INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Y.2720

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(01/2009)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

NGN identity management framework

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Recommendation ITU-T Y.2720 (Y.ngnIdMframework):

NGN identity management framework

[This page intentionally left blank for this distribution version]

Recommendation ITU-T Y.2720 (Y.ngnIdMframework):

NGN identity management framework

Summary

This Recommendation provides a framework for Identity Management (IdM) in Next Generation Networks (NGN). The primary purpose of this framework is to describe a structured approach for designing, defining, and implementing IdM solutions and for facilitating interoperability in a heterogeneous environment.

The management of entity identity information (e.g., identifiers, credentials and attributes) is not new. However, as we move towards a converged network environment where services are based on contexts and roles and may be accessed anywhere, anytime, the assurance, security and management of identity information becomes more complex. Additionally, there may be different and independent solutions resulting in the need for interoperability. Therefore new, enhanced, automated and interoperable capabilities are needed for the following reasons:

- end users are increasingly using multiple identities,
- these identities may be associated with different contexts and service privileges,
- the identities may only partially identify the end user,
- the identities may be used anywhere and at anytime, and
- the identities may not be interoperable between providers,

IdM addresses this situation, and is a set of functions and capabilities (e.g. administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- assurance of identity information (e.g., identifiers, credentials, attributes),
- assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects), and
- enabling business and security applications.

This framework is intended to be used as a foundation to develop and specify specific aspects of IdM, such as detailed requirements, mechanisms and procedures, as needed. It also provides a clear and coherent overview of the totality of IdM in NGNs.

The framework provided in this Recommendation is intended for NGN (i.e., managed packet networks) as defined in ITU-T Recommendation Y.2001, *General Overview of NGN*. However, it could be applied as appropriate to other types of networks (e.g., corporate and enterprise networks).

Note: the use of the term 'Identity' in this Rrecommendation relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation of a person.

1 Scope

This Recommendation provides an IdM framework for NGNs. The primary purpose of this Recommendation is to describe the fundamental concepts, functional components and capabilities of IdM that can be used to organize and guide structured solutions for NGNs. The scope of this Recommendation includes:

- describing the business motivations, benefits, and advantages of IdM services, and the generic capabilities used to provide identity assurance and defining IdM concepts applicable to NGN and based on the NGN Functional Requirements and Architecture (FRA) as defined in [ITU-T Recommendation Y.2012], [*Functional Requirements and Architecture of the NGN Release 1*],
- identifying and describing the functional entities, roles, relationships, enablers and communications supporting IdM services and capabilities for NGN,
- identifying and describing the intra-network relationships for supporting IdM services and capabilities within an NGN, and
- identifying and describing the relationships for supporting IdM services and capabilities between NGN providers (e.g., within a federation), and between NGN providers and other providers (e.g., inter-federation).

The framework provided in this Recommendation is intended for NGN (i.e., managed packet networks) as defined in [ITU-T Recommendation Y.2001], *General overview of NGN*. However, it could be applied as appropriate to other types of networks (e.g., private corporation and enterprise networks).

This framework is intended to be used as a foundation to develop and specify specific aspects of IdM for NGNs, such as detailed requirements, mechanisms and procedures, as needed. It also provides a clear and coherent overview of the totality of IdM in NGNs.

Note: the use of the term 'Identity' in this recommendation relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation of a person.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2001] ITU-T Recommendation Y.2001 (2004), *General overview of NGN.*

[ITU-T Y.2011] ITU-T Recommendation Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional Requirements and Architecture of the NGN Release 1.*

[ITU-T Y.2701] ITU-T Recommendation Y.2701 (2007), *Security Requirements for NGN Release 1.*

[ITU-T Y.2702] ITU-T Recommendation Y.2702 (2008), *NGN Authentication and Authorization Requirements.*

[ITU-T Y.2205] ITU-T Recommendation Y.2205 (2008), *Next Generation Networks – Emergency Telecommunications – Technical Considerations*

[ITU-T E.107] ITU-T Recommendation E.107 (2007), *Emergency Telecommunications Service (ETS) and Interconnection Framework for National Implementations of ETS.*

3 Definitions

3.1 Terms defined in other ITU recommendations

This Recommendation uses the following terms defined in other documents.

anonymity [X.1121]: Ability to allow anonymous access to services, which avoid tracking of user's personal information and user behaviour such as user location, frequency of a service usage, and so on.

authentication [X.811]: The provision of assurance of the claimed identity of an entity.

authorization [X.800]: The granting of rights, which includes the granting of access based on access rights.

claimant [X.811]: An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

delegation [X.911]: The action that assigns authority, responsibility or a function to another object.

identifier [Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects).

Next Generation Network (NGN) [Y.2001]: A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

principal [X.811]: An entity whose identity can be authenticated.

security domain [X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain. [used once]

verifier [X.811]: An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

3.2 Terms defined in other non-ITU standards

attribute [ETSI TS102 042]: Descriptive information bound to an entity that specifies a characteristic of an entity such as condition, quality or other information associated with that entity.

3.3 Terms defined in this Recommendation

This Recommendation defines the following terms:

assurance: a measure of confidence that the security features and architecture of the Identity Management capabilities accurately mediate and enforce the security policies understood between the Relying Party and the Identity Provider.

authentication assurance: See Assurance.

assurance level: a quantitative expression of Assurance agreed between a Relying Party and an Identity Provider.

credential: An identifiable object that can be used to authenticate the claimant is what it claims to be and to authorize the claimant's access rights.

discovery: The act of locating a machine-processable description of a network-related resource that may have been previously unknown and that meets certain functional criteria. It involves matching a set of functional and other criteria with a set of resource descriptions. The goal is to find an appropriate service-related resource.

entity: Anything that has separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices. An entity may have multiple identifiers.

f**ederation:** establishing a relationship between two or more entities or an association comprising any number of service providers and identity providers.

f**ederated identity:** An identity that can be used to access a group of services or applications that are bounded by the policies and conditions of a federation.

identity: Information about an entity that is sufficient to identify that entity in a particular context.

identity provider: An entity that creates, maintains and manages trusted identity information of other entities (e.g., user/subscribers, organizations, and devices) and offers identity-based services based on trust, business and other types of relationship.

identity management: Set of functions and capabilities (e.g. administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- assurance of identity information (e.g., identifiers, credentials, attributes),
- assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects), and
- enabling business and security applications.

pattern: A structured expression derived from the behaviour of an entity that contributes to or provides identification; this may include the reputation of the entity. Patterns may be uniquely associated with an entity, or a class with which the entity is associated.

personally identifiable information: the information pertaining to any living person, which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person).

presence: A set of attributes that characterizes an entity relating to current status.

privacy: the protection of Personally Identifiable Information.

relying party: An entity that relies on an identity representation or claim by a Requesting/ Asserting entity.

trust: A measure of reliance on the character, ability, strength, or truth of someone or something.

4 Abbreviations

API	Application Programming Interface
CSCF	Call Session Control Function
FRA	Functional Requirements and Architecture
GBA	General Bootstrapping Architecture

IdM	Identity Management
IdP	Identity Provider
NGN	Next Generation Network
OAM&P	Operation, Administration, Maintenance and Provisioning
PII	Personally Identifiable information
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
RP	Relying Party
SAML	Security Assertion Markup Language
SBC	Session Border Controller
SIP	Session Initiation Protocol
SP	Service Provider
SS7	Signaling System No. 7
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol

5 Introduction

5.1 Identity management (IdM) overview

The management of entity identity information (e.g., identifiers, credentials and attributes) is not new. However, as we move towards a converged network environment where services are based on contexts and roles and accessed anywhere, anytime, the assurance, security and management of identity information becomes more complex. Additionally, there may be different and independent solutions resulting in the need for interoperability. Therefore new, enhanced, automated and interoperable capabilities are necessary. The primary purpose of this framework is to describe a structured approach for designing, defining, and implementing solutions that will facilitate interoperability in heterogeneous environment.

IdM addresses this situation, and is a set of functions and capabilities (e.g. administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- assurance of identity information,
- assurance of the identity of an entity, and
- enabling business and security applications.

Figure 1 provides a general overview of IdM.

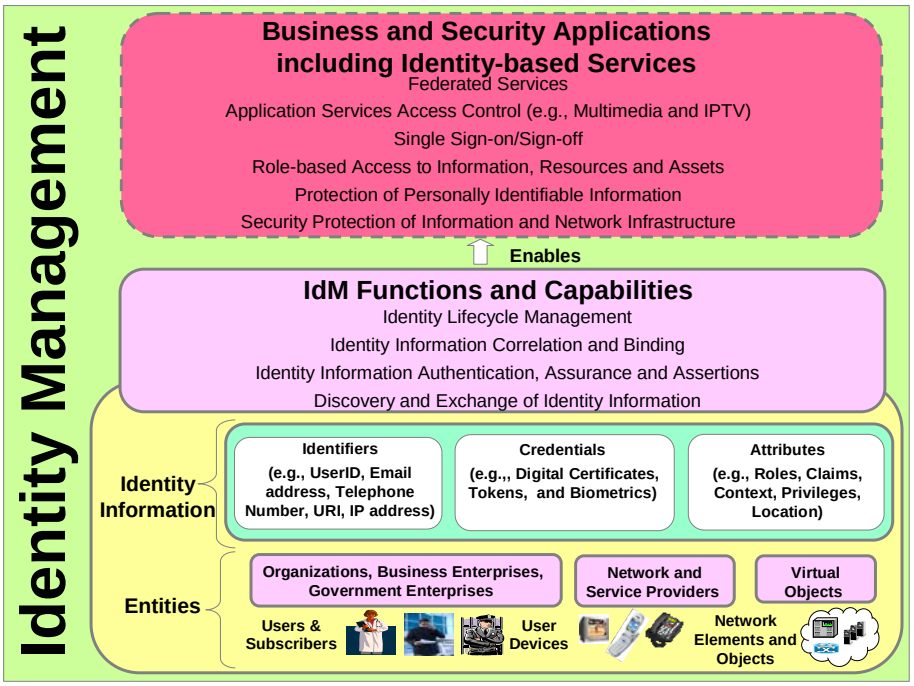

Figure 1 – IdM Overview

Identity information associated with an entity can be grouped as follows:

- identifiers (e.g., UserID, email addresses, telephone numbers, URI and IP addresses),
- credentials (e.g., digital certificates, tokens and biometrics), and
- attributes (e.g., roles, claims, privileges, patterns and location).

IdM functions and capabilities are used to assure identity information; assure the identity of an entity; and support business and security applications including identity-based services.

In addition, IdM services and capabilities also allow users/subscriber entities to control how their identity information is used and disseminated. IdM also allows federated identity information to be shared and used by members of a federation (e.g., business partners) to support federated services.

IdM enables various applications to be developed. Example applications are, but not limited to,

- business applications:
  - single sign-on and sign-off (e.g., access to multiple applications and services without having to individually authenticate to each application or service platform)
  - federated services (e.g., access to services across different service providers or NGN providers)
- identity-based services:
  - identifier, credential and attribute services
  - bridging services (mapping and interworking of identity information in a heterogeneous environment)
  - pattern information services
- security applications:
  - access control for network and application services (e.g. VoIP, IPTV and data)
  - role-based access control to information, resources and assets
  - authorization and privilege management

- security protection services (e.g., security features to protect network infrastructure resources and users/subscribers identity information and assets).
- Protection of personally identifiable information (PII).

In a multiple service provider and federated environment, IdM services and capabilities are used to discover and communicate information to establish confidence in the identity(s) of an entity among different network entities such as subscribers/claimants, relying parties (e.g., users, service providers and network providers) and identity service providers (e.g., credential providers and verifier providers) across network and security domains. For example, identifiers, credentials and attributes associated with an identity can be verified by a selected identity provider (e.g., authentication/verifier provider) and communicated through assertions to a relying party (e.g., a service provider) to facilitate access control, business decisions, and enforcement of applicable policies (e.g., privacy and protection of personally identifiable information).

5.2 Business drivers and motivations

In addition to being an enabler of NGN security, IdM enables and facilitates new and emerging NGN business applications and services (e.g., converged fixed and mobile applications and web-based applications). Specifically, IdM services, capabilities and functions support a broad range of end users/subscribers, business enterprises (e.g., networks, service providers, corporations) and government enterprises applications and services as shown in Figure 2.

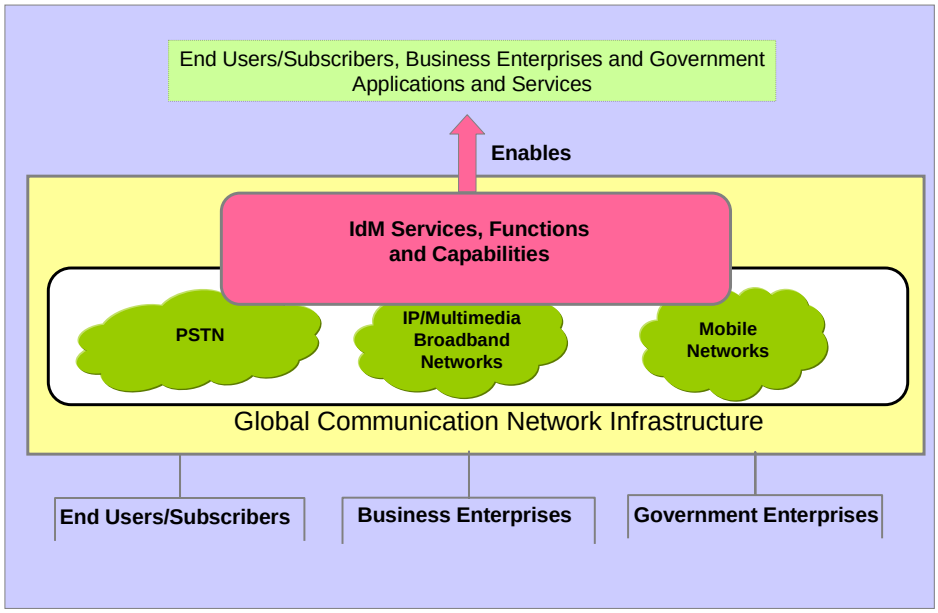

Figure 2 – Use of IdM Services

IdM is a critical component in managing NGN security and enabling the nomadic, on-demand access to NGN services and applications that characterizes end-users' expectations in the information age. Along with other defensive mechanisms (e.g. firewalls, intrusion detection systems, and virus protection), IdM plays an important role in protecting the NGN infrastructure and services and applications from cybercrimes such as fraud and identity theft. In addition, since users will have confidence that NGN transactions will be secure and reliable, IdM will enable new identity based service offerings. The use of IdM will therefore significantly enhance existing services and network capabilities. The drivers and motivations of IdM are summarized in Table 1.

Perspective	IdM Drivers and Motivations
End Users/Subscribers	• User control of personal information and protection of personally identifiable information – provides the ability to control who is allowed to access (i.e., providing consent) to personal information and how it is used. • Single sign-on / sign-off – provides uniform access to multiple applications/services and across multiple service providers/federations. • Flexible access control for network and application services (e.g. VoIP, IPTV and data). • Social Networking – provides dynamic and flexible identity capabilities to access social networking services with confidence. • Security – provides confidence in transactions, to include identity theft protection.
Business Enterprises (e.g., NGN Providers)	• Enables access to subscription based services from anywhere, anytime and any device. • Provides identity assurance functions and capabilities to support multiple applications and services. • Enables dynamic/automatic connectivity between multiple partners (e.g., end users, visited and home networks) compared to pair-wise arrangements to establish service arrangements, exchange identity information and enforce policy. • Enables new applications and services (e.g., fixed and mobile convergence) including identity-based services such as identifier, credential and attribute services to subscribers and other service providers. • Enables a standard API and data scheme for application design across multi-vendor and service delivery platforms. • Enables federated identity and services. • Provides protection of application services, network infrastructure and resources. • Enables easier compliance with regulatory requirements.
Government Enterprises	• Enables identity assurance services and capabilities, and enhancing the level of trust and confidence in identities to support ➢ Electronic government (eGovernment) services (e.g., web-based transactions)

	➢ public safety services (e.g., emergency 911 services) ➢ law enforcement services (e.g., lawful intercept) ➢ Emergency Telecommunications Service ➢ early warning services ➢ national security services • Enables federated government services • Provides protection of the communication infrastructure (i.e., against cybersecurity threats)

Table 1 – IdM Drivers and Motivations

5.3 Identity provider (IdP)

This Recommendation does not impose any restriction on who provides Identity Provider (IdP) services.

An IdP is an entity that creates, maintains and manages trusted identity information of other entities (e.g., users/subscribers, organizations, and devices) and offers identity-based services based on trust, business and other types of relationships.

In a multiple service provider environment, it is possible for an NGN provider to be an Identity Provider. It is also possible for an NGN provider to offer IdP services (e.g., identity-based services) to other providers. In addition, it is possible to use third party IdP services.

5.4 NGN functional architecture and use of identifiers

As described in [ITU-T Y.2012], *Functional requirements and architecture of the NGN release 1*, the NGN consists of multiple functional elements that use identifiers of entities to perform their functions in order to support and facilitate services and applications. Figure 3 shows examples of identities mapped into NGN functional diagram, i.e. the NGN architecture shown in [ITU-T Y.2012].

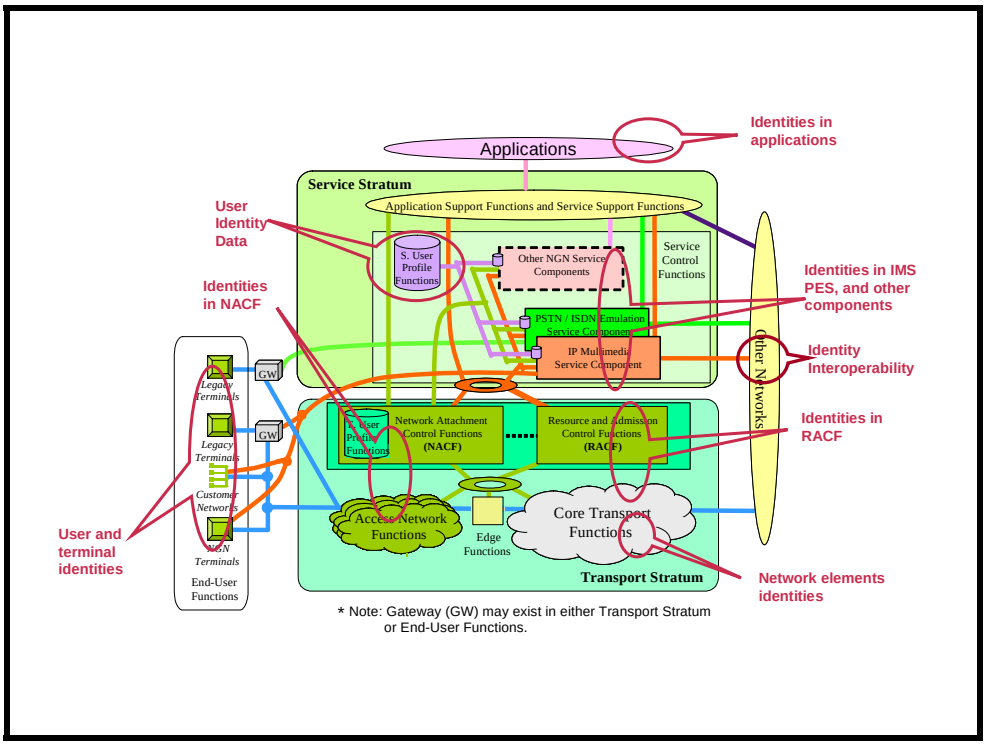

Figure 3 - Example NGN Identities

Since all NGN operations use these various identities, it is important to maintain their integrity. IdM provides assurance services, capabilities and functions to maintain their integrity and the use of NGN identities.

In the NGN network environment, a single entity may have multiple identity attributes. Different network elements may use these identity attributes (e.g., in different NGN provider domains or different strata of the NGN (i.e., the service stratum or transport stratum)). Different entities in different locations may also use these identity attributes. It is therefore necessary for IdM to provide capabilities that allow secure information exchange between entities (and/or locations) such as Relying Parties (e.g., application or service providers) and Identity Providers (IdP). Note, the NGN provider can also be an IdP. The exchange of IdM information is based on established policies and on trust established between these entities in a multiple service provider environment. This trust is based on the assertion and validation of the entities' identities across distributed NGNs. IdM also provides capabilities to protect the privacy of the entities' information (e.g., specific identity attributes), and to ensure that only authorized information is disseminated across NGNs.

6 IdM framework overview

The framework is organized as shown in Figure 4.

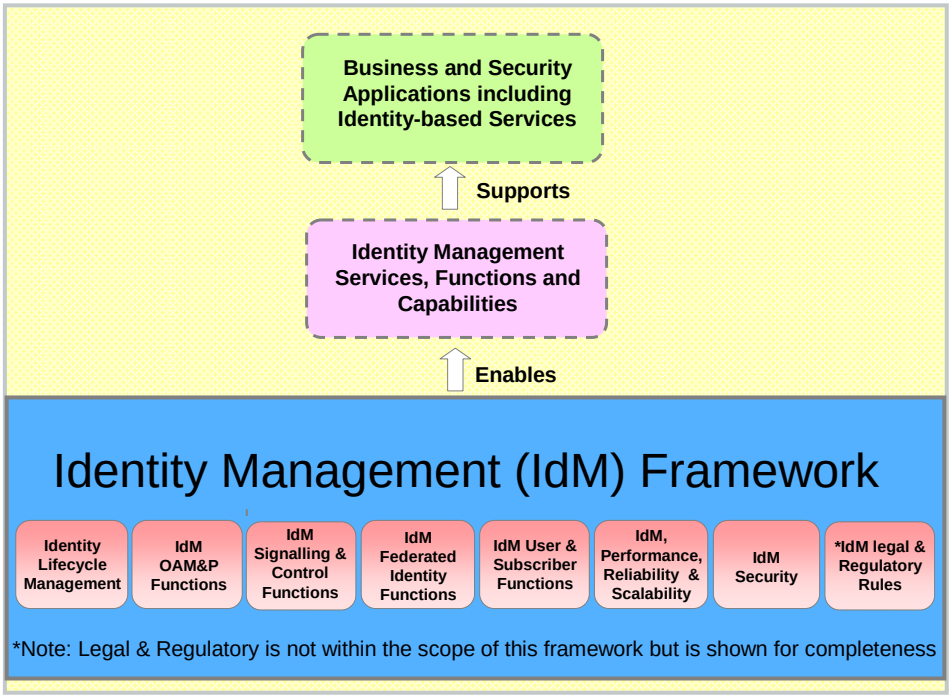

Figure 4 - IdM Framework Overview

The framework consists of the following IdM functions and capabilities:

1. Identity Lifecycle Management

   This includes Lifecycle Management processes and functions for identities and identity information (e.g., identifiers, credentials, and attributes). Identity lifecycle management involves the processes and procedures associated with the enrolment and issuance of identity data and information associated with an identity of an entity.

2. Identity Management (IdM) Operation, Administration, Maintenance and Provisioning (OAM&P) Functions

   This includes Operation, Administration, Maintenance and Provisioning (OAM&P) management functions and capabilities specifically related to support of IdM. OAM&P is a group of management functions that provide system or network fault indication, performance monitoring, security management, diagnostic functions, configuration and user provisioning. Specifically, it includes functions and capabilities supported by network management systems, typically called OSS (Operations Support System) and BSS (Business Support System).

3. Identity Management (IdM) Signalling and Control Functions

   This includes signalling and control functions and capabilities used for the support of IdM services, capabilities and functions. This includes signalling and control for both real-time and near-real time communications.

4. Identity Management (IdM) Federated Identity Functions

This includes functions and capabilities for identity federation and support of federated services.

5. Identity Management (IdM) User and Subscriber Functions

   This includes functions and processes related to control by end users and subscribers of their identity related information (e.g., PII, personal preferences and location). This includes functions to control, delegate and authorize use and dissemination of identity-related information.

6. Identity Management (IdM) Performance, Reliability, and Scalability

   This includes functions and procedures addressing performance, reliability and scalability of IdM systems and solutions.

7. Identity Management (IdM) Security

   This includes functions and procedures addressing the security protection of IdM systems, services and capabilities.

8. Identity Management (IdM) Legal and Regulatory Rules

   Legal and regulatory regulations are not within the scope of this Recommendation. (Note: this item is shown here for completeness).

The detailed description of each item is provided in clause 8.

7 IdM in the context of NGN architectures and reference models

7.1 General relationship with NGN architectures and aervices

Figure 5 illustrates the relationship of the IdM framework in the broader context of NGN networks.

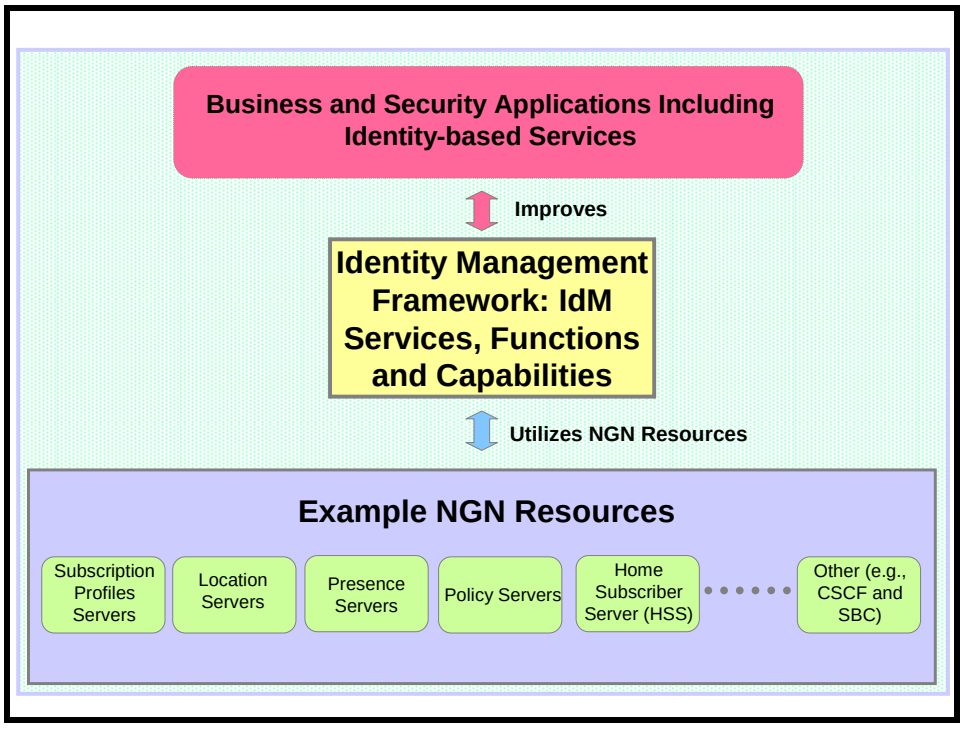

Figure 5 – Relation with NGN Architectures and Services

As shown in the diagram, the framework utilizes the resources of the NGN network (e.g., information in subscription, location, policy, presence and home subscriber servers and other

network elements such as Call Session Control Function (CSCF) and Session Border Controller (SBC)). The IdM services, functions and capabilities provided by the framework are used to support and enhance business and security applications including identity-based services.

7.2 ITU-T Recommendation Y.2011 (General principles and general reference model for NGN) reference models

This clause describes the IdM services, functions and capabilities in context of the NGN architectural models and references defined in [ITU-T Y.2011], *General principles and general reference model for Next Generation Networks*.

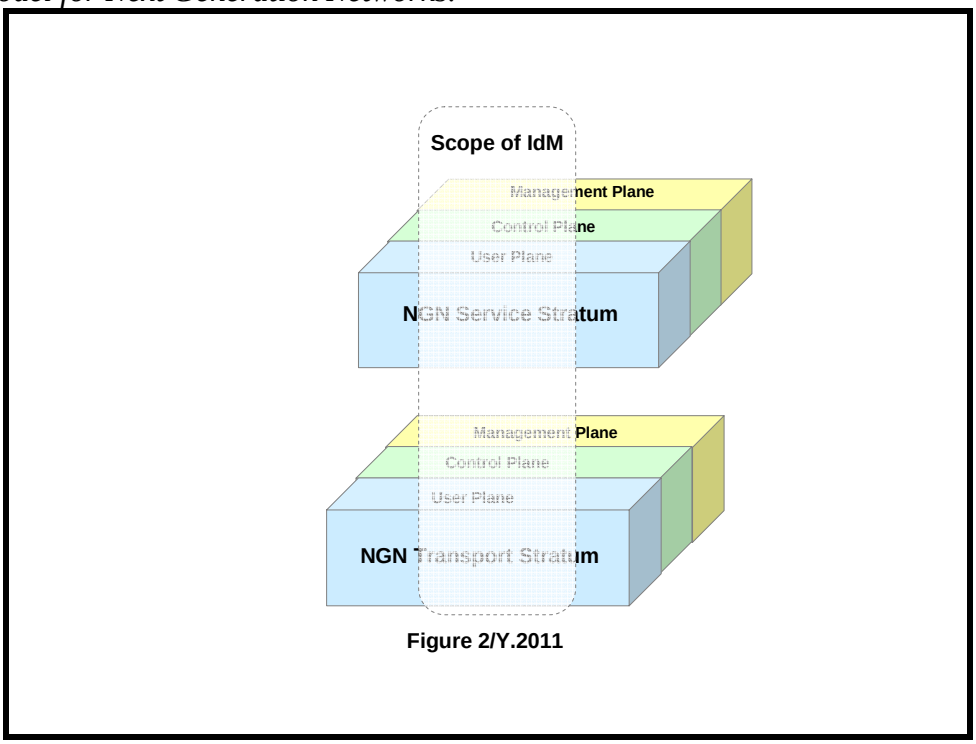

Figure 6 – Scope of IdM in Context of Figure 2/Y.2011

Figure 6 shows the scope of IdM in context of the NGN reference architectural model defined in Figure 2 of [ITU-T Y.2011]. It shows that IdM-related functions may be found in the user, control and management planes.

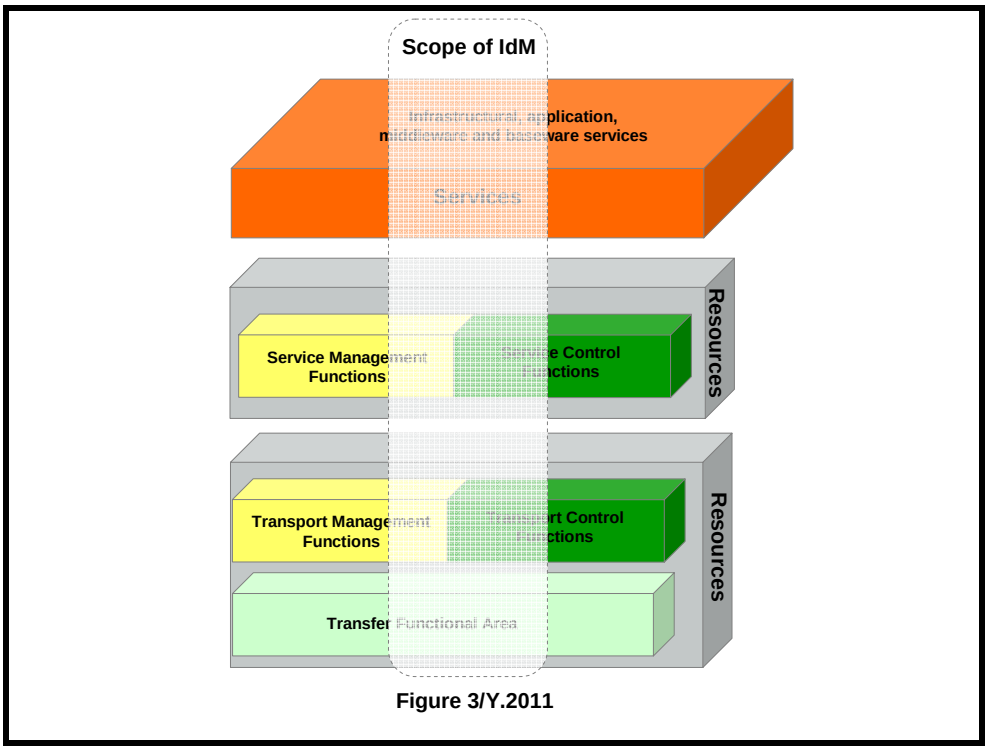

Figure 7 – IdM in Context of the Figure 3/Y.2011

Figure 7 shows the scope of IdM in context of the NGN reference architectural model defined in Figure 3 of [ITU-T Y.2011]. It shows that IdM-related functions may be included in all of the vertical layers of the NGN architecture.

8 Identity management framework

This clause provides detailed description of functional groups mentioned in clause 6.

8.1 Identity lifecycle management

8.1.1 Proofing and enrolment

A first step of creating an identity for an entity (e.g., subscriber, device, organization, NGN provider or object) begins with the identity or credential proofing and enrolment process. That is the process for subscribing an identity or credential associated with a particular entity which may be based on a particular context (e.g., roles).

In the case of end user subscribers this is the process where an applicant applies to become a subscriber of an IdP or of an NGN provider.

For end user subscribers, the subscriber's name may be a verified name. A verified name is associated with the identity of an entity. Before an applicant can receive credentials or enrolment of a token associated with a verified name, the applicant needs to demonstrate that the identity is a real identity, and that it is the entity that is entitled to use that identity. This process is called identity proofing. Once the name is verified, it can be associated with pseudonyms to allow anonymity.

Proofing includes verifying attributes and claims associated with an identity. It involves processes and procedures to verify and validate information when enrolling an entity into an identity system.

The overall effectiveness of IdM depends initially on the proofing and enrolment process. Well-defined assurance requirements are needed and appropriate policy and management procedures are

necessary to be put in place to ensure that the overall enrolment process is properly designed and implemented.

Guidelines to consider include:

- Training of personnel involved in the enrolment process
- Quality of documents and other evidence supporting enrolment of an entity
- Processes for avoiding masquerade at enrolment
- Processes for avoiding multiple or duplicate enrolment of the same entity.

8.1.2 Issuance and revocation

Successful completion of the enrolment process results in the granting of a means (e.g., a credential) by which the entity can be authenticated in the future. For example, the issuance of a credential(s) by an IdP (or NGN provider) binds it to the identity or related attribute (e.g., privilege or claim) of the identity associated with an entity.

Identity revocation is the process of rescinding an identity and the associated credentials. The party or system (e.g., IdP or NGN provider) that issues an identity or credential is responsible for the maintenance and protection of the information associated with the identity. Revocation is required to prevent the continued use of an identity or credential that is no longer valid or has a security breach.

Guidelines to consider include:

- establishment of criteria for issuance and revocation,
- establishment of criteria for updates and modifications,
- synchronization of identity information,
- establishment of processes and procedures for issuance and revocation,
- auditing and review of issuance and revocation processes,
- procedures and processes for notification of issuance, updates and revocation of identity or credentials (i.e., all systems and processes with which an identity has been established needs to be able to determine that the identity or credentials have been issued, updated and revoked),
- well-defined procedures and processes for the issuance and revocation of an identity or credential and appropriate policy. Management procedures are also necessary to ensure that the overall process is properly designed and implemented, and
- mechanisms to protect the revocation processes and procedures from security threats.

8.2 Identity management OAM&P functions

8.2.1 Data model and schema

Each NGN provider, federation or enterprise may have its own formats, schemas, definitions or semantics to represent and share identity-related data and information. For example, the same information such as date of birth may be represented differently by two different systems (e.g., month/day/year or day/month/year). Also, the semantics, schemas and protocols used to request and exchange identity related information can be different resulting in interoperability problems. For example, identity information in Public Switched Telephone Network (PSTN) such as calling party number and caller identity are represented using specific semantics and retrieved using specific protocols (e.g., SS-7), and they are different from SIP based VoIP systems.

Solutions to allow interoperability between heterogeneous IdM systems using different data models, structures and schemas are important.

Guidelines to consider include:

- data model and schemas to facilitate interoperability between heterogeneous IdM systems (e.g., identity data sources) within an NGN provider domain (i.e., different supplier products),
- data model and schemas to facilitate interoperability between different NGN providers (inter-network), and
- Data model and schemas to facilitate interoperability between different federations (e.g., NGN provider and wed services providers).

8.2.2 Identifier management

The identity(s) of an entity (e.g., user/subscriber, organization, federation, enterprise, service provider, device and objects) may have one or more identifiers associated with the identity that have to be managed and maintained.

An identifier is any designation that is used to represent the identity of an entity, such as a user ID, a network ID, an email address, a pseudonym, a group name, etc. For example, the following identifiers may be associated with the identity of a user/subscriber:

- User ID
- Email address
- Telephone number
- URI
- IP address.

The overall effectiveness of IdM depends on the assurance of the individual identifiers that may be correlated and bound to assure the identity on an entity. Therefore, well-defined requirements and procedures for the management of the identifiers are needed.

Guidelines to consider for IdM designs and implementations include:

- There are different types of identifiers with various characteristics that would have to be managed. For example, some identifiers may be global (i.e., unique across different federations), pseudonyms that are meaningful within a system, or one-time identifier that has a temporary period of validity.
- Identifiers may have different characteristics with privacy implications with respect to guarding against inappropriate correlation of user actions.

8.2.3 Attribute management

Identity attributes are descriptors of an entity, such as entity type, preferred IP address, domain, address information, telephone number. Attributes may also contain claims, rights, privileges, delegate lists, and special restrictions. Other types of attributes include information being tracked for intrusion detection, such as failed identity assertion attempts, rekeying counters, etc.

The effectiveness of IdM would depend on the assurance of attributes that may be correlated and bound to assure the identity on an entity. This includes storing and provisioning of attributes. Therefore, well-defined requirements and procedures for the management of attributes are necessary to be put in place.

Pattern is a special type of attribute, which is any characteristic associated with the behaviour of an entity. Pattern information may be assigned by IdM systems based on reputation and past interactions, as opposed to being set by the entity itself. Examples of pattern information that can be used to assess identity assurance include IP address, access point, location information, time of

usage, and systems accessed. Intelligent features may additionally take into consideration current events to predict future usage patterns.

Guidelines to consider for attribute management include:

- pattern information may be considered as PII,
- stringent requirements and procedures for the management of pattern information,
- use of pattern information to minimize identity theft, and
- compliance with PII policy.

8.2.4 Credential Management

Credentials are used to authenticate a claimed identity. Credentials include;

- username/passwords,
- digital certificates,
- tokens and smart cards,
- security hints,
- PKI-related information, such as keys, certificates, signing certificate authority, cryptographic information, etc., and
- biometrics.

Entity credential management encompasses the operational activities to create, issue, and manage information used to authenticate identity claims. The effectiveness of IdM depends on the credential management processes, procedures and capabilities. Therefore, well-defined requirements and procedures for credential management are needed.

Guidelines for credential management include:

- establishment and maintenance of credential policies,
- credential lifecycle management processes and procedures (a subset of identity lifecycle management discussed in clause 8.1), and
- policies and service agreements in multiple service/network provider environments (negotiates credential policies, comply with federation requirements, publish credential information, such as public keys).

8.2.5 Logging and auditing

Logging and auditing functions and capabilities are important to the effectiveness of IdM solutions. Example auditing and compliance measures include maintaining security logs to satisfy accountability requirements, protecting and appropriately using personal information, and providing notification to the appropriate systems or entities (e.g., identity owners).

Guidelines for logging and auditing include:

- logging and auditing of IdM related events (e.g., access to identity information, unauthorized access attempts, updates timestamps, etc) for forensic analysis,
- mechanisms and procedures to enable trace-back,
- detection of non-compliance to applicable policies, and
- assurance of National regulatory requirements.

8.3 Identity management signalling and control functions

8.3.1 Introduction

Signalling and control functions are used to discover and communicate trusted identity information (e.g., identifiers, attributes, claims) associated with an entity (e.g., user/subscriber, group, organization, network element, service provider) to support IdM services, functions and capabilities.

This clause describes signalling and control functions related to IdM.

8.3.2 Discovery of identity information

In a distributed environment such as NGN identity information may exist in different network elements (e.g., subscription server, location server, presence server, home subscription server, etc). Structured means to discover identity information sources are an integral part of IdM. For an application to make use of identity information, it needs to know that it exists. In a dynamic and evolving NGN environment, identity information and sources of identity information is expected to be dynamic as well. Therefore, relying parties and entities (e.g., applications) would need structured means to learn the existence and discover identity information. This also includes discovery of IdM functions services and capabilities.

Guidelines to consider in specifying and implementing discovery capabilities include:

- discovery within a NGN provider domain (intra-network),
- discovery between different NGN provider domains (inter-network), and
- discovery among federation members. See Clause 8.4.2. (Federation Discovery).

Discovery also includes capabilities to find or locate IdPs. Discovery is necessary in the NGN IdM framework because there may be multiple IdPs. In situations where there is only one IdP (e.g. enterprise), there is no need for a discovery operation because it will be known where to obtain the identity attributes. In addition, within a single NGN provider network there may be multiple systems providing various identity management related functions and appropriate discovery functions.

Discovery is similar to a Web search for an identity. The inputs to the search engine are the identity features and the output is a list of identifiers and IdPs that match the requirements. This query and response scenario typically requires IdPs to register themselves as providers of a particular identity service for a given user/device.

The available methods used to support the associated needs for authoritative discovery and access roughly fall into two categories: 1) overlay root-of-roots approaches, and/or 2) inferential discovery. The former relies on some entity assuming the role of a master registrar of namespaces with a supporting server, while the latter approach relies on well-known rules by which the address for a supporting server may be recursively obtained. Mixtures may also be used.

8.3.3 IdM Communications

This includes capabilities and functions to discover and exchange identity information (e.g., identifiers, credentials and attributes) associated with an entity's identity that is located in different network systems (e.g., in a subscription server, location server, presence server, etc) within an NGN provider network that could be correlated and verified (i.e., by an IdM application server providing authentication and correlation functions) in order to to provide identity assurance capabilities. Assertions of identity and associated attributes (e.g., claims and privileges) can be communicated to relying systems (e.g., application services) to make access control decisions. This would allow different application services (i.e., of different vendor platforms) to make use of a common

infrastructure for IdM, as opposed to independent and autonomous solutions. Communications relationships to consider include:

- intra-network: communications with a NGN provider domain (e.g., between network elements),
- inter-network: communications between two different NGN providers, and
- federation: communications between members of a federation.

8.3.3.1 Real-time and near real-time communications

The solution used to discover and exchange identity information needs to take into account whether real-time or near real-time communications are required. This would depend on the specific applications being supported.

8.3.3.2 Signalling and Control Protocols and Interfaces

Figure 8 shows external interfaces that are applicable to support IdM communications. For example, interfaces are used to exchange identity information or control IdM services, functions and capabilities.

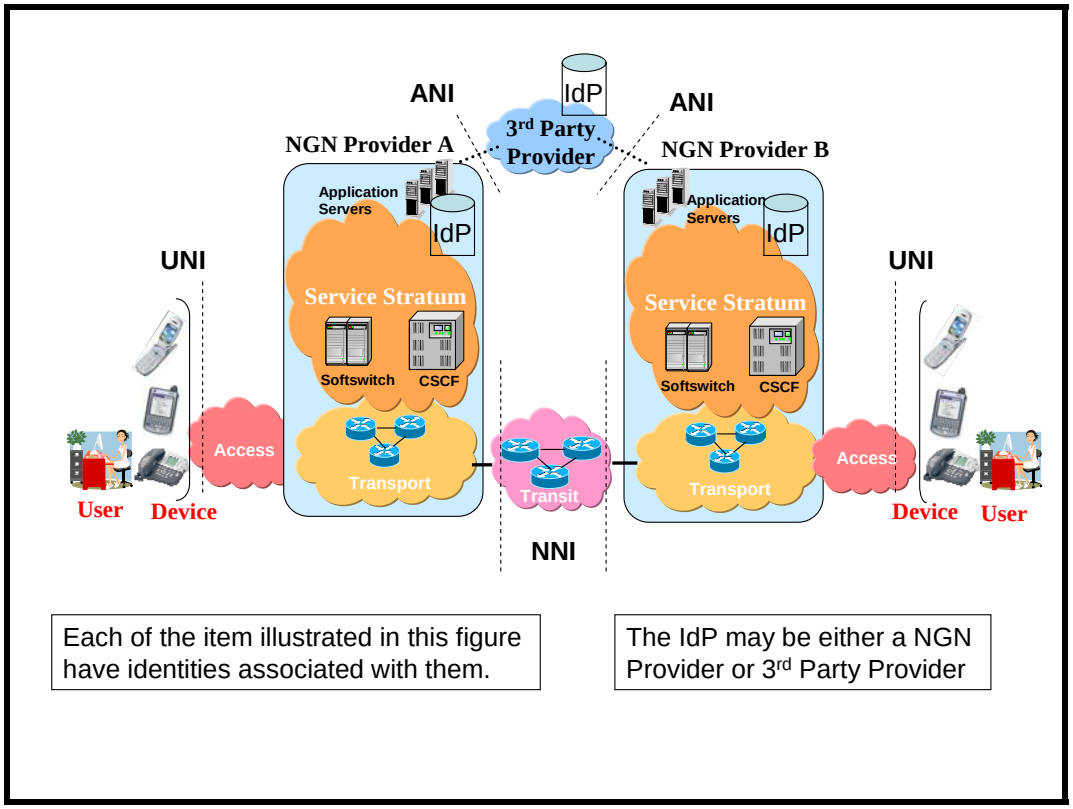

Figure 8 – External Interfaces

External interfaces includes

- User-to-Network Interface (UNI)
- Application-to-Network Interface (ANI), and
- Network-to-Network Interface (NNI).

Specific requirements and protocols to be used depend on the specific interface, information to be communicated or control functions to be performed. Specific requirements and protocol options and profiles to be used should be identified and specified to facilitate interoperability. The interface solutions depend on factors such as specific application and services needs (e.g., real-time versus near-real time), protocol solutions (e.g., SAML, Diameter, RADIUS), and mechanisms and approaches (e.g., X.509, General Bootstrapping Architecture (GBA)).

In addition to the external interfaces, internal interfaces are also important to the overall solutions. Within an NGN network, identity information may be located in different network elements and application services (e.g., subscription, location, and presence servers and other network elements such as CSCF and SBC). The internal interfaces and protocols to be used to discover and exchange identity information are important considerations for multi-vendor interoperability.

8.3.3.3 Mechanisms and procedures

The mechanisms and procedures used to implement a specific IdM function or capability should be identified and specified. For example, the specific mechanisms or protocols and where and how it is used should be identified and specified. Example mechanisms and protocols include

- SAML
- X.509
- GBA, and
- E.115

8.3.4 Correlation and binding

The identity information (e.g., identifiers, credential and attributes) may be correlated to establish a binding to assure the identity of an entity. For example, the identity information associated with a subscriber (e.g., UserID), a subscriber device (e.g., DeviceID), and location information may be correlated to establish a binding to provide a higher assurance of the subscriber.

Guidelines to consider in specifying and implementing correlation and binding include:

- enforcement of applicable policy (e.g., anonymity or privacy policies).

8.3.5 Authentication

Authentication is the process of establishing confidence in the identity of an entity. One means of achieving authentication assurance is to describe the objectives and guidelines necessary to quantify the risks that an entity is who or what it claims to be. This includes establishing which entity identifiers are more important than others in the identification process and why certain identifiers used in authentication should not have the same authentication value.

Traditionally, trust is achieved by issuing user-ID and password pairs for individual systems. However, in the NGN this approach is undesirable, operationally inefficient, and can lead to insecure practices. Guidelines to consider in specifying and implementing authentication include:

- Confidentiality and integrity of the authentication mechanisms
- Credentials strong enough to be trusted across systems.

8.3.6 Authentication assurance

Authentication assurance is the process of establishing confidence in the identities and claims that are presented to an information system. Not all information used for authentication should be treated equally or necessarily have the same assurance value. For example, the confidence in an

authentication using biometric is significantly different from an authentication using User ID/password. Relative value based on fundamental principles need to be assigned to each identifier in order to quantify the confidence that an authenticated entity is the valid entity.

The objective of authentication assurance is to quantify the risks that an entity is who or what it claims to be. Not all identifiers used in an authentication decision process are treated equally or necessarily have the same authentication value. In addition, as the consequence of an authentication error becomes more serious, the required level of authentication assurance should increase depending on the risk implication (e.g., critical nature of the impact) of an authentication error.

A mechanism to quantify and communicate authentication assurance allows relying parties to make decisions regarding their confidence in the authentication process used to validate the identity or claims of an entity.

Primary benefits of authentication assurance include ability to determine the level of confidence that an entity is that which is claimed throughout the identity's life cycle. Standard criteria for assigning and communicating relative assurance value of authentication process, mechanisms and the data (e.g., password, credentials, biometrics) across different federation is critical for supporting federated services and cyber-security protection.

An authentication assurance process should take into account the following:

- Authentication mechanism: Static passwords are weaker than one-time passwords, and a hardware token with a PIN is generally better than software token.
- Authentication protocol: A protocol that is known to be secure against man-in-the-middle attacks or one based on cryptographic operations is generally considered strong.
- Characteristics of the device used to authenticate: Authentication confidence is partly based on the characteristics of the device being used by the user, i.e. a Commercial Off the Shelf computer owned and controlled by the organization or a dedicated tamper resistant device is better then a publicly accessible Commercial Off the Shelf device.
- Location of the entity being authenticated: The location of the user should be considered, e.g. within the organization's area or in public kiosk, Internet Café, etc. Authentication confidence will be higher if it is difficult for a public terminal in a kiosk to convince the authentication server that it is located within an organization's physical boundaries.
- Communications path: Authentication typically involves a communications path (wireless networks, commercial leased lines, etc.) between the entity being authenticated and the server providing authentication and/or access decisions. Information used for authentication is needed to be reliably conveyed to the authentication server and not be susceptible to spoofing by an attacker.
- Relative ease of authentication manipulation by malicious behaviour: It is important to assess the risk associated with the compromise of cryptographic keys.

8.3.7 Delegation

Delegation involves actions and processes for the transferring of privileges to perform certain action on behalf of a principal from an entity that has the privileges to another entity that does not have the privileges.

For example, delegation authority begins with the ability to define which accounts have the ability to perform certain managerial actions (such as creating new accounts) or managing specific functions (such as changing an account password). Thus, given the ability to delegate the actions or

effort of administration, the goal then is to provide an environment wherein this task is undertaken in a secure and responsible manner.

8.3.8 Policy enforcement

The design and implementation of IdM solutions should take into account that the applicable policies are enforced. For example, enforcement of policy are usually associated with:

- anonymity and privacy,
- creation and collection of identity information, and
- use and dissemination of identity information.

8.3.9 Support of services requiring priority treatment

Design and implementation of IdM solutions should take into consideration support of application services and communication sessions requiring priority treatment such as Emergency Telecommunications Service (ETS). For example, any interactions with IdM systems to set-up and maintain ETS communication sessions should be provided priority treatment. Refer to [ITU-T E.107] and [ITU-T Y.2205] for information on services and capabilities requiring priority treatment.

8.4 Identity management federated identity functions

8.4.1 Federated identity

The general concept of federation is to allow each federation member to remain independent while facilitating sharing of specific identity information to allow federated services. For example, certain identity information of a user/subscriber (e.g., subset of a subscriber profile) could be federated (i.e., made available to federation members).

8.4.2 Federation discovery

Federation discovery consists of functions and mechanisms to discover and exchange federated identity information. For example, certain identity information about a user/subscriber may be federated such as a subset of the subscriber profile information.

The main aspect of federation discovery is to identify or discover a candidate IdP or the IdP that is the authoritative source for a particular identity information associated with an entity (e.g., location information).

Discovery is necessary in any architecture in which there are multiple IdPs, or for which the location of IdPs is potentially dynamic. In situations where there is only a single identity provider (e.g. an enterprise) there is no need for a discovery operation because any RP/SP will implicitly know where to obtain the entity's identity information.

8.4.3 Bridging and interworking

In general each NGN provider, enterprise or federation member may have its own formats, schemas, definitions or semantics to represent and share identity-related data and information. For example, the same information such as date of birth may be represented differently by two different systems. Also, the semantics, schemas and mechanisms used to request and exchange identity related information can be different resulting in interoperability problems. Therefore, appropriate capabilities to allow bridging and interworking between different federations will be necessary.

8.5 Identity management user and subscriber functions

Functions to allow an end user/subscriber to provide information regarding the control of their identity information are needed for effective IdM solutions. This includes functions and capabilities to enable an entity such as an end user/subscriber to provide service providers and IdPs information about conditions, restrictions, consents, authorization regarding creation, collection, use and dissemination of their identity information.

These functions are related to the enforcement of applicable policies such as policies regarding protection of PII, anonymous or pseudonymous identity information.

Guidelines to consider include:

- means for end users/subscribers to convey information to NGN provider about the control of their identity information,
- compliance with applicable policies regarding protection of PII, and
- ease of use for the end user/subscriber.

8.6 Performance and reliability

8.6.1 Performance

IdM capabilities and functions will be used to support and enhance a wide range of business and security applications. For example, IdM functions may be used to assure the identity of communication entities before allowing a communication session (e.g., VoIP, IPTV or Data sessions). Therefore the performance implications of IdM on the higher level application services being supported (e.g., VoIP, IPTV, data) is import for the overall effectiveness of the solution. For example, IdM should not negatively impact the higher level applications services that are being supported so that the over all Quality of Service (QoS) and Quality of Experience (QoE) of end users/subscribers are affected.

Performance management considerations are important in IdM solution designs. Performance management includes gathering and analyzing statistical data for performance monitoring purposes. Performance monitoring is the systematic assessment of a network system ability to carry out its assigned function through the continuous collection and analysis of appropriate performance data. Performance monitoring procedures are intended to capture intermittent error conditions and troubles resulting from the gradual deterioration of network equipment. Pro-active maintenance techniques such as performance monitoring enable early detection of troubles before they escalate in severity.

8.6.2 Timestamp accuracy

Timestamp accuracy is a factor for IdM. Auditing describes the occurrence of events within those timeframes. For auditing purposes, time-stamps are essential; and the quality if not the usability of audit data is determined by timestamp accuracy.

The accuracy of timestamps is determined by three factors – the precision with which the local timestamp clock is read, the traceability of the local clock to a reference clock, and the mathematical uncertainty of the local clock measured against a reference.

8.6.3 Reliability and availability

Reliability and resiliency of network elements and systems providing IdM functions and capabilities are an important aspects of the design and implementation of solutions because IdM will be used to support and enhance a wide range of business and security applications that may

have specific availability requirements. Therefore, requirements and guidelines for reliability factors such as the following need to be considered:

- system designs (e.g., redundancy) for robustness and resiliency and
- diversity (e.g., geographical diversity) for availability.

In addition, design and implementation of IdM solution should also consider failsafe measures. For example, the relying application may allow certain limited privileges if the entire IdM system was to fail or become unavailable.

8.7 IdM security

8.7.1 Security protection of network elements providing IdM

Because identity information and resources are valuable, sensitive, and used to support business applications and services, network elements providing IdM services, functions and capabilities will be targeted for security attacks and therefore will require security protection.

Appropriate requirements and measures to secure and protect the network elements and systems providing IdM functions, services and capabilities are necessary. Example security considerations are:

- security protection of the IdM services, functions and capabilities,
- security protection of the signalling and communication interfaces, and
- security protection of the management interfaces of IdM systems (i.e., interfaces used to configure and manage identity information).

8.7.2 Protection of personally identifiable information (PII)

Protecting PII is a highly important aspect of IdM. Specific capabilities to protect PII should be defined and implemented. This is related to enforcement of applicable policy on PII protection subject to national and regional regulations. Function and capabilities to consider include:

- capabilities for users/subscribers to communicate preferences regarding PII,
- capabilities to provide transparency (i.e., capabilities to make sure that only authorized entities have access to or can observe PII), and
- capabilities to provide notices regarding dissemination and use of identity information.

Appendix I: Bibliography

1. Open Group's Identity Management White Paper: http://www.opengroup.org/online-pubs?DOC=7699959899&FORM=PDF

2. *NIST SP800-63, Electronic Authentication Guidelines,* http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

3. ETSI TISPAN Work item 04004: Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks, draft ETSI Guide.

4. ETSI TISPAN Work item 04006: Interconnect issues related to Numbering Naming and Addressing (NAR); Draft Technical Report.

5. ETSI TISPAN Work item 04008: Number Portability for NGNs; Draft Technical Report.

6. ETSI TISPAN Work item 04010: Types of numbers used in an NGN environment, Draft Technical Report.

7. ETSI TISPAN Work item 04011: Naming/Numbering Address resolution function (NARF); Draft Technical Report.

8. [EG 202 072] Universal Communications identifier (UCI); Placing UCI in Context; Review and analysis of existing identification schemes, 09/2002

9. [EG 202 236] Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Design guide; Use of non-numeric name

10. [RFC 3650] Handle System Overview

11. [ETSI TS102 042] Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, December 2007.

12. [ITU-T X.1141] ITU-T Recommendation X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*