Requirements for Identity Management in Next Generation Networks

S.Subenthiran, Dr.K.Sandrasegaran, R.Shalak
Faculty of Engineering University
of Technology Sydney P.O.Box
123, Broadway
NSW 2007, Australia
Email: {ssuben, kumbes, rshalak}@eng.uts.edu.au

Abstract — Identity management will become crucial to the success of Next Generation Networks (NGN). However, until now very little research has been done in this field. This paper presents the requirements for identity management in NGN which are currently being investigated by our research group. Our analysis is based on the characteristics and requirements of NGN architectures, services, network operators, end users, identity management requirements for web services, recent standardization efforts by various bodies, etc.

Keywords-Next generation networks, network convergence, identity management, personalized services, mobility, credentials, authentication, authorization, access control.

I. Introduction

The concept of identity management is not new. For a long time, identity management was important for governments to maintain identities of its citizens relating to various contexts such as collecting taxes, providing welfare, etc. Information from a number of government departments are being consolidated together so as to provide better services to the citizens.

Identity management in large enterprise networks has been the focus of recent work. It has recently emerged as a critical foundation for realizing the Internet's business benefits in terms of cost saVing, management control, operational efficiency, and most importantly, business growth [I].

Solution and system providers have come up with various solutions for identity management in enterprise environments and web services [2]. For web users, there have been standardization efforts on identity management for web services, mainly driven by Web single sign-on (SSO) [3].

The requirements for identity management vary depending on the purpose, applications and the environment. For example, requirements for identity management in NGNs are different from identity management requirements in governments, enterprises or web services.

The objective of this paper is to analyze the requirements for identity management in an NGN. Sections 2 and 3 provide overviews of Next Generation Network and identity management respectively. Section 4 presents requirements for identity management in NGNs to meet the needs of end users, network operators, network roaming, application service providers, regulatory and legal bodies in terms of some of NGN's key functions such as operational, security, personalization, etc.

2. Next Generation Networks

The ITU-T Gil project defines an NGN as "... the provision of various services by a variety of service providers over a variety of network technologies from different industry sectors ..." [4). With NGN, multiple services such as telephony, Internet, video on Demand (VoD) and other multimedia applications along with new emerging services will be delivered over one network. The circuit based telecommunication networks will evolve into a packet based technology. Some of these services may rely on multitude of third service providers. Users will be accessing the network services from different locations using different access networks, network technologies and user terminals.

The NGN concept is commonly referred to through various fundamental characteristics. Some of the characteristics which *are* of interest to us are support of generalized mobility [5], personalized services [6) and location based services.

Mobility

In general, mobility refers to users' ability to change access point and/or terminal while getting their services in a consistent manner. Several service levels could be considered for mobility such as personal mobility, terminal mobility, nomadism and roaming (7).

In personal mobility the user is able to change location and/or terminal and/or access technique (WLAN, UMTS, Bluetooth, etc.). In terminal mobility the user is able to change location or access technique, while keeping the same terminal.

Nomadism means the user is able to change his network access point as he moves but there is no hand-over possible. It is assumed that the users need· to tenninate their service session before moving to another access point.

With roaming, the users are able to get access from a visited network different from the home network they have subscribed to.

Location Based Services

Location Based Service or LBS, is the ability to find the geographical location of the mobile device and provide services based on this location infonnation [8].

For example, if a person at a shopping mall wants to find out details of local restaurants then he needs only names and addresses of those restaurants within say one square km, out of the database of thousands of restaurants in the city spread over a large metropolitan area.

Personalized Services

In general, personalization or customization means something different to everyone. Personalization may involve tailoring information services to user needs, enable content filtering, providing conformance to service level agreement (SLA) such as maintaining quality of service (QoS) according to subscriber status, etc.

To perform personalization, identification and exchange of user profiles are required.

3. Identity Management

In its simplest form, identity management involves secure consolidation, management and exchange of user identity information also known as digital identity, discussed below, enabling accurate, reliable and secure services can be provided to clients over distributed network architecture.

Identity management involves the integration of processes and technologies into a unified framework and it encompasses user authorization, authentication, accountability, and access control.

Digital Identity

The definition of digital identity [1] varies depending on the context, environment, application, use etc. In an NGN, the focus of digital identity is for personalized, secure and trusted interactions with distributed networks and applications.

A digital identity consists of two parts [9]:

1. Who one is (identity)
2. The credentials that one holds (i.e. attributes of that identity, such as passwords, user profiles, etc.)

The simplest possible digital identity consists of an ID, such as a user name and an authentication secret, such as a password. This password is sometimes referred as authentication credential.

In general, these credentials that define a digital identity can have widely differing values and uses. This digital identity representation only needs to be as complete as a particular transaction requires.

Federated Network Identity

Federated Identity allows users to link identity information between accounts without centrally storing personal information [10]. Once users are authenticated by one trusted company or website, they can then be recognized by other affiliated companies or websites and obtain personalized contents and services without having to re-authenticate or sign on with separate usemames and passwords.

This ability to login once and obtain personalized contents and services by securely exchanging authentication credentials and profiles between trusted sites is also known as single sign-on (SSO).

Identity Management in NGN

In traditional telecommunication networks, identity management has not been an issue as networks, applications and billing for different services have not been integrated. For example, if a service provider offers telephone, Internet access and cable TV, then all of these services are treated separately. Each service has its own subscriber database containing subscriber records and identity information.

In an NGN, to provide seamless ubiquitous support to various services in a larger service provider environment, identity management becomes critical. Identity management in an NGN will be more complex than enterprise and web service solutions. It involves consolidation, management and exchange of identity information of users to ensure the users have fast, reliable and secure access to distributed network resources across multiple service providers.

Controlling multiple robust identities in an electronic World is a crucial issue in developing the next generation of distributed applications [II]. Digital identity information has to be exchanged between various entities in the network for the purpose of authentication, authorization, personalized on line configuration, access control, and accountability. The identity information in an NON could include a combination of names, unique user identifiers, terminal identifiers, addresses, user credentials, SLA parameters, personal profiles, etc. A digital identity may also depend on the context or role in which a user is interacting with the electronic world. For example, an employee will have different roles (or identity contexts) when accessing network services from an office and from home. Each of the roles could have different entitlements which could be defined in his or her personal profile.

The term personal profile refers to personal preferences, tools, resources, etc. Typically, a user profile may be composed of service subscription, user preferences, attributes of user terminals, resources, interests, groups they belong to and so on. The types of information stored and exchanged with a user profile can vary depending on the applications, environments, etc.

Benefits ofIdentity Management

A carefully researched identity management framework has number benefits. User experience is often improved as users can ubiquitously access services and applications of their choice over a number of service providers without going through separate logins and avoiding the need to remember multiple usemames and passwords or use multiple tokens. Service delivery can be improved, for example, the time required to get new subscriber access is reduced and it supports flexible user requirements and pe'rsonalization.

[1] In a networked environment, digital identity is also referred as network identity.

For the enterprise, there are numerous benefits such as reductions in the cost of new service launch, O&M (operation and maintenance) and increased ROI (Return on investment). In addition, it is a requirement to support distributed network architectures where entities communicate through open but secure interfaces. It is necessary for seamless user mobility across networks and terminals. It improves the security of the NGN and the user confidence in the use of the services. There are other benefits such as efficient implementation of current and new legal and compliance initiatives about·user data, behaviour and privacy.

However, introducing identity management solution can bring new form of security issues and threats. As you consolidate the identity related information, you create a new target for security attacks. But the advantage of implementing identity management is that you do not have to wony about protecting disparate solutions. Now you are able to consolidate your defense to one point.

Identity Management Solutions

In general, directories such as X.500 and LDAP form the basis for general purpose identity management solutions in enterprise networks and web services. X.500 has provided mechanism for representing identity around the world mainly in government and educational installations. X.500 and LDAP provide solution for secure consolidated identity information repository and access protocol [12].

In the 1990's LDAP has gained modest acceptance for some application developments but does not solve all the issues in identity management. One of the major challenges to identity management is controlling information when the entities that need to access it are dispersed and highly diverse [I].

As a result, recently numerous efforts have been initiated to resolve identity management in enterprise and web service environments to cater for the new requirements [12]. One of the bodies working on the standardization is the Liberty Alliance. It is an alliance of more than 160 companies, non-profit and government organizations from around the globe [13]. The consortium is committed to developing an open standard for federated network identity that supports all current and emerging network devices. Federated identity offers businesses, governments, employees and consumers a more convenient and secure way to control identity information in today's digital economy, and is a key component in driving the use of e-commerce, personalized data services, as well as web-based services. This Liberty Alliance Project standard is based on SAML (Security Assertion Markup Language) which is a work of OASIS (Organization for the Advancement of Structured Information Standards) [14]. It is an Extensible Markup Language (XML) standard that provides session based security solution for Web SSO by exchanging authentication, attribute, and authorization information between affiliated web sites.

Microsoft Corporation has launched and widely deployed its .NET passport service for Web-based SSO. It provides similar functionality to a Version 1.1 Liberty Alliance Project specification. Microsoft's.Net Passport is a centralized user authentication service thai allows easy and secure authentication of users to participating web sites [15].

Until recently there has not been much published research of identity management in NGN. We believe that identity management will be a hot topic as we move in to the era of Next Generation Networks.

4. Requirements for Identity Management

In this section, an analysis of the requirements for identity management in NGNs is presented. The analysis caters for the needs of end users, network operators, network roaming, application service providers, regulatory and legal bodies in terms of some of NON's key functional classifications such as operational, security, personalization, etc.

4.1 End User Requirements

Self Service

Self service is the ability of a user to actively manage his or her own records without requiring the intervention of help desk or support staff[l2].

All NGN users should be able to securely manage some of their own identity information such as changing passwords, subscription status, choosing their mobility status, changing roaming authorization, modifYing user profiles, enabling location based services, etc. Users should be able to view their up-to-date billing records and service usage patterns. To increase trust, users should be able to view their self service activity journal. Self service activity journal displays all the self service activities performed by a user. A user should also be able to delegate self service privileges to another user such as maintaining accounts of family members. Users should also be able to modifY content filtering options for upstream and downstream traffic.

Single Sign-on

Single sign-on should be implemented so that users login only once when they start a session. Subsequent access to other secure services should be possible by transparently and securely exchanging authentication credentials with third party service providers.

Security/Privacy

To increase privacy, users should be able to choose end to end data encryption. Users should also be able to stay anonymous while accessing network services. Unauthorized users should not be allowed to access, view or modifY identity information.

Mobility and Access Network Selection

NGN users should be able to choose access network of their choice using wide range of terminals, move between different access technologies with minimum configuration change and get access consistently to their set of services according to their user profiles.

Users should have a single identity regardless of the access technology or network used. Note that mobility across the heterogeneous environment requires service adaptation for terminal mobility as well as personal mobility [7]. That is, in the event of service difficulty during mobility, users should

receive user friendly notification with choices of actions to restore the service without the *need* to Contact support staff.

4.2 Network Operator Requirements

Identity Management Server General Requirements

The Next Generation Network operator should be able to maintain a single identity for each user, tenninal, network element, etc., regardless of service and technologies used. For example, in a mobile communication network, each user has an IMSI (International Mobile Subscriber Identifier), each terminal equipment has an IMEI (International Mobile Equipment Identifier), and each network element has an IP address or logical name associated with it. If the user is using faulty or dubious terminal equipment, it should be possible to bar services to the user.

Identity data stored in a network should cater for various types of identity information and data structures. Proper implementation of account lifecycle management is required [12], i.e., administrators should be able to manage the state of a user account for the complete span of that account. Even if an account is deleted or disabled, an audit history of the account should be maintained. The network operator should be able to remove self service privilege of some users.

The identity management framework should support open standards in order to interact with multi-vendor terminals and network elements. **It** should be compatible with existing legacy systems and be able to adapt to emerging technologies, methods and procedures.

Scalability and Performance Requirements

The identity management framework should be able to store, retrieve and exchange billions of identity information in a highly seamless and scalable manner. The identity management implementation should exchange this information in a quick and efficient manner to facilitate multiple real-time service requests.

It should achieve a high level of availability by incorporating fault tolerant redundant system implementation. Furthermore, it should implement geographically distributed identity management servers in order to increase performance efficiency by load sharing and providing high availability. **It** should also maintain integrity and consistency of identity data across distributed identity information stores.

Mobility Management Requirements

According to the type of service and subscription level, the users should have personal and/or terminal mobility, roaming or nomadism. Mobility management may require a combination of identification, authentication, access control, authorization, location management, IP address allocation and management, user environment management and user profile management functions.

Network should cater for both foreign and visited network IP address or home network IP address allocation scheme.

Security Requirements

Security requirements should cover privacy, confidentiality, integrity, authenticity, non-repudiation, availability, intrusion detection and maintenance of audit records as described below.

Users and terminals should be reliably authenticated using a nominated set of authentication credentials such as passwords, smart cards, biometrics and other industry standard methods. All the identity data should be kept in a very high secure and scalable manner. Unauthorized access to identity data should be prevented.

Intrusion detection is required to detect and prevent security breaches. This can also be done to minimize the fraudulent use of resources in a network

Network administrators should be granted different levels of access to according to their authority within the organization. For accountability and security reasons, consistent and reliable audit records of administrative activities must be kept.

In order to apply user and data security such as confidentiality, integrity and authenticity, the identity management server should securely store and exchange relevant encryption and decryption keys.

Billing Requirements

Up to date, accurate and detailed billing information should be maintained in accordance to the subscriber agreement The network operator should be able to charge based on usage, access networks, time, geographical area, etc

4.3 Network Roaming Requirements

Access to services through a visited network with which the home network has signed a roaming agreement is a requirement [7]. ln order to implement network roaming, the home network operator should support federated identity management and should securely exchange some authentication credentials and personal profiles with the visited network operator to provide secure access and exchange billing information.

Identity of each user should be uniquely and reliably identified among multiple network operators. The network operators may have to rely on third PartY identity service providers where the user has already established an account.

The identity management and related systems should support open standards with choices of technologies in order to intemperate with other entities.

Billing records of the user and the visited network operators' accounts should be dynamically updated according to the usage.

4.4 Application Service Provider Requirements

A user may require *services* from a third party application service provider. In this scenario, the home operator and the application service provider should support federated identity management to provide secure access and exchange of billing information.

Similar to the network roaming requirements, identity of each user should be uniquely and reliably identified among multiple application service providers and network operators. The application service providers may have to rely on third party identity management service providers where the user has already established an account. Billing records of the user should be dynamically updated according to the usage.

The identity management and related systems should support open standards with choices of n_umber of technologies in order to intemperate with other entities.

4.5 Regulatory Requirements

The entities should support open standards and choices number of technologies to promote · competition and flexibility. Privacy and confidentiality of subscribers' personal information should be maintained at all times.

4.6 Legal Requirements

Privacy and confidentiality of subscribers' personal information and prevention of unauthorized access should be maintained at all times. Subscribers should have a choice of what information can be shared with various third parties. Reliable audit record of administrative and user activity should be kept which could be retrieved and submitted to courts and other entities to meet legal requirements.

Legal interception of subscriber data should be possible. One of the new requirements for telecommunication network operators is to collect and pass on real-time transactions of target subscribers to law enforcement authorities [16]. Legal interception of subscriber data should be possible whichever network or service a subscriber is using.

5. ConeIusion

In this paper we analyzed the requirements for identity management in an NON to meet the needs of end users, network operators, network roaming, application service providers, regulatory and legal bodies in terms of some of NGN's key functions such as operational, security, personalization, etc.

In an NGN, to provide seamless ubiquitous support to various services in a larger service provider environment, identity management becomes critical. Until now very little research has been done in this field. We believe that identity management will be a hot topic as we move in to the era of Next Generation Networks.

REFERENCES

[1] Duncan A. Buell, Ravi Sandhu, "Identity Management", IEEE Computer Society, Nov/Dec 2003.

[2] Liberty Alliance Project, "Liberty Alliance Project- Enabled products", http://v. v\v_prnjectlibertv org/resources/enabled html December, 2003

(3) Wason, Thomas, "Liberty ID-FF Architecture Overview,Version 1.2, Liberty Alliance Project (12 November 2003). http://www.projectliberty.orglspecs

[4] Moore, Brian W, "The ITU's Role in the Standardization of the GII", IEEE Communications Magazine, September 1998, pp.98-106.

[5] T. Dagiuklas, "NGN Architecture and Characteristics", ETSI, http://docbox etsi.org/NGN/SG/50-Meeting/0106-02Sophia/0205%20NGN Architecture and Charactcristics.doc, June 2001

[6] Valerie Blavette, "Framework for personalisation of services and applications in next generation services", EURESCOM Project P-1308, hl!Irf/wv.w. eurcscqm. deiP..M!llilip..!9$f:!s/P1300-s 1)08/

[7] France Telecom, "Inter-network mobility requirements considerations in NGN environments", STIJDY GROUP 13 DELAYED CONTRIBUTION 322, TELECOMMUNICATION STANDARDIZATION SECTOR (WP 2/13), Geneva, 29 October- 8 November 2002.

[8] Maneesh Prasad, "Location based services", GIS Development, http://v.v..'\v_gisdevelopment.net/technologv/Jbsltechlbs003.htm

[9] Digital Identity World, "What is Digital Identity?" http://www.digitalidworld.com/

[IO]Liberty Alliance Project, ..."Frequently Asked Questions" http://w.\w.projectliberty.org/about/faq.html, April 2003

[11] Damiani, De Capitani di Vimercati, Samarati, "Managing Multiple and Dependable Identities", IEEE Computer Society, Nov/Dec 2003.

[12]Reed, Archie, "Definitive Guide to Identity Management", Rainbow Technologies, 2002

[13)Liberty Alliance Project, "Introduction to the Liberty Alliance Identity Architecture Revi.O", March 2003

[14] OASIS, "OASIS Security Services TC", htto://v.ww_oasis·ooen org/committees/secumy/

(15]Microsoft, ".NET Passport: Balanced Authentication Solutions", http://wv.v.·_microsoft.com/netlservices/passoortlbalanced asp April 2003

[16]Council of Europe, "ETS No. 185 ·Convention on Cybercrime", Article 21, European Treaty Series (ETS) http://conventions.coe.intffreaty/enff reaties!Htm l/1 85_htm, Budapest, 23 November2001