated."*
Compliance Manager	*"Identity owner's control over their own information and DigI verification without storing PII are the two main strengths of this architecture. This takes away a lot of compliance burden off our shoulders"*
Digital Identity Architect	*"The decentralized nature of CDigI allows all the exchange of trustworthy documents regardless of the jurisdiction or context"*
Compliance Manager	*"The regulatory requirements for DDigI systems are mentioned in regulations but there is no definition of a structured approach to effectively extract and validate the requirements. RRM presented in this research provides a novel approach for integrating business processes to regulatory articles for regulatory compliant-DDigI."*
Compliance Manager	*"DigIVPM considerably reduces manual review time and fraud risk. Every time the DigI information is accessed, the identity owner is notified which creates transparency and trust."*
Digital Identity Architect	*"The validity threshold and star-based system is a very good way of keeping the DigI information up to date along with building a web of trust among verifiers."*
Digital Identity Architect	*"The VC enables reusability and interoperability of DigI without repeating the tedious process of scanning and uploading the ID documents and verifying them."*
IT Manager	*"Every time the DigI is accessed, a log entry is maintained in DLT. This is a very good way of transaction monitoring and fulfilling our legal obligation of record keeping without including any form of PII into it."*
IT Manager	*"iSEA privacy and security is paramount."*
Business Analyst	*"Based on ADIVRA, identity ecosystems can be built that let identity owners and service providers share DigI in a simple, secure and privacy-preserving way."*
Workshop ID	**Evolve Workshop-I**
Compliance Manager	*"DigI verification process includes processing of PII. It is very important to maintain compliance with every changing regulatory requirement. It is very important to match the pace of regulatory requirements."*
Privacy Officer	*"With a faster pace of innovation and a rapidly evolving privacy threats, risks and vulnerabilities that impact the protection of DigI information, change is required continuously for compliance operating model, privacy capabilities and technology"*
Business Analyst	*"Staying competitive in DigI verification business poses a continual need for DigI solutions to adapt to change"*
Digital Identity Architect	*"Increasing digital transformation is changing the methods of DigI verification. New technologies are introduced and hence new ways. A DigI verification solutions should be able to identify the changing trends in the DigI verification space and adapt to these changes as early as possible"*
IT Manager	*"The borders between organizations and governments will become more and more blurry as individuals adopt multiple roles in different contexts. DigI verification solutions need to evolve."*
Workshop ID	**Evolve Workshop-II**
Business Analyst Privacy Officer	*"Identifying the change requirements requires a lot of effort and time."*

IT Manager	
Compliance Manager	*"There is no boundary between identification of change requirements and analysis of change requirements. What marks the transition from one level to the next? The existing version of DigIVAM is not applicable in many situations and may not be able to cover all important facets"*
Digital Identity Architect	*"A more structured approach will save a lot of time and effort. For instance, if we can classify the change i.e. if it's a regulatory requirement change or a privacy risk related change or a change in business needs. In this way only the SMEs and people with relevant skills and knowledge will work on the change for better adjustment. It will save time for all other people who can invest their time during the implementation plan."*
Workshop ID	**Evolve Workshop-III**
Digital Identity Architect	*"DigIVAM is a useful tool to identify and understand the need and impact of change in DigI operating environment"*
Compliance Manager	*"This model is not limited to regulatory, privacy risk or business-related change. Following the steps of DigIVAM, change in any area can be identified and addressed"*
Privacy Officer	*"The stepwise approach adopted in DigIVAM can help in reducing disruptive aspects and risks associated with change in an end-to-end identity ecosystem."*
IT Manager	*"The change backlog created while following the steps of DigIVAM creates an opportunity for the development and documentation of best practices that can be useful for others."*
Business Analyst	*"The ADIVRA evolve components help in assessing the impact of change before it is actually implemented. This creates a blueprint for what new solutions might look like and what other units might be impacted."*
Digital Identity Architect	*"The probability of unsuccessful change might be reduced by following the steps of DigIVAM"*

Appendix J- Intervention

a) Intervention of IdMPAM in IDZ organizational setting

IdMPAM was used to evaluate four DigI Verification Solutions as below.

1. ShoCard

ShoCard **is** a mobile-identity platform which is built on blockchain technology. It offers an easy-to-use mobile application for identity verification. ShoCard claims that its technology meets GDPR's Privacy by Design standards. However, the analysis, based on publicly available information, raises certain questions. The user's data does not seem to be stored in the solution's database; however hashes of data are stored on the blockchain. Considering the immutability of blockchain, there is not much information about how ShoCard is fulfilling the "right to erasure" for its customers. Users can remove the consent that they might have given earlier. The immutability of blockchain also hinders the "right to be informed." Customers create their own identity by uploading identity documents, however, if any document changes or/and end-user cannot rectify the existing record, then they need to upload a new document. Requests to access, erase and correct user data are reduced because data is not stored in local database servers. Third-party evaluators acquire proof of consent for sensitive user data adhering to the "right to be informed." The ShoCard solution enables the permission-based retrieval of a user's data by providing maximum control in the hands of the data subject and fulfilling the "right to restrict processing," meanwhile recording a log about the consent on the blockchain. The individuals can revoke their consent whenever they want, hence adhering to GDPR's right to erasure. Once a document is uploaded, PII data is extracted field by field and hashed, which enables "Zero-Knowledge Proof" for verification. The user interacts with ShoCard's mobile application and provides a QR code wherever needed, making use of automation. The user's PII is exposed only if the end-user provides the QR code to a relying party. ShoCard provides credential parsing provided relying parties have already established a partnership with the company's federated servers for attribute endorsement. There is no information about how ShoCard handles and notifies data breaches. By using blockchain as a source of verification, the ShoCard solution seems to preserve the user's privacy since the original data is never stored in an identifiable form. It can only be used with the user's permission to identify the authenticity of the user independently. ShoCard seems to provide security combined with ease of use. ShoCard supports the verification of multiple identity documents e.g., driving license, passport, etc. It has a well-maintained communication blog which is regularly updated and also provides comprehensive white papers on their solution. Their website has well-explained use cases where ShoCard's solution may be used. They offer solutions that seem to support multiple platforms i.e., Android, iOS, and Web. They seem to offer a range of costing or pricing models for their solution features i.e. basic MFA is for $1/user/month, Geo-fencing for $1.50/user/month, biometrics for $2/user/month.

2. Civic

Civic is a decentralized, secure identity platform with the BC and biometrics providing multi-factor authentication (MFA) on web apps as well as mobile apps. Users can download and interact with Civic's mobile application, which is the first step towards using Civic's Secure Identity

Platform. It makes use of certain automated features such as Bluetooth, QR code and NFC, etc. A user can then provide the requested PII, which is sent to a trusted third-party identifier. After verifying the user's information from the issuing authority, Civic attests the document. This confirmation about the authenticity of the customer's identity is sent to the blockchain, where it stays forever in an immutable form. It is important to note here (as per our assessment model) that this contradicts with the criteria "right to erasure" and "right to rectification." Whenever an evaluator wants to verify the identity, the user can willingly accept the request for certain information required, which makes the evaluator confident about legitimacy. The identity owner can re-use the civic verified identity with any service provider without again going through the tedious process of identity verification. Organizations can conveniently get proof of certain information validated by a trusted institution, hence, removing the sharing of extra information. The user is in control of their secure data and they only provide the information that they are comfortable sharing. Data resides on the identity owners' phones where they can easily access and revoke information. However, the data is not completely revoked because the hashes are saved on the blockchain and cannot be altered or reversed. The information on the blockchain is secured using sophisticated security protocols e.g., encryption, hashing, digital signatures, etc. Civic's Secure Private Sign-up (SPS) and Secure Private Login (SPL) offer privacy in data transactions along with enhanced user identity trust. The Civic app sends notifications to data subjects in the case of identity theft. The notification is accompanied with the payment of theft recovery to customers. There is no indication of how Civic conducts and manages data breach notification. Low cost with no humans involved in the process is one of its appealing features. Civic mentioned in the whitepaper that it is paying users to provide identity info, verifiers for verifying identity, and similar scenarios, but no evidence has been seen yet. Finally, it seems that Civic provides support for multiple identity documents, however this varies from country to country.

3. Evernym

Founded in 2013, Evernym develops software solutions that use blockchain to deliver each data subject or device with a secure, private and irreversible identity. Evernym does not store any data on blockchain, giving the end-user the right to erasure. Evernym uses Sovrin as its core technology, where users can select digital identity usage and attribute sharing. It extracts fields from identity documents and puts metadata on blockchain that helps to meet the requirement of minimal disclosure. Neither the credentials themselves nor hashes of credentials are stored on the blockchain. Blockchain contains schemas and schema IDs, credential definition and credential definition IDs, DIDs, revocation registries, and agent authorization policies. The identity owners have full control over their credentials and identity attributes. Private pairwise connections and corresponding shared ledgers allow the identity owner to put a limit on the processing and sharing of PII. Data is available only to trustworthy parties which are selected by the user along with entrusted agencies who act on their behalf. Processing is carried out through an automated means. Evernym does not have information on data breach procedures. The identity platform is custom-built from the very beginning with privacy by design and default approach using digital identity attributes, zero-knowledge proof, permissioned ledgers, and trust frameworks. Data portability and the transfer of personal data requires that the transferring party takes reasonable measures to verify the identity of the receiving party. Evernym maintains a blog on their website that highlights past and upcoming events related to their solution. Evernym supports multiple identity documents such

as passports, driving licenses, etc. Evernym claims to reduce costs, transform customer experiences, and provide reliable digital credentials. There is no mention of specific scenarios where the Evernym solution might fit, however they have mentioned their customers on the website. No clear information regarding platform support was found.

4. Jumio

Jumio adopts a hybrid approach to online the identity verification process. It is a combination of technologies like biometrics, machine learning and artificial intelligence, which are empowered with human supervision. Jumio's identity platform provides enhanced transparency for the reasoning of acceptance/rejection criteria to the provided transaction of DigI verification. Enterprise clients of Jumio are provided with customizable policies to support unique business need-based data retention. It does not store information after a user stops using its service. The end-user still has no right to access, rectify, or restrict the processing of information about themselves. Controllers gather, process, accumulate, and "own" data along with the end user's relationship. The end-user is not explicitly informed about the expected use of their collected information. End-users scan their identity documents from which data is extracted and verified from various data sources. This data can be used to provide only the information which is needed e.g., proof of age, proof of address. The results of the verification activity are shared only with the requesting party. The identity proof provided by Jumio is not reusable across multiple institutions, which means that the interworking of different identity schemes and credentials is not possible. All PII elements, inclusive of ID's and selfies, are encrypted in which the entire data undergoes encryption in transit (TLS encryption) and AES encryption. Jumio has well-managed notification processes to recurrently test and report data breaches. It seems to support multiple industries i.e., finance, airline and travel, education, retailers, telcos, and gaming. The application masks credit card numbers and other sensitive personal information as required. It also extracts a broad range of information from various Latin-based character documents. Jumio provides support for multiple platforms i.e., mobile and web. Jumio costs $2/ verification.

Table J1. Evaluation result summary of non-BC and BC enabled solutions using IdMPAM

IdMPAM Assessment Criteria		ShoCard	Civic	Evernym	Jumio
BC		Yes	Yes	Yes	No
1.	Right to be Erasure	Data is not stored in the company's DB but is stored on the blockchain. Users can remove previously given consent anytime.	Once recorded, data cannot be erased. Hashed identity data is written on blockchain	Since no personal data is stored on the public ledger, the right to erasure will not apply.	Jumio's enterprise customers can customize data retention policies based on their unique business needs. It does not store information after it ceases to have a customer relationship with the customer through which the client used Jumio's identity verification service
2.	Right to be informed	Mobile App notifies the user and takes consent before sharing info.	User approves the request of evaluator before data sharing	Uses Sovrin where users can choose which digital identities are utilized and which attributes are uncovered	
3.	Right to Access	The data lives in the customer's mobile and is shared via blockchain	The data lives in the customer's mobile as well as on blockchain	The identity owner has full control over their credentials and identity attributes	The third-party data controller reserves the right to access their identity owner's data.
4.	Right to Rectification	The customer creates his own identity by uploading his ID documents using a mobile app	Identity data can be revoked by the authenticating body	Neither credentials themselves nor hashes of credentials are stored on the Sovrin ledger	The third-party data controller reserves the right to rectify identity owner's data
5.	Right to Restriction of Processing	Customer is asked before sharing of data	The decision is in the hands of the user to accept or reject all requests for PII	Private pairwise Connections and corresponding shared Microledgers allow the identity owner to exert this right over any personal data shared with a verifier	The third-party data controller reserves the right to modify processing of identity owner's data
6.	Minimal Disclosure	Data is extracted field by field from the trusted ID document	Organizations can effortlessly prove identity data being authenticated by a trusted institute, consequently removing the sharing of needless information.	Sharing of information based on the principle of zero-knowledge proofs permits users to share the information that is least expected to identify [them] within multiple contexts	Provides proof of address, proof of age, etc
7.	Data Breach Notification	Not Clear	Fraud notifications, pay theft recovery to customers, No breach notification system	Not clear	Breach notification and mitigation processes is managed by Jumio's business customers

8.	Privacy by Design	Claims to meet PbD, shares PII through blockchain	Use of biometric, digital signature, multifactor authentication	Pairwise pseudonym digital identity permissioned ledger, a web of trust based on the reputation mechanism, supports in protecting individuals against fraud	The machine learning approach used by Jumio builds data privacy and security throughout the machine learning workflow involving early data capture, identity pre-processing, data tagging, algorithm training, and model deployment
9.	Use of Automation	End-user interacts using a mobile application. Reliably pursues a QR code–scanning model for all uses	User interaction led by the mobile application. Supports a Bluetooth low energy, QR code, and near field communications, to name a few	Processing is carried out by automated means	Jumio adopts a hybrid method to IdM solution, merging AI, machine learning, biometrics, computer vision and, paired with human intervention and review
10.	Justifiable Parties	ShoCardID is disclosed to a relying party only if the process is initiated by the identity owner	Data is shared with trusted parties only	Attributes are available only to the parties that the user selects, and to the institutions delegated to act on their behalf	Data is shared with trusted data controller only
11.	Design for pluralism of operators and technology	ShoCard has support to parse existing reliable attributes, but relying parties must interact with ShoCard centralised servers for validating the credentials	Only when the user registers with the Civic app to get verified, he can submit his data. The data, once submitted can be reused later	Data portability and the transfer of personal data thereunder requires that the transferring party take reasonable measures to verify the identity of the receiving party	Not reusable
12.	Affordability	Pricing packages differ by product lines	Low cost with no humans involved in the process, is one of its high selling points	Evernym claims to cut costs, improve customer experiences, and surpass their competition with innovative, trusted digital credentials	Jumio costs $2/ verification, which is relatively higher
13.	Simplicity	ShoCard provides robust security combined with ease of use	The civic app is easy and simple in use	Evernym claims transform customer experiences	The app is simple and easy to use
14.	Multiple Document Support	ShoCard supports verification of multiple identity documents e.g., driving license, passport, etc	Multiple ID documents are supported by civic. The support varies from country to country	Multiple document support	The app masks credit card numbers other sensitive personal information as required. It also extracts a broad range of information from various Latin-based character documents
15.	Use Cases	Their website has well-explained use cases where ShoCard's solution fits best	Not enough use cases have been explained in the available documentation	Not clear	It supports multiple industries i.e., finance, airline and travel, education, retailers, telcos and gaming
16.	Platform Support	Android, iOS, and Web	Although this is nice for iOS, it is questionable for Android devices	Not clear	Jumio provides support for multiple platforms i.e., mobile and web

b. Intervention of PESTLE+ model for risk analysis of Coronavirus

Table J2.a PESTLE+ Risk Analysis for COVID-19

	P	E	S	T	E	L	+
	Political	**Economic**	**Social**	**Technological**	**Environmental**	**Legal**	**H**
Political	Government scrutiny	Poor market performance	Panic	Teleworking technologies e.g., ZOOM	Pollution	Social distancing	**Health (COVID-19)**
Economic	Changes in trade	Lack of workers, government stimulus, layoffs, insolvency and bankruptcy	Racism, unemployment	Advances in virology, Increased use of technology for communication, Shortage of medical supplies	Lower fuel consumption,	Fines, tax	
Social	Social distancing, fines, mass quarantine	Work from home, travel bans	Travel fear, lifestyle, Values, cultural ideation	Increased use of technology for communication	Surging care needs, increased volume of unrecyclable waste	Shopping restrictions, closure of schools, travel ban	
Technological	Contact tracing apps	Fraud, scams, Price increases, supply chain disruption	Remote working	Increased use of technology, cybercrimes,	Increased use of heating/cooling systems at home	Cybercrime	
Environmental	Reduced air and road traffic	Frequent use of plastic bags	Stress and anxiety due to social distancing restrictions	Shortage of necessary medical technology e.g., ventilators	Climate change, cuts in agricultural, reduced tourism	Taxation	
Legal	Government stimulus	Government stimulus	Social distancing, quarantine requirements	Strict confidentiality, integrity, and availability requirements	Shipping restriction on agricultural and fishery supplies, illegal deforestation, fishing, and wildlife hunting.	Travel ban	

Case Study

During the design and review workshops, we conducted a risk analysis with the PESTLE+ model in IDZ as the case study. In the age of social distancing, doing most of the routine tasks online is the new norm. The entire identity ecosystem is stunned as multiple institutions around the world deal with the impact of COVID-19. Solutions like eIDV, electronic know your customer onboarding, electronic anti-money laundering, contactless payments, etc. are the need of the hour. The need to accurately identify and authenticate people and to authorize tasks and transactions through digital channels has accelerated. Hence, there is an increased demand for identity and authentication solutions that work seamlessly across endpoints that are application-appropriate, that comply with regulations, that reduce or maintain acceptable levels of fraud, and meet sudden surges of demand (scale). IDZ has an eIDV platform that provides identity verification services in a secure and cost-effective manner. Within IDZ's customer base, numbers have increased with significant upticks in financial services, telehealth, banking, online examinations, and online

gaming over the last few months. With the arrival of COVID-19, the threat landscape has also changed significantly, increasing the risk of identity theft and identity crimes. Consequently, the regulations have changed amid COVID-19. In circumstances like these, IDZ wants to conduct a thorough risk analysis to understand what this means for eIDV. How can IDZ adapt quickly to the new-normal in a heavily regulated industry? What additional risks are emerging as the world starts to place more trust in the digital world? Therefore, the overall objective for conducting the PESTLE+ analysis model is to analyze whether IDZ can reduce costs and maintain security and privacy protocols whilst growing their customer base and do both while their customers might have restricted freedom of movement.

The initial management review meeting concluded that IDZ needs to scale up to meet the high demand, ensure the availability of 99.9% uptime, maintain high standards of individual's privacy, security and trust, reduce the cost of eIDV services, while complying with applicable regulations. The increased demand for eIDV and the changing regulatory landscape highlights two major macro-environmental factors for IDZ, technology and legal. These are the key risk factors also mentioned in the digital

Table J2.b IDZ Risk Analysis using PESTLE+ Risk Analysis Model

Criteria	Risk
H(Technological x Economic)	• Some consumers are not able to afford the cost associated with emerging technology enabled eIDV services due to unemployment and pay cuts
H(Technological x Social)	• Due to the increased demand, there is a substantial surge in online scams including some medical goods, personal protective supplies and medicinal products. • Criminals are misusing fears about COVID-19 to add malware on personal computers or mobile devices • Some people might be less knowledgeable about using online banking programs, and thus more vulnerable to scam.
H(Technological x Political)	• Authorities, businesses and end users are rapidly opting for online approaches to facilitate remote work. The risk of identity theft is therefore, increasing • Criminals are impersonating government officials requesting personal details resulting in identity theft
H(Technological x Environmental)	NA
H(Technological x Legal)/ H(Legal x Technological)	• Due to a huge increase in worldwide remote working, cybercriminals are also manipulating vulnerabilities in businesses' network security to get access to customer contact and transaction data. • Strict information security and privacy compliance requirements
H(Legal x Political)	• Rise of privacy advocacy and monitoring groups in the wake of COVID-19. • The relaxation and introduction of new KYC procedures for some businesses leaves a big opportunity open for criminal activity
H(Legal x Economic)	• Restricted physical operations of Banks and financial institutions • Risk of becoming pre-engaged with business continuity matters whilst needing to deal with surveillance on suspicious financial transactions.
H(Legal x Social)	• Fraudsters can falsely allege to grant access to stimulus funds to acquire sensitive financial data
H(Legal x Environmental)	• Regulatory flexibility with respect to customer due diligence requirements

identity guide by the Financial Action task Force (FATF 2020). The guide mentions that to determine whether the use of an eIDV platform is secure and sufficient in these unprecedented times, governments, financial institutions, health professionals, academic institutes and other participants should ensure the security assurance presented by eIDV platform based on its technology, architecture and governance to determine its reliability and independence. During the workshop we conducted the H(technology) and H(legal) risk analysis using the PESTL+ model (see Table J2).

To bridge the gap caused by lockdowns and social distancing, there is a rise in the need for texting, schooling and education apps as well as for online shopping, streaming websites, video games and delivery services. There is an increased need for eIDV than ever before specifically from financial institutions and telehealth services. As a result, there is need for well-designed eIDV solutions that employ the latest technology, such as facial matching, artificial intelligence and machine learning, to verify an individual's claim about their identity. The technologies use many resources which will eventually increase the cost of the eIDV process. However, with the current surge of unemployment and pay cuts, consumers cannot afford costly eIDV services. Hence, balancing the demand and cost vectors is a risk for IDZ. In addition, with everything moving online, this has created opportunities for identity thieves and scammers to take advantage of unsuspecting people. Scammers are preying upon fears of infection (via fake COVID-19 websites, phishing emails and fraudulent phone calls,) and using this fear to steal personally identifiable information (PII), bank credentials and even health-related data. Consumers who are not familiar with technology are more vulnerable to identity fraud. This requires IDZ to be more vigilant and accurate in providing eIDV services. The changes in regulatory and compliance requirements are creating additional challenges for eIDV service providers during this disruptive period. In many countries, the AML guidelines support adaptable KYC practices and methods. In Australia, AUSTRAC has amended their requirements (Rules 4.3.12, 4.4.16, 4.5.8, 4.6.8, 4.7.8 and 4.15) to facilitate flexible KYC procedures for the duration of the COVID-19 crisis to make sure that organizations can depend on substitute proof of identity (AUSTRAC 2020). Not all the impacts of COVID-19 on IDZ are negative. As an example, the technological-environmental impact of COVID-19 is due to the decline of paper-based identity verification to almost 0% thus reducing the air and water pollution associated with paper manufacturing. However, COVID-19 has undoubtedly put more pressure on IDZ to ensure the privacy and security of their clients along with complying with regulatory requirements. Therefore, IDZ has to face the challenge of creating and maintaining a strong business continuity plan that covers any consequences or risks that could interfere with their most important business endeavors.

a. Intervention of *i*SAM2

As illustrated in Table J3, we were able to audit IDZ's ISMS against each of the assessment criteria, which enabled us to determine the IA maturity level for IDZ. From our analysis, the evaluation results indicate that the *i*SAM2 accurately measured IDZ's IA maturity level which matches our expectation of the maturity of the ISMS implemented in the organization. These *i*SAM2 results are then used by organizations to create improvement plans specifically customized to their organizational context. The IA maturity level for IDZ was found to be compliance focused. To improve the internal audit maturity level, a corrective and preventive action plan was made for IDZ that suggests IDZ do the following:

- Increase management contribution for the enhancement of risk management, compliance, and regulatory processes.

- Align ISMS with business strategy, long-term organizational goals and objectives.
- Undertake regular reviews
- Ensure clear and concise communications with the auditee and other involved parties.

Table J3 *i*SAM2 Implementation in IDZ

Basic																												
Audit Criteria	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11	1.12	1.13															Maturity Level
IDZ	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y															1
Compliance Focused																												
Audit Criteria	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13	2.14	2.15	2.16	2.17	2.18	2.19	2.20	2.21							Maturity Level
IDZ	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							2
Managed																												
Audit Criteria	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9	3.10	3.11	3.12	3.13	3.14	3.15	3.16	3.17	3.18	3.19	3.20	3.21	3.22	3.23	3.24	3.25	3.26		Maturity Level
IDZ	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y	Y		NA
Optimised																												
Audit Criteria	4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9	4.10	4.11	4.12	4.13	4.14	4.15	4.16	4.17	4.18	4.19	4.20	4.21	4.22						Maturity Level
IDZ	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N						NA

c. Intervention of *RRM*

IDZ intends to redesign its current DigI verification solution and implement a blockchain-based DigI verification solution. DigI returns control to users by issuing them with verifiable claims (VC) that can be self-custodied and shared only with trusted parties. The technological innovations of blockchain have made possible the issuance, storage, and verification of verifiable claims, irrespective of the involved parties meeting each other. The interaction of different entities in a blockchain-based DigI ecosystem is shown in Figure J1. IdP verifies the IO's identity from PII and issues VC to IO who registers and stores the VC on blockchain. The VC is presented to SP who verifies the signatures, trusts the DigI and identifies the IO upon success. The high-level business processes corresponding to each entity in the DigI lifecycle are detailed in Table J4.

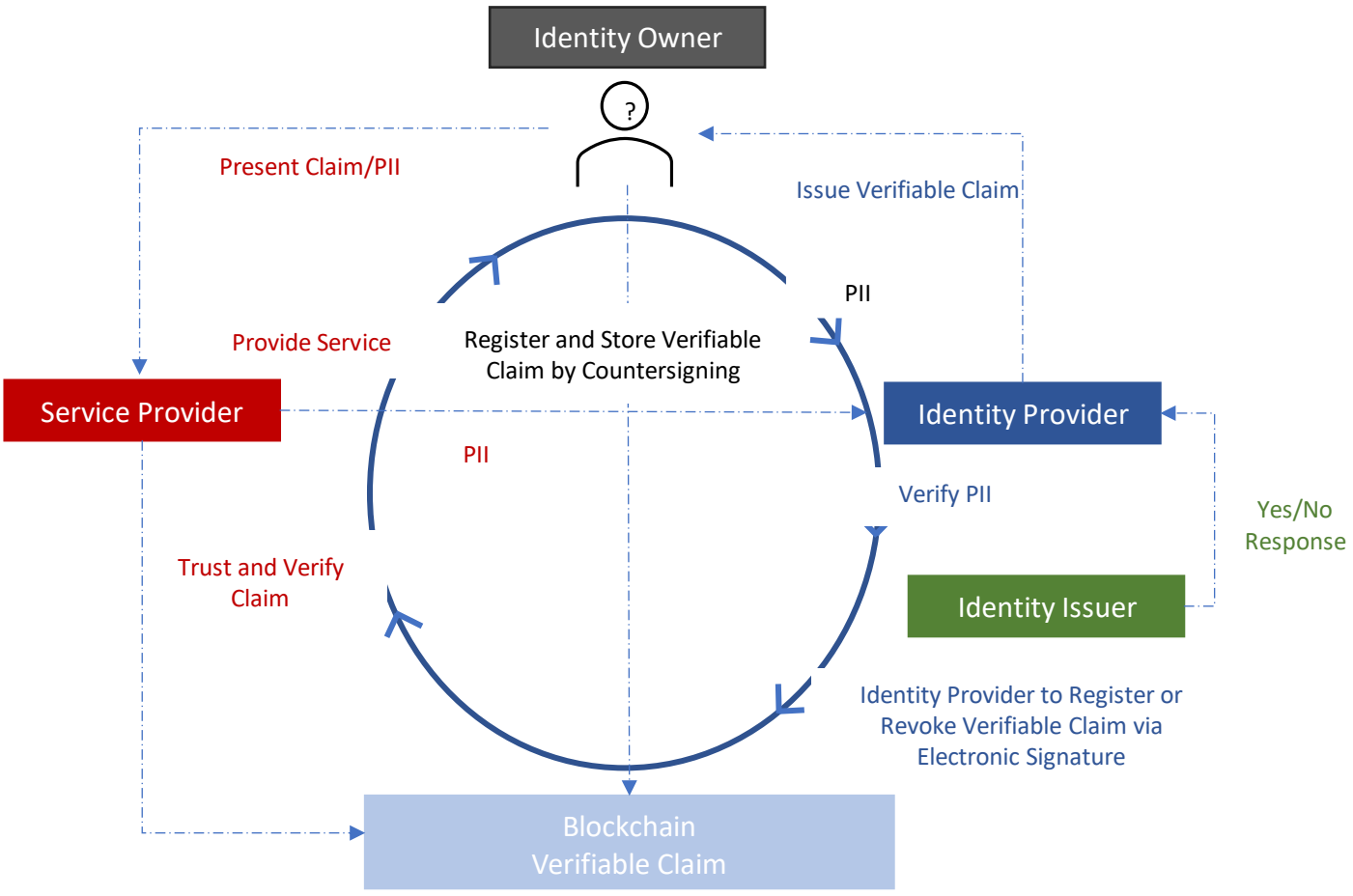


Figure J1. DDigI Lifecycle

Table J4. DDigI Business Process

Entity	Business Process
Identity Owner	Register a VC, Store VC, Present VC,
Identity Provider	Issue VC, Register a VC, Revoke VC
Identity Issuer	Verifies Identity document
Service Provider	Trust VC, Verify VC

Similar to GDPR, eIDAS is an EU regulation that changes the way digital interactions are executed. IDZ evaluates the generalization of RRM by extracting the regulatory requirements based on eIDAS. The RRM evaluation starts with reviewing articles from eIDAS in alignment with IDZ goals and integrating requirements from selected articles to the business processes identified in the previous section (See Table J5). Any article that addresses any of the DDigI business process (See Table J4) either fully or partly was included in the requirements.

Table J5 Mapping of IDZ Goals with eIDAS Articles

IDZ Goal	X Regulation Article (eIDAS)
Availability	Art.6, Art.12
Privacy and Security	Art 8, Art4, Art.10, Art.17
Confidentiality/Reliability	Art.17, Art.20-42
Technology Adoption	Art.7, Art.9
Non-Repudiation	Art.4, Art.17
Adaptability	Art.12
Compliance	Art.46

As a result, the requirement backlog comprising eight requirements was developed (see Table J6). Table J6 shows that RRM successfully extracted the regulatory requirements satisfying all the IDZ goals. Hence, no further changes were suggested for RRM during the design and review workshops.

Table J6. eIDAS based Regulatory Requirements for DigI Verification

X Regulation Article(eIDAS)	Requirement	Business Process	Description
Article-6	req-1: Mutual Recognition	Trust VC, Verify VC	DigI issued by one issuer must be mutually recognized by all others, provided it meets the regulation's requirements and the involved parties have been notified and it has been published in a list of recognized DigI providers.
Article-8	req-2: Assurance Levels- Low-Medium-High	Issue VC, Trust VC, Verify VC	A DigI must specify one of three levels of assurance (low, substantial, or high) for the form of a verifiable claim issued by the notified issuer.
Article- 7,9	req-3: Notification	Issue VC, Store VC, Trust VC, Verify VC	When notifying all the stakeholders of DigI, information must be provided on: the level of assurance and the issuer of DigI in that system; the relevant supervisory and liability entities; the entity handling the registration of VC
Article-10	req-4: Security Breach	Revoke VC, Trust VC	In case of a security breach incident for the DigI system or authentication, the notifying body: • Should immediately stop/revoke the VC authentication or the compromised parts of the DigI; and • notify all involved parties in the DigI life cycle
Article-12	req-5: Cooperation and interoperability	Issue VC, Present VC, Trust VC	Notified DigI systems must be interoperable and technology neutral.
Article-17	req-6: Supervision	Trust VC	• All parties involved in the DigI lifecycle must appoint a supervisory authority for the supervisory activities under this regulation. The supervisory bodies must not be biased and should work in cooperation with data protection authorities where needed. • A newly introduced concept of **EU trust mark** will recognize the competent trust services by service providers.
Article-20-42	req-7: Qualified Trust	Trust VC	• The regulation defines trust services as the establishment, authentication and authorization of electronic signatures, electronic seals or electronic time stamps, electronically registered delivery services and certificates related to those services; or • DigI verification solutions are deemed 'qualified' if they meet the regulation's minimum criteria. After qualifying, they are legally eligible to deliver **qualified trust services.**
Article 46	req-8: Legal effects of electronic documents	Register VC, Issue VC Store VC, Present VC, Trust VC, Verify VC	• An electronic form of identity e.g., DigI will not be rejected from having a legal impact and acceptability as proof in legal proceedings purely on the basis of being in an electronic form.

d. Evaluation of DigIVPM Using IdMPAM

The DigIVPM was evaluated during the design and review workshop using a simple scenario of a loan application. The workflow was executed on paper and evaluated using IdMPAM criteria. It was found that DigIVPM is comprehensive, useful and applicable in any DigI verification context. The details are shown in Table J7.

Table J7. Evaluation of DigIVPM using IdMPAM

IdMPAM Assessment Criteria	ADIVRA-Design	Description
Data Subject's Rights		
1.Right to be Erasure	**X**	User can delete their information anytime they want.
2.Right to be informed	**X**	Every time a user's information is accessed, they receive a notification. The information will only be shared if the user gives their consent
3.Right to Access	**X**	Information is stored on the user's phone and is accessible to him
4.Right to Rectification	**X**	The user can rectify the information anytime by providing a proof.
5.Right to Restriction of Processing	**X**	ADIVRA design component processes information for which the user has consented
Data Protection		
6.Minimal Disclosure	**X**	Only information needed for the purpose at hand is shared implementing the principle of Zero Knowledge Proof.
7.Data Breach Notification	**X**	User will be notified within 48 hours if any breach occurs
8.Privacy by Design	**X**	Privacy is embedded into the design of the DigI verification architecture. iSEA is made part of the ADIVRA design component to embed privacy into the design
Technology		
9.Use of Automation	**X**	OCR, Biometric and liveness test is used for authentication
10.Justifiable Parties	**X**	DigI is reusable.
11. Pluralism of operators and technology Design	**X**	
General		
12. New – Affordability	**X**	Reusability reduces cost and time required to conduct DigI verification
13. New – Simplicity	**X**	The ADIVRA design component is easy for inexperienced users to use
14. New – Multiple Document Support	**X**	ADIVRA design component supports multiple documents i.e. passport, driver's license etc.
15. New – Use Cases	**X**	ADIVRA can be applied to a generalized class of problems
16. New - Platform Support	**X**	Works both for iOS and Android as well as webapp

e. Evaluation of *CDigI*

To evaluate the potential of a compound digital identity from multiple sources and assess how it allows interactions that are difficult via an identity document based DigI structure, a real-life scenario of an accident at the gym was used.

The accident at the gym involving injuries or a serious medical situation entails multiple, independent flow of identity attributes in a complicated situation that includes several parties. The initial flow of identity attributes is shown in Figure J2.

In this scenario, a gym member, Alice, has had an accident resulting in serious injuries. The police arrive at the incident location to produce an incident report. Both Alice and the gym have a number of identity attributes that will be crucial in crafting the investigation report:

- Insurance certificate or equivalent document by an authorised insurance company.
- Gym equipment details.
- Alice's medical insurance

- Police officer's credentials representing his professional identity
- Business license of gym owner

Usually, each of these credentials is paper based, or at best, digital documents that need to be verified individually. Some of the credentials might not be recorded anywhere. Hence, the idea of verifying all the credentials digitally raises the challenge of a complicated identity verification process flow with patchy approval by the multiple players and authorities. CDigI modifies this by offering a flexible, decentralised system that enables swapping of heterogeneous credentials. All the identity attributes listed above can be separately issued by the relevant issuer, held by Alice, gym management, or the police, and shown to any entity approved by the identity owner. Alice controls her CDigI, the gym management controls their CDigI, and the police controls theirs.

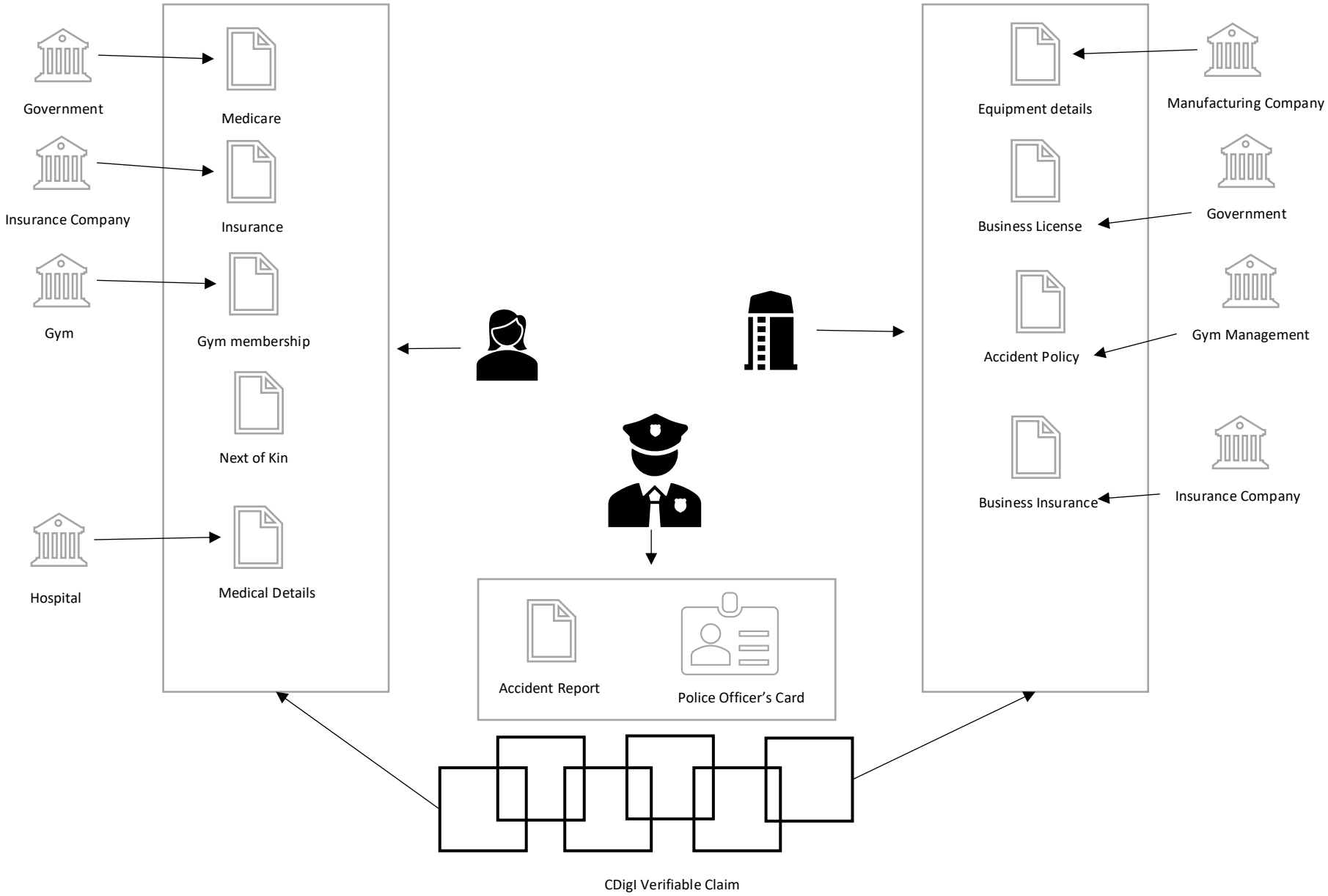


Figure J2. CDigI Credential Flow

f. Evaluation of *iSEA*

The *i*SEA was evaluated during the design and review workshops by creating an interaction diagram to dry run the flow of events as shown in Figure J3.

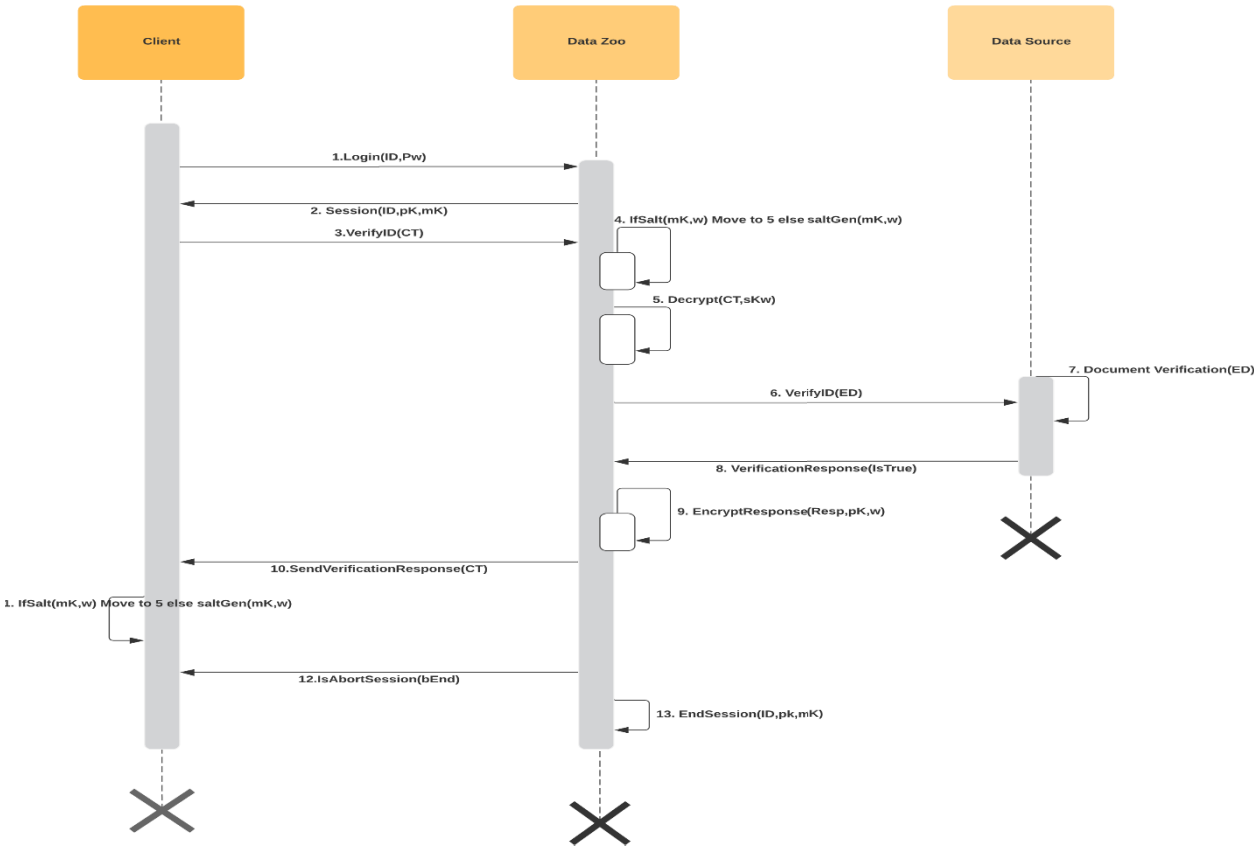


Figure J3. *i*SEA Sequence Diagram

g. Evaluation of *DigIVAM*

The DigIVAM was evaluated by applying it to IDZ's case. IDZ wants to extend their ISO 27001 Information Security management System (ISMS) to ISO 27701 Privacy Information Management System (PIMS). The design and review workshops analyzed how to adapt this change using DigIVAM. The details of the evaluation are presented in Table J8.

Table J8. Digital Identity Verification Adaption Model Activities

DigIVAM Stage	Activities	Description
Change Acquisition	**Identify source:** ISO 27001 Official Documentation, ISO 27701 Official Documentation **Cause:** Extending Information Security Management System to Privacy Information Management System for better GDPR compliance **Area of change:** compliance/regulation/standard	The source of this change is newly introduced privacy information management standard ISO17702:2019. The cause for this change is developing a baseline for GDPR compliance. The change will affect regulatory compliance of IDZ's DigI verification solution
	Change Classification: Major	This will be a major change in compliance. It will define IDZ's role as data controller, data processer or joint controller
	Prioritize change: Medium.	IDZ is already ISO27001, hence the priority of this change is medium
Manual Analysis	**Impact:** High	The impact of this change is high due to higher relevance of ISO27701with GDPR. It will provide IDZ with a baseline for GDPR compliance
	Risk: There is no risk associated with this change	Risks associated with adapting to change
Change Reaction	**Action Plan:** there should be no time constraint on breach notification.	ISO27001 requires companies to notify any breach incident within 72 hours whereas ISO27701 has no restriction on notification time. Hence, the constraint of 72 hours needs to be removed from the design.
	Implementation Plan: Timeline	The time required to implement ISO27701 Privacy Information Management system on top of ISO 27001 Information Security Management System is 4 months.