

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2720

(01/2009)

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

Next Generation Networks – Security

NGN identity management framework

Recommendation ITU-T Y.2720

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

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
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

Recommendation ITU-T Y.2720

NGN identity management framework

Summary

Recommendation ITU-T Y.2720 provides a framework for identity management (IdM) in next generation networks (NGN). The primary purpose of this framework is to describe a structured approach for designing, defining, and implementing IdM solutions and for facilitating interoperability in a heterogeneous environment.

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

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

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

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

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

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

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

Source

Recommendation ITU-T Y.2720 was approved on 23 January 2009 by ITU-T Study Group 13 (2009-2012) under the WTSA Resolution 1 procedure.

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/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in other non-ITU standards	2
3.3	Terms defined in this Recommendation.....	2
4	Abbreviations.....	4
5	Introduction	4
5.1	Identity management (IdM) overview	4
5.2	Business drivers and motivations	6
5.3	Identity provider (IdP).....	8
5.4	NGN functional architecture and use of identifiers.....	9
6	IdM framework overview	9
7	IdM in the context of NGN architectures and reference models	11
7.1	General relationship with NGN architectures and services.....	11
7.2	Recommendation ITU-T Y.2011 (General principles and general reference model for NGN) reference models	12
8	Identity management framework.....	13
8.1	Identity lifecycle management	13
8.2	Identity management OAM&P functions.....	14
8.3	Identity management signalling and control functions	16
8.4	Identity management federated identity functions	21
8.5	Identity management user and subscriber functions	21
8.6	Performance and reliability	21
8.7	IdM security.....	22
	Bibliography.....	24

Recommendation ITU-T Y.2720

NGN identity management framework

1 Scope

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

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

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

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

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

2 References

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 anonymity [b-ITU-T X.1121]: Ability to allow anonymous access to services, which avoid tracking of user's personal information and user behaviour such as user location, frequency of a service usage, and so on.

3.1.2 authentication [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.

3.1.3 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

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

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

3.1.6 identifier [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).

3.1.7 next generation network (NGN) [b-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.

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

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

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

3.2 Terms defined in other non-ITU standards

3.2.1 attribute [b-ETSI TS 102 042]: Descriptive information bound to an entity that specifies a characteristic of an entity such as condition, quality or other information associated with that entity.

3.3 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.3.1 assurance: A measure of confidence that the security features and architecture of the identity management capabilities accurately mediate and enforce the security policies understood between the relying party and the identity provider.

3.3.2 authentication assurance: See Assurance.

3.3.3 assurance level: A quantitative expression of assurance agreed between a relying party and an identity provider.

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

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

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

3.3.7 federation: Establishing a relationship between two or more entities or an association comprising any number of service providers and identity providers.

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

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

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

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

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

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

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

3.3.14 presence: A set of attributes that characterize an entity relating to the current status.

3.3.15 privacy: The protection of personally identifiable information.

3.3.16 relying party: An entity that relies on an identity representation or claim by a requesting/asserting entity.

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

4 Abbreviations

This Recommendation uses the following abbreviations:

API	Application Programming Interface
BSS	Business Support System
CSCF	Call Session Control Function
FRA	Functional Requirements and Architecture
GBA	Generic Bootstrapping Architecture
IdM	Identity Management
IdP	Identity Provider
NGN	Next Generation Networks
OAM&P	Operation, Administration, Maintenance and Provisioning
OSS	Operations Support System
PII	Personally Identifiable Information
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
RP	Relying Party
SAML	Security Assertion Markup Language
SBC	Session Border Controller
SIP	Session Initiation Protocol
SP	Service Provider
SS7	Signalling System No. 7
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol

5 Introduction

5.1 Identity management (IdM) overview

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

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

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

Figure 1 provides a general overview of IdM.

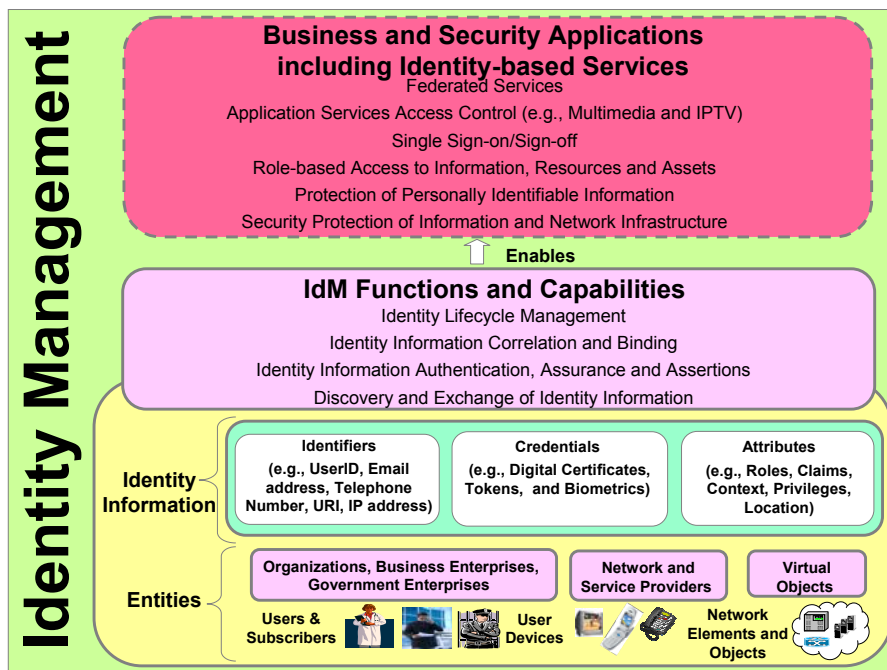


Figure 1 – IdM overview

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

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

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

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

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

- *business applications*
 - single sign-on and sign-off (e.g., access to multiple applications and services without having to individually authenticate each application or service platform)
 - federated services (e.g., access to services across different service providers or NGN providers)