

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2722

(01/2011)

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

Next Generation Networks – Security

NGN identity management mechanisms

Recommendation ITU-T Y.2722



International
Telecommunication
Union

Documents
Document Sharing Hub

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
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

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

Recommendation ITU-T Y.2722

NGN identity management mechanisms

Summary

Recommendation ITU-T Y.2722 specifies the mechanisms that can be used to meet the identity management (IdM) requirements and deployment needs of next generation networks (NGN).

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2722	2011-01-28	13

Keywords

Federated identity, identity management, identity management mechanisms, 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 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 2011

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
4	Abbreviations.....	2
5	Conventions	3
6	Mechanisms and procedures supporting IdM functions.....	4
6.1	Lifecycle management.....	4
6.2	Authentication and authentication assurance	4
6.3	Correlation and binding	24
6.4	Discovery.....	25
6.5	IdM communications and information exchange	26
6.6	Protection of personally-identifiable information (PII).....	30
6.7	Federated identity functions	30
6.8	Identity information access control	31
6.9	Single sign-on.....	31
6.10	Single sign-off	32
7	Security	35
	Appendix I – WSS ITU-T X.509 v3 message authentication.....	36
	Appendix II – "OpenID + OAuth"-based mechanism for access control	38
II.1	OAuth [b-IETF RFC 5849]	38
II.2	Using OpenID in conjunction with OAuth.....	38
II.3	OpenID + OAuth authorization flow.....	38
	Bibliography.....	41

Downloaded from: 192.168.1.100

Recommendation ITU-T Y.2722

NGN identity management mechanisms

1 Scope

[ITU-T Y.2721], *NGN identity management requirements and use cases*, specifies identity management (IdM) requirements for the next generation networks (NGN). This Recommendation describes the specific IdM mechanisms and suites of options that should be used to meet the requirements specified in [ITU-T Y.2721]. In addition, it provides best practices and guidelines to support interoperability and other needs.

This Recommendation is intended to be used together with [ITU-T Y.2720] and [ITU-T Y.2721], as the fundamental architectural concepts, requirements and use cases are not repeated in this Recommendation.

NOTE – Implementers and users of the described mechanisms shall comply with all applicable national and regional laws, regulations and policies. Some specific regulations and legislations may require implementation of mechanisms to protect personally-identifiable information.

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 X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [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 X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.
- [ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of NGN release 1*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for 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*.
- [3GPP TS 23.228] 3GPP TS 23.228 (in force), *IP Multimedia Subsystem (IMS); Stage 2*.
- [ATIS 33102] ATIS.3GPP.33.102V710-2007, *Security Architecture*.
- [IETF RFC 2289] IETF RFC 2289 (1998), *A One-Time Password System*.

3 Definitions

This Recommendation relies on the terms defined in [ITU-T Y.2720] and [ITU-T X.1252]. Particularly, the following definitions are adopted from [ITU-T X.1252]:

3.1 identity provider (IdP): See identity service provider (IdSP).

3.2 identity service provider (IdSP): An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

AKA	Authentication and Key Agreement
ASP	Application Service Provider
AuC	Authentication Centre
AV	Authentication Vector
BSF	Bootstrapping Server Function
CK	Ciphering Key
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IdM	Identity Management
IdP	Identity Provider
IdSP	Identity Service Provider
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
LDAP	Lightweight Directory Access Protocol
MS	Mobile Station
NAF	Network Application Function
NGN	Next Generation Networks
OASIS	Organization for the Advancement of Structured Information Standards

OTP	One-Time Password
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RP	Relying Party
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol
SLF	Subscriber Locator Function
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSO	Single Sign-On
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identifier Module
WAP	Wireless Application Protocol
WSS	Web Services Security
XML	eXtensible Markup Language
XRDS	eXtensible Resource Descriptor Sequence

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which 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 which 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 which 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 which 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 appendices, 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 Mechanisms and procedures supporting IdM functions

6.1 Lifecycle management

Refer to [ITU-T Y.2720], *NGN identity management framework*, 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.

Specific authentication mechanisms 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)) can be used by the IdSP for specific applications or services based on the context and on the needed level of assurance. The authentication method (or methods) is selected based on the assurance level requirements. The IdSP may request information to determine the authentication methods that satisfy the service provider's assurance level requirements.

6.2.1 Authentication based on WS security SAML profile

6.2.1.1 SAML assertions

Security assertion markup language (SAML), [ITU-T X.1141], specifies the format of assertions that can be used for exchanging security information for IdM. 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 the 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 SAML assertions used for communicating authentication, attribute and authorization information are conveyed in simple object access protocol (SOAP) messages. When SOAP messages are exchanged over an unprotected transport, it is strongly recommended that XML signature [b-W3C XML signature] be 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* [b-OASIS SAML token] standard describes how:

- SAML assertions (also referred to as SAML tokens) are carried in and referenced from a SOAP message.
- 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 Recommendation is depicted in 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 could make access control decisions.

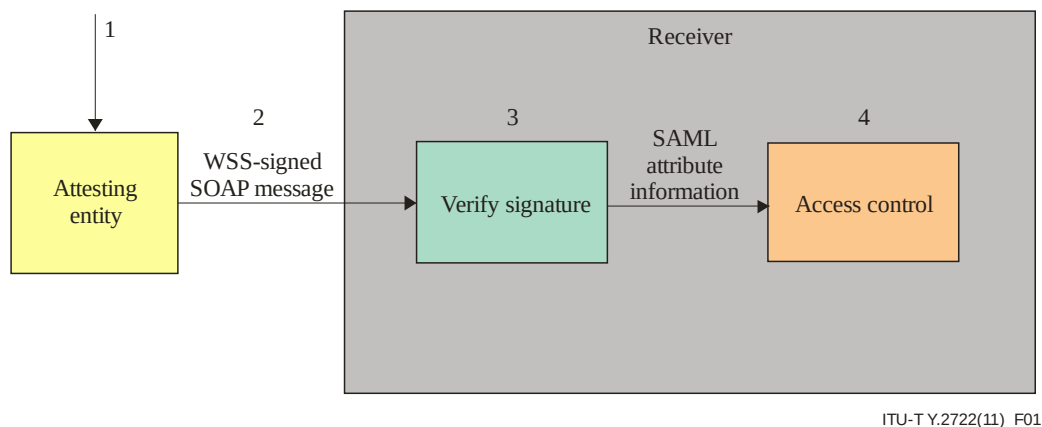


Figure 1 – Typical steps of construction and processing of a SOAP message with a SAML token

- 1) The attesting entity obtains a SAML assertion with an attribute statement, constructs and includes it in a SOAP message according to [b-OASIS SAML token].
- 2) The attesting entity sends the WSS-signed SOAP message to the receiver.
- 3) The receiver verifies the digital signature.
- 4) The information of the SAML statement may be used for access control decisions.

6.2.1.2 Subject confirmation methods of the SAML tokens

The OASIS Standard, *Web Services Security: SAML Token Profile 1.1* [b-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 [b-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 [b-OASIS WSS SOAP]. The signature's value is provided in the <ds:SignatureValue> element of the digital signature <ds:Signature>.

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

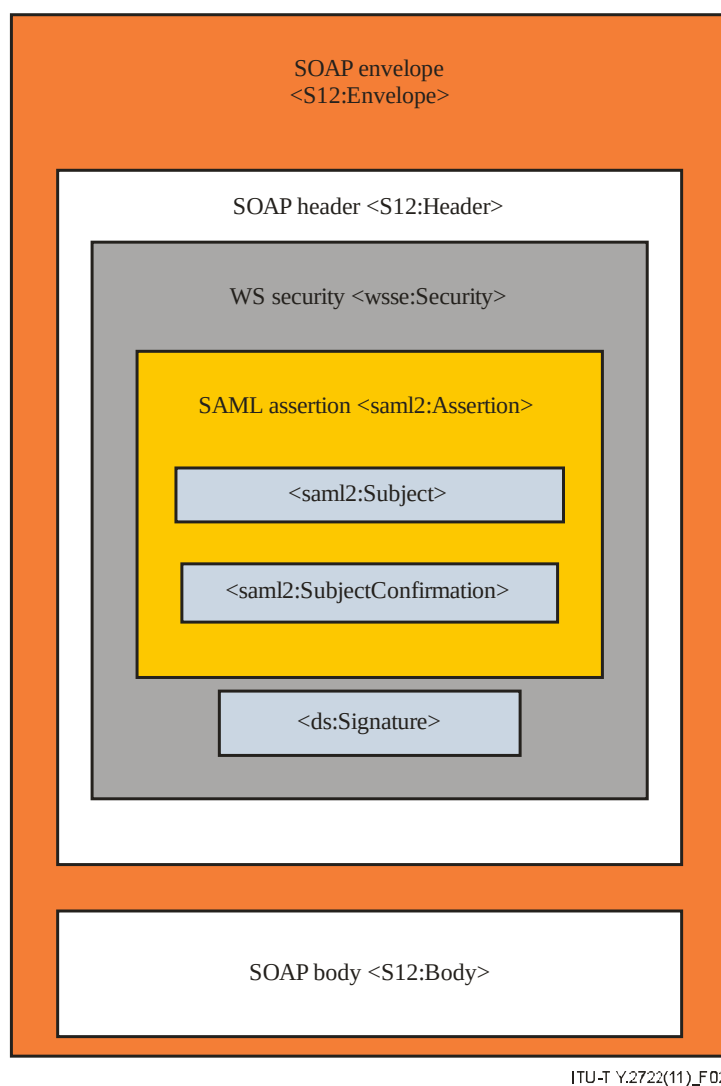


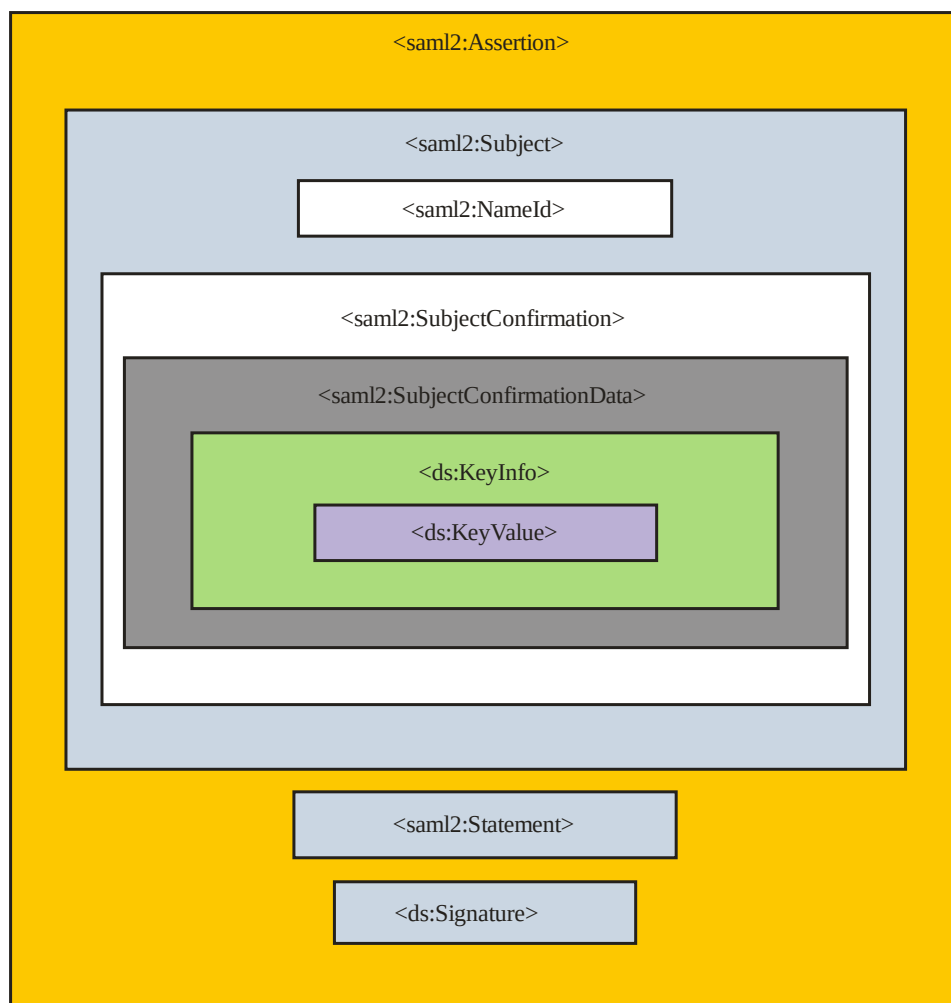
Figure 2 – Structure of the SOAP message with SAML assertion

The following clauses describe the two subject confirmation methods.

6.2.1.2.1 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 the 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 a secret key that is used to confirm the identity of the subject. The method further specifies that the sender may do so 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.



ITU-T Y.2722(11)_F03

Figure 3 – Structure of the SAML assertion used for the holder-of-key subject confirmation method

The receiver of the SOAP message obtains the key using information that is provided by the attesting entity in the `<ds:KeyInfo>` element. The receiver then computes the digital signature of the SOAP body and checks whether it matches the signature provided by the attesting entity. If it is the case, then the subject and statements of the SAML assertion may be attributed to the attesting entity and the content of the SOAP body whose integrity is protected by the key may be considered as provided by the attesting entity.

6.2.1.2.2 Sender-vouches subject confirmation method

Figure 4 depicts the structure of the SAML assertion used for the sender-vouches subject confirmation method. The method attribute of the element `<saml2:SubjectConfirmation>` indicates the method of the subject confirmation (sender-vouches).

The attesting entity is trusted by a receiver to make SAML assertions regarding a subject under the condition that value of the method attribute of the `<SubjectConfirmation>` element indicates the sender-vouches method.

The attesting entity obtains one or more assertions or references to assertions from one or more authorities and includes them in a SOAP message. It then computes a signature of the digest of the SAML assertions and the body of the SOAP message. The signature is contained in the element `<ds:Signature>` of the WS security header (shown in Figure 2). The attesting entity optionally

provides information to the receiver on the key that was used to compute the signature. If there is no such information, the receiver is expected to identify the key by other means.

The receiver checks the validity of the signature. If the signature is valid, the receiver establishes the fact that the statements have been made about the subject by the attesting entity.

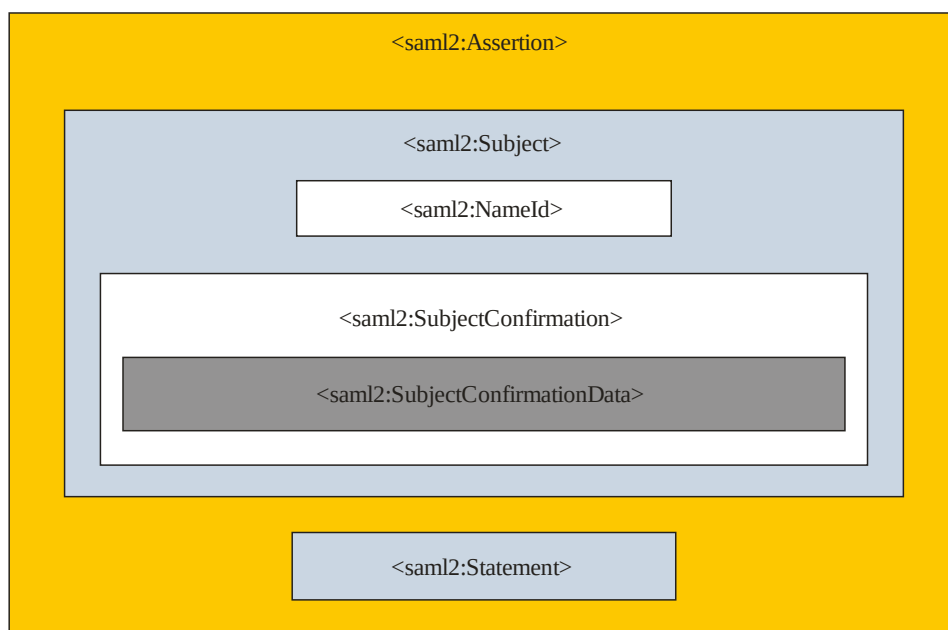


Figure 4 – Structure of the SAML assertion used for the sender-vouches subject confirmation method

6.2.2 Certificate-based authentication

[ITU-T X.509] certificates may be used for specific application or service based on the context and the needed level of assurance. The use of [ITU-T X.509] certificates for authentication is described in [ITU-T Y.2704], *Security mechanisms and procedures for NGN*.

6.2.3 Password-based authentication

Password-based authentication may be used for specific applications or services based on the context and the needed level of assurance. Refer to [ITU-T X.1035] for a description of a password-based authentication mechanism.

6.2.4 One-time password

One-time password (OTP) may be used for specific application or service based on the context and the needed level of assurance. One method of implementing OTP is described in [IETF RFC 2289].

6.2.5 Use of authentication and key agreement (AKA) for mutual authentication

The universal mobile telecommunications system (UMTS) authentication and key agreement (AKA) protocol can be used to provide mutual authentication of the mobile station (MS) and the network. The UMTS AKA is a challenge-response protocol, which uses a long-term key shared between the universal subscriber identity module (USIM) and the authentication centre (AuC). These entities reside on the universal integrated circuit card (UICC) of the MS and in the mobile station's home network respectively. In certain business arrangements, the functions of the AuC could be provided by an IdSP. The AKA protocol is specified in [ATIS 33102].

6.2.6 Integration of PKI-based authentication with IMS

IP multimedia subsystems (IMSs) security is based on the AKA mechanism, which uses a shared secret and a challenge-response protocol for user-network authentication. However, security of certain NGN services (e.g., IPTV) is based on the public key infrastructure (PKI) certificates. To allow blending of NGN services using PKI certificates and IMS security, it may be desirable to integrate PKI-based authentication with the IMS authentication in such a way that leverages the strength of IMS security.

Integration of the IMS authentication with PKI-based authentication allows the user equipment and the network to authenticate each other, based on their respective certificates, and to agree on a set of cryptographic keys based on the same key generation algorithms as in AKA. To this end, the user equipment and network need to be provisioned with the respective private keys and certificates, and be able to perform the PKI operations.

With respect to the agreement on the ciphering key (CK) and the integrity key (IK), the described mechanism for integration specifies two options:

- 1) Establishing an agreement on the CK and IK keys with the use of a shared secret between the end-user function and the S-5 – Service user profile functional entity (SUP-FE) defined in [ITU-T Y.2012].
- 2) Establishing an agreement on the CK and IK keys without the use of the shared secret.

The generic call flows for the first option and the second option are depicted in Figures 5 and 6, respectively.

6.2.6.1 Conventions

The following conventions are used in this clause:

- "|" designates the string concatenation.
- *CK* designates the ciphering key.
- *IK* designates the integrity key.
- *K()* designates a symmetric key encryption.
- $N_{pr} []$ designates encryption with the network private key N_{pr} .
- $N_{pu} []$ designates encryption with the network public key N_{pu} available from the network certificate.
- $U_{pr} []$ designates encryption with the user private key U_{pr} .

6.2.6.2 Entities involved in authentication

- S-5 – Service user profile functional entity (SUP-FE).
- End-user function: The entity is capable of running a SIP client.
- S-n call session control functional entity (CSC-FE), where S-n stands for one of the following entities:
 - S-1 Serving call session control functional entity (S-CSC-FE);
 - S-2 Proxy call session control functional entity (P-CSC-FE);
 - S-3 Interrogating call session control functional entity (I-CSC-FE).

The S-n is used to denote one of these entities when there are no differences between them as far as the described authentication procedure is concerned. Refer to [ITU-T Y.2012] for descriptions of the NGN functional entities (S-1, S-2, S-3, S-5 and end-user function).

Copyright International Telecommunication Union (ITU) 2011