International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2721

(09/2010)

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

Next Generation Networks – Security

NGN identity management requirements and use cases

Recommendation ITU-T Y.2721

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Future networks	Y.2600–Y.2699
Security	**Y.2700–Y.2799**
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2721

NGN identity management requirements and use cases

Summary

Recommendation ITU-T Y.2721 provides identity management (IdM) example use cases and requirements for the next generation network (NGN) and its interfaces. IdM functions and capabilities are used to increase confidence in identity information and support and enhance business and security applications including identity-based services.

The requirements provided in this Recommendation are intended for NGN (i.e., managed packet networks) as defined in Recommendation ITU-T Y.2001.

The objectives and requirements in this Recommendation are based on the IdM framework provided in Recommendation ITU-T Y.2720 and an analysis of use case examples relevant to NGN. The example use cases are informative and are documented in the appendices of this Recommendation.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2721	2010-09-16	13

Keywords

Federated identity, identity management, next generation network, security.

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 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/.

CONTENTS

Recommendation ITU-T Y.2721

NGN identity management requirements and use cases

1 Scope

This Recommendation provides identity management (IdM) objectives, requirements, guidelines and example use cases for the next generation network (NGN) and its interfaces. IdM functions and capabilities are used to increase confidence in identity information and support and enhance business and security applications including identity-based services.

The scope of this Recommendation includes objectives, requirements, guidelines and example use cases addressing:

- Increasing confidence in the identity information of an NGN entity (e.g., user, group, user device, service provider, enterprise, federation, network element and object).
- Secure management of the lifecycle (e.g., registration, validation, revocation) of identity information subject to user's specific and informed consent.
- IdM as an enabler of business (e.g., single sign-on and sign-off for multiple application services) and security applications (e.g., access controls) including identity-based services (e.g., authentication, assertions and federated identity).
- Secure discovery and exchange of information associated with an NGN entity's identity or identities subject to user's specific and informed consent. This includes information that may be located within an NGN and across different administrative domains or federations.
- Interworking/interoperability among the IdM systems and capabilities within a NGN provider domain (i.e., intra-network).
- Interworking/interoperability of the IdM systems and capabilities among different provider domains or federations subject to user's specific and informed consent where user information is concern (e.g., among NGN providers, web services providers and content providers).
- Enforcement of applicable policy (e.g., protection of personally identifiable information) associated with an entity's identity or identity information.
- Security of IdM systems, functions, capabilities, data and communications.

The objectives and requirements provided in this Recommendation are intended for NGN (i.e., managed packet networks) as defined in [ITU-T Y.2001], *General overview of NGN*.

The objectives and requirements in this Recommendation are based on the IdM framework provided in [ITU-T Y.2720] and an analysis of use case examples documented in the appendices.

NOTE 1 – In this Recommendation, the use of the term 'Identity' relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation of a person.

NOTE 2 – In this Recommendation, a user can be a person, groups, companies, juridical entities, or any other entities which make use of NGN services.

NOTE 3 – In this Recommendation, the term "NGN/identity service provider (NGN/IdSP)" is used to indicate that it could be an NGN provider or a third party that provides IdM services.

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 E.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS.*

[ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

[ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

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

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN.*

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

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN Release 1.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 anonymity [ITU-T X.1252]: A situation where an entity cannot be identified within a set of entities.

NOTE – Anonymity prevents the tracing of entities or their behaviour such as user location, frequency of a service usage, and so on.

3.1.2 assertion [ITU-T X.1252]: A statement made by an entity without accompanying evidence of its validity.

3.1.3 attribute [ITU-T X.1252]: Information bound to an entity that specifies a characteristic of the entity.

3.1.4 authentication [ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

3.1.5 authentication assurance [ITU-T X.1252]: The degree of confidence reached in the authentication process that the communication partner is the entity that it claims to be or is expected to be.

NOTE – The confidence is based on the degree of confidence in the binding between the communicating entity and the identity that is presented.

3.1.6 authorization [ITU-T X.1252]: The granting of rights and, based on these rights, the granting of access.

3.1.7 binding [ITU-T X.1252]: An explicit established association, bonding, or tie.

3.1.8 claim [ITU-T X.1252]: To state as being the case, without being able to give proof.

3.1.9 claimant [ITU-T X.1252]: An entity that is or represents a principal for the purposes of authentication.

NOTE – A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

3.1.10 context [ITU-T X.1252]: An environment with defined boundary conditions in which entities exist and interact.

3.1.11 credential [ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.12 delegation [ITU-T X.1252]: An action that assigns authority, responsibility, or a function to another entity.

3.1.13 discovery [ITU-T Y.2720]: 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.

3.1.14 entity [ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in context.

NOTE – An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

3.1.15 emergency telecommunications (ET) [ITU-T Y.2205]: ET means any emergency related service that requires special handling from the NGN relative to other services. This includes government authorized emergency services and public safety services.

3.1.16 emergency telecommunications service (ETS) [ITU-T E.107]: A national service providing priority telecommunications to the ETS authorized users in times of disaster and emergencies.

3.1.17 federation [ITU-T X.1252]: An association of users, service providers, and identity service providers.

3.1.18 federated identity [ITU-T Y.2720]: 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.

3.1.19 identifier [ITU-T X.1252]: One or more attributes used to identify an entity within a context.

NOTE – In the context of NGN as defined in [b-ITU-T 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).

3.1.20 identity [ITU-T X.1252]: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

NOTE – Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity. However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.

3.1.21 identity assurance [ITU-T X.1252]: The degree of confidence in the process of identity validation and verification used to establish the identity of the entity to which the credential was issued, and the degree of confidence that the entity that uses the credential is that entity or the entity to which the credential was issued or assigned.

3.1.22 identity management [ITU-T Y.2720]: 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.

3.1.23 identity pattern [ITU-T X.1252]: A structured expression of attributes of an entity (e.g., the behaviour of an entity) that could be used in some identification processes.

3.1.24 identity provider: See identity service provider (IdSP).

NOTE – The term "identity provider (IdP)" is used in [ITU-T Y.2720] and in specifications by other organizations. However, to avoid misinterpretation that it could be construed to mean an entity that provides identities, rather than an entity that manages identities, the term identity service provider (IdSP) is used in this Recommendation.

3.1.25 identity service provider [ITU-T X.1252]: An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

3.1.26 next generation network [ITU-T 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.

3.1.27 personally identifiable information (PII) [ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

3.1.28 presence [ITU-T Y.2720]: A set of attributes that characterizes an entity relating to current status.

3.1.29 principal [ITU-T X.811]: An entity whose identity can be authenticated.

3.1.30 privacy [ITU-T X.1252]: The right of individuals to control or influence what personal information related to them may be collected, managed, retained, accessed, and used or distributed.

3.1.31 relying party (RP) [ITU-T X.1252]: An entity that relies on an identity representation or claim by a requesting/asserting entity within some request context.

3.1.32 security domain [ITU-T X.1252]: A set of elements, a security policy, a security authority, and a set of security-relevant activities in which the elements are managed in accordance with the security policy.

3.1.33 trust [ITU-T X.1252]: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.

3.1.34 user [ITU-T X.1252]: Any entity that makes use of a resource, e.g., system, equipment, terminal, process, application, or corporate network.

NOTE – In the context of NGN, according to [b-ITU-T Y.2091], it includes end user, person, subscriber, system, equipment, terminal (e.g., Fax, PC), (functional) entity, process, application, provider, or corporate network.

3.1.35 verifier [ITU-T X.1252]: An entity that verifies and validates identity information.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

3G	3rd Generation
AKA	Authentication and Key Agreement
ANI	Application-to-Network Interface
API	Application Programming Interface
BSS	Business Support System
CSP	Communications Service Provider
DDoS	Distributed Denial of Service
DeviceID	Device Identity
DoS	Denial of Service
EAG	External Application Gateway
EDS	Enterprise Directory Service
ET	Emergency Telecommunications
ETS	Emergency Telecommunications Service
EV-DO	Evolution Data Optimized
FE	Functional Entity
FTTX	Fibre-To-The-X
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber Server
IBGC-FE	Interconnection Border Gateway Control Functional Entity
IdM	Identity Management
IdMCC-FE	IdM Coordination and Control Functional Entity
IdSP	Identity Service Provider
IDPS	Intrusion Detection and Prevention Systems

ID-WSF	Identity Web Services Framework
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	IP Television
ISC	IMS Service Control
IT	Information Technology
KDC	Key Distribution Centre
LS	Location Server
LTE	Long Term Evolution
MNO	Mobile Network Operator
MSISDN	Mobile Subscriber Integrated Service Director Number
NACF	Network Attachment Control Functions
NGN	Next Generation Networks
NNI	Network-to-Network Interface
OAM&P	Operation, Administration, Maintenance and Provisioning
OSS	Operations Support System
PC	Personal Computer
P-CSC-FE	Proxy Call Session Control Functional Entity
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
POTS	Plain Old Telephone System
PS	Presence Server
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RFID	Radio-Frequency Identification
RP	Relying Party
SAA-FE	Service Authentication and Authorization Functional Entity
SAML	Security Assertion Markup Language
S-CSC-FE	Serving Call Session Control Functional Entity
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SN	Service Node
SNI	Server-to-Network Interface
SP	Service Provider
SUP-FE	Service User Profile Functional Entity

TGS	Ticket Granting Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
UNI	User-to-Network Interface
URI	Uniform Resource Identifier
UserID	User Identity
VoD	Video-on-Demand
VoIP	Voice over Internet Protocol
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WS	Web Server
WSG	Web Services Gateway
xDSL	x Digital Subscriber Loop

5 Conventions

In this Recommendation:

The keywords "**is required to"** indicate a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended"** indicate a requirement that is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**is prohibited from"** indicate a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**can optionally"** indicate an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

In the body of this Recommendation and its annexes, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix or in material explicitly marked as *informative* are to be interpreted as having no normative intent.

6 IdM overview

6.1 General

[ITU-T Y.2720] provides a framework for IdM. IdM functions and capabilities are used to increase confidence in identity information of an entity and support business and security applications (e.g., access control and authorization) including identity-based services. An entity is considered to be something that has separate and distinct existence and that can be identified in a context. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices.

The NGN will be supporting a broad range of application services for end user subscribers, governments, and business enterprises. To provide integrity and security protection of application services, it is recommended that the NGN supports the necessary functions and capabilities to assure the identity and identity data associated with an entity based on specific context. Refer to [ITU-T X.1252] for a definition of IdM.

The example uses cases, documented in the following appendices, are taken into consideration in defining IdM requirements:

- Appendix I – General IdM use cases
- Appendix II – IdM use cases for NGN applications
- Appendix III – Emergency telecommunications service (ETS) related IdM use cases
- Appendix IV – Mobile-related use cases

In addition, the following factors associated with end user identity in an NGN environment are taken into consideration in defining IdM requirements:

- End users are increasingly using multiple identities
- An identity may be associated with differing contexts and service privileges
- An identity may only partially identify an end user
- Pseudonyms may be used as identity
- Identities may be used anywhere, anytime and from any device
- Identities may not be interoperable between NGN providers

6.2 IdM relationships

Figure 1 provides a general overview of IdM relationships based on the framework in [ITU-T Y.2720].

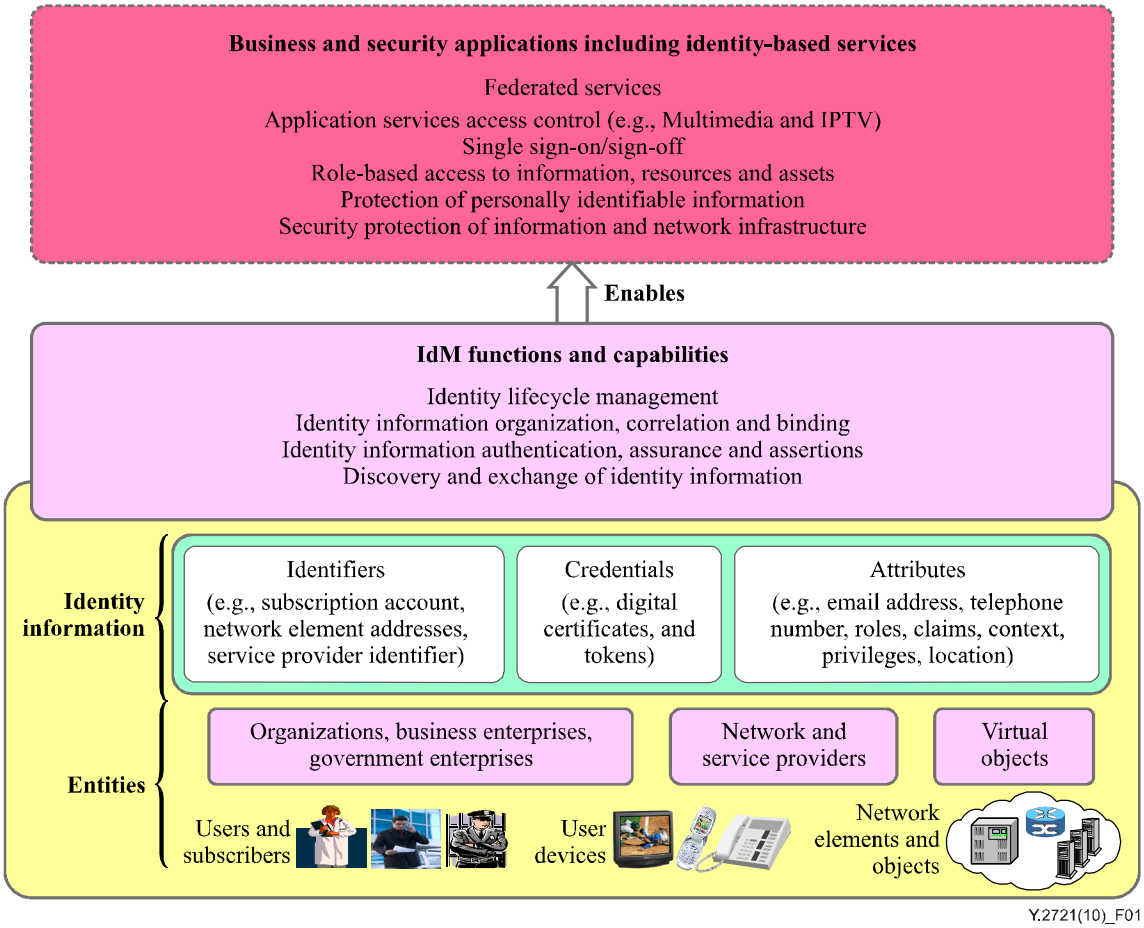


Figure 1 – IdM relationships

The entities can range from individual human users to broad organizations, e.g., businesses and virtual objects such as electronic applications. The identity information associated with each may range in sensitivity from relatively public data, for example, a telephone number listed in a public directory to highly sensitive identity data such as passwords, digital certificates, and other private authenticators.

An entity may have one or more identities. These identities may be used to represent multiple roles (such as citizen, spouse, parent, customer, and patient) and used for specific transactions ranging from commercial to social activities. A person or individual may be associated with multiple digital identities based on different contexts as shown in Figure 1. In addition, a person acting through digital identities may be familiar to others as one or more persona assumed or displayed in public or society, or through roles (e.g., emergency responder) that are assigned or granted by some authority.

Figure 1 shows the following:

a) Entities:

In a NGN environment where services are based on contexts and roles and accessed anywhere, anytime, and from any device, multiple forms of identity-related information may be associated with an entity. In addition, an entity may have one or more identities based on context. Example entities include:

- User and subscribers.
- User devices, network elements and objects.
- Organizations, groups, business enterprises and government enterprises.

- Network and service providers.
- Virtual objects.

b) Identity information:

The identity information associated with an entity can be grouped as follows:

- Identifiers (e.g., subscription account, network element addresses, service provider identifier).
- Attributes (e.g., email addresses, telephone numbers, URI, IP addresses, roles, claims, privileges, authentication method, patterns and location).
- Credentials (e.g., digital certificates and tokens).

c) IdM functions and capabilities:

IdM functions and capabilities are used to increase confidence in identity information of an entity and support or enhance business and security applications including identity-based services. Example IdM functions and capabilities are:

- Identity lifecycle management.
- Identity information organization, correlation and binding.
- Authentication, authentication assurance and assertion.
- Discovery and exchange of identity information.
- Functions and capabilities to bridge different IdM systems to facilitate interoperability.

d) Business and security applications:

IdM functions and capabilities support and enhance business and security applications including identity-based services.

Example business applications include:

- Federated services (e.g., access to services across different federations or NGN providers).
- Single sign-on and sign-off (e.g., access to multiple applications and services without having to resubmit the authentication credentials to each application or service platform).

Example security applications include:

- Access control.
- Authorization management of privileges.
- Protection of personally identifiable information (PII).

Example identity-based services include:

- Identifier, credential and attributes services.
- Bridging services (mapping and interworking of identity information in heterogeneous environment.
- Pattern information services.

IdM includes life-cycle management processes, plus the functions and capabilities to discover and obtain identity sources that can be used to verify and validate an identity. IdM services and capabilities allow entities to control how their identity information is used and disseminated. IdM provides entities (e.g., relying parties) with the necessary information to make decisions regarding authentication and have confidence in the associated transactions and communications. IdM also allows federated identity information to be shared and used by members of a federation (e.g., different NGN providers, business enterprises or government enterprises) to support federated services. For example, federated identity services would allow authorized entities from members of the federation to obtain access to resources based on roles and privileges in accordance with the

rules and policies of the federation without having to register and authenticate to each member of the federation.

6.3 Drivers and motivations

Because many NGN services and capabilities involve service based on subscriber identity and preferences and access from any device, anywhere and anytime, IdM solutions must be able to respond in real time to increasingly complex interactions as users may move between devices, access technologies, payment methods, and even identities. In addition, end users are also demanding easy or user-friendly capabilities. More important, end users are demanding capabilities to allow user control of privacy and personally identifiable information (PII).

Drivers and motivation for IdM come from end users (e.g., subscribers of applications and services), NGN providers, business and government enterprises, all of whom want to see their interests and needs met by IdM implementations. The following factors are taken into consideration in defining the IdM requirements for NGN:

- End users/subscribers need to control and protect their identity information, a desire to have flexible and uniform methods of access to resources, and a need to balance the benefits of social networking and the exposure of personal information.
- NGN providers (network and service providers) need to protect their network infrastructure resources, services and applications, enable federated services, promote broadly-available subscription-based services, and meet end users' needs for privacy and protection of personally identifiable information (PII).
- Business enterprises and users need to protect their business interests, have confidence in authentication capabilities for business transactions and protection of business partner's identity data.
- Protection of the network infrastructure against cyberattacks, and protection of private data.
- Governmental organizations support of electronic governmental services, public safety services, early warning services, emergency telecommunications service (ETS) and other national services.

6.4 Multiple service provider and federated environment

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. For example, identifiers, credentials and attributes associated with an identity could be verified by an identity service provider which is regarded as trusted by the relying party and communicated, through assertions, to the relying party (e.g., a user, a service provider) to support authentication, which may be a basis for access control, business decisions, and enforcement of applicable policy (e.g., privacy and protection of personally identifiable information).

Additionally, there may be different and independent IdM solutions resulting in the need for interoperability among service providers.

6.5 Identity service provider (IdSP)

This Recommendation does not impose any restriction on who provides identity service provider (IdSP) services.

An IdSP is an entity that maintains, manages, and may create 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.

In a multiple service provider environment, it is possible for an NGN provider to also be an IdSP and offer identity management services (e.g., identity-based services) to other providers.

In this Recommendation, the term "NGN/IdSP" is used to indicate that it could be an NGN provider or third party that provides IdM services.

6.6 IdM in the context of NGN architectures and reference models

6.6.1 Relationship with NGN functional architecture

In the context of the NGN reference architecture model defined in [ITU-T Y.2012], it is possible for IdM related functions to reside in the different planes (e.g., user, control and management) and different strata of the distributed architecture (e.g., service stratum and transport stratum). From a realization or implementation perspective, support of IdM services and capabilities could involve the use of existing network elements or it could involve the use of additional network elements (e.g., specialized application servers) in a NGN.

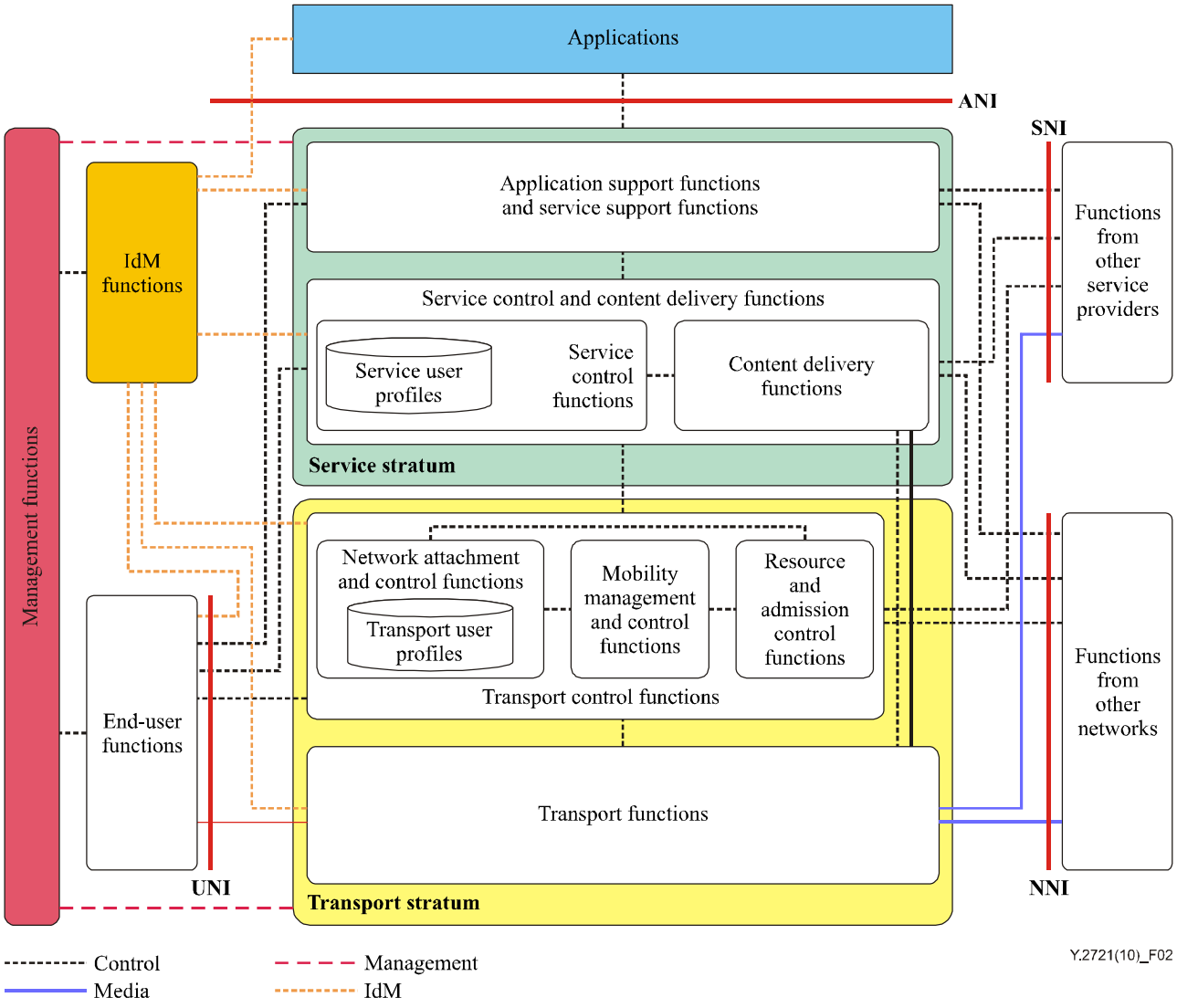


Figure 2 – NGN architecture overview

Figure 2 is based on Figure 7-1 of [ITU-T Y.2012], which includes a functional block representing IdM functions in the NGN functional architecture. Figure 7-1 of [ITU-T Y.2012] illustrates the general concepts that the support of IdM services and capabilities may involve interaction with specific functional entities (FEs) to enable and support services including identity services. This may include interactions with FEs in the following functional blocks depending on the specific IdM service or capability being supported and the implementation design:

– applications;
– service stratum: application support functions and service support functions, service control functions and content delivery functions;
– transport stratum: transport control functions and transport functions;
– end-user functions;
– management functions.

In the NGN functional architecture, IdM functions may reside in different planes (e.g., user, control and management) and different strata of the distributed architecture (e.g., service stratum and transport stratum). Although IdM functions are shown in a stand-alone group of functions, this is not intended to impose any design and restrictions for IdM implementations. Implementation of IdM functions is subjected to the compliance with relevant policies, such as national and regional regulations and legislations for protection of identity data (e.g., PII). Specifically, implementation and use of IdM functions must ensure the compliance with the relevant policies for basic data protection principles:

• binding of data to a specific purpose;
• no data sharing between applications for different purposes;
• limitation of data to the minimum needed for a specific purpose;
• right of persons to have control over their PII.

NOTE – For some specific national regulations, this may imply implementation of separated IdM functions in the different strata of the NGN.

6.6.2 External interfaces and IdM communications

The standard interfaces defined in [ITU-T Y.2012] are used to exchange identity data among different administrative domains and federations. This may include the following interfaces as applicable:

• user-to-network interface (UNI);
• network-to-network interface (NNI);
• application-to-network interface (ANI);
• server-to-network interface (SNI).

The interface solutions would depend on factors such as specific application and services needs (e.g., real-time versus near-real time), protocol solution (e.g., SAML, Diameter, RADIUS, SIP), and mechanisms and approaches.

Refer to Appendix VI for an example IdM realization scenario showing how the NGN external interfaces may be applicable.

6.6.3 Transactional models

[b-ITU-T X.1250] provides descriptions of example transactional models involving multiple parties (e.g., users, IdSPs and relying parties). Refer to Appendix V for a summary of the transactional models described in [b-ITU-T X.1250].

7 IdM objectives

The following are general objectives for IdM:

1) Facilitate trust decisions between entities.
2) Support of IdM solution(s) minimizing impacts on users/subscribers.
3) Solution(s) involving new capabilities would provide appropriate transition solution.

4) Support of interoperable IdM solutions within an NGN provider domain. For example, interoperability between different vendor products supporting multiple application services (e.g., VoIP, IPTV, video and data).

5) Support of interoperable IdM solutions across different NGN provider and service provider domains and federations based on applicable business arrangements and relationships and under application of regulation and policies for PII protection.

6) Support of bridging of heterogeneous IdM systems and federations. For example, capability to allow bridging between NGN provider IdM systems and other types of IdM systems (e.g., web services, content and 3rd party provider IdM systems) based on applicable business arrangements and relationships and under application of regulation and policies for PII protection.

7) End users/subscribers being able to interact and use application services in an easy and intuitive fashion while retaining control of their personal data throughout their life cycle. This includes how and when the information is used and by whom.

8) End users/subscribers being able to reveal only the minimally necessary information to establish mutual trust and conduct transactions based on the applicable policies.

9) End users/subscribers being able to check the authenticity of the entity requesting identity data and PII. It is an objective for an end user/subscriber to be able to use multiple identifiers based on context.

10) End user/subscriber being able to operate anonymously, pseudonymously or intentionally known based on the application context and applicable policies.

8 IdM requirements

This clause describes IdM requirements applicable to NGN, in alignment with the high-level requirements of NGN described in [ITU-T Y.2201].

8.1 General requirements

The following are general requirements for identity management:

R-1 NGN/IdSP is required to support functions and capabilities for the identity management of the various types of entities supported by NGN, including:

a) Users/groups.

b) Organizations/federations/enterprise/service providers.

c) Devices/network elements/systems.

d) Objects (e.g., application process, content, data).

R-2 NGN/IdSP is required to support:

a) Secure management of the lifecycle (e.g., from issuance to revocation of identities).

b) Secure discovery and exchange of identity information. This includes discovery and exchange of identity information that may be located within an NGN and across different administrative domains.

R-3 NGN/IdSP is required to support enforcement of applicable policies associated with an entity's identity or identity information.

R-4 NGN/IdSP is required to support IdM functions and capabilities for both real-time (e.g., VoIP and IPTV) and near-real time applications (e.g., web-based data transactions).

R-5 NGN/IdSP is required to support IdM functions and capabilities to allow anonymous assertion of identity information (e.g., identity and attributes), subject to applicable policy.

R-6 NGN/IdSP is required to support secure interworking for IdM among network elements within a NGN provider domain (i.e., intra-network) and among different provider domains (e.g., other NGN provider, web services providers).

R-7 NGN/IdSP is required to support end user's ease-of-use services and features such as:

a) Single sign-on/sign-off to multiple application services.

b) Converged services (e.g., fixed and mobile convergence).

c) Control and protection of personally identifiable information (PII).

R-8 NGN/IdSP is required to support single sign-on to applications using credentials associated with a subscriber device (e.g., UICC credentials) or credentials associated with a user/subscriber (e.g., SIP Digest credentials) as appropriate based on the security requirement of the applications. Specifically:

- It shall be possible to use subscriber credentials (e.g., SIP Digest credentials) to support single sign-on for applications accessed via mobile devices.
- It shall be possible to use subscriber credentials (e.g., SIP Digest credentials) to support single sign-on for applications accessed via fixed devices.

8.2 Identity lifecycle management requirements

Identity lifecycle management involves the process and procedures associated with the enrolment and issuance of identity information (e.g., identifiers, credentials, and attributes).

R-9 NGN/IdSP is required to establish and enforce applicable policies for identity lifecycle management. This includes processes, procedures and policies for the proofing, enrolling, issuing and revoking identity information.

8.2.1 Enrolment and issuance

Enrolling an entity (e.g., subscriber, device, organization, NGN provider or object) into a context begins with the identity or credential proofing and enrolment. Enrolment is the process of inauguration of an entity into a context and includes the recording of the entity's identity and possibly assignment of specific attributes (e.g., identifiers) or credentials or roles. In the case of end user subscribers, this is the process where an applicant applies to become a subscriber of an IdSP or of an NGN provider.

Proofing includes verifying and validating attributes and possibly associated credentials.

R-10 NGN/IdSP is required to verify and validate an entity's identity during enrolment according to the requirements of the context. The recording of the entity's identity and the assignment of identifiers, credentials and attributes for the specific context is subject to a successful confirmation of the applicable proofing criteria and policies.

The proofing process and policies shall be based on the value of the resources (e.g., services, transactions, information and privileges) allowed by the identity and the risks associated with an unauthorized entity obtaining and using the identity. Specifically, measures to ensure the following is required:

- An entity (e.g., person, organization or legal entity) with the claimed attributes exists, and those attributes are suitable to distinguish the entity sufficiently according to the needs of the context.
- An applicant whose identity is recorded is in fact the entity to which the identity is bound.
- It is difficult for an entity which has used the recorded identity and credentials to later repudiate the registration/enrolment and dispute an authentication.

Successful completion of the enrolment and proofing process results in the recording of the identity which may include assigned attributes and/or credentials by which the entity can be authenticated in the future.

R-11 It is required that identity information (e.g., identifiers, credentials and attributes) associated with an identity only be issued after successful identity proofing of the entity.

In some scenarios this may involve recording and issuance of electronic credentials such as digital certificates and tokens binding to an identity or making a claim (i.e., attribute) about an identity. Depending on the type of token being used, the NGN/IdSP will either create a new token and supply the token to the subscriber, or require the subscriber to register a token that the applicant already possesses or has newly created.

R-12 In either case, the mechanism for transporting the token from the token origination point to the other party is required to be secured to ensure that the confidentiality and integrity of the newly established token is maintained.

8.2.2 Maintenance and updates

After an identity(s), including any identity information (identifiers, credentials and attributes), has been registered and issued, both the NGN/IdSP and the subscriber have responsibilities during the operational and use phase to keep it secure.

R-13 NGN/IdSP is required to securely manage and maintain the data and the status of data (e.g., identifiers, credentials, attributes) associated with an identity.

R-14 NGN/IdSP is required to securely manage and log any updates or changes to an identity.

R-15 NGN/IdSP is required to periodically validate the status of an identity.

R-16 NGN/IdSP is required to support procedures to provide notifications about the updates or changes to an identity(s) or any of the data associated with the identity(s) to the systems and network elements that need to be aware of the updates or changes.

R-17 NGN/IdSP is required to provide functions to inform the user about its identity data and to change or delete it.

The subscriber is also responsible for security of assigned credential based on business and policy agreements with the NGN/IdSP. For example, a subscriber has responsibilities to manage his or her electronic credentials (e.g., tokens) and keeps it secure.

R-18 NGN/IdSP is required to take measures based on business and contractual agreements to ensure that an entity (e.g., subscriber, or other NGN/IdSP) securely manages and uses the issued credentials (e.g., digital certificates or tokens) associated with an identity subject to the applicable regulations and policies.

8.2.3 Revocation

Identity revocation is the process of rescinding an identity and the associated credentials. The party or system (e.g., NGN/IdSP) that manages identity or credentials is responsible for its termination or decommission. Revocation is required to prevent the continued use of an identity or credential that is no longer valid or has a security breach.

R-19 NGN/IdSP is required to establish and enforce applicable policies for revoking an identity(s). Specifically, capabilities to terminate or destroy the credentials (e.g., digital certificates or tokens) associated with an identity(s) when the credential is no longer valid or has a security breach shall be supported.

R-20 NGN/IdSP is required to support procedures to provide notifications about the revocation or termination of an identity(s) or any of the data associated with the identity(s) to the entity and to the systems and network elements that needs to be aware (i.e., all systems and processes with which the identity can be used for access have to be notified that the identity is no longer valid).

8.3 Identity management OAM&P functions

8.3.1 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. Clause 8.2.1 of [ITU-T Y.2720] describes the need for interoperability between heterogeneous IdM systems using different data models, structures and schemas.

R-21 NGN/IdSP is required to support functions and capabilities to allow interoperability between heterogeneous IdM systems that are using different data models, structures and schemas as needed.

8.3.2 Management of identity data

Clause 8.2 of [ITU-T Y.2720] describes the need for management of identity data (e.g., management of identifiers, credentials and attributes). Detailed requirements for identity data management is beyond the scope of this Recommendation.

In an NGN, different identity data (e.g., identifiers such as email address, telephone numbers, URIs and IP addresses) may be managed by different management systems and operations processes (e.g., operations support system (OSS)/business support system (BSS)). The following general requirements are provided in the context of providing a structured and coordinated approach for interactions between the different management systems and customer care systems in support of IdM services and capabilities.

R-22 NGN/IdSP is required to support a standard interface (e.g., customer portal) to allow end users/subscribers to interact with applicable NGN management systems and processes in support of end user/subscribers identity data management transactions (e.g., changes and updates) subject to applicable data protection regulations and policies.

R-23 NGN/IdSP is required to support the necessary interfaces, functions and capabilities to facilitate consistent transactions and work flows between the different management systems and processes related to the management of identity data (e.g., changes and updates that need to flow through different OSS/BSS, customer care systems and application services platforms), as appropriate, subject to applicable data protection regulations and policies.

R-24 NGN/IdSP is required to support functions and capabilities to log and store (e.g., backup data) records of transactions related to identity data management subject to applicable data protection regulations and policies.

R-25 NGN/IdSP is required to support functions and capabilities to synchronize changes and updates to identity data between the different management systems and processes, as appropriate, subject to applicable data protection regulations and policies.

R-26 NGN/IdSP is required to support functions and capabilities to verify linkages between the identity data associated with an entity (e.g., subscriber) and contracted services (e.g., access, voice, data, video) subject to applicable data protection regulations and policies.

8.4 Signalling and control functions

8.4.1 Discovery of identity information

In a distributed NGN environment, identity information may exist in different network elements (e.g., subscription server, location server, presence server, home subscription server, etc.). For an application to make use of identity information, it needs to know that it exists and where to locate it.

R-27 NGN/IdSP is required to support functions and capabilities to discover sources of identity information within an NGN/IdSP domain. For example, functions and capabilities for an identity management server to discover the existence of identity information in other network elements such as location, presence or subscription servers or for an application/service to discover identity management or other servers hosting identity data.

R-28 NGN/IdSP is required to support functions and capabilities using standard interfaces and protocols to discover sources of identity information across different NGN/IdSP domains. For example, use of standard interfaces and protocols to discover sources of identity information in other NGN/IdSP domain based on applicable inter-network agreements.

R-29 NGN/IdSP is required to support capabilities for the protection of discovery capabilities and mechanisms.

8.4.2 Identity information access control

Identity data should only be accessible to entities that are authorized to have access to the information.

R-30 It is required that identity information only be accessible to authorized entities subject to applicable regulations and policies. Specifically:

- NGN/IdSP is required to authenticate the entity (e.g., relying party) requesting identity data or perform mutual authentication.
- NGN/IdSP is required to authenticate an entity (e.g., relying party or requesting party) requesting identity data, and verify and validate its authorization before access to the information is provided or the requesting identity data is exchanged.

8.4.3 IdM communications

Network systems and elements need to establish communication sessions to exchange identity information (e.g., identifiers, credentials and attributes) located in different network systems (e.g., identity management server, subscription server, location server, presence server, etc.) that could be correlated and verified (i.e., by an IdM application server providing authentication and correlation functions) to provide identity assurance capabilities.

NGN/IdSP can communicate assertions of identity and associated attributes (e.g., claims and privileges) to the relying parties e.g., for making access control decisions. This would allow different application services (i.e., of different vendor platforms) to use a common available IdM service as opposed to independent and autonomous solutions. Communication 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.
- Federation: Communications between members of a federation.

8.4.3.1 Real-time and near real-time communications

The solution used to discover and exchange identity information would have to take into account whether real-time or near real-time communications are required. This would depend on the specific applications being supported. Certain applications (e.g., VoIP and IPTV) may need the validation of

the requesting user/subscriber identity and authorization for the application service. Other applications (e.g., data and messaging services) may only need near-real-time communication sessions to validate the requesting user/subscriber identity and authorization for the application service.

R-31 NGN/IdSP is required to support capabilities to establish communication sessions according to the specific application service requirement to exchange identity information in real-time or near-real time. This includes communication sessions to exchange identity information within a NGN provider domain, between two different NGN providers and between members of a federation.

Attribute information can be, but is not required to be, limited to membership status, affiliated functions (billing, operations), attributes used by other services (such as a directory service or certificate service). This allows the relying party to provide customized information and contents for users based on their attributes.

R-32 It shall be possible for NGN/IdSP and the relying party to exchange assertions associated with an identity. This includes assertion of attributes.

8.4.4 Correlation and binding

The identity information (e.g., identifiers, credentials 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 other related information such as location and pattern data may be correlated to establish a binding to provide a higher degree of assurance of the subscriber's identity (i.e., confidence of the identity validity).

R-33 NGN/IdSP is required to support capabilities to correlate multiple pieces of identity related data (e.g., location and pattern) to support the establishment of the appropriate binding to the identity of the entity subject to applicable data protection regulations and policies. The use of these capabilities requires user's specific and informed consent.

NOTE – It is possible that some national data protection regulations and policies may restrict support of this requirement.

8.4.5 Authentication requirements

Authentication is the process of establishing confidence in the binding between an identity and the entity. One means for 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.

Refer to [ITU-T Y.2702] for NGN authentication requirements.

The following are security requirements for authentication aspects of IdM:

R-34 Mutual authentication between entities (e.g., user, NGN/IdSP, relying party) shall be possible.

R-35 It shall be possible for a relying party to send requests to the NGN/IdSP for authentication of an entity (e.g., user/subscriber).

R-36 It shall be possible for the NGN/IdSP to support authentication of an entity (e.g., user/subscriber) and provide assertions to a relying party.

R-37 It shall be possible for a relying party to be able to request re-authentication of an entity specifying the current or an alternative method of re-authentication that is required.

8.4.6 Authentication assurance

Authentication assurance is the degree of confidence reached in the authentication process that the communication partner is the entity that it claims to be or is expected to be. The confidence is based on the degree of confidence in the binding between the communicating entity and the identity that is presented. Entities (e.g., users, application services, etc.) may have different authentication assurance needs based on context. There are cases that require different authentication strengths for access to different resources depending upon the sensitivity and value of information and transactions envisaged. In such cases, relying parties (e.g., users, NGN/IdSPs) would need to have more detail (e.g., authentication methods, number of factors of authentication, authentication contexts, etc.) than usual to meet the expected authentication assurance. This involves assessment of the potential risks associated with the consequences of authentication errors or to determine the appropriate level of assurance in an entity identity. Authentication errors with potentially worse consequences will require higher levels of assurance.

R-38 NGN/IdSP is required to support appropriate authentication method(s) depending on the needed level(s) of assurance.

R-39 It shall be possible for a relying party to be able to indicate to the NGN/IdSP the needed assurance level for the authentication of an entity.

R-40 It shall be possible to negotiate assurance level between NGN/IdSP, the relying party and the entity being authenticated.

8.4.6.1 Assurance of user device identity and integrity

NGNs will be supporting a variety of user devices (e.g., fixed telephones, wireless handsets, personal computers, PDA, IPTV set top boxes). The hardware and software components of the devices attaching to the NGN ranges from simple to complex, and if stolen and compromised, can be used to orchestrate a variety of attacks. It is recognized that NGN would also need to support devices (such as "dumb" terminal or POTS devices), which will be unable to provide the required degree of protection.

R-41 It shall be possible for an NGN/IdSP to support end user devices which hold security capabilities and encrypted identity management data (e.g., passwords, digital keys, and certificates) in tamper-resistant hardware components.

R-42 It shall be possible for an NGN/IdSP to communicate with the security capabilities in tamper-resistant hardware components of an end user device via standardized interfaces to support security application services relying on the specialized tamper-resistant hardware component as a trust anchor to uniquely identify and assure the identity of the end user device.

Applications that execute on subscriber devices to let subscribers interact with services and local device features could potentially compromise the integrity of the device. Popular Internet applications, such as web browsers and email, could introduce vulnerabilities that alter the integrity of subscriber devices. Software and file downloads, particularly from an untrusted source, make subscriber devices vulnerable to malicious code, worms, viruses, and Trojan horses. Specialized tamper-resistant hardware component could potentially be designed and implemented in an end user device to provide integrity verification of the device. For example, the specialized tamper-resistant hardware component could contain vendor-specific algorithms and functions to check for integrity compromises. The special hardware component could include a reference model with a set of known-good integrity metrics specifically to identify the correct code and provide reference values for the device. The known-good integrity metrics would be used to compare actual reported values to the configuration and determine if the unit is within compliance.

R-43 It shall be possible for an NGN/IdSP to support end user devices with specialized tamper-resistant hardware component to provide integrity checks and confirmation of the device integrity compliance to applications and services.

R-44 It shall be possible for an NGN/IdSP to communicate with security capabilities in tamper-resistant hardware component of end user devices via standardized interfaces to support security application services relying on the integrity checks and confirmation of the device integrity compliance.

Loss or theft of a device with PII and other sensitive data could result in serious consequences to individuals, business and government enterprises. The specialized hardware component designed to uniquely indentify and confirm integrity of trusted devices could also potentially support capabilities to encrypt and protect PII and other sensitive data on end user devices.

R-45 It shall be possible for an NGN/IdSP to support end user devices with specialized tamper-resistant hardware component to encrypt and protect PII and other sensitive data on end user devices.

8.4.7 Support of services requiring priority treatment

The IdM systems and capabilities of NGNs will have to support application services and communication sessions requiring priority treatment relative to other services. [ITU-T Y.2205] describes emergency telecommunications (ET) requiring special handling from the NGN. A specific example is emergency telecommunications service (ETS) defined in [ITU-T E.107]. ETS leverages the IdM capabilities used for ordinary services (e.g., identity assurance and discovery of trusted identities). Therefore, the IdM systems must support the necessary functions and capabilities to recognize and provide priority treatment when setting up and maintaining an ETS call/session, based on applicable national rules and policies. Refer to [ITU-T E.107] and [ITU-T Y.2205] for information on services and capabilities requiring priority treatment.

R-46 NGN/IdSP IdM systems are required to support the functions and capabilities necessary to recognize and provide priority treatment when setting up and maintaining an ETS call/session, based on applicable national rules and policies.

R-47 IdM network elements and databases used to support ETS calls/sessions are required to provide priority treatment based on applicable national rules and policies. This includes, but is not limited to:

- Intra-network IdM communications (e.g., interactions within an NGN provider IdM system).
- Inter-network IdM communications (e.g., interactions between two NGN provider systems based on bilateral agreements and policies).
- Federated IdM communications (e.g., interactions between members of the federations based on applicable federated identity rules and policies).

Refer to Appendix III for ETS related use case examples.

8.5 Identity management federated identity functions

Federation involves establishing a relationship between two or more entities or establishing an association comprised of any number of service providers and/or identity service providers. 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) bounded by the policies and conditions of the federation and data protection regulations and policies. Federated identity enables the portability and transmission of identity information across otherwise autonomous security domains bounded by the policies and conditions of a federation and subject to applicable rules, regulations and policies. Federated identity enables users of one domain to securely access data or systems of another domain without the need for completely redundant user administration.

R-48 It shall be possible to discover and exchange federated identity information among members of a federation, subject to applicable rules, regulations and policies.

R-49 NGN/IdSP is required to support capabilities to allow a subscriber to provide the necessary authorization to federate its identities.

R-50 NGN/IdSP is required to support capabilities to provide a subscriber the option to terminate participation in all or specific federated identity services and applications and to terminate the federation of its identities.

R-51 NGN/IdSP is required to support capabilities to allow a subscriber to be able to set permissions and prohibitions regarding its federated identity information. It shall be possible for subscribers to control which personal data are given to whom and for what purposes.

NOTE – The requirements for PII protection in clause 8.6 are also applicable to federated identities.

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, technologies and mechanisms used to represent, request and exchange identity related information can be different resulting in interoperability problems. Therefore, appropriate capabilities to allow bridging and interworking among trusted federations will be necessary.

R-52 It shall be possible to accomplish bridging and interoperability among trusted federations that are using different IdM systems, semantics, schemas, mechanisms and technologies. For example, it shall be possible for relying parties in different domains (e.g., NGN domain and web services/Internet) using different IdM capabilities and technologies to interwork and interoperate. In particular, the secure transmission of federated identity information shall be assured.

8.6 User/subscriber functions and protection of PII

End users/subscribers need to be provided with applicable institutive interfaces and capabilities to control their PII and make informed decisions and consent regarding their personal data. End users/subscribers should be able to express their privacy policies and preferences and negotiate the terms of data disclosure with the NGN/IdSP.

Disclosure of personal data should only be made to authorized entities based on applicable policies (e.g., user/subscriber consent, government regulatory rules). In addition, collecting, storing, and use of PII should be minimized and adhere to the applicable policies.

R-53 NGN/IdSP is required to provide IdM services and confidentiality protection of PII, in accordance with applicable regulations, policies and rules.

R-54 It shall be possible for end users/subscribers to communicate to the NGN/IdSP, preferences regarding their personal data (e.g., set privacy preferences) according to the applicable regulations and policies (e.g., stated consent of the individuals, providers' policies, or regulatory rules).

R-55 It shall be possible for the end user/subscriber to be able to verify the authenticity of the entity requesting PII before providing the requested information.

R-56 NGN/IdSP is required to delete PII when specified purposes of data collection and retention are met based on applicable regulations, policies and rules.

R-57 It shall be possible for the end user/subscriber to operate anonymously or pseudonymously based on the application context and applicable regulations, policies and rules.

8.7 Security

Identity information and data are highly sensitive and targeted by intruders. In addition, since IdM services and capabilities will be used for access control to business, governments and social networking applications, the network elements and systems (e.g., network elements and databases supporting IdM functions and capabilities) will be targeted for security attacks and intrusions. Therefore, appropriate security measures must be implemented to secure and protect the network elements and systems providing IdM functions, services and capabilities.

8.7.1 System and data access control

System access control involves security measures to prevent unauthorized access to network elements and systems and their associated access points. There are threats associated with unauthorized access to network elements and systems supporting IdM functions, capabilities and data. Therefore, appropriate access control measures to prevent unauthorized access must be established and enforced.

R-58 NGN/IdSP is required to support and enforce system access control measures to prevent unauthorized access to network elements and systems supporting IdM functions and capabilities. NGN/IdSP shall not allow an entity to gain access to the network elements and databases supporting IdM functions and capabilities unless the entity is identified, authenticated and authorized. This applies to all entities (i.e., persons, processes, and remote systems).

Data access control involves security measures to prevent unauthorized access to stored or provisioned data and data in transit. There are threats associated with unauthorized access to provisioned or stored IdM related data. Therefore, appropriate access control measures to prevent unauthorized access must be established and enforced.

R-59 NGN/IdSP is required to support and enforce access control measures to prevent unauthorized access to IdM data. This includes any identity data stored or provisioned in IdM databases, application servers, home subscriber servers (HSS), or any other network element. The NGN/IdSP shall not allow an entity to gain access to IdM data unless the entity is identified, authenticated and authorized. This applies to all entities (i.e., persons, processes, and remote systems).

8.7.2 System and data integrity

Network elements, systems and functions supporting IdM services and capabilities must have integrity protection. This includes the IdM databases and application servers.

R-60 NGN/IdSP is required to provide integrity protection of all network elements, systems, and functions supporting IdM services and capabilities.

Stored identity information and data must be provided with integrity protection to prevent any corruption or manipulation of the data impacting the integrity.

R-61 NGN/IdSP is required to provide integrity protection of IdM provisioned data.

R-62 NGN/IdSP is required to provide integrity protection of any data distribution, communication, updates or changes, and any offline data associated with IdM.

8.7.3 Data confidentiality

R-63 NGN/IdSP is required to support and enforce measures to protect provisioned IdM data from being observed by unauthorized entities (e.g., unauthorized insiders).

R-64 NGN/IdSP is required to support and enforce measures to protect IdM data distribution, communications, updates or changes, and any offline IdM data from being observed by unauthorized entities (e.g., unauthorized insiders).

8.7.4 Security protection of IdM communications

IdM communications (signalling and media) have to be protected against unauthorized access, corruption, manipulation and interception (e.g., eavesdropping).

R-65 NGN/IdSP is required to provide integrity and confidentiality protection of intra-network and inter-network IdM communications. All IdM related signalling and media traffic crossing network-to-network interface (NNI), application-to-network interface (ANI) or server-to-network interface (SNI) between network domains shall be provided integrity protection.

8.7.5 Management security

Management access to NGN network elements and configured data must be secure and protected against unauthorized access and controls.

R-66 NGN/IdSP is required to prevent unauthorized access to management interfaces and controls of network elements and functional entities supporting IdM.

Management traffic must be secure and protected against corruption, manipulation and unauthorized observation.

R-67 NGN/IdSP is required to provide integrity and confidentiality protection of management traffic associated with the support of IdM.

8.7.6 Security and auditing log

Security and auditing log for the purpose of recording events that will support after-the-fact investigation of specific activities are needed.

R-68 NGN/IdSP is required to generate security logs for the purpose of recording events that will support after-the-fact investigation of specific activities (e.g., logins, modification of critical system resources and data, management access to configured NGN parameters and resources) related to the support of IdM.

8.7.7 Protection against denial of service (DoS) and distributed DoS (DDoS) attacks

IdM services and capabilities must be highly available and therefore must be protected against DoS and DDoS threats potentially affecting availability.

R-69 NGN/IdSP is required to provide protection against DoS, DDoS and other types of attacks impacting availability of IdM services and capabilities. This includes the support and use of capabilities and tools as appropriate to detect, isolate, and mitigate DoS and DDoS and other types of attacks.

8.7.8 Monitoring and intrusion detection

R-70 NGN/IdSP is required to support and use security monitoring and intrusion detection tools as appropriate to detect fraud, abuse, and intrusion into IdM network elements and systems.

Appendix I

General IdM use cases

(This appendix does not form an integral part of this Recommendation)

I.1 Introduction

This appendix provides general uses cases for IdM organized as governments, business enterprises and end users/subscribers.

I.2 Governments

IdM capabilities can be used by governments to enhance and support applications and transactions between government enterprises and citizens; between different governmental organizations (federated government services) and agencies; and between different governments (e.g., inter-government federated services). Examples of governmental use cases include:

- Assurance of citizen identification: IdM can be used by governments to validate the identity of citizens to receive electronic governmental services while improving protection of PII. Consider health care as an example, the sensitivity of health-related information highlights the importance of data minimization and more broadly the need for security and privacy of identity information.
- Assurance of governmental employee identification for federated governmental services: IdM capabilities can be used by government enterprises to develop common solutions for secure and reliable forms of identification for government employees that offer enhanced security, efficiency, reduced identity fraud, and the protection of personal privacy.
- Enhancement and support of federated services between different governments: IdM can be used to enhance and support federated services between different governments. For example, governments may collaborate to develop enhanced IdM solutions for citizens travelling between different countries addressing security, privacy, and user experience.

I.3 Business enterprise

IdM can be used to assist business organizations to enhance and support new and existing businesses while improving security, privacy and PII protection. Examples of business enterprise use cases include:

- Federated identity services: IdM can be used to support single sign-on and sign-off services across multiple business partners (including NGN, web services, content and 3rd party providers).
- Communications services: IdM can be used by NGN providers to enable end users/subscribers to be provided with application services over different platforms (e.g., managed IP networks, Internet and mobile platforms) and to allow users to access their chosen applications over multiple platforms in ways that are customized to their own preferences.
- Electronic financial transactions and applications: IdM can be used to enhance and support applications for electronic payments for e-commerce transactions.

I.4 End user/subscribers

For end users/subscribers, IdM can be used to enhance experience and control PII. Examples of end user/subscriber use cases include:

- User control of PII: IdM can be used to provide an enhanced user experience, and to allow control of PII. Individuals can use multiple pseudonyms to participate in different activities such as checking news feeds, publishing blog posts, managing social networks and swapping photographs or music. IdM can help provide individuals with more choices about how they participate in different communities, and the degree to which they want aspects of their different identities to be linked (i.e., control of their PII).
- Social networks: IdM can be used to enhance and support social networking applications by providing the necessary tools for effective user control of PII and accountability.

Appendix II

IdM use cases for NGN applications

(This appendix does not form an integral part of this Recommendation)

II.1 Introduction

This appendix provides example identity management (IdM) use case examples for NGN. The example use cases would be used as a basis for developing the IdM requirements for NGN.

II.2 Basic use case example

Figure II.1 shows a basic use case example involving three basic elements. There are other possible scenarios beyond this basic example. Refer to Appendix V for a description of the other possible scenarios (e.g., user centric scenarios).

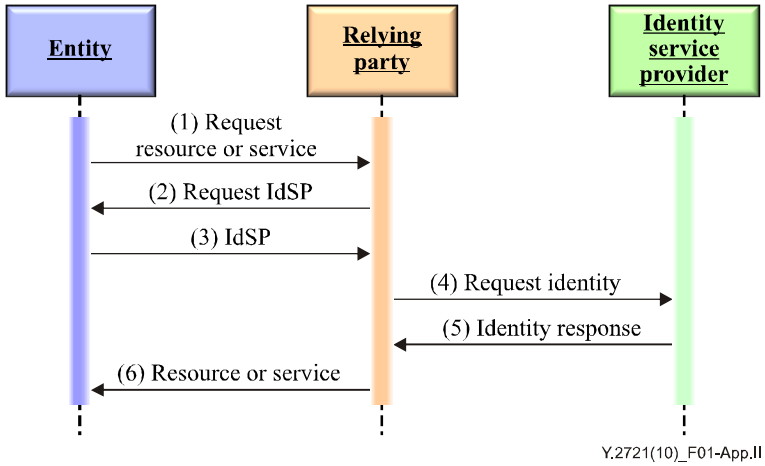


Figure II.1 – Basic use case example

The three elements consist of an entity (an asserting party or principal) who seeks services from a relying party (an RP, which could be a network or an application), and who obtains an associated identity assertion, including anonymous or pseudonymous assertions, from an identity service provider (IdSP) based on trust and security policy.

In Figure II.1, the following high-level IdM information flow is shown.

1) The entity provides a claimed identity to the relying party (the resource or service provider) and requests a resource or service from that relying party.
2) The relying party (network or application) needs to have the entity authenticated before providing the requested resource or service. For authentication, the relying party needs information from the appropriate IdSP, which must be determined and contacted. The relying party returns a "Request for IdSP info" to the entity, asking the entity to provide the appropriate IdSP name.
3) The entity responds to this "Request for IdSP info" by identifying the appropriate IdSP to the relying party. The entity may identify multiple IdSPs.
4) The relying party in turn queries the appropriate IdSP(s) to validate the entity's claimed identity to a sufficient trust level (assurance level), as required.
5) The IdSP confirms the entity's claimed Identity. The IdSP functions may include delegation (meaning that the IdSP may delegate some aspects of the authentication process to other IdSPs by relaying the identity assertion to them). There may be subsequent requests from

the relying party to the IdSP(s), in the event of the need for higher assurance level authentication, or for other implementation-specific capabilities.

6) The relying party, after receiving validation of the entity's claimed identity from the IdSP(s), provides the requested resource or service.

Combinations of these three elements (entity, relying party, and IdSP) are possible. The underlying media involved are not relevant. The only requirement is that these communication mechanisms should be "well-structured" with syntaxes and profiles that are known or potentially obtainable by the parties involved, if they possess the necessary permissions to use the mechanisms. Where appropriate, standard mechanisms for trusted, global interoperability should be used.

In addition, other high-level IdM information flows are possible. For example:

1) An RP can request authentication credentials directly from an entity.
2) The entity can provide its authentication credentials to a trusted IdSP.
3) The IdSP can validate the given credentials from the entity, and then generate new credentials for the entity, in order to satisfy the authentication request from the RP.
4) The entity (or its delegate) can obtain the generated credentials from the IdSP and give them to the RP.
5) The generated credentials sent from the entity to the RP can either contain 1) a copy of the identity claims generated by the IdSP, or 2) a reference to them.

In addition, the entity may decide not to give the IdSP-generated authentication credentials to the RP.

It is also possible to have a hierarchy of identity providers or a hierarchy of relying parties. It is also possible that an entity may have more than one delegate.

II.3 Use of common IdM systems to support multiple application services (e.g., voice, data, IPTV) within a service provider network

II.3.1 Overview

Network/service providers (e.g., NGN providers) would be supporting and hosting multiple applications and services. The distributed nature of the NGN environment allows the possibility that different application services might be hosted on different network elements and vendor-specific platforms (e.g., VoIP, data and IPTV). Each service may have its own vendor-specific or technology-specific means for access control that may not be compatible with each other, and therefore would have to be configured, managed and used separately.

An approach leveraging a common IdM infrastructure enabling multiple applications/services may provide cost and business efficiency benefits. It could also provide a standard approach to allow application developers to utilize common enablers for IdM rather than having each application/service supporting specific IdM functions (e.g., vendor-specific access control capabilities and mechanisms) and allow an efficient process to design, implement and offer application services. In addition, a common approach can assist to manage the security risks to each application service and the overall network infrastructure as a whole.

The IdM approach for NGN would include both intra-network solutions (i.e., solutions within a NGN provider domain) and inter-network solutions (i.e., solutions between different NGN providers including 3rd party providers). For the intra-network scenario, this may involve approaches to allow interactions between different network elements or components within a NGN provider domain for IdM (e.g., claimants, relying systems and identity systems). For inter-network scenarios, this may include specification of approaches to allow interaction between the network element entities across different NGN domains for IdM (e.g., claimants, relying parties and IdSP).

NOTE – An NGN provider may also be an IdSP.

II.3.2 Use case description

This use case example illustrates how multiple application services (e.g., VoIP, data, and IPTV) use a common identity management infrastructure for access control and security protection of the application service. The use case involves interactions between the following entities:

- End users (i.e., end user and/or end user device).
- Relying system (i.e., application service or network system).
- IdM system (i.e., network system providing IdM services such as registration, authentication and authorization, subscription profile information).

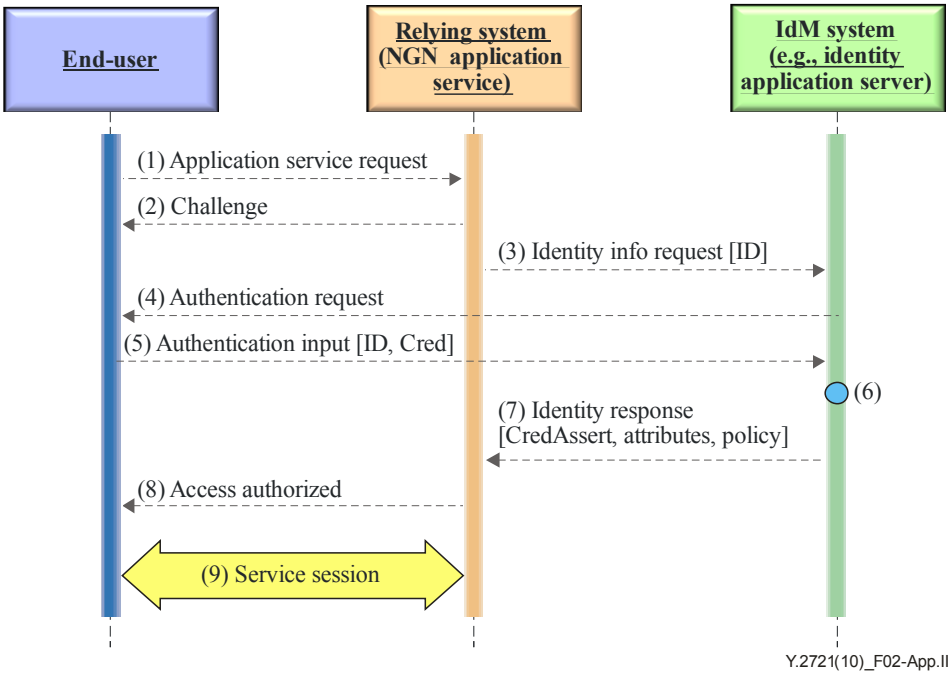


Figure II.2 – Basic use case example

Figure II.2 illustrates a basic example where an application service uses the services of an IdM system that is external or independent of the application service for access control and the management of privileges. The example call flows are as follows:

1) Application service request: This information flow represents the end user request to invoke the application service.
2) Challenge: The application service sends a response challenging user access.
3) Identity information request [UserID]: The application service sends a request to the IdM system to assert the user identity and provide attributes associated with the UserID. This may include information such as service profile, privileges, preferences and policy information, for example, any policy or restrictions associated with the identity.
4) Authentication request: The IdM systems send the user a request for authentication.
5) Authentication input [Credentials]: The user provides information for authentication (e.g., UserID and password or personal identification number).
6) Authentication: The IdM system performs authentication and obtains other needed information. This may involve obtaining information from other network systems (e.g., HSS).
7) Identity information response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the UserID (e.g., privileges and preferences) and policy

associated with the identity information (e.g., any restriction regarding use, display and dissemination).

8) Access authorization: The application service provides the user with an indication that access to the service is granted.

9) Application service session: This information flow represents the user successful session with the application service.

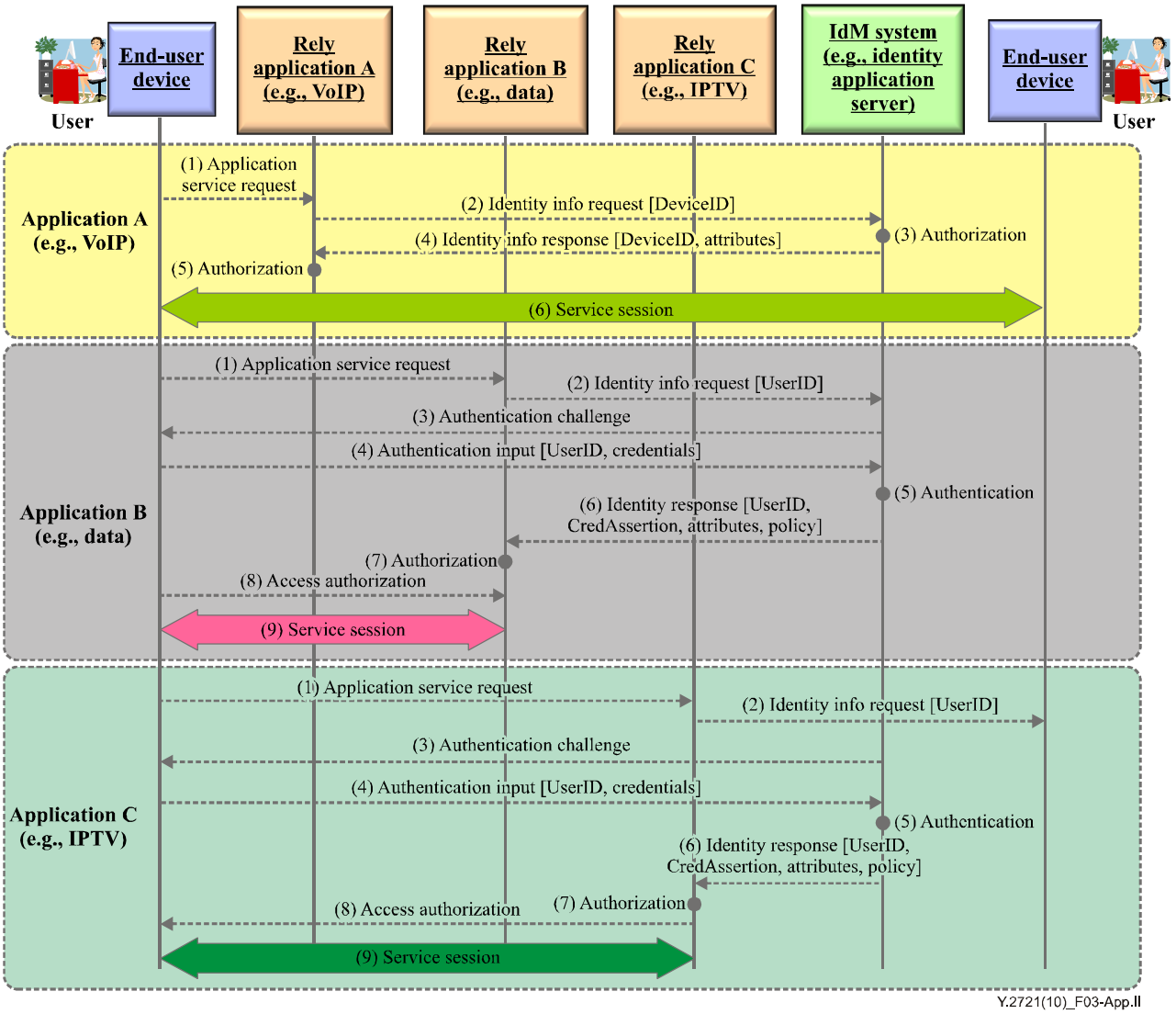


Figure II.3 – Multiple application services use of common IdM infrastructure

Figure II.3 illustrates an example use case where multiple application services (e.g., VoIP, data, and IPTV) are using a common IdM system that is external and independent of the application services. This example assumes that the end user device has registered and is attached to the service provider using the normal procedures.

The example flows for application A (VoIP) are as follows:

1) Application service request: This information flow represents the end user initiating a call.

2) Identity info request [DeviceID]: The application service sends a request to the IdM system to verify whether the end user device is authorized for VoIP service. This example assumes that VoIP service is based on the subscription profile of the user device or line (e.g., xDSL subscription).

3) Authorization: The IdM system determines whether the end user is authorized for VoIP service.

NOTE 1 – It is assumed that this would involve retrieving subscription profile information for the end user device or line (e.g., xDSL). It is also assumed that for VoIP, authentication of the end user is not needed.

4) Identity information response [DeviceID, attributes]: The IdM system provides attributes associated with the DeviceID (i.e., whether the device is authorized for VoIP service). This would include relevant information obtained from the subscription profile (e.g., privileges and preferences).

5) Access authorization: The application service provides the user with an indication that access to the service is granted.

6) Application service session: This information flow represents the user successful call session.

The example call flows for application B (data) are as follows:

1) Application service request: This information flow represents the end user request to invoke the application service.

2) Identity information request [UserID]: The application service sends a request to the IdM system to assert the user identity and provide attributes associated with the UserID. This may include information such as service profile, privileges, preferences and policy information, for example, any policy or restrictions associated with the identity.

3) Authentication challenge: The IdM systems send the user a request for authentication.

4) Authentication input [Credentials]: The user provides information for authentication (e.g., UserID and password or personal identification number).

5) Authentication: The IdM system performs authentication and obtains other needed information. This may involve obtaining information from other network systems (e.g., HSS or other subscription database).

6) Identity information response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the UserID (e.g., privileges and preferences) and policy associated with the identity information (e.g., any restriction regarding use, display and dissemination).

7) Authorization: The application service processes the information and determines that the user is authorized for the service.

8) Access authorization: The application service provides the user with an indication that access to the service is granted.

9) Application service session: This information flow represents the user successful session with the application service.

The example call flows for application C (IPTV) are as follows:

1) Application service request: This information flow represents the end user request to invoke the application service.

2) Identity information request [UserID]: The application service sends a request to the IdM system to assert the user identity and provide attributes associated with the UserID. This may include information such as service profile, privileges, preferences and policy information, for example, any policy or restrictions associated with the identity.

3) Authentication challenge: The IdM systems send the user a request for authentication.

4) Authentication input [Credentials]: The user provides information for authentication (e.g., UserID and password or personal identification number).

5) Authentication: The IdM system performs authentication and obtains other needed information. This may involve obtaining information from other network systems (e.g., HSS or other subscription database).

6) Identity information response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the UserID (e.g., privileges and preferences) and policy associated with the identity information (e.g., any restriction regarding use, display and dissemination).

7) Authorization: The application service processes the information and determines that the user is authorized for the service.

8) Access authorization: The application service provides the user with an indication that access to the service is granted.

9) Application service session: This information flow represents the user successful session with the application service.

NOTE 2 – To provide mutual authentication (i.e., to authenticate the application or service provider), further functionalities and flows will be necessary. However, this is not shown in Figure II.3.

II.3.3 Implied requirements

The following requirements are implied by this use case example:

- The NGN can have a common IdM solution to be used by multiple application and services independent of the application platform or vendor solution.
- Common IdM functions shall not be used, if they contradict the principles of data collection limitation, data minimization, data separation, purpose specification and use limitation.
- The NGN shall support a standard and structured approach to allow application services to discover the IdM system(s) and exchange identity data securely.

II.4 Single sign-on/single sign-off to multiple application services (e.g., voice, data, and IPTV) within a service provider network

II.4.1 Overview

Users typically have to sign-on to multiple systems hosting application services (e.g., VoIP, data, and IPTV), necessitating an equivalent number of sign-on dialogues, each of which may involve different usernames and authentication information. System administrators are faced with managing user accounts within each of the multiple systems to be accessed in a coordinated manner in order to maintain the integrity of security policy enforcement.

End user subscribers are demanding ease of use features such as "Single Sign-on/Sign-off." The premise of "Single Sign-On" is that an end user, device, or end user and device combination can sign-on once (i.e., providing credential input for authentication and authorization) to a service in a next generation network (NGN), and as a result be authenticated with one or more additional services in the same NGN (i.e., the end user is not burdened with authentication for each service). The word "Sign-On", as used here, means the same thing as the word "Register with", "Log-On", or "Log-In", where the end-user/device "registers with", "logs-on" or "logs-in" to a service. Similar "Single Sign-off" provides the use with a feature to avoid having to "Sign-off" each application service in a given session.

Benefits provided by single sign-on/sign-off services include:

- Reduction in the time taken by users in sign-on operations to individual domains, including reducing the possibility of such sign-on operations failing.
- Improved security through the reduced need for a user to handle and remember multiple sets of authentication information.

- Reduction in the time taken, and improved response, by system administrators in adding and removing users to the system or modifying their access rights.
- Improved security through the enhanced ability of system administrators to maintain the integrity of user account configuration including the ability to inhibit or remove an individual user's access to all system resources in a coordinated and consistent manner.

II.4.2 Use case description

This use case example illustrates the use of an IdM system to support "Single Sign-on/Sign-off" to multiple application services (e.g., VoIP, data, and IPTV) within a NGN provider domain. The use case involves interactions between the following entities:

- End users (i.e., end user and/or end user device).
- Relying system (i.e., application service or network system).
- IdM system (i.e., network system providing IdM services such as registration, authentication and authorization, subscription profile information).

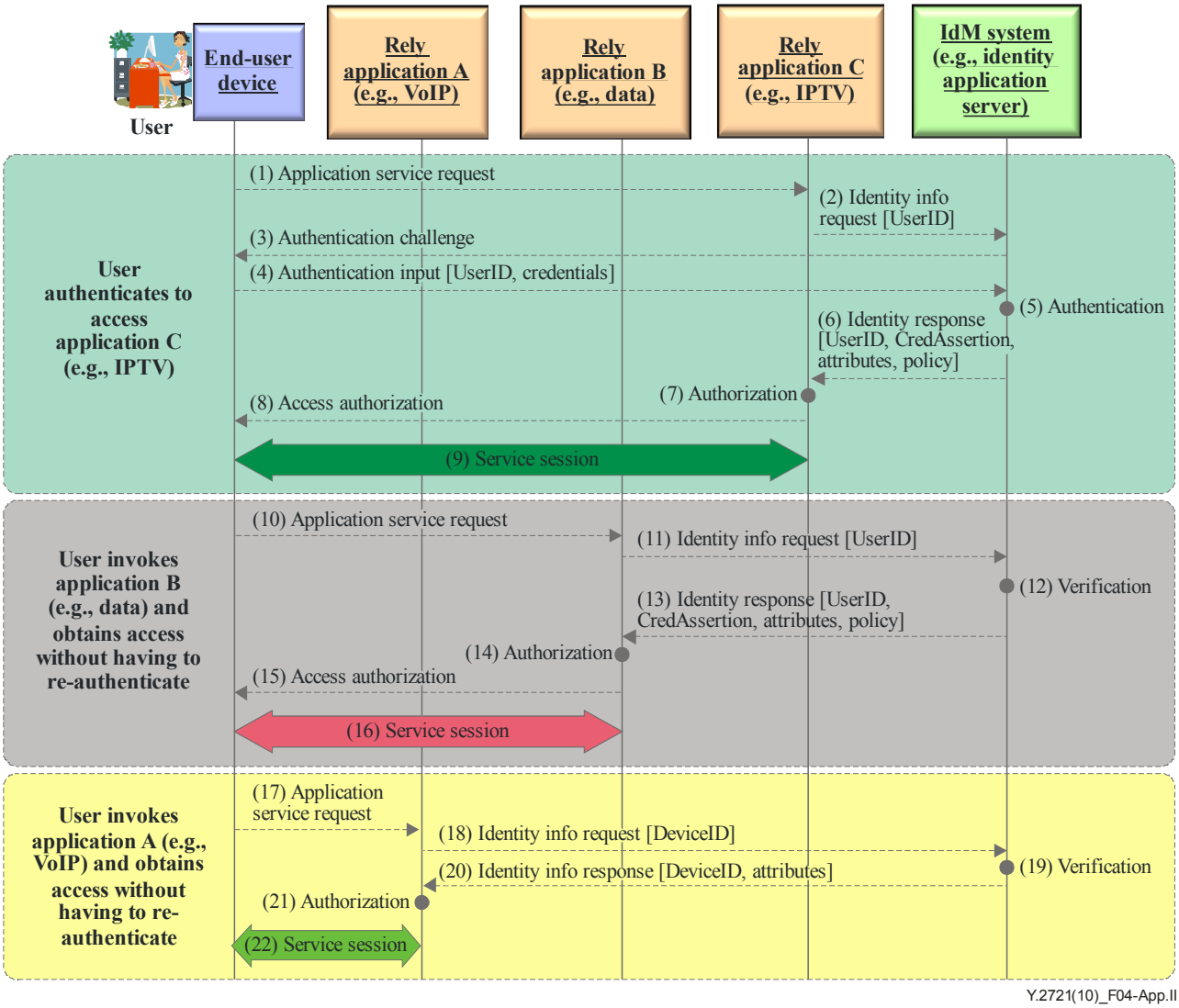


Figure II.4 – Single sign-on service

Figure II.4 illustrates an end user subscriber using a single sign-on service to access multiple application services (e.g., VoIP, data, and IPTV). This example assumes that the end user device has registered and is attached to the NGN using the normal procedures.

The call flow examples are as follows:

1) Application service request: This information flow represents the end user request to invoke application service C (IPTV).
2) Identity information request [UserID]: Application service C (IPTV) sends a request to the IdM system to assert the user identity and provide attributes associated with the UserID. This may include information such as service profile, privileges, preferences and policy information, for example, any policy or restrictions associated with the identity.
3) Authentication challenge: The IdM system challenges the user for authentication.
4) Authentication input [Credentials]: The user provides information for authentication (e.g., UserID and password or personal identification number).
5) Authentication: The IdM system performs authentication and obtains other needed information. This may involve obtaining information from other network systems (e.g., HSS or other subscription database).
6) Identity information response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the UserID (e.g., privileges and preferences) and policy associated with the identity information (e.g., any restriction regarding use, display and dissemination).
7) Authorization: Application service C (IPTV) processes the information and determines that the user is authorized for the service.
8) Access authorization: Application service C (IPTV) provides the user with an indication that access to the service is granted.
9) Application service session: This information flow represents the user successful session with application service C (IPTV).
10) Application service request: This information flow represents the end user request to invoke application service B (data).
11) Identity information request [UserID]: Application service B (data) sends a request to the IdM system to assert the user identity and provide attributes associated with the UserID. This may include information such as service profile, privileges, preferences and policy information, for example, any policy or restrictions associated with the identity.
12) Verification: The IdM system processes the request, determines that single sign-on is applicable and verifies that user authentication is still valid.
13) Identity information response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the UserID (e.g., privileges and preferences) and policy associated with the identity information (e.g., any restriction regarding use, display and dissemination).
14) Authorization: Application service B (data) processes the information and determines that the user is authorized for the service.
15) Access authorization: Application service B (data) provides the user with an indication that access to the service is granted.
16) Application service session: This information flow represents the user successful session with application service B (data).
17) Application service request: This information flow represents the end user request to invoke application service A (VoIP).

18) Identity information request [DeviceID]: Application service A (VoIP) sends a request to the IdM system to assert the user identity and provide attributes associated with the DeviceID.

19) Verification: The IdM system processes the request, determines that single sign-on is applicable and verifies that user authentication is still valid.

20) Identity information response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the DeviceID (e.g., privileges and preferences) and policy associated with the identity information (e.g., any restriction regarding use, display and dissemination).

21) Authorization: Application service A (VoIP) processes the information and determines that the user is authorized for the service.

22) Application service session: This information flow represents the user successful session with application service A (VoIP).

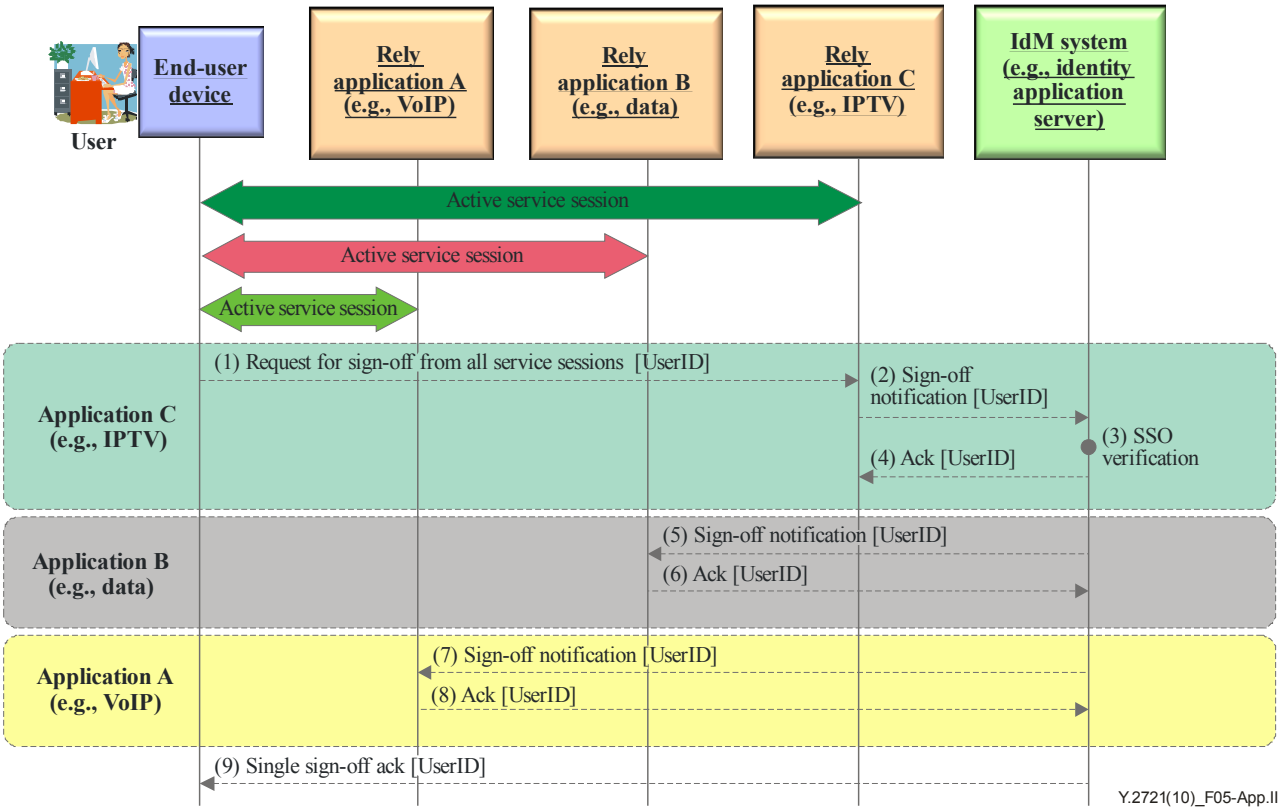


Figure II.5 – Single sign-off service

Figure II.5 illustrates a "Single Sign-off" service allowing the user to automatically sign-off from multiple application services (VoIP, data, and IPTV) without having to sign-off from each application service in the session. This use case assumes that the user is in a service session with active application services A (VoIP), B (data) and C (IPTV).

The call flows are as follows:

1) Service sign-off [UserID]: This call flow represents the user request to end all service sessions.

2) Sign-off notification [UserID]: Application service C (IPTV) notifies the IdM system of user request to sign-off.

3) SSO verification: The IdM system determines single sign-off is applicable and verifies the active application services.

4) Ack [UserID]: The IdM system sends an acknowledgement to application service C (IPTV) about the end of service session.

5) Sign-off notification [UserID]: The IdM system notifies application service B (data) of sign-off.

6) Ack [UserID]: Application service B (data) acknowledges the sign-off.

7) Sign-off notification [DeviceID]: The IdM system notifies application service A (VoIP) of sign-off.

8) Ack [UserID]: Application service A (VoIP) acknowledges sign-off.

9) Single sign-off Ack [UserID]: IdM system sends an acknowledgement to the user confirming sign-off from all active application services in the session.

II.5 Correlation of distributed identity information for multi-factor authentication assurance

II.5.1 Overview

This use case illustrates the use of IdM to correlate and bind multiple pieces of identity information (e.g., identifiers, credentials and attributes) to assure the identity of an end user/subscriber. For example, the identity information associated with a subscriber (e.g., UserID), the subscriber device (e.g., DeviceID), and location information may be correlated to provide a higher assurance of the subscriber.

II.5.2 Use case example

Figure II.6 illustrates a use case example binding the user identity with the device identity and correlating with presence and location information to provide a higher level of assurance of the identity and the claims associated with the identity.

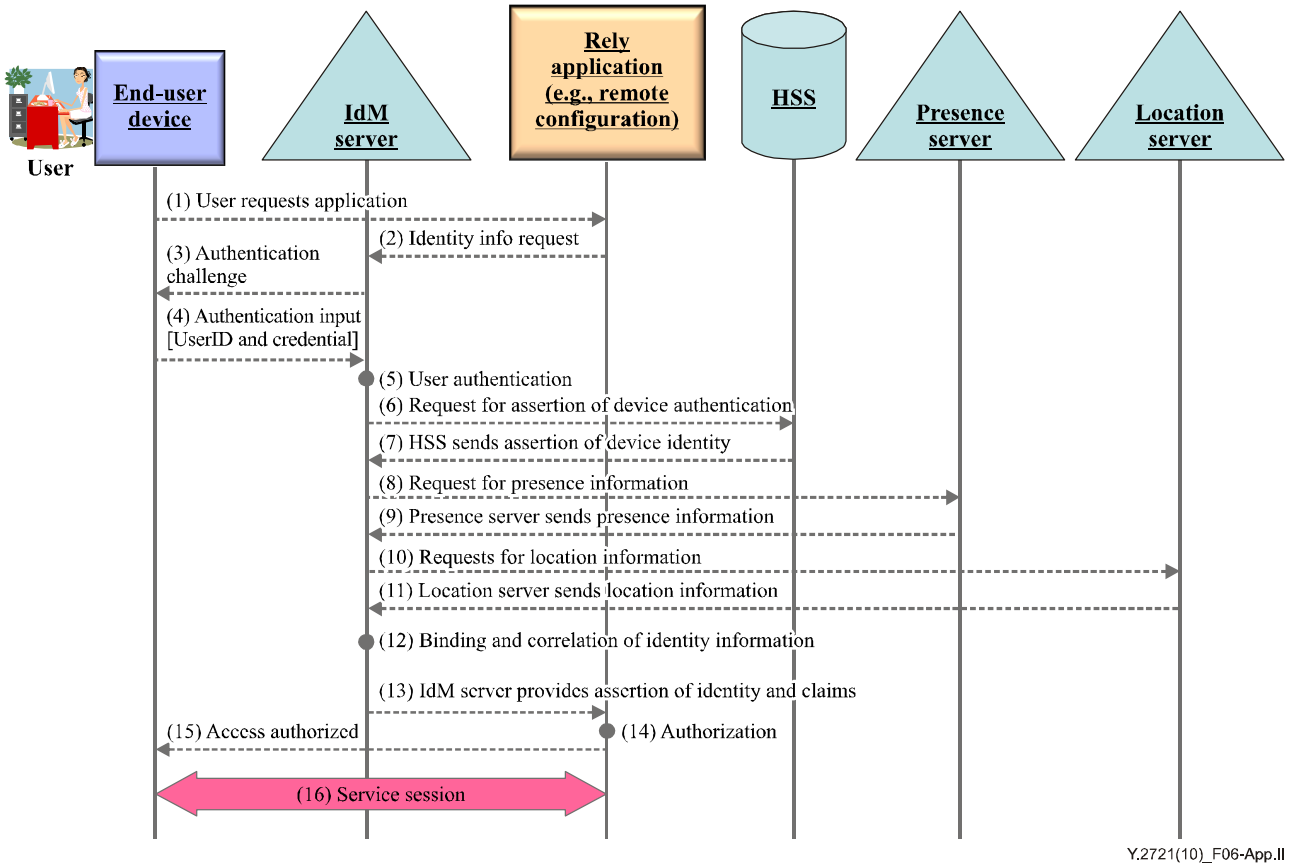


Figure II.6 – Correlation of identity information

In this example, the end user/subscriber is attempting to access an application that requires a high level of assurance of the user identity and the privileges associated with the identity because the security risks associated with allowing unauthorized access to the application or resource can be costly.

The example call flows are as follows:

1) The user requests access to the application.
2) The application sends a request to the IdM server for assertions of the user identity and the claims associated with the identity.
3) The IdM server sends an authentication challenge to the user.
4) The user provides input for authentication (e.g., UserID and credentials) to the IdM server.
5) The IdM server authenticates the user.
6) The IdM server sends a request to the HSS for an assertion of the user's device identity (Note that it is assumed that the user device registers with and is authenticated by the network using normal procedures).
7) The HSS sends an assertion of the user's device identity.
8) The IdM server sends a request to the presence server for presence information.
9) The presence server provides presence information to the IdM server.
10) The IdM server sends a request to the location server for location information.
11) The location server provides location information to the IdM server.

12) The IdM server binds the user identity and user device identity information. The combined identity is correlated with presence and location information to verify the claims (e.g., privileges) associated with the identity.

13) The IdM server provides the application with assertions of the user identity and the claims associated with the identity.

14) The application determines whether the user is authorized for access.

15) The user is granted access to the application.

16) Service session is established.

II.6 Enforcement of user control of personally identifiable information (e.g., preferences) across peer network/service provider domains

II.6.1 Overview

Protection of PII is very important for end users/subscribers. An important feature of IdM is to enable end users/subscribers to provide service providers and IdSPs information about conditions, restrictions, consents, authorization regarding creation, collection, use and dissemination of their identity information.

II.6.2 Use case description

This use case is related to the enforcement of applicable policies such as policies regarding anonymous or pseudonymous identity information.

Figure II.7 illustrates an example use case where a user requests anonymity.

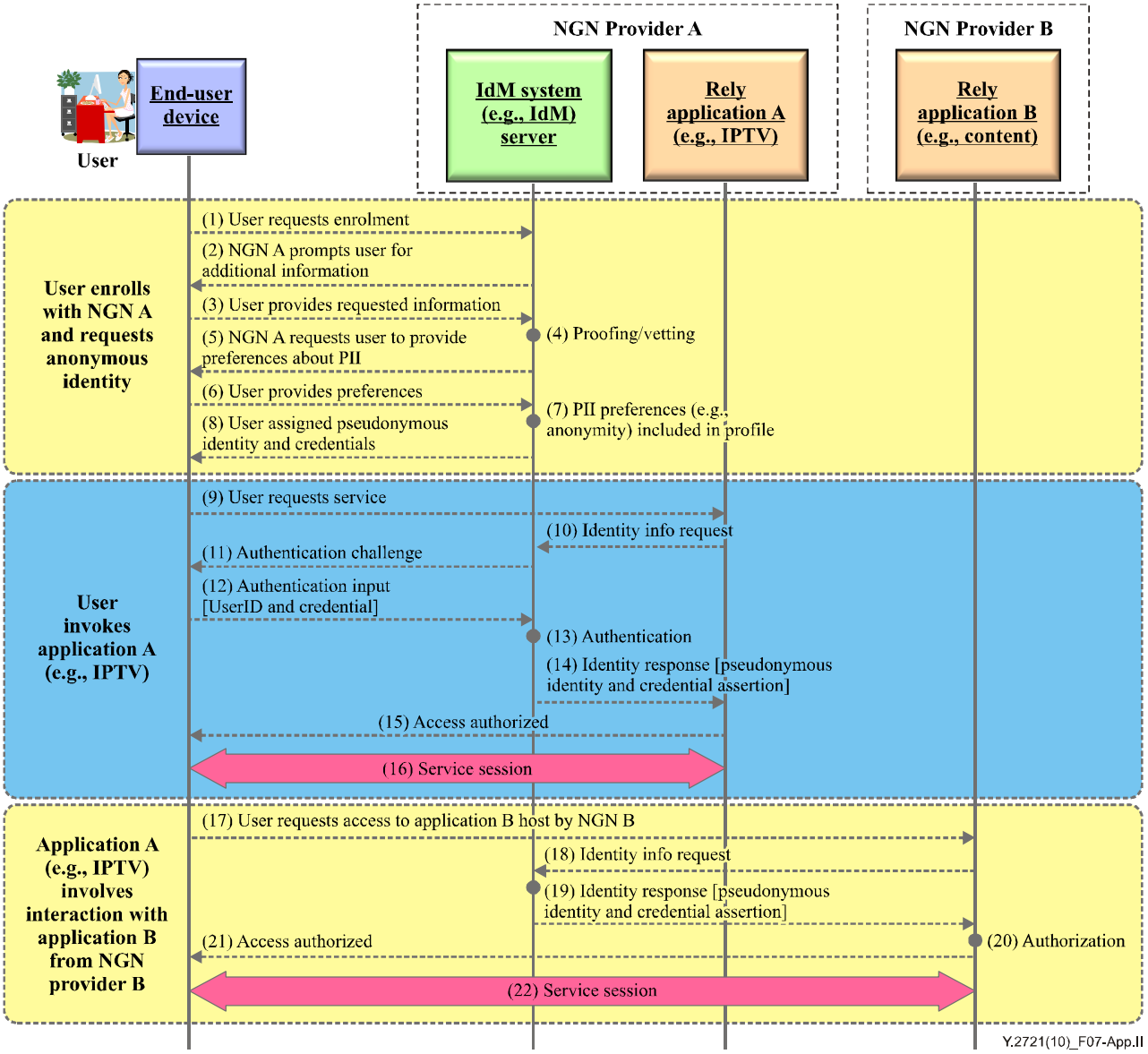


Figure II.7 – Anonymous user identity

NOTE – The term IdM system is used as a generic term to represent any network element that might be providing IdM functions and allow different realization/implementation possibilities.

The use case example shows an NGN provider (NGN provider A) assigning an identity using pseudonyms based on a request for anonymity from the end user/subscriber. The pseudonymous identity is used for interactions with NGN provider B to protect the end user subscriber's personally identifiable information.

The example call flows are as follows:

1) The user requests enrolment with NGN provider A.
2) NGN provider A prompts the user for additional information.
3) The user provides requested information to NGN provider A.
4) NGN provider A proofs and vets the information.
5) NGN provider A prompts the user to provide information about preferences concerning the personally identifiable information (PII).
6) The user indicates preference for anonymity.

7) NGN provider A includes anonymity preference to the user profile information.

8) The user is assigned a pseudonymous identity and credential binding the identity.

9) The user invokes application A (e.g., IPTV) hosted by NGN provider A.

10) The relying application A requests identity information about the user from the IdM system (e.g., IdM server).

11) The IdM system sends authentication challenge to the user.

12) The user provides input for authentication to the IdM system (e.g., UserID and credential).

13) The IdM system authenticates the user.

14) The IdM system sends assertions of the user identity and credentials to the relying application A.

NOTE – Only pseudonymous identity information is provided to enforce anonymity.

15) The user is authorized for access to application A.

16) Service session.

17) The user requests access to application B hosted by NGN B.

18) Application B sends requests to the IdM system for information asserting the user identity and associated claims.

19) The IdM system provides assertion of the user identity and associated claims. Only pseudonymous identity information is sent to enforce policy for anonymity.

20) Application B verifies information for authorization.

21) Authorization for access is provided to the user.

22) Service session is established.

II.7 Bridging/mapping between heterogeneous IdM systems

II.7.1 Overview

In order to enable a user to receive multiple services offered by the various components of the NGN, the NGN needs to have the mechanisms for bridging among various IdM systems. Such a need is illustrated by a use case described in clause II.7.2.

II.7.2 Use case description

This scenario describes access by a subscriber of a NGN to a resource (e.g., a directory server) located in an enterprise network with the use of her or his handset. Because the NGN and enterprise networks employ different IdM mechanisms, there is a need for bridging between the IdM systems of these networks.

The following entities are involved in an example illustrating the scenario:

- The IdM system of the NGN. This system is modified in such a way that it is capable, in addition to supporting mutual AKA-based authentication of the user's handset, to provide it with the credentials for authentication to the IdM system of the enterprise network.
- The IdM system of the enterprise network (e.g., key distribution centre).
- The enterprise directory server (EDS) located in the enterprise network.
- The user's handset.

- These entities perform the following interactions:
  - The user's handset and the mobile network authenticate each over using the AKA method.
  - The user, using a handset, sends a request to the enterprise directory server (EDS) located in the enterprise network.
  - The EDS replies with an authentication request.
  - The user obtains from the IdM system of the NGN the authentication credentials (e.g., a Kerberos ticket), which are based on the results of the AKA authentication, and are valid for authentication to the enterprise IdM system.

For example, the user's handset obtains a ticket to the key distribution centre (KDC) of the enterprise network. Specifically, the ticket allows the user to get authenticated by the ticket granting server (TGS), which is a part of the KDC.

- The user requests from the TGS a ticket for authentication to the EDS.
- The TGS validates the presented credentials and responds to the user with a ticket to the EDS.
- The end user responds to the EDS's authentication request with the ticket received from the TGS.
- The EDS authenticates the user and responds with its own credentials for authentication to the user and a confirmation for the requested service. After validating the EDS credentials, the user can access the EDS.

II.7.3 Implied requirements

- The IdM system of the NGN must support the AKA authentication mechanism and the authentication mechanism (e.g., Kerberos) used by the enterprise network.
- The IdM system of the NGN must be capable of issuing authentication credentials (e.g., a Kerberos ticket) to the end user device for authenticating the user to the enterprise IdM system.
- The IdM system of the NGN must manage the user identity and credentials.
- The enterprise IdM system must manage the server identity and credentials.

NOTE – a) No new capability is required of 3G networks (which thus may serve as an example); b) The requirements here apply specifically to the support of the above use case.

II.8 Support of converged services (e.g., fixed and mobile access) within a service provider network

II.8.1 Overview

A promise of next generation networks is the support for a myriad of converged services over fixed and mobile access networks. A user, thus, would have the flexibility to invoke a service using an access device and network of convenience at a particular moment. (In return, the service provider would expand its customer base and increase its revenue.) Since the underlying security mechanisms suitable for fixed and mobile environments are typically different, an important enabler would be a converged IdM system that can address the differences. The converged IdM would manage the identities and credentials of end users and network servers regardless of access technology.

II.8.2 Use case description

This scenario describes access by a subscriber of a 3G network to a resource (e.g., a video-on-demand server) located in a fixed network with the use of her or his handset. In this scenario, the 3G network and a resource in a fixed network support different IdM-related mechanisms. The following entities are involved in an example illustrating the scenario:

- The IdM system of the 3G network. This system is modified in such a way that it is capable, in addition to supporting mutual AKA-based authentication of the user's handset, to provide it with the credentials for authentication to the video-on-demand (VoD) server.
- The VoD server located in the fixed network.
- The user's 3G handset.
- These entities perform the following interactions:
  - The user's handset and the mobile network authenticate each over using the AKA method.
  - The user, using a handset, sends a request to the VoD server.
  - The VoD server replies with an authentication request to the user.
  - The user obtains authentication credentials (e.g., a Kerberos ticket) from the IdM system of the 3G network, which generates such credentials based on the results of the AKA authentication.
  - The user responds to the VoD server with the authentication credentials (a ticket).
  - The VoD server authenticates the user and responds with confirmation for the requested service.

II.8.3 Implied requirements

- The IdM system of the 3G network must support the AKA authentication mechanism and the authentication mechanism (e.g., Kerberos) used by the VoD server.
- The IdM system must be capable of issuing authentication credentials (e.g., ticket) to the user device for authenticating the user to the VoD server.
- The IdM system of the 3G network must manage the user identity and credentials.
- The IdM system of the 3G network must manage the VoD server's identity and credentials.

NOTE – The requirements here apply specifically to the support of the presented use case.

II.9 Example use case – User authentication and authorization of NGN provider (mutual authentication and authorization)

Figure II.8 illustrates an example use case involving the user authentication of an NGN provider. This example assumes an open service environment where NGN providers are capable of advertising services to the user. This use case example illustrates gaps or lack of capabilities for the user to authenticate and authorize NGN providers (or mutual authentication) in an open service and multi-provider environment.

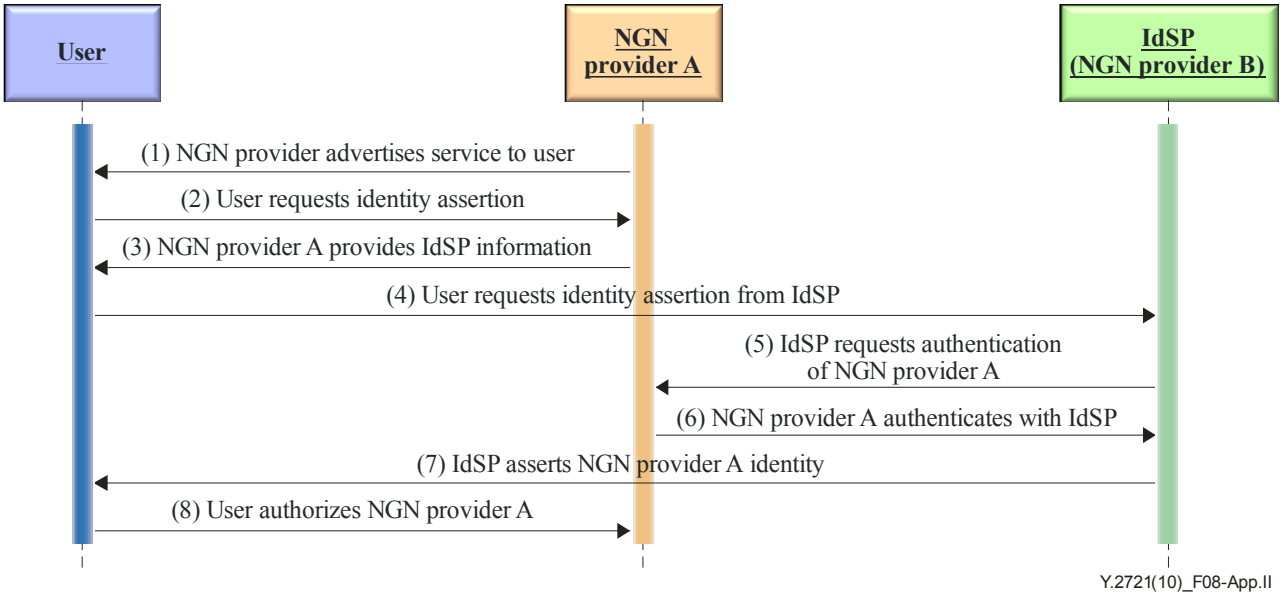


Figure II.8 – Example use case: User authentication and authorization of NGN provider

The example call flows are summarized as follows:

1) NGN provider A advertises services to the user.
2) The user requests assertion of NGN provider A identity.
3) NGN provider A provides the user with the address of an IdSP.
4) The user sends requests to the IdSP for assertion of NGN provider A Identity.
5) The IdSP sends requests to NGN provider A to authenticate.
6) NGN provider A provides authentication information.
7) The IdSP sends information to the user asserting identity of NGN provider A.
8) The user authorizes NGN provider A to provide services.

NOTE – This example does not show the flows related to the NGN provider authentication and authorization of the user.

II.10 Example use case – Peer user assertion (non-cash transactions)

Currently, there is a lack of NGN IdM capabilities allowing users to authenticate communication origination or data sources. In general, the IdM approaches that are being specified are focused mainly on IdM for cash transactions and electronic commerce. The NGN would need to support IdM capabilities for a broader range of transactions and communications. This is especially important for certain emergency services that would have to be supported by NGN. Figure II.9 shows an example use case illustrating the need for NGN IdM capabilities to allow users to assert the identity of each other for peer communications and non-cash transactions. For example, a user may need to authenticate the source of a received message (e.g., email or instant message), the request for communication (e.g., voice or video or data communication) or received data. Currently, there is a lack of NGN specification to support such IdM capabilities.

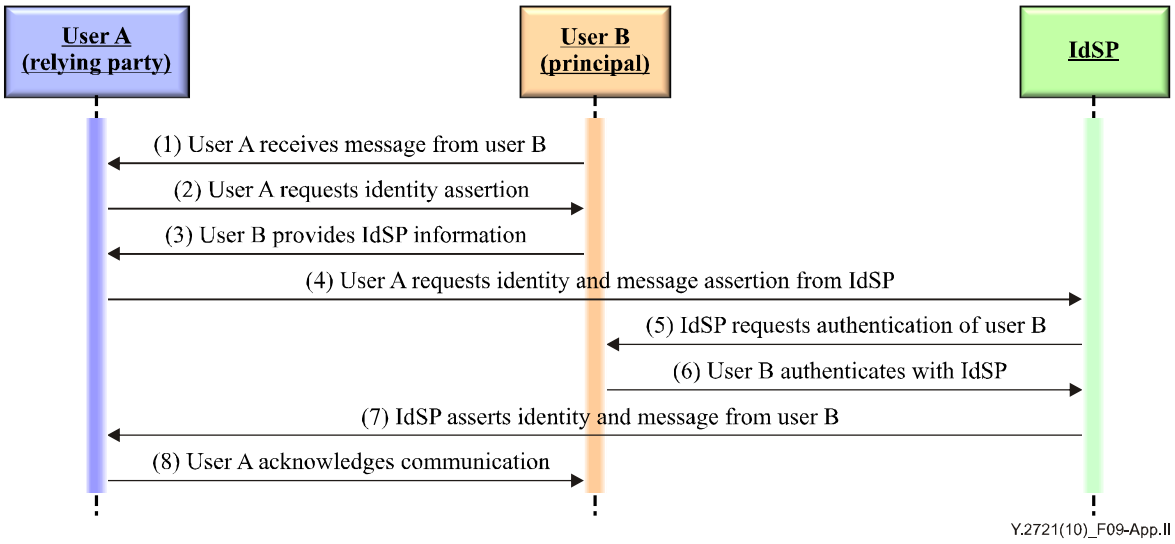


Figure II.9 – Example use case: Peer user assertion (non-cash transactions)

The example use case illustrated in Figure II.9 assumes that user A receives a message or request for communication from user B and would like to assert the identity of user B and the received data. The example call flows are summarized as follows:

1) User A receives message or communication request from user B.
2) User A requests assertion of user B identity and authentication of information received from user B.
3) User B provides user A with address information of identity provider (IdSP).
4) User A sends requests to IdSP to assert the identity of user B and authenticate the received information.
5) IdSP sends the request to user B for authentication.
6) User B responds and is authenticated by IdSP.
7) IdSP sends the response to user A asserting the identity of user B and the received information.
8) User A acknowledges communication to user B.

II.11 IdM use case – Assurance of end user device identity and integrity

NGNs will be supporting a variety of user devices (e.g., fixed telephones, wireless handsets, personal computers, PDA, IPTV set top boxes). The hardware and software components of the devices attaching to the NGN ranges from simple to complex, and, if stolen and compromised, can be used to orchestrate a variety of attacks.

Special security capabilities could be designed and implemented as part of tamper-resistant hardware component in end user devices to hold identity management data in encrypted form and support specialized security capabilities to validate the identity and integrity of the end user devices. This clause describes example use cases where specialized security hardware component could be designed and implemented as part of end user devices and used to support identity management services to:

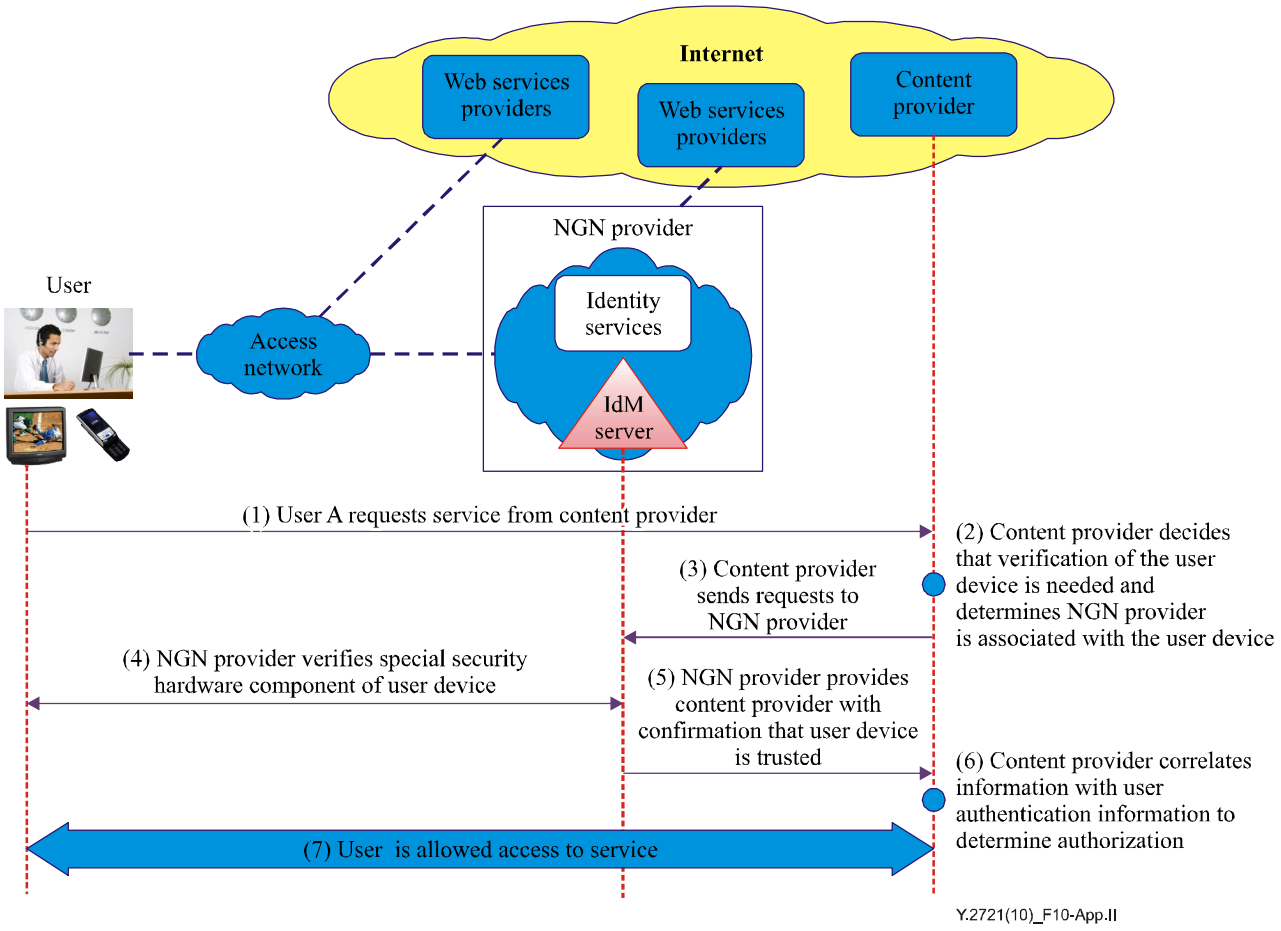
1) Assure the identity of an end user device.
2) Assure the integrity of an end user device (i.e., verify that the configured software and hardware have not been compromised).
3) Allow users to encrypt and protect PII and other sensitive data on end user devices.

II.11.1 Example use case – Assurance of user and device authentication

This use case involves the support of specialized tamper-resistant hardware component in end user devices to provide unique identification of the device. For example, passwords, digital keys, and certificates can be stored in specialized tamper-resistant hardware component of the device to provide unique identification of the device. The specialized hardware component could support standardized application programming interfaces (API) to allow support of security application services relying on the specialized hardware component as a trust anchor for the end user device.

The unique identification and authentication of the tamper-resistant hardware component could be correlated with identification and authentication of the user to provide a higher degree of assurance for access control in a multi-service provider environment.

Figure II.10 illustrates an example use case where specialized tamper-resistant hardware component is designed and implemented in end user devices to provide unique identification of the device. In this example, it is assumed that specialized tamper-resistant hardware component is controlled by the NGN provider through contractual agreement with the subscriber. Subject to qualified user consent, the NGN/IdSP provider could provide identity services to other providers (e.g., content providers, web services providers, and 3rd party providers) and partners assuring the identity and authentication of the end user device. This would allow service providers to have confidence in the identity and authentication of the end user device. The information about the user device identity and authentication can be correlated with the user authentication for a higher degree of assurance and confidence.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure II.10 – Correlation of user and device authentication for assurance

The following is a summary of the call flows:

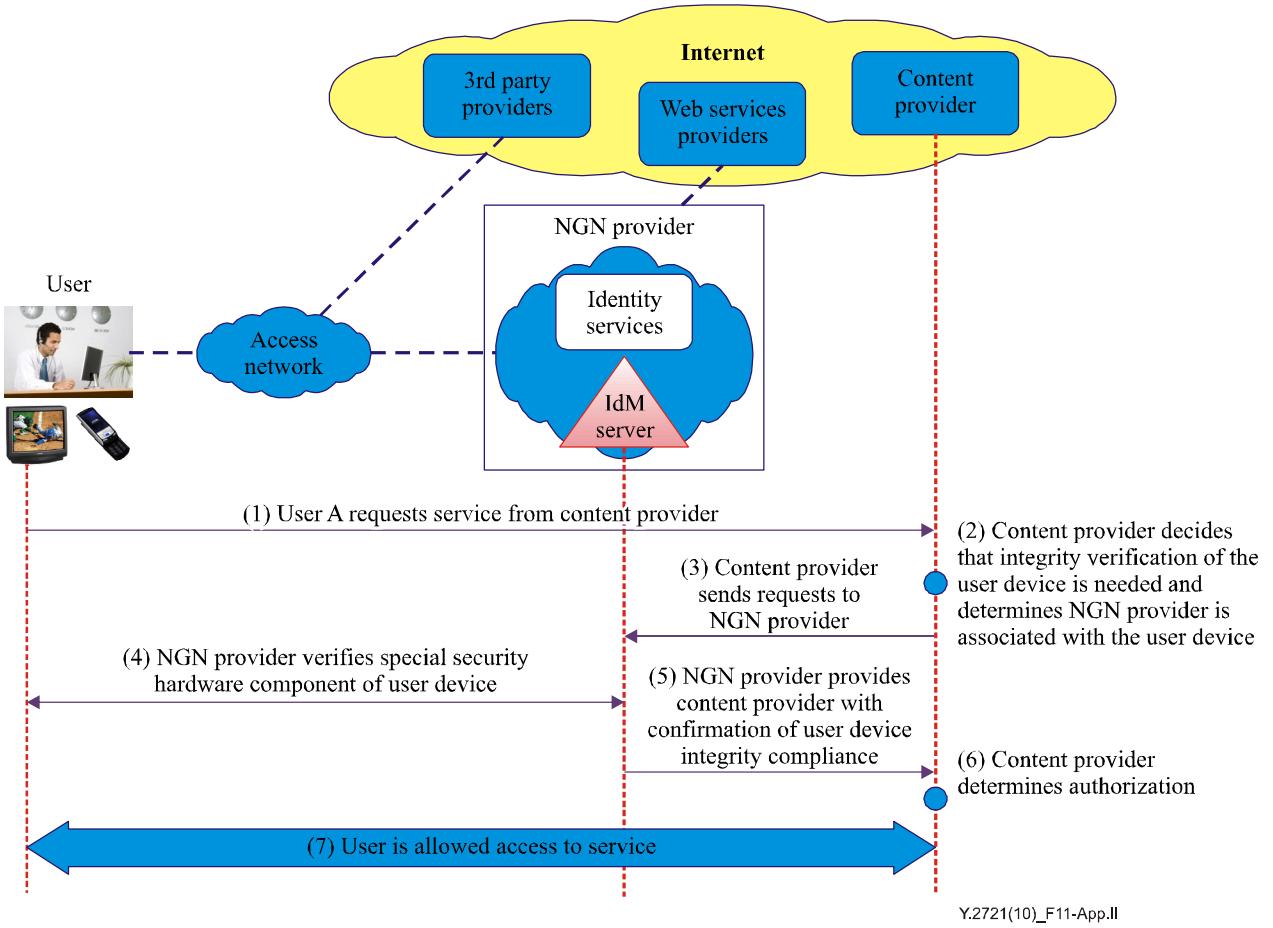
1) The user requests service from a content provider.
2) The content provider decides that verification of the user device is needed to allow access to the service, and determines that the NGN provider is associated with the user's device.
3) The content provider sends requests to the NGN provider to assert the user device identity and authentication.
4) The NGN provider identifies and authenticates special security hardware component of the user device (e.g., by verifying certificates stored in tamperproof security hardware component of device).
5) The NGN provider sends a response to the content provider validating the user device identity and authentication.
6) The content provider correlates the information from the NGN provider with user authentication information and determines authorization to the service.
7) The user is allowed access to the service (e.g., content).

II.11.2 Example use case – Assurance of user device integrity

In today's security environment, subscribers attach to the network using different devices (e.g., fixed telephones, wireless handsets, personal computers, PDA, IPTV set top boxes). The integrity of end user devices (e.g., the configured software and hardware) could be easily compromised unknowingly to the user/subscriber. Popular Internet applications, such as web browsers and email, and other applications that execute on subscriber devices to allow subscribers to interact with services and local device features, could potentially compromise integrity of the device by introducing vulnerabilities. For example, these applications may have inherent security flaws or support features, such as file downloads, software applets, browser plug-ins and embedded links, which can be exploited. Software and file downloads, particularly from an untrusted source, make subscriber devices vulnerable to malicious code, worms, viruses, and Trojan horses. Keyloggers (which record all key entries, including user names and passwords, and then relay the information to an attacker who can use it to gain unauthorized access) are a popular type of malicious code. Other types of malicious code include spyware (programs that track subscriber activity), and adware (programs that push unwanted advertisements, often based upon information collected by monitoring a subscriber). Some of these programs literally hijack subscriber devices and obfuscate their presence by embedding themselves deep in the operating system.

This use case involves the support of specialized tamper-resistant hardware component in end user devices to provide integrity checks and provide confirmation of the device integrity to applications and services. For example, the specialized tamper-resistant hardware component could contain vendor-specific algorithms and functions to check for integrity compromises. The special hardware component could include a reference model with a set of known-good integrity metrics, specifically to identify the correct code and provide reference values for the device. The known-good integrity metrics would be used to compare actual reported values to the configuration and determine if the unit is within compliance.

Figure II.11 illustrates an example use case where specialized tamper-resistant hardware component is designed and implemented in an end user device to provide integrity verification of the device. In this example, it is assumed that specialized tamper-resistant hardware component is controlled by the NGN provider through contractual agreement with the subscriber. Subject to qualified user consent, the NGN/IdSP could provide identity services to other providers (e.g., content providers, web services providers, and 3rd party providers) and partners validating the integrity and compliance of the end user device.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure II.11 – Assurance of device integrity

The following is a summary of the example call flows:

1) The user requests the service from the content provider.

2) The content provider determines that verification of the user device integrity is needed and determines the NGN provider associated with the user device.

3) The content provider sends requests to the NGN provider for user device integrity confirmation.

4) The NGN provider interacts with the special security hardware component of the user device to verify integrity compliance.

5) The NGN provider provides the content provider with the confirmation of user device integrity.

6) The content provider determines authorization.

7) The user is allowed access to the service (e.g., content).

II.11.3 Example use case – Encryption of PII and sensitive files/data

Loss or theft of a device with PII and other sensitive data could mean serious consequences to individuals, business and government enterprises. The specialized hardware component designed to uniquely indentify and confirm integrity of trusted devices could also support capabilities to encrypt and protect PII and other sensitive data on end user devices. With encrypted confidential data, unauthorized parties cannot access the data on computers, cell phones or storage devices, thus avoiding extensive corrective action as well as cost.

Appendix III

Emergency telecommunications service (ETS) related IdM use cases

(This appendix does not form an integral part of this Recommendation)

III.1 Introduction

This appendix provides example ETS related IdM use cases. ETS is a service that requires priority treatment. See clause 8.4.7.

III.2 Authentication assurance using device and user combination

Authentication of authorized users of ETS is necessary to protect the availability and integrity of ETS, and associated networks. Two basic authentication methods that are currently used for legacy ETS applications are:

1) A PIN-based method; and

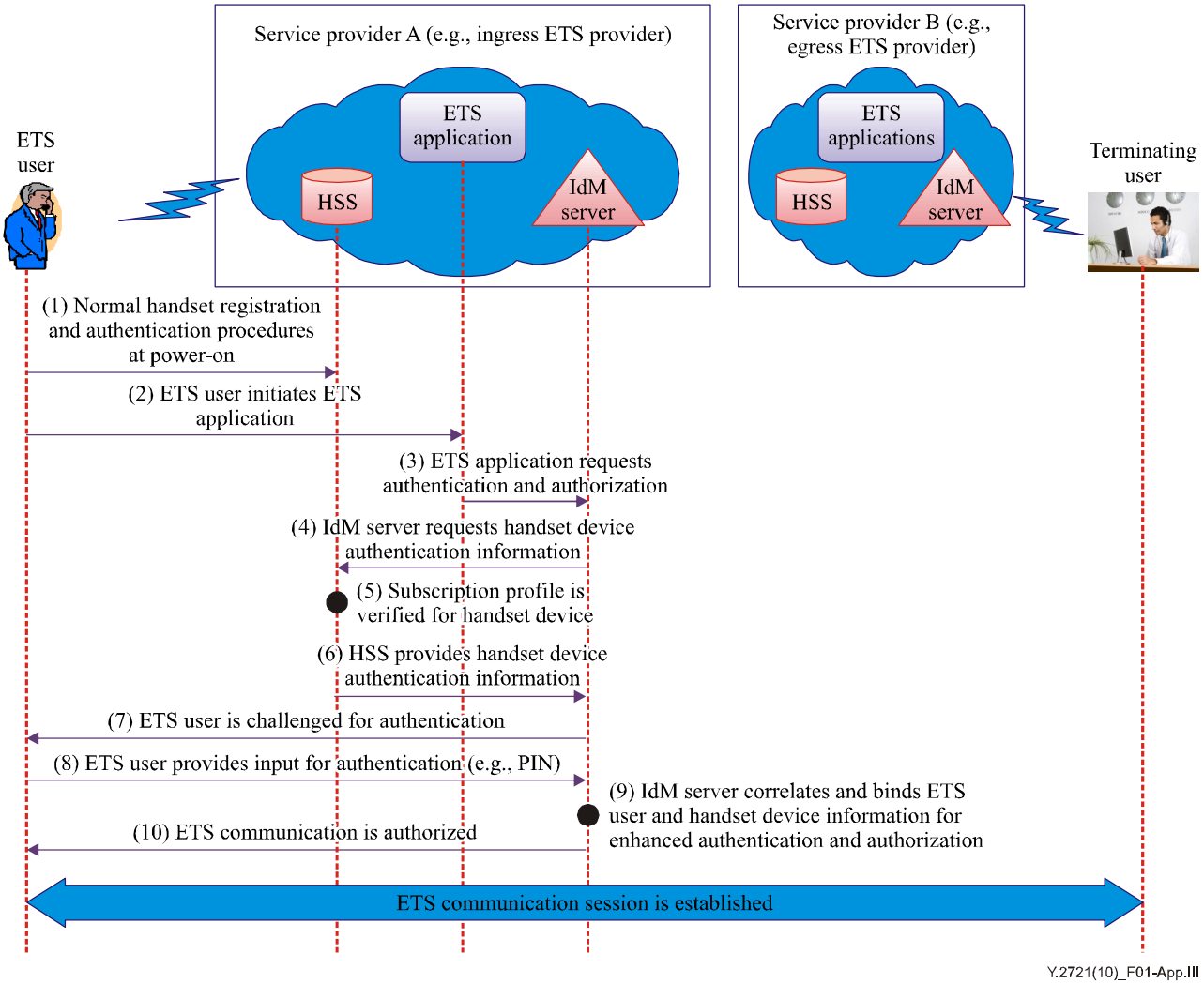
2) A subscription-based method.

The first method involves the use of a personal identification number (PIN) for authentication and authorization. Validation of the PIN authenticates the user, thus authorizing the user for ETS. This approach identifies the user and not the user device. Therefore, it is normally used in cases where the user is allowed to invoke ETS from any device.

The second method involves authentication and authorization based on the subscription profile information associated with a particular terminal or end user device. The user device or terminal identity is authenticated as part of the NGN provider (i.e., ETS provider) normal registration and authentication, and individual ETS calls/sessions are authorized by checking the service subscription profile (i.e., verifying whether the service subscription allows ETS calls/session from the device). This approach authenticates the user's device (i.e., wireless handset) and not the user.

The use of the simple PIN-based and subscription-based methods is adequate for legacy ETS applications. However, the simple PIN-based and subscription-based methods are not adequate for all types of ETS applications in the NGN environment. Specifically, applications such as multimedia priority services (e.g., data and video services) would require a higher degree of assurance or confidence of the ETS user's identity and of the level of authorization to access the ETS application and its associated resource. Therefore, in addition to supporting the existing PIN-based and subscription-based authentication methods, the NGN would also need to support enhanced mechanisms to authenticate and authorize ETS users and devices.

An approach to consider in the transitioning of ETS (i.e., priority voice services) to the NGN environment is the use of IdM to correlate and bind authentication of the user and the identification and authentication of the user device. This will provide enhanced assurance (i.e., confidence) of the identity and authorization of the user for access to ETS. The concept is described in the following general use case example.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.1 – Combined user and device authentication

Figure III.1 shows a use case example where IdM functions are used to combine user and device authentication for enhanced assurance of authorization of ETS users.

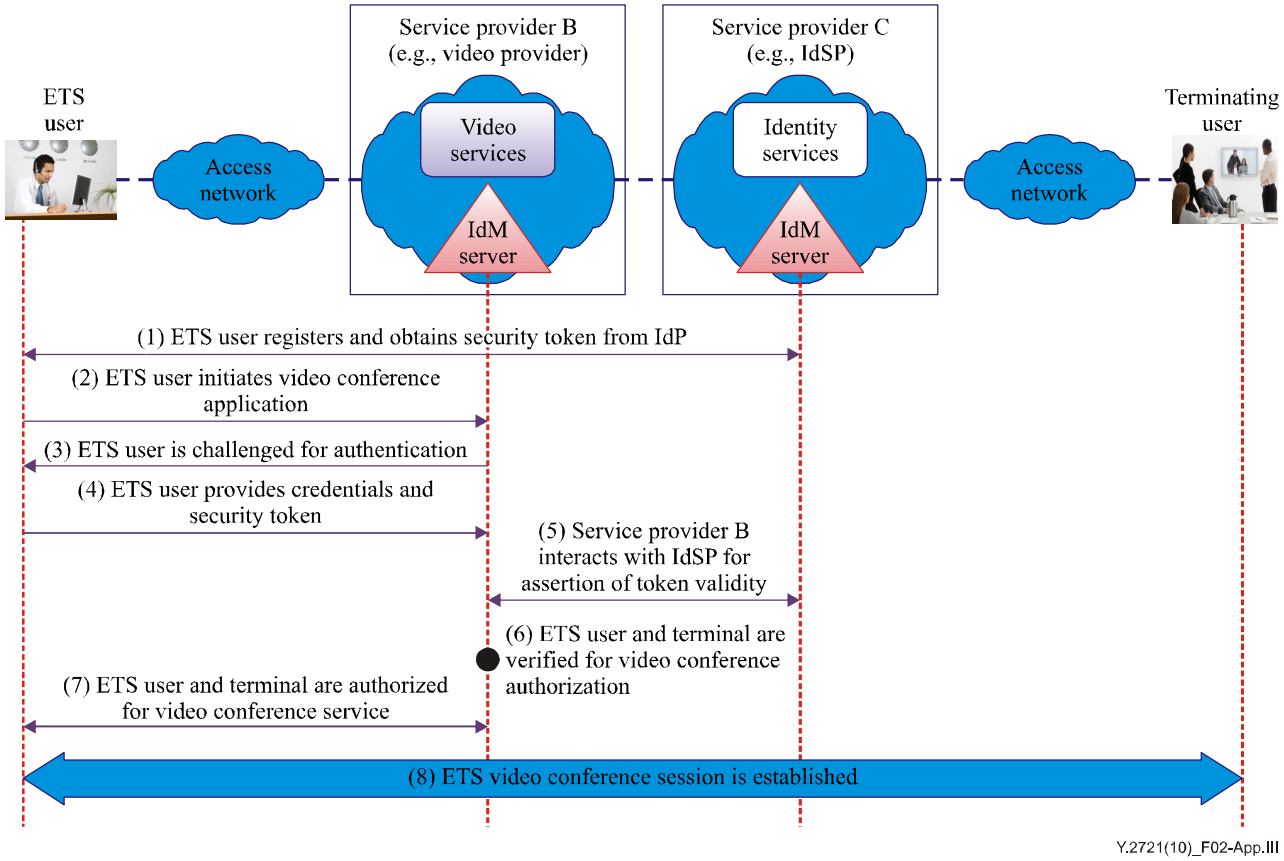
The example call flows are summarized as follows:

1) The user handset device is registered and authenticated using the normal procedures upon power-on.
2) The ETS user initiates an ETS application.
3) The ETS application requests authentication and authorization from the IdM server.
4) The IdM server requests handset device authentication information from the HSS.
5) The HSS verifies subscription profile of handset.
6) The HSS provides IdM server handset device authentication information.
7) The ETS user is challenged for authentication.
8) The ETS user provides input for authentication (e.g., PIN).
9) The IdM server correlates and binds ETS user and handset device information for enhanced authentication and authorization.
10) The ETS communication session is authorized.

The result of this example flow is enhanced assurance of the identity of the ETS user and authorization to use the service. Combining authentication of the device with the user would require additional interactions with the ETS user for authentication and might be viewed as burdensome. However, this may not be needed for all ETS sessions. It could be considered for ETS sessions requiring higher levels of assurance.

III.3 Enhanced authentication of ETS users for next generation priority services (priority multimedia services)

As the communications environment transitions to an NGN/IMS environment, ETS users will need to keep up with the technology changes and new trends in communications. For instance, ETS users are increasingly becoming dependent on communications beyond voice communications such as instant messaging, text messaging, and emails to carry out their mission. In general, there are initiatives in the planning and development stages to allow ETS users to obtain priority access to multimedia services such as voice, data, and video services. However, the PIN-based and subscription-based mechanisms used for ETS in the PSTN environment will not be adequate for multimedia services in the NGN/IMS environment. Specifically, applications such as multimedia priority services (e.g., data and video services) would require a higher degree of assurance or confidence of the ETS user's identity and of the level of authorization to access the ETS application and its associated resource because of the higher level of security risks and threats of the NGN environment in general. Also, unlike existing ETS supported in the PSTN, it is expected that next generation multimedia priority services may only be authorized to a selected population of ETS users. In addition, given the general objective for ETS users to have easy and user friendly access from anywhere, anytime, and from any device, it is important that more advanced IdM mechanisms be considered and leveraged as appropriate. High assurance of ETS user identity will be critical to protect the integrity and availability of the ETS multimedia services and resources and the overall NGN/IMS infrastructure as a whole during disasters and emergencies. Multimedia data and video applications (e.g., web information or video clips downloads) are bandwidth and resource intensive compared to voice applications. Without adequate controls, unauthorized access to ETS data and video applications could potentially have negative impacts on ETS applications themselves and the entire communications infrastructure in general. For example, unauthorized access to resource intensive ETS application could potentially be used to cause network congestions or carry out denial of service attacks. Therefore, more sophisticated approaches using special security tokens, digital certificates, voice recognition or biometric capabilities to authenticate and authorize ETS users and/or terminals should be considered.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.2 – Enhanced authentication for next generation priority services

Figure III.2 illustrates an example use case involving enhanced authentication of authorized users for next generation multimedia priority services (e.g., video conferencing). This use case assumes that the identity credential (i.e., security token or digital certificate) is provided by an IdSP that is different from the provider of the multimedia service (although it is possible that the service provider and IdSP could be the same). If the IdSP and the service provider are different, it would require prior establishment of the necessary business and trust arrangements. It would also require mutual authentication between the IdSP and the service provider.

The following is a summary of the call flows:

1) The ETS user registers and obtains credential (i.e., security token or digital certificate) identifying the ETS user and privileges for multimedia services.

2) The ETS user initiates video conference application.

3) The ETS user is challenged for authentication.

4) The ETS user provides credentials (e.g., security token or digital certificate) for authentication.

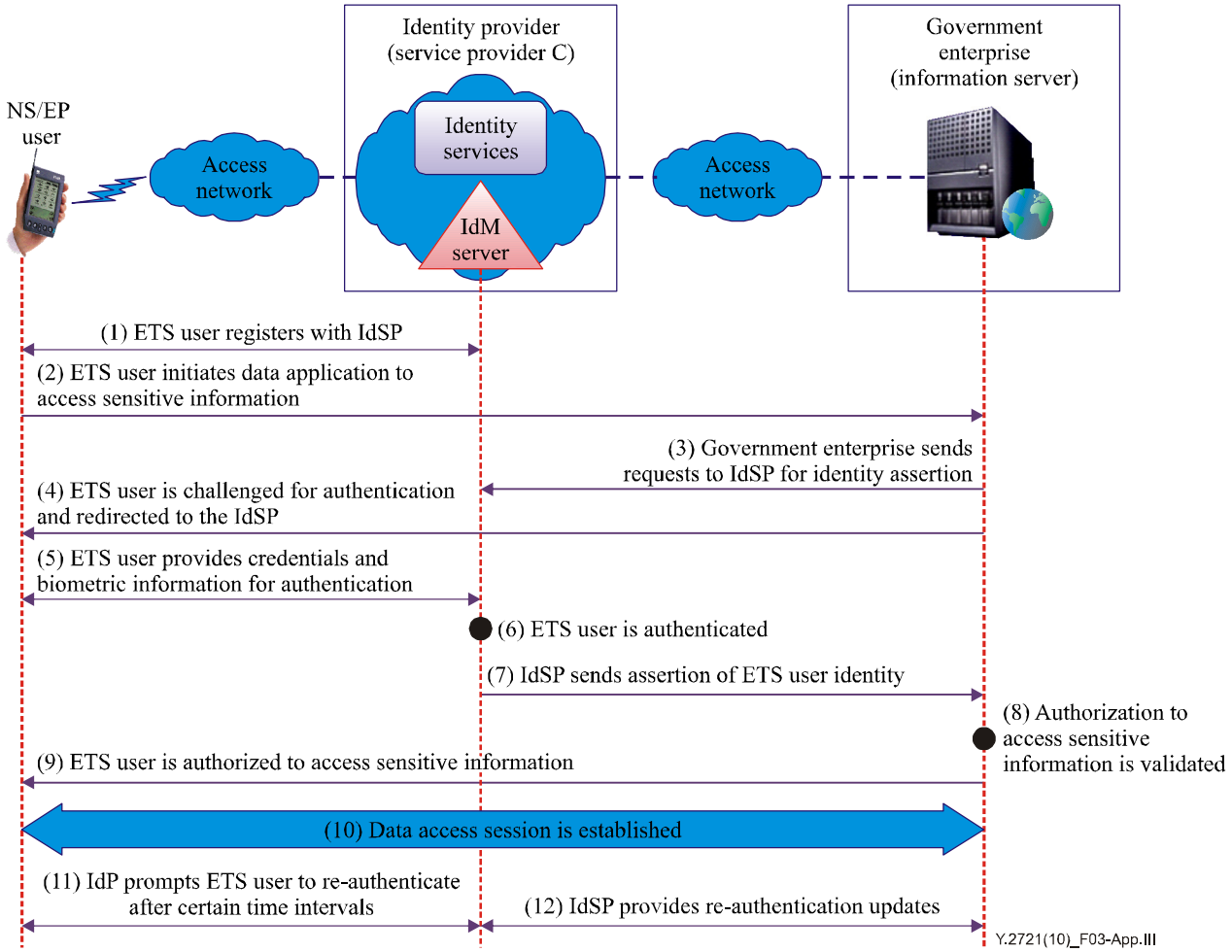
5) Service provider B interacts with identity service provider (IdSP) requesting validation of the credentials (e.g., security token or digital certificate).

6) Service provider B processes and verifies information to determine whether the ETS user and the terminal are authorized for multimedia priority services.

7) The ETS user is authorized to initiate multimedia priority service (e.g., video conference) after successful authentication.

8) Multimedia session is set up and established.

It is possible that certain next generation multimedia communications may require the use of biometric information to authenticate authorized ETS users. For example, the sensitive nature of certain information may require that it only be shared among a subset of authorized ETS users. In such a scenario, a high degree of confidence in the validation of the ETS user identity is critical. In these cases, biometric mechanisms may be considered as candidate validation technologies.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.3 – Biometric use case example

Figure III.3 shows an example use case involving biometrics. In this example, it is assumed that the user handset is equipped with the appropriate capability to read biometric information. It is also assumed that the ETS user pre-registers with the IdSP and the necessary biometric information is obtained and stored. Note that it is also possible for the government enterprise to host and provide the identity services (e.g., registering and keeping ETS user identity and biometric information) as opposed to using third-party service provider services. The following is a summary of the call flows:

1) The ETS registers with the IdSP to activate biometric authentication service. It is assumed that the necessary process to collect and prove the biometric and other identity information has already occurred (e.g., in-person registration).

2) The ETS user initiates communication for remote access to a government enterprise database hosting sensitive information.

3) The government enterprise security policy indicates that a high level of assurance is needed to allow access, and initiates a redirection procedure to the IdSP.

4) The ETS user is challenged for authentication and redirected to the IdSP.

5) The ETS user provides input for authentication. For example, the ETS user scans his or her thumb on a special biometric chip scanner integrated in the wireless handset.

6) The IdSP uses the input information to authenticate the ETS user.

7) The IdSP sends the information to the government enterprise asserting the identity of the ETS user.

8) The government enterprise verifies whether ETS identity is authorized for access to information server hosting the sensitive data.

9) ETS is authorized for access.

10) Data access session is established.

11) The IdSP prompts the ETS user to re-authenticate after specific time-interval as a result of the security policy for access to the government enterprise information server.

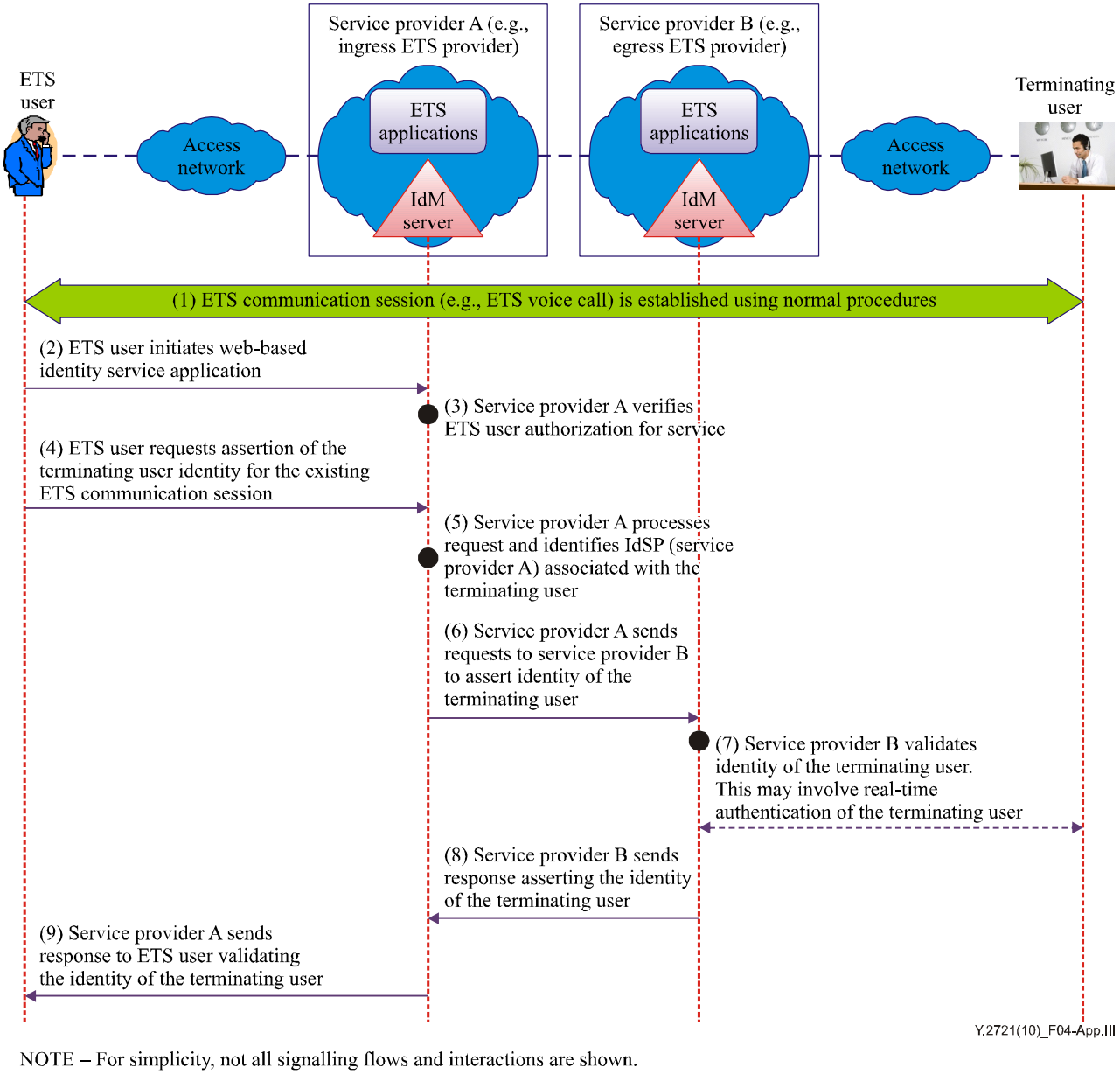
12) The IdSP provides information about ETS user re-authentication to the government enterprise.

III.4 Authentication of called party and data communication sources

Currently there are no specific mechanisms as part of ETS application themselves to authenticate the called party of the communication session (i.e., the terminating side of the ETS call). In the closed PSTN environment, this was not much of an issue. However, the transition to NGN/IMS environment with IP transport allows for the possibility of forging of called party number and routing information resulting in masquerading threats.

In the future, it might be possible to leverage identity management services offered by communications service providers (CSPs) and third-party service providers to authenticate the called party or the terminating side of ETS communication sessions. Specifically, the ETS service provider could support IdM capabilities to provide identity services to authenticate users and assert user identities. Example identity information could be simple line and calling name verifications or use of stronger authentication mechanisms such as security tokens, smart cards, or digital certificates to assure the user's identity.

Figure III.4 illustrates a use case example involving assertion of the terminating user of an ETS communication session (e.g., an ETS voice call). Specifically, this use case assumes that the ETS user is pre-registered with the ETS service provider for web-based identity services. After establishing an ETS communication (e.g., ETS voice call) to a user in the public network, the ETS user initiates an identity service through a web portal to verify the identity of the terminating user on the other end of the ETS communication. In this use case example, the establishment of the ETS communications session is independent of the identity service that is used to assure the identity of the terminating user.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.4 – Assertion of terminating user identity

The following is a summary of the call flow and interactions:

1) The ETS user initiates an ETS communication session (e.g., ETS voice call). The ETS communication session is established using the normal procedures.

2) The ETS user initiates web-based identity service (e.g., via a web portal of service provider A, the ingress ETS provider) to validate the user on the terminating end of the established ETS communication session.

3) Service provider A verifies the ETS user authorization for the service.

4) The ETS user requests validation of the identity of the user on the terminating end of the established communication session.

5) Service provider A processes the request and determines the IdSP associated with the terminating user (i.e., the egress ETS provider).

6) Service provider A sends a request to service provider B to assert the identity of the terminating user.

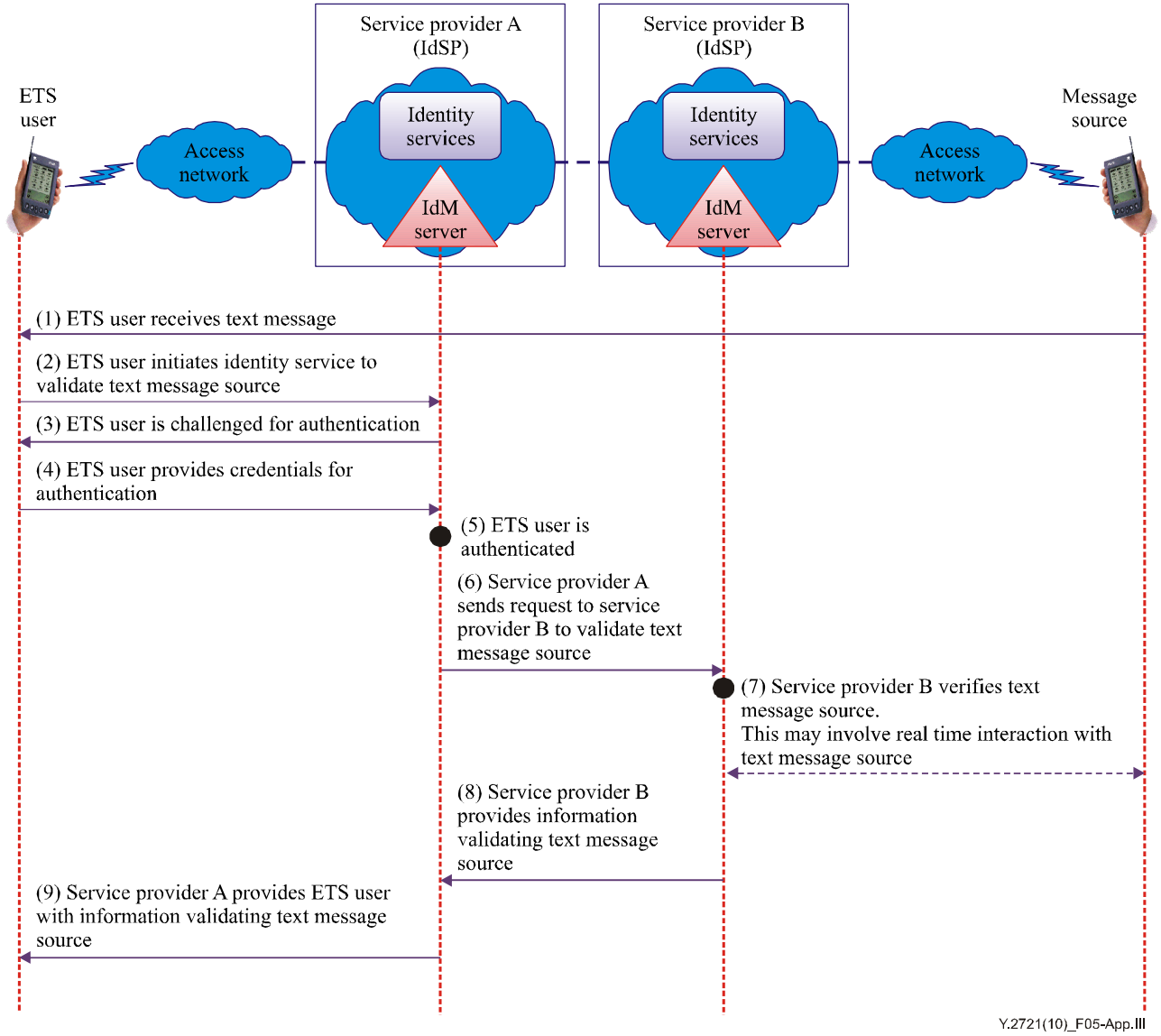
7) Service provider B validates the identity of the terminating user. This may involve real-time authentication of the terminating user.

8) Service provider B sends a response asserting the terminating user identity.

9) Service provider A sends a response to the ETS user (e.g., visual web display) validating the identity of the terminating user of the ETS communication session.

ETS users are also increasingly dependent on the use of data services such as emails, instant messaging, and text messaging. In certain situations, it may be necessary to authenticate or validate the sources of such data services. Given the abundance of junk and spam mails, the ability to distinguish and validate authentic messages during certain disaster events will be critical for ETS users.

Figure III.5 illustrates an example use case asserting the source of a text message. In this example, it is assumed that the ETS user receives a text message originated from a source that may or may not be another ETS user. To obtain assurance of the text message source, the identity services of a service provider are used. The identity service to assert the text message source may or may not be part of the text message service itself.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.5 – Assertion of text message source

The following is a summary of the interactions:

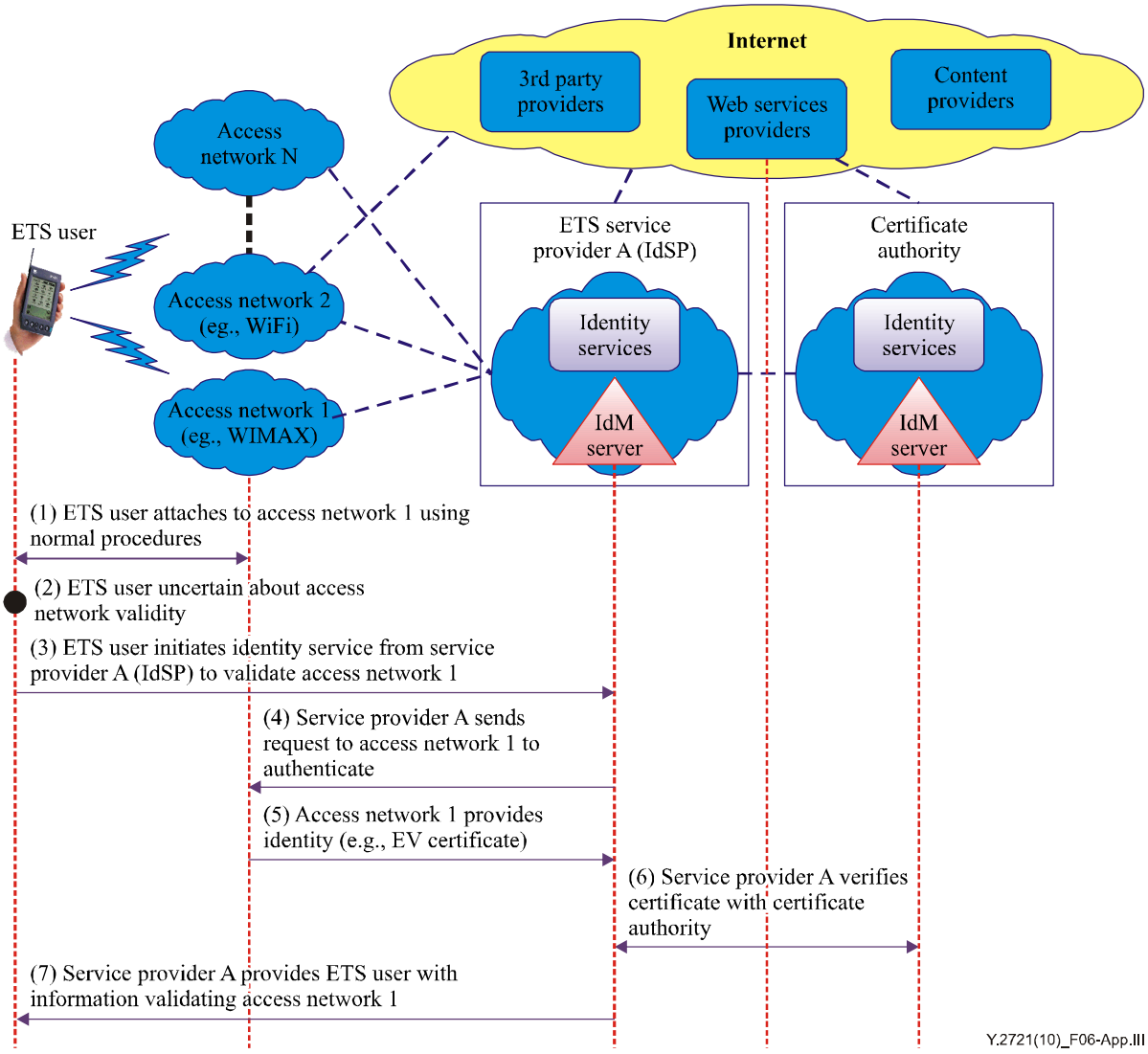
1) The ETS user receives a text message.
2) The ETS user wants to verify the authenticity of the text message source and initiates identity services from service provider A.
3) The ETS user is challenged for authentication.
4) The ETS user provides credentials for authentication.
5) Service provider A authenticates ETS user and verifies authorization for identity service.
6) Service provider A sends requests to service provider B to assert text message source.
7) Service provider B processes requests and verifies text message source. This may involve interaction with the text message source.
8) Service provider B sends a response to service provider A asserting the identity of the text message source.
9) Service provider A sends the ETS user information validating the text message source.

III.5 Trusted identification and authentication of service providers in a multi-provider environment

Today's communication infrastructure has evolved into a multi-provider environment that includes multiple fixed and mobile access providers using different technologies (e.g., xDSL, cable, FTTX, WiFi, WiMAX, EV-DO, LTE), communications service providers using "managed core IP networks", web services providers, content providers, and 3rd party providers. In this multi-provider environment, the identity of the service provider can no longer be implicitly trusted, as it was in the closed PSTN environment.

In the open multi-provider environment, there is a lack of capabilities to provide trusted identification, authentication, and authorization of service providers, which can result in the possibility of illegitimate entities masquerading, forging, or misrepresenting legitimate service providers. Therefore, IdM capabilities to identify and validate service providers are critical to infrastructure protection. When the service providers are supporting ETS services, such capabilities are critical to national security.

Figure III.6 shows an ETS use case example where the ETS user is attempting to obtain network access in a multi-provider environment. Specifically, the ETS user is roaming and the mobile handset device could potentially attach to one of a set of access network providers offering services in the area (not all the service providers may be authorized ETS service providers). In this use case example, it is assumed that the ETS user attaches to access network 1 as the first choice. After attaching to access network 1, the ETS user would like to validate the network before conducting any sensitive ETS communications. There are multiple options and variations for consideration to validate the access network provider, including direct authentication by the ETS user. This example assumes that the ETS user uses the identity services of ETS service provider A to validate the access network. In this example, the ETS user trusts service provider A and will accept the validation information service provider A sends about access network 1.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.6 – Validation of access service provider

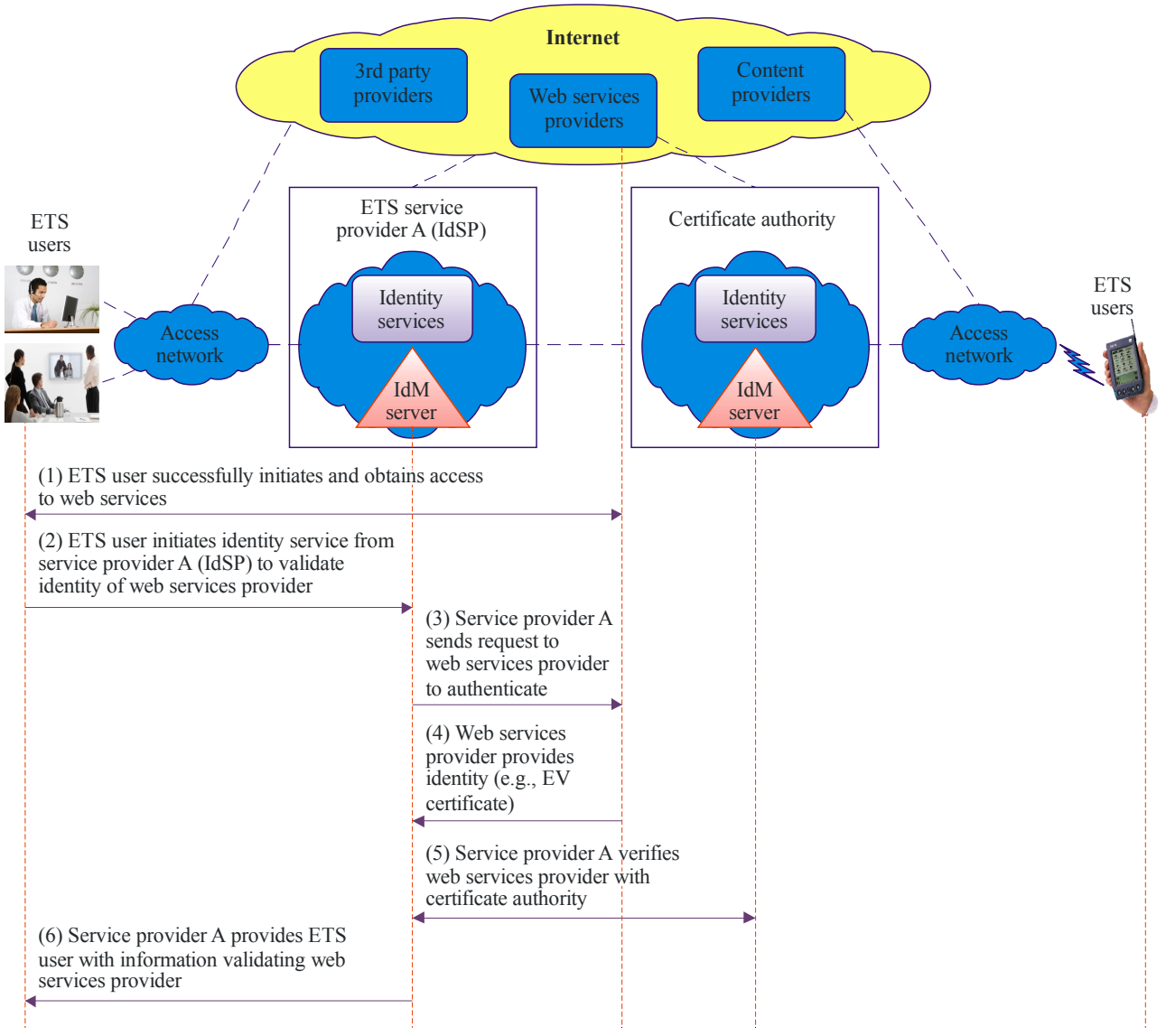
The following is a summary of the interactions:

1) The ETS user is roaming with a mobile handset device that is capable of attaching to multiple access network types (e.g., WiFi, WIMAX, LTE or EV-DO). The ETS user mobile handset device attaches to network 1 (i.e., first choice based on factors such as known ETS providers and signal strength).
2) The ETS user would like to validate network 1 before authorizing services.
3) The ETS user initiates identity services from ETS service provider A to validate access network 1.
4) Service provider A sends authentication requests to access network 1.
5) Access network 1 provides identity information for authentication (e.g., extended validation ITU-T X.509 certificate).
6) ETS service provider A verifies network 1 certificate with the certificate authority.
7) ETS service provider A providers ETS user with information validating access network 1.

This allows the ETS user to proceed with confidence that his mobile handset device is attached to an authorized access network.

After obtaining network access, the ETS user could potentially use the services of several service providers in the multi-provider infrastructure. For example, it is possible that the ETS user may need to use the services of web services providers (e.g., earth and other map/data providers) or content providers (e.g., service providers offering real-time streaming of monitoring camera or weather reports or video). It is possible that the ETS user may access the services of web services and content providers directly through Internet access or indirectly through the services of NGN providers. In any of these cases, the ETS user may need to validate the provider of a specific service.

Figure III.7 illustrates a use case example, where the ETS user needs to validate the identity of a web services provider. As in the use case above, there are many options and variations for consideration to validate the web services provider, including direct authentication by the ETS user. This example assumes that the ETS user uses the identity services of ETS service provider A to validate the web services provider. As in the previous example, the ETS user trusts service provider A and will accept the validation information service provider A sends about the web services provider.



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.7 – Validation of web service or content provider

The following is a summary of the interactions:

1) The ETS user successfully initiates and accesses web services. However, the ETS user would like to validate the web services provider to have confidence in the data.
2) The ETS user initiates identity service of ETS provider A to validate the web services provider.
3) ETS service provider A sends requests to web services provider for authentication.
4) Web services provider provides information for authentication (e.g., EV[1] certificate).
5) ETS service provider A verifies the information with the certificate authority.
6) ETS service provider A provides the ETS user with information validating the identity of the web services provider.

Validation of the web services provider allows the ETS user to have confidence in the identity of the web services, which may boost his confidence in the information obtained from the web services.

III.6 Single sign-on and single sign-off

Users typically have to sign on to multiple systems hosting application services (e.g., VoIP, data, and video), necessitating an equivalent number of sign on dialogues, each of which may involve different usernames and authentication information. System administrators are faced with managing user accounts within each of these multiple systems in a coordinated manner in order to enforce security policy.

ETS users may need to leverage IdM capabilities such as "Single Sign-on/Sign-off". The premise of single sign-on is that an end user, device, or end user and device combination can sign on once (i.e., by providing credential input for authentication and authorization) to a service and thus be authenticated to one or more additional services in the same NGN domain, or in the case of federated services, across multiple NGN domains. The value of single sign-on is that the end user is not burdened with authentication for each service. The word "Sign-On" as used here means the same thing as "Register with", "Log-On", or "Log-In", where the end user or device "registers with", "logs-on" or "logs-in" to a service. Similarly, "Single Sign-off" provides a comprehensive "Sign-off" from multiple application services in a given session.

Potential benefits of single sign-on/sign-off capabilities to ETS users may include:

- Reduction in the time taken by users in sign-on operations to individual domains, including reducing the number of sign-on failures. Improved security through the reduced need for a user to handle and remember multiple sets of authentication information.
- Reduction in the time taken by system administrators in adding and removing users to the system or modifying their access rights.
- Improved security through the enhanced ability of system administrators to maintain the integrity of user account configuration, including the ability to inhibit or remove an individual user's access to all system resources in a coordinated and consistent manner.

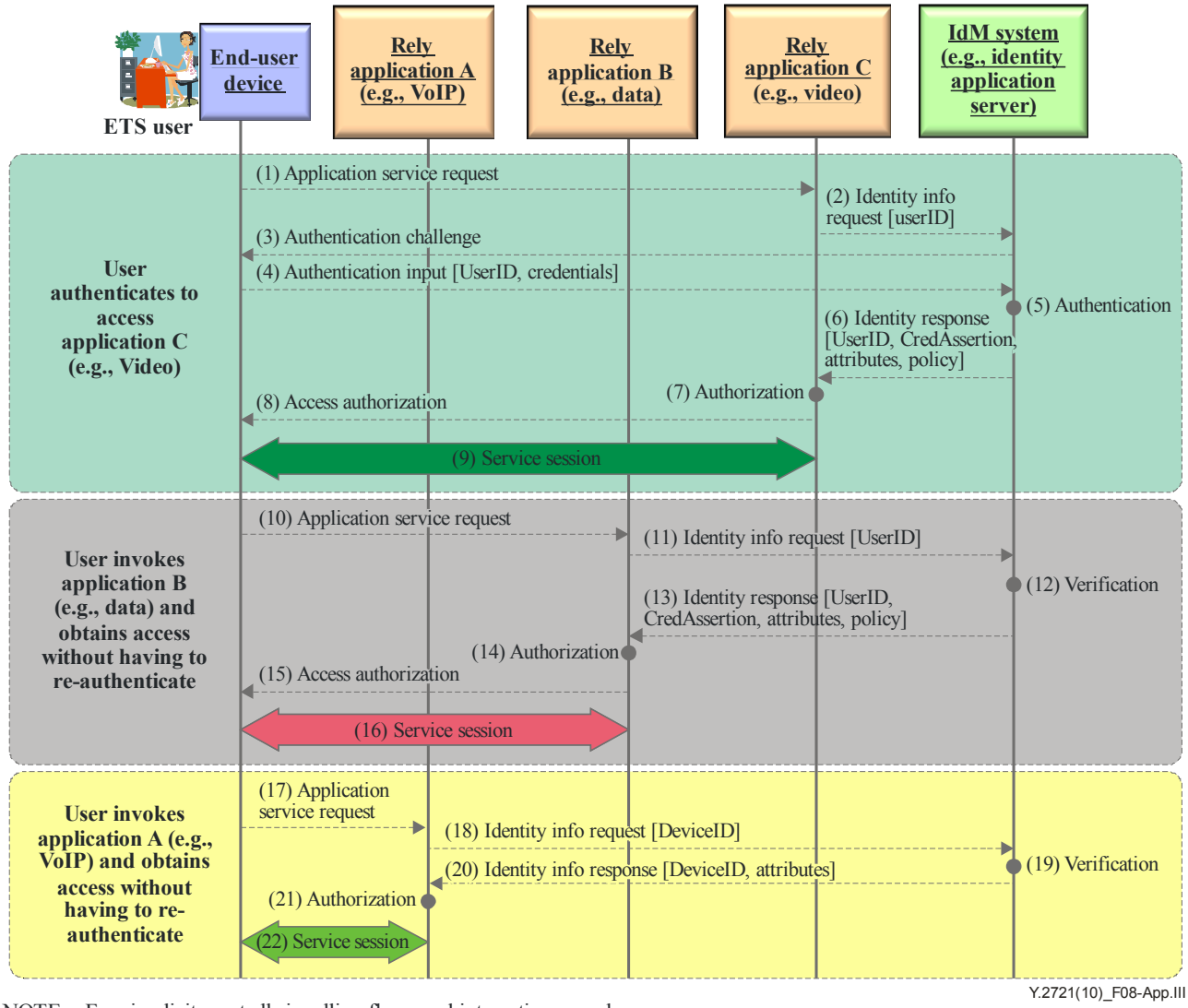
Figure III.8 illustrates a use case example involving the use of an IdM system to support "Single Sign-on/Sign-off" to multiple application services (e.g., VoIP, data, and video) within an NGN provider domain. The use case involves interactions between the following entities:

- End users (i.e., end user and/or end user device).
- Relying system (i.e., application service or network system).

---

[1] Extended validation certificates are a special type of ITU-T X.509 certificate which requires extensive investigation of the requesting entity by the certificate authority before being issued.

- IdM system (i.e., network system providing IdM services such as registration, authentication and authorization, subscription profile information).



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.8 – Single sign-on

This example assumes that the end user device registers and attaches to the NGN using the normal procedures.

The call flows are as follows:

1) Application service request: This information flow represents the ETS end user request to invoke application service C (video).

2) Identity information request [UserID]: Application service C (video) sends a request to the IdM system to assert the user identity and provide attributes associated with the UserID. This may include information such as service profile, privileges, preferences and policy information. For example, any policy or restrictions associated with the identity.

3) Authentication challenge: The IdM system challenges the user for authentication.

4) Authentication input [Credentials]: The user provides information for authentication (e.g., UserID and password or personal identification number).

5) Authentication: The IdM system performs authentication and obtains other needed information. This may involve obtaining information from other network systems (e.g., HSS or other subscription database).

6) Identity response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the UserID (e.g., privileges and preferences) and policy associated with the identity information (e.g., any restriction regarding use, display and dissemination).

7) Authorization: Application service C (video) processes the information and determines that the user is authorized for the service.

8) Access authorization: Application service C (video) provides the user with an indication that access to the service is granted.

9) Service session: The user's successful session with application service C (video) is established.

10) Application service request: The user requests invocation of application service B (data).

11) Identity information request [UserID]: Application service B (data) sends a request to the IdM system to assert the user's identity and provide attributes associated with the UserID. This may include information such as service profile, privileges, preferences, and policy information. For example, any policy or restrictions associated with the identity.

12) Verification: The IdM system processes the request, determines that single sign-on is applicable, and verifies that user authentication is still valid.

13) Identity information response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the UserID (e.g., privileges and preferences) and policy associated with the identity information (e.g., any restriction regarding use, display and dissemination).

14) Authorization: Application service B (data) processes the information and determines that the user is authorized for the service.

15) Access authorization: Application service B (data) provides the user with an indication that access to the service is granted.

16) Service session: The user session with application service B (data) is initiated successfully.

17) Application service request: The user requests invocation of application service A (VoIP).

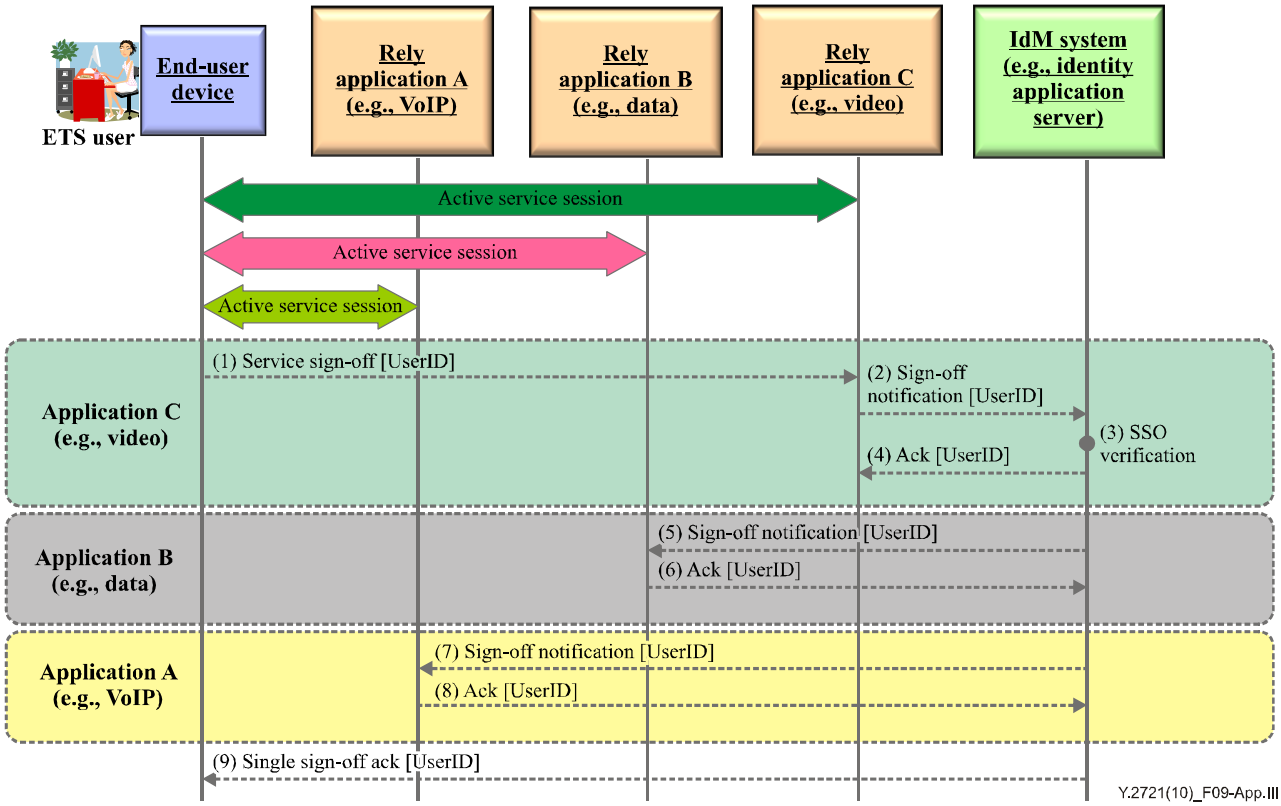
18) Identity information request [DeviceID]: Application service A (VoIP) sends a request to the IdM system to assert the user's identity and provide attributes associated with the DeviceID.

19) Verification: The IdM system processes the request, determines that single sign-on is applicable, and verifies that the user authentication is still valid.

20) Identity information response [Credential assertions, attributes, policy]: The IdM system provides information asserting the credentials. Other information that may be included are attributes associated with the DeviceID (e.g., privileges and preferences) and policy associated with the identity information (e.g., any restriction regarding use, display and dissemination).

21) Authorization: Application service A (VoIP) processes the information and determines that the user is authorized for the service.

22) Application service session: The user establishes a session with application service A (VoIP).



NOTE – For simplicity, not all signalling flows and interactions are shown.

Figure III.9 – Single sign-off

Figure III.9 illustrates a "Single Sign-off" service allowing the user to automatically sign-off from multiple application services (VoIP, data, and video) without having to sign-off from each application service in the session. This use case assumes that the user is in a service session with active application services A (VoIP), B (data) and C (video).

The call flows are as follows:

1) Service sign-off [UserID]: The ETS user signals a request to end the service session.
2) Sign-off notification [UserID]: Application service C (video) notifies the IdM system of the user's request to sign off.
3) SSO verification: The IdM system determines that single sign-off is applicable and verifies the active application services.
4) Ack [UserID]: The IdM system sends an acknowledgement to application service C (video) to end the service session.
5) Sign-off notification [UserID]: The IdM system notifies application service B (data) of the sign-off.
6) Ack [UserID]: Application service B (data) acknowledges the sign-off.
7) Sign-off notification [UserID]: The IdM system notifies application service A (VoIP) of the sign-off.
8) Ack [UserID]: Application service A (VoIP) acknowledges the sign-off.
9) Single sign-off Ack [UserID]: The IdM system sends an acknowledgement to the user confirming sign-off from all active application services in the session.

Appendix IV

Mobile-related use cases

(This appendix does not form an integral part of this Recommendation)

IV.1 Introduction

This appendix provides example mobile-related IdM use cases. The example use cases in this appendix are based on the use cases described in 3G Americas White Paper, *Identity Management: Overview of Standards and Technologies for Mobile and Fixed Internet* [b-3G Americas White Paper].

IV.2 Use case examples

IV.2.1 A mobile user with a UICC-enabled 3G device accesses the MNO's portal (web store) to purchase a ringtone.

Actors:

- Mobile user.
- MNO (mobile network operator).
- SP (service provider) is the MNO.

User benefits:

- Single sign-on experience with access to different MNO services.

Key constraints:

- SP and MNO are in the same circle of trust (as per Liberty Alliance).

IV.2.2 A mobile user with a UICC-enabled 3G device accesses the MNO's portal web store; he or she navigates the portal digital merchandises catalog, sees the special promotion item (e.g., a video game, with which the MNO has an exclusive content distribution deal) and makes a purchase; he or she then agrees to charge the payment to his or her mobile phone bill; the user is able to download the video game from a secure link redirected from the MNO to the content provider.

Actors:

- Mobile user.
- MNO.
- SP-a is the MNO; SP-b is the external content provider (e.g., video game).

User benefits:

- Single sign-on experience to a MNO and an external vendor portal.
- Ability to use his or her credentials from his or her MNO to complete a transaction with an external content provider.

Key constraints:

- SP-a MNO and SP-b video game content provider are in the same circle of trust.

IV.2.3 A mobile user is using his or her UICC-enabled 3G smartphone and is roaming in another country; while surfing on the Net, he or she signs up for a paid-subscription of a foreign auto magazine and charges it to his or her credit card (attributes from his or her user profile kept by his or her MNO are selectively disclosed to complete the magazine subscription application process); payment is authorized by the credit card company on behalf of the mobile user to the auto magazine portal.

Actors:

- Mobile user.
- MNO.
- SP-a is the content provider (auto magazine); SP-b is the credit card company.

User benefits:

- Single sign-on experience with his or her MNO and the credit card company.
- Ability to use his or her credentials from his or her MNO to authorize payment from his or her credit card company to complete a transaction with an external content provider.
- Ability to reuse his or her personal attributes from his or her MNO subscriber profile to complete an external service subscription; hence minimizing re-entering much of these details.

Key constraints:

- The MNO and SP-b credit card company are in the same circle of trust.
- SP-a foreign auto magazine provider is not in the circle of trust.

IV.2.4 A mobile user is using his or her UICC-enabled 3G notebook while roaming in another country and waiting at an airport, he or she signs up for the airport WiFi service for several hours; the WLAN operator has an alliance with the mobile user's MNO; hence, it can accept the user's WiFi usage charges to his or her mobile phone bill; also the mobile user, while using the WiFi service, accesses several web portals with which he or she frequently interacts, including: a bank, a travel agency and a financial investment firm portal; the user wishes to be able to use the services provided by these web merchants without re-login, and also be able to exchange private personal information securely.

Actors:

- Mobile user.
- WLAN operator.
- MNO.
- SP-a is the MNO; SP-b is the bank, SP-c is the travel agency, and SP-d is the financial investment firm.

User benefits:

- Single sign-on experience with his or her MNO and the WiFi operator.
- Ability to use his or her credentials from his or her MNO to authorize WiFi service charges.
- Ability to access several web-based service providers not affiliated with the MNO with simplified log-in procedures and secured transfer of private information.

Key constraints:

- The MNO and WLAN operator are in the same circle of trust.
- SP-b bank, SP-c travel agency and SP-c financial investment firm are not in the same circle of trust.

IV.2.5 A mobile user is using his or her UICC-enabled 3G notebook while at home, he or she surfs the Net via his or her residential broadband DSL service through which he or she accesses his or her MNO portal; he or she pays his or her mobile account service bill (using his or her credit card, pre-authorization is on file) and adds a new feature to his or her mobile subscription; next he or she accesses a movie rental site and downloads a movie which is charged to his or her credit card (not pre-authorized).

Actors:

- Mobile user.
- Fixed network DSL carrier.
- MNO.
- SP-a is the MNO; SP-b is the movie rental portal; SP-c is the credit card company.

User benefits:

- Single sign-on experience with his or her fixed network operator and MNO.
- Ability to use his or her credentials from his or her fixed network operator to authenticate his or her mobile service account and orders additional MNO services.
- Ability to authorize content purchase charges from an external service provider (e.g., movie rental) to his or her credit card account.

Key constraints:

- The MNO, fixed network carrier and SP-c credit card company are in the same circle of trust.
- SP-b movie rental provider is not in the same circle of trust.

IV.2.6 A mobile user with UICC-enabled 3G device wants to access resources (e.g., enterprise directory service) located in an enterprise network.

Actors:

- Mobile user.
- MNO.
- Enterprise IdM system.
- Enterprise directory services server (EDS server).

The high-level interactions among these actors are described below. The mobile user requests service from the EDS server.

- The EDS server requests authentication from the user.
- The user, who has been authenticated by the MNO system, obtains authentication credentials from the MNO for authentication by the enterprise IdM system.
- The user submits the credentials to the enterprise IdM system and, upon successful authentication, obtains from it credentials for authentication to the EDS server.
- The user responds to the EDS server's request with the credentials received from the enterprise IdM system.
- The authenticated user obtains the requested service from the EDS server.

User benefits:

- The mobile user can access resources available in his or her enterprise network (e.g., enterprise directory service) in a cost-effective way while fulfilling stringent security requirements typically imposed by enterprise IT (information technology) environments.

Key constraints:

- A two-factor authentication (e.g., uid/password/PIN) may be required by the enterprise IdM system in addition to the MNO provided user credentials.
- The MNO IdM and enterprise IdM systems are in the same circle of trust.

Appendix V

Example IdM transaction models

(This appendix does not form an integral part of this Recommendation)

V.1 Introduction

This appendix provides example IdM transaction models. The models provided in this appendix are described in [b-ITU-T X.1250]. Other models beyond those included in this appendix are also possible.

V.2 Examples of possible identity management transaction models

One of the primary transactions in identity management is the basic query-response process common to most structured information exchange shown in Figure V.1. The most basic form of message exchange involves two parties using an agreed-upon protocol and information model.

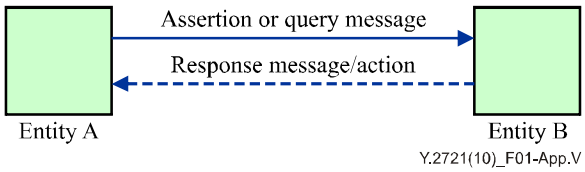


Figure V.1 – Basic query/response information exchange process

The parties that participate in this process may be any kind of entity. An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these individuals. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc. They can be any physical or virtual object, such as network equipment, software, terminal devices, sensors, actively tagged physical objects (e.g., using RFIDs or optical codes), passively tagged objects. Network devices, for instance, may be treated as entities subject to special IdM capabilities on behalf of end users, providers, and governmental authorities. In the context of digital rights management, the entity may be intellectual property or copyright protected material, such as multimedia or IPTV content. A special type of entity is the group. The group's identity is the intersection of the identities (common attributes) of the group members.

Most identity management use cases involve complex models. For example, where the relying party who originally receives the claim is not the identity service provider, and as illustrated in Figures V.2 and V.3, the function of being an identity service provider is separate and distinct from the relying party; the relying party evaluates the responses from the identity service provider(s) and decides whether there is a sufficient level of entity authentication assurance. The primary function of an identity service provider is to manage the creation, update, verification, suspension, and deletion of identity information.

There are many possible identity information exchange models. One model in common use is a three-party query response model shown in Figure V.2. Some of the new open IdM protocols are predicated on this model.

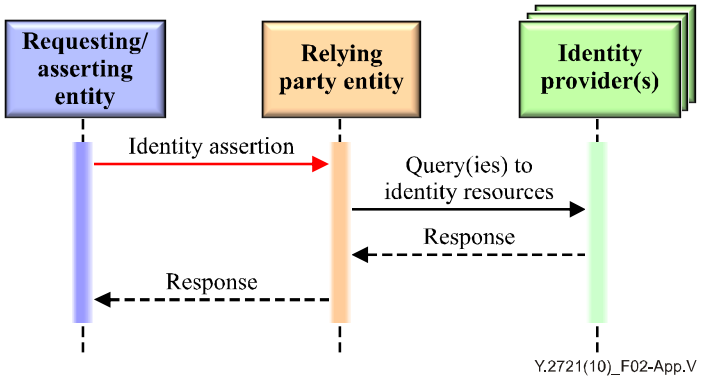


Figure V.2 – An example of a three-party identity management model

Another identity management model that provides the requesting party with more control of the identity relationships is depicted in Figure V.3.

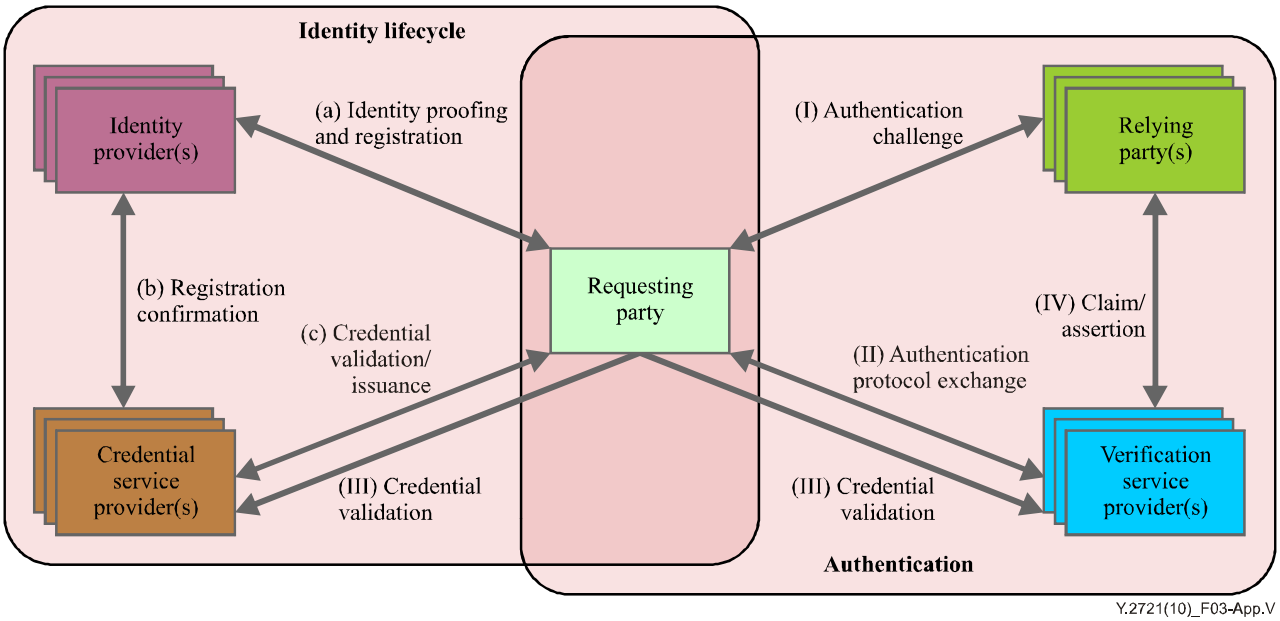


Figure V.3 – An example of a user-centric five-party identity management model

"User-centric" models (i.e., that require full requesting party control be enabled over use of their identities) are receiving significant attention and may also be mandated in national and regional jurisdictions. Figure V.3 shows an example where specialized roles and capabilities for identity management are provided by different service providers. All queries/responses are directed through the requesting party. For the purposes of these kinds of model, the entities are defined as:

- Identity provider: An entity that maintains and manages, and may create, trusted identity information of other entities (e.g., end user, organizations, and devices) and offers identity based services. This entity responsible for assigning and issuing attributes (i.e., involving the identity (e.g., for a subscriber to a credential provider) for a specific context) – also described as enrolment – is responsible for the lifecycle management of the identity which includes proofing, registration and maintenance of the identity, including revocation.

- Credential service provider: The entity providing capabilities related to the issuance of credentials and tokens (e.g., credentials that bind tokens to verifiable identifiers and attributes).
- Verification service provider: The entity providing capabilities of assessing identity information (e.g., claims and credentials) and classifying its validity.
- Relying party [ITU-T Y.2720]: An entity that relies on an identity representation or claim by a requesting/asserting entity within some request context.

Appendix VI

Example illustrative deployment scenario for IdM in NGN

(This appendix does not form an integral part of this Recommendation)

VI.1 Introduction

This appendix provides an example deployment scenario for IdM in NGN.

VI.2 IdM architecture deployment

NGN may deploy IdM infrastructure with capabilities supporting identity-based services to its users leveraging web services capabilities and specifications defined by the Liberty Alliance Project and OpenID, for example, IdM capabilities to allow its users to access services among different service and application providers, including federated application services. In addition, NGN may support IdM capabilities to offer IdSP services to other applications and service providers (e.g., assertion of user device identity and authentication, location and other relation identity information).

Support of IdM capabilities to offer IdSP services or to partner with other applications and service providers that are using different types of IdM systems based on different semantics, schemas, mechanisms and technologies would require appropriate bridging and interworking functions to facilitate interoperability. For example, to support IdM service and capabilities with other applications and service providers (e.g., web services and content providers), NGN could support capabilities for the following:

- 3GPP GBA interworking with Liberty Alliance Framework.
- 3GPP GBA interworking with OpenID.
- Other mechanisms for interworking with OpenID and Liberty Alliance Framework.

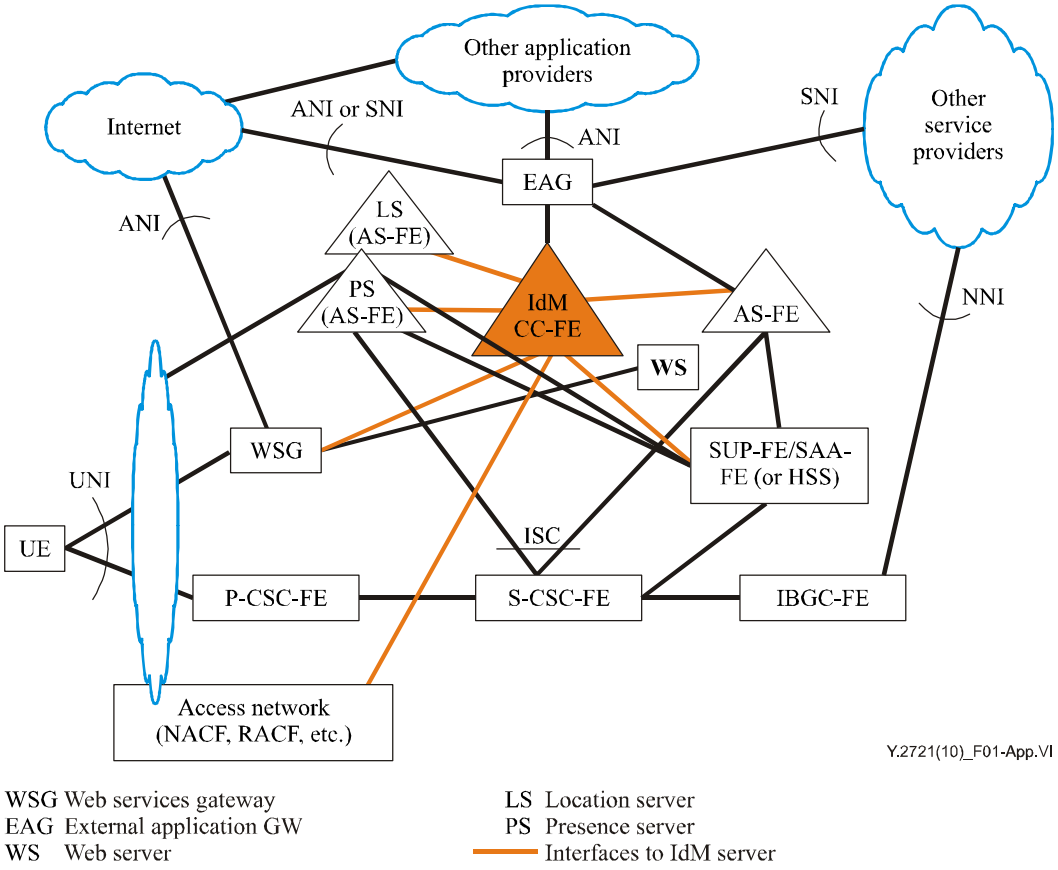


Figure VI.1 – Example IdM deployment in NGN

Figure VI.1 illustrates an example IdM deployment for NGN. This example shows the use of an IdM server which may be a stand-alone box, or a set of functions that are distributed, and or located in the HSS. The IdM server interfaces and interacts with network elements that support functional entities defined for NGN. For example, the IdM server may interface with:

- service enabling application servers (ASs), such as a location server (LS) or a presence server (PS), or other applications in order to provide a higher level of authentication assurance and to support identity-based application services;
- policy and network attachment and control servers for authentication assurance and policy management.

NOTE – For some specific national regulations, this may imply implementation of separated IdM functions in the different strata of the NGN.

To support certain IdM services for users/subscribers and to offer IdSP services or to partner with other applications and service providers, the NGN would need to support specific capabilities to control access and IdM exchanges with other applications and service providers (e.g., web services and content providers). This illustrative example shows the use of a web services gateway (WSG) and an external application gateway (EAG) to support certain IdM services leveraging or partnering with other applications and service providers. Specifically, Figure VI.1 shows the IdM server interfacing with the user via a web services gateway (WSG) which authenticates the user and provides the user with an interface to manage his/her identity profile. Mutual authentication between the user and service provider is also supported, as needed. The IdM server also interfaces with an external application gateway (EAG) that allows the user to access web-based services in the NGN or from other applications or service providers.

Bibliography

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

[b-ITU-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2009), *A framework for user control of digital identity*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.

[b-NIST SP 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*.

[b-NIST SP 800-94] NIST Special Publication 800-94 (2007), *Guide to Intrusion Detection and Prevention Systems (IDPS)*.

[b-CA/Browser Forum] CA/Browser Forum, *Guidelines For The Issuance And Management Of Extended Validation Certificates*.

[b-3G Americas White Paper] 3G Americas White Paper (2009), *Identity Management, Overview of Standards and Technologies for Mobile and Fixed Internet*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011