

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 12

(04/2010)

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

ITU-T Y.2720 – Supplement on NGN identity management mechanisms

ITU-T Y-series Recommendations – Supplement 12

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.

Supplement 12 to ITU-T Y-series Recommendations

ITU-T Y.2720 – Supplement on NGN identity management mechanisms

Summary

Supplement 12 to ITU-T Y-series Recommendations provides a description of some example mechanisms that can be used to meet certain identity management (IdM) requirements and deployment needs of NGN.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y Suppl. 12	2010-04-30	13

Keywords

Authentication, authorization, identity management, next generation network, single sign-on.

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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 2010

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
4 Abbreviations.....	2
5 Conventions	3
6 Mechanisms and procedures supporting IdM functions	3
6.1 Lifecycle management.....	3
6.2 Authentication and authentication assurance	3
6.3 IdM communications and information exchange	22
6.4 Identity information access control	25
6.5 Single sign-on.....	25
Appendix I – ITU-T X.509 v3 message authentication	27

Copyright International Telecommunication Union/ITU Telecommunication Sector

Supplement 12 to ITU-T Y-series Recommendations

ITU-T Y.2720 – Supplement on NGN identity management mechanisms

1 Scope

This supplement provides a description of some example mechanisms that can be used to meet certain identity management (IdM) requirements and deployment needs of NGN.

NOTE – This supplement provides only a subset of the IdM mechanisms needed for NGN. The purpose of this supplement is to provide the information in a timely manner while the work to develop a Recommendation specifying a more complete set of IdM mechanisms progresses. The objective of this work is to define the IdM mechanism in support of the requirements specified in [ITU-T Y.2721].

2 References

- [ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frame works*.
- [ITU-T X.1035] Recommendation ITU-T X.1035 (2007), *Password-authenticated key exchange (PAK) protocol*.
- [ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.
- [ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.
- [ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.
- [ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.
- [ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.
- [ITU-T Y.2721] Recommendation ITU-T Y.2721 (2010), *NGN identity management requirements and use cases*.
- [ATIS 33102] ATIS.3GPP.33.102V710-2007, *3G Security; Security Architecture*.
- [IETF RFC 2289] IETF RFC 2289 (1998), *A One-Time Password System*.
<<http://www.ietf.org/rfc/rfc2289.txt>>
- [IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*.
- [IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.
- [IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*.
<<http://www.rfc-editor.org/rfc/rfc3310.txt>>
- [IETF RFC 4169] IETF RFC 4169 (2005), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2*. <<http://www.ietf.org/rfc/rfc4169.txt?number=4169>>
- [IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.

[3GPP TR 33.924]	3GPP TR 33.924 Release 9 (2009), <i>3rd Generation Partnership Project; Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking (Release 9)</i> .
[OpenID v.2]	OpenID <i>OpenID Authentication 2.0</i> . < http://openid.net/specs/openid-authentication-2_0.html >
[OASIS WSS X.509 profile]	OASIS (2006), <i>Web Services Security X.509 Certificate Token Profile 1.1</i> .
[OASIS SAML token]	OASIS (2006), <i>SAML Token Profile 1.1, OASIS Approved Erratta 1</i> .
[OASIS WSS SOAP]	OASIS (2004), <i>Web Services Security (WSS) SOAP Message Security 1.1</i> .
[LA ID-WSF security]	Liberty Alliance Project (2007), <i>Liberty ID-WSF Security Mechanisms Core Version 2.0-errata Version 1.0</i> .
[LA SOAP binding]	Liberty Alliance Project, <i>Web Services Security (WSS) (2006), Liberty SOAP Binding Ver-2.0</i> .
[W3C XML signature]	World Wide Web Consortium (W3C) (2008), <i>XML Signature Syntax and Processing (Second Edition)</i> .

3 Definitions

This supplement relies on the terms defined in [ITU-T Y.2720].

4 Abbreviations

This supplement uses the following abbreviations and acronyms:

AKA	Authentication and Key Agreement
ASP	Application Service Provider
AV	Authentication Vector
BSF	Bootstrapping Server Function
CK	Ciphering Key
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IdM	Identity Management
IdP	Identity Provider
ID-WSF	Identity Web Services Framework
IK	Integrity Key
IMPI	IP Multimedia Private User Identity
IMPU	IP Multimedia Public User identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IPTV	Internet Protocol Television
ISIM	IMS Subscriber Identity Module

NAF	Network Application Function
NGN	Next Generation Network
OASIS	Organization for the Advancement of Structured Information Standards
OTP	One Time Password
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol
SLF	Subscriber Locator Function
SOAP	Simple Object Access Protocol
SSO	Single Sign-On
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
WSS	Web Services Security
XML	eXtensible Markup Language

5 Conventions

None.

6 Mechanisms and procedures supporting IdM functions

This clause describes mechanisms and procedures that support IdM functions.

6.1 Lifecycle management

Refer to [ITU-T Y.2720] for information on identity lifecycle management.

6.2 Authentication and authentication assurance

This clause describes mechanisms for authentication and assurance of identities and identity information. It references authentication mechanisms defined elsewhere.

The identity provider (IdP) supports authentication methods such as authentication based on web services (WS) security assertion markup language (SAML) profile, certificate-based authentication, or password-based authentication (including one time password (OTP)). The authentication methods are selected based on the assurance-level requirements. The IdP may request assurance-level information to find the authentication methods that satisfy the service provider's assurance-level requirements.

6.2.1 Authentication based on the WS security SAML profile

This clause describes SAML-based authentication.

6.2.1.1 SAML assertions

The security assertion markup language (SAML) [ITU-T X.1141] specifies a format of assertions that can be used in identity management for exchanging security information. Among the IdM functions that can be implemented with the use of SAML are authentication, attribute sharing, and authorization, which correspond to three types of statements about a subject of a SAML assertion:

- Authentication statement – conveys information that the assertion subject was authenticated by a particular means at a particular time.
- Attribute statement – conveys information that the assertion subject is associated with the listed attributes.
- Authorization decision statement – conveys information that access to a specified resource was granted to the assertion subject, or the subject was denied such access.

The content of a SAML assertion can be described at a high level as follows: assertion **A** was issued at time **t** by issuer **R** regarding subject **S** provided conditions **C** are valid.

The use of the SAML assertions for conveying authentication, attribute and authorization information in simple object access protocol (SOAP) messages is a special and important application of SAML. When SOAP messages are exchanged over an unprotected transport, it is strongly recommended that XML signature [W3C XML signature] is used to verify the relationship between the SOAP message and the statements of the assertions carried in the message. The *Web Services Security (WSS): SAML Token Profile* [OASIS SAML token] standard describes how:

- SAML assertions (also referred to as SAML tokens) are carried in and referenced from a SOAP message;
- an XML signature is used to bind a subject and the statements of a SAML assertion with a SOAP message.

A typical use of a SAML token with a SOAP message constructed according to this specification is depicted by Figure 1 and described below.

In this example, a signed SOAP message contains a SAML assertion with an attribute statement. Based on the information in this statement, the receiver decides whether to allow access to the requested resource.

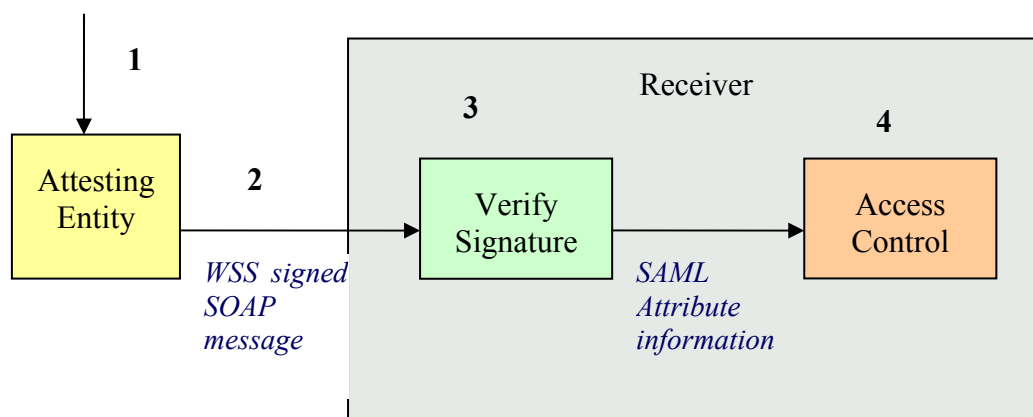


Figure 1 – Typical steps of construction and processing of a SOAP message with a SAML token

1. The attesting entity obtains a SAML assertion with an attribute statement and constructs and includes it in a SOAP message constructed according to [OASIS SAML token].
2. The attesting entity sends a SOAP message to the receiver.
3. The receiver verifies the digital signature.
4. The information of the SAML statement is used for access control.

6.2.1.2 Subject confirmation methods of the SAML tokens

The OASIS Standard, [OASIS SAML token] specifies how to attach a SAML assertion to a SOAP message and defines two mandatory subject confirmation methods:

- holder-of-key;
- sender-vouches.

The main XML elements of the SOAP message constructed according to [OASIS WSS SOAP] are depicted in Figure 2.

The SAML assertion is placed into the `<wsse:Security>` header, which also contains the digital signature `<ds:Signature>`. The digital signature is used by the receiver of the SOAP message to verify that the sender of the message knows the key used for computing the signature over the digest of the SOAP body and for checking its integrity. The digest algorithm is SHA 1 and the signature algorithm is RSA_SHA 1 as specified in [OASIS WSS SOAP]. The signature's value is provided in the `<ds:SignatureValue>` element of the `<ds:Signature>`.

Two subject confirmation methods define different ways for conveying information on the key to the receiver.

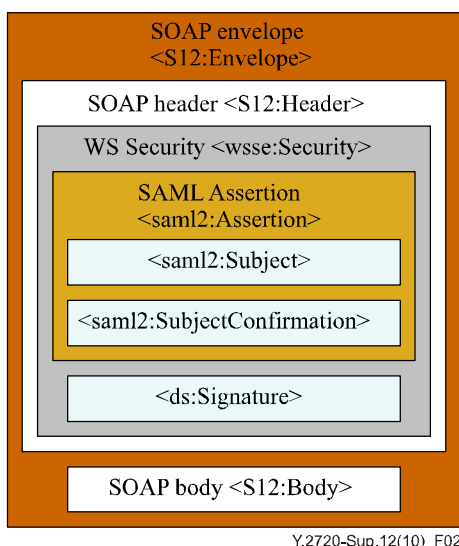


Figure 2 – Structure of the SOAP message with SAML assertion

The following clauses describe two subject confirmation methods.

6.2.1.2.1 The holder-of-key subject confirmation method

Figure 3 depicts the structure of the SAML assertion used for the holder-of-key subject confirmation method. The method attribute of element `<saml2:SubjectConfirmation>` indicates the method of the subject confirmation (holder-of-key).

The method specifies that the sender (also known as the attesting entity) must prove that it is entitled to make the statements about the subject by demonstrating knowledge of the key, which is identified in the `<ds:KeyValue>` element contained in the `<ds:KeyInfo>` element of the SAML assertion. The `<ds:KeyInfo>` element identifies a public or secret key that is used to confirm the identity of the subject. The method further specifies that the sender may do it by signing a digest of the SOAP body with that key. The signature is contained in the element `<ds:Signature>` of the WS security header as shown in Figure 2.