

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2702

(09/2008)

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

Next Generation Networks – Security

Authentication and authorization requirements for NGN release 1

Recommendation ITU-T Y.2702

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.2702

Authentication and authorization requirements for NGN release 1

Summary

Recommendation ITU-T Y.2702 specifies authentication and authorization requirements for next generation networks (NGNs).

Source

Recommendation ITU-T Y.2702 was approved on 12 September 2008 by ITU-T Study Group 13 (2005-2008) under the WTSA Resolution 1 procedure.

Keywords

Attributes, Authentication, Authorization, Identifiers, Identity Management (IdM), Next Generation Network (NGN), Privileges and Security.



Documents

Document Sharing Hub

Rec. ITU-T Y.2702 (09/2008)

1

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	Definitions from [ITU-T X.800]	2
3.2	Definitions from [ITU-T X.810]	2
3.3	Definitions from [ITU-T X.811]	2
3.4	Definitions from [ITU-T Y.2701]	3
3.5	Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	3
5	Reference models.....	5
5.1	ITU-T X.811 authentication framework.....	5
5.2	Authentication threats.....	9
5.3	Authentication assurance.....	11
5.4	Authorization and privilege management	13
5.5	End-to-end reference architectural model	13
5.6	Relationship with NGN architecture specified in [ITU-T Y.2012].....	14
6	General Requirements	16
7	Authentication and authorization of user for network access.....	16
7.1	Description	16
7.2	General reference model.....	17
7.3	Requirements.....	20
8	Service NGN provider authentication and authorization of user for access to service/application	23
8.1	Description	23
8.2	Requirements.....	24
9	User authentication and authorization of NGN providers	27
9.1	Description	27
9.2	Objectives and requirements	27
10	NGN provider supported user peer-to-peer authentication and authorization.....	28
11	Mutual network authentication and authorization	28
11.1	Description	28
11.2	Mutual network authentication requirements.....	29
12	NGN provider authentication and authorization of 3rd party service/application provider.....	30
12.1	Description	30
12.2	Requirements.....	30
13	Use of 3rd party authentication and authorization service	31
13.1	Description	31

	Page
13.2 Requirements.....	31
14 Authentication and authorization of objects.....	31
14.1 Description	31
14.2 Requirements.....	32
Appendix I – SAML use case	33
I.1 Use of [b-ITU-T X.1141], Security Assertion Markup Language (SAML 2.0)	33
I.2 Service/application authentication procedures	33
I.3 Service/application authentication – Call flow examples	33
I.4 Security of service/application authentication procedures and mechanisms	34
Appendix II – ETS authentication and authorization.....	35
II.1 Overview	35
II.2 ETS user authentication and authorization.....	35
II.3 NGN provider authentication and authorization for ETS.....	36
II.4 ETS authentication and authorization use case examples	36
Appendix III – 3GPP Generic bootstrapping architecture	41
Appendix IV – Identity management (IdM) call flow examples	43
IV.1 Overview	43
IV.2 Call flow examples	43
Bibliography.....	54

Recommendation ITU-T Y.2702

Authentication and authorization requirements for NGN release 1

1 Scope

This Recommendation provides authentication and authorization requirements for next generation networks (NGN) based on [ITU-T Y.2012]. This includes requirements for authentication and authorization across the user-to-network interface (UNI), the network-to-network interface (NNI) and the application-to-network interface (ANI) as well as any entities internally with a network that may require authentication and authorization. The scope of this Recommendation includes:

- 1) Authentication and authorization of user for network access (e.g., authentication and authorization of an end user device, a home network gateway, or an enterprise gateway to obtain access or attachment to the network)
- 2) Service provider authentication and authorization of user for access to service/application (e.g., authentication and authorization of a user, a device or a combined user/device where the authentication and authorization apply to NGN service/application access)
- 3) User authentication and authorization of Network (e.g., user authenticating the identity of the connected NGN network or of the service provider)
- 4) User peer-to-peer authentication and authorization (e.g., authentication and authorization of the called user (or terminating entity), authentication and authorization of the originating entity, or data origin authentication as network functions)
- 5) Mutual network authentication and authorization (e.g., authentication and authorization across NNI interface at the transport level, or service/application level)
- 6) Authentication and authorization of service/application provider
- 7) Use of 3rd party authentication and authorization service
- 8) Authentication of objects (e.g., application process, message content and data content identifiers).

The items above include authentication of flows of the signalling, bearer and management traffic as applicable.

In addition, this Recommendation also provides reference models for NGN authentication and authorization.

NOTE 1 – NGN authentication and authorization is viewed as part of the broader topic of NGN identity management (IdM). Specifically, the authentication and authorization functions and capabilities described in this Recommendation should be used to support identity assurance capabilities for NGN IdM.

NOTE 2 – In this Recommendation, the use of the term "user" is not intended to be restricted to a person. A user could be a person, groups, companies, or juridical entities.

NOTE 3 – Authentication of an entity is not intended to indicate 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 X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnections for CCITT applications*.
- [ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open System Interconnection – Security framework for open systems: Overview*.
- [ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open System Interconnection – Security frameworks for open system: Authentication framework*.
- [ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.
- [ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

3 Definitions

3.1 Definitions from [ITU-T X.800]

This Recommendation makes use of the following terms defined in [ITU-T X.800]:

- 3.1.1 authentication information:** Information used to establish the validity of a claimed identity.
- 3.1.2 authorization:** The granting of rights, which includes the granting of access based on access rights.
- 3.1.3 credential:** Data that is transferred to establish the claimed identity of an entity.
- 3.1.4 data origin authentication:** The corroboration that the source of data received is as claimed.
- 3.1.5 peer-entity authentication:** The corroboration that a peer entity in an association is the one claimed.

3.2 Definitions from [ITU-T X.810]

This Recommendation makes use of the following terms defined in [ITU-T X.810]:

- 3.2.1 trust:** Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.
- 3.2.2 trusted third party:** A security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy).

3.3 Definitions from [ITU-T X.811]

This Recommendation makes use of the following terms defined in [ITU-T X.811]:

- 3.3.1 asymmetric authentication method:** A method of authentication, in which not all authentication information is shared by both entities.
- 3.3.2 authenticated identity:** A distinguishing identifier of a principal that has been assured through authentication.
- 3.3.3 authentication:** The provision of assurance of the claimed identity of an entity.

- 3.3.4 authentication certificate:** A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.
- 3.3.5 authentication exchange:** A sequence of one or more transfers of exchange authentication information (AI) for the purposes of performing an authentication.
- 3.3.6 authentication information (AI):** Information used for authentication purposes.
- 3.3.7 authentication initiator:** The entity that starts an authentication exchange.
- 3.3.8 claimant:** 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.
- 3.3.9 claim authentication information (claim AI):** Information used by a claimant to generate exchange AI needed to authenticate a principal.
- 3.3.10 exchange authentication information (exchange AI):** Information exchanged between a claimant and a verifier during the process of authenticating a principal.
- 3.3.11 principal:** An entity whose identity can be authenticated.
- 3.3.12 symmetric authentication method:** A method of authentication in which both entities share common authentication information.
- 3.3.13 verification authentication information (verification AI):** Information used by a verifier to verify an identity claimed through exchange AI.
- 3.3.14 verifier:** An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

3.4 Definitions from [ITU-T Y.2701]

This Recommendation makes use of the following terms defined in [ITU-T Y.2701]:

- 3.4.1 border element:** Network element providing functions connecting different security and administrative domains.
- 3.4.2 corporate network:** A private network that supports multiple users and may be in multiple locations (e.g., an enterprise, a campus).
- 3.4.3 security domain:** 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. The policy will be administered by the security authority. A given security domain may span multiple security zones.
- 3.4.4 terminal equipment border element:** Border element providing security functions between customer premises equipment and service provider network.

3.5 Terms defined in this Recommendation

This Recommendation defines the following term:

- 3.5.1 service level agreement (SLA):** Formal agreement between two or more parties that is reached after a negotiating activity with the scope to define service characteristics, responsibilities and priorities of every part. A SLA may include statements about security, performance, tariffing and billing, service delivery and compensations.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL Access Control List

AI	Authentication Information
ANI	Application-to-Network Interface
AS	Application Server
BE	Border Element
BSF	Bootstrapping Server Function
B-TID	Bootstrapping Transaction Identifier
CSCF	Call Session Control Function
DSL	Digital Subscriber Loop
ENI	ETS National Implementation
ETS	Emergency Telecommunications Service
FE	Functional Entities
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GUSS	GBA User Security Settings
HSS	Home Subscriber System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Security
IAD	Integrated Access Device
I-CSCF	Interrogating Call Session Control Function
ID-FF	Identity Federation Framework
IdM	Identity Management
IdP	Identity Provider
ID-WSF	Identity Web Services Framework
IMS	IP Multimedia Service
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IWF	InterWorking Function
LUAD	Liberty enabled User Agent or Device
MAC	Media Access Control
MS	Media Server
NACF	Network Attachment Control Function
NAF	Network Application Function
NAP	Network Access Point
NGN	Next Generation Network
NNI	Network-to-Network Interface
OAM&P	Operations, Administration, Maintenance and Provisioning
OSI	Open System Interconnection

P-CSCF	Proxy Call Session Control Function
PES	PSTN/ISDN Emulation Service
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PII	Personally Identifiable Information
PSK	Pre-shared Keys
RACF	Resource and Admission Control Function
RBAC	Role-Based Access Control
RP	Relying Party
RPH	Resource-Priority Header
RSVP	Resource Reservation Protocol
SAML	Security Assertion Markup Language
SASL	Simple Authentication and Security Layer
SBC	Session Border Controller
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SIM	Subscriber Identification Module
SLA	Service Level Agreement
SLF	Subscriber Locator Function
SOAP	Simple Object Access Protocol
SP	Service Provider
SSOS	Single-Sign-On Service
TDR	Telecommunication for Disaster Relief
TE	Terminal Equipment
TE-BE	Terminal Equipment – Border Element
TLS	Transport Layer Security
UAI	User Authentication Interface
UE	User Equipment
UNI	User-to-Network Interface
URL	Uniform Resource Locator
WS	Web Server
XML	eXtensible Markup Language

5 Reference models

5.1 ITU-T X.811 authentication framework

This Recommendation makes use of the basic concepts of authentication described in [ITU-T X.811] as summarized below.

5.1.1 Basic concepts of authentication

Authentication provides assurance of the claimed identity of an entity. Authentication is meaningful only in the context of a relationship between a principal and a verifier. Two important cases are:

- the principal is represented by a claimant which has a specific communications relationship with the verifier (entity authentication); and
- the principal is the source of a data item available to the verifier (data origin authentication).

Entity authentication provides corroboration of the identity of a principal, within the context of a communication relationship. The principal's authenticated identity is assured only when an authentication service is invoked.

NOTE 1 – When using data origin authentication, it is also necessary to have adequate assurance that the data has not been modified. This may be accomplished by using an integrity service, for example:

- by using environments in which data cannot be altered;
- by verifying that the data received matches a digital fingerprint of the data sent;
- by using a digital signature mechanism; or
- by using a symmetric cryptographic algorithm.

NOTE 2 – The term "communications relationship" used in defining entity authentication may be interpreted in a broad way and could refer, for example, to an OSI connection, inter-process communication, or interaction between a user and a terminal.

5.1.2 Identifiers

A principal is an entity whose identity can be authenticated. A principal has one or more distinguishing identifiers associated with it. Authentication services are used by an entity to verify purported identities of principals. A principal's identity which has been so verified is called an authenticated identity. Similarly, a principal whose identity has been verified is called an authenticated entity.

Examples of principals that can be identified and hence authenticated are, but are not limited to:

- human users;
- NGN providers;
- processes;
- real open systems;
- OSI layer entities;
- enterprises, and
- flows in the bearer, signalling and management traffic.

Distinguishing identifiers are used to unambiguously claim an identity within a given security domain. Distinguishing identifiers distinguish a principal from others in the same domain, in one of two ways:

- 1) by virtue of membership in a group of entities considered equivalent for purposes of authentication (in this case the entire group is considered to be one principal and has one distinguishing identifier); or
- 2) by identifying one and only one entity.

When authentication takes place between different security domains, a distinguishing identifier may not be sufficient to unambiguously identify an entity, as different security domain authorities may use the same distinguishing identifiers. In this case, distinguishing identifiers have to be used in conjunction with a security domain identifier in order to provide an unambiguous identifier for the entity.

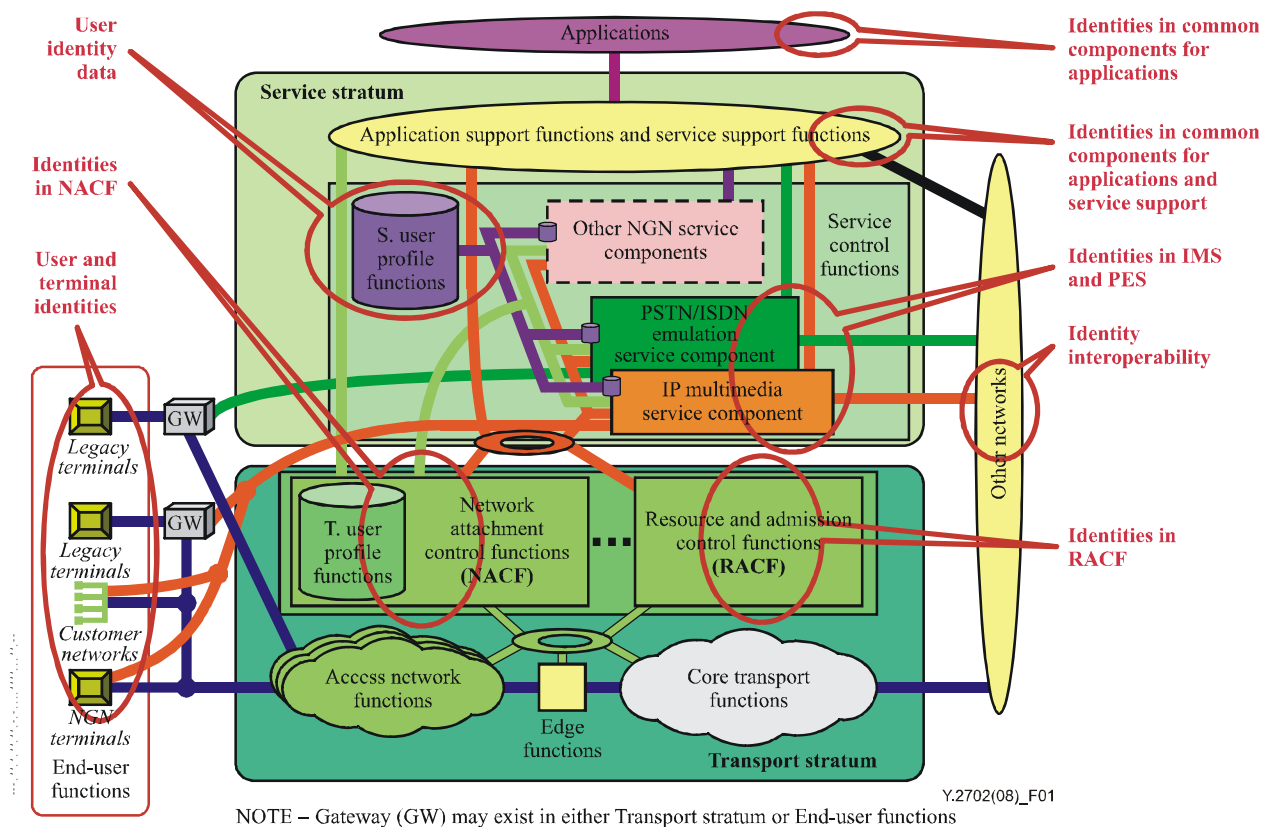


Figure 1 – Example NGN identifiers

Identifiers used to identify a principal or entity might be used by the components and functional elements in the different stratum and layers of the NGN. Figure 1 shows example identifiers for NGN based on Figure 8 (NGN Components) of [ITU-T Y.2012].

Examples of typical distinguishing identifiers are:

- directory names;
- network addresses;
- AP-titles and AE-titles;
- object identifiers;
- names of persons (unambiguous within the context of the domain);
- quintuples that contain:
 - source IP address;
 - destination IP address;
 - source port number;
 - destination port number; and
 - protocol number.

5.1.3 Authentication entities

The term "claimant" is used to describe the entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in an authentication exchange on behalf of a principal.

The term "verifier" is used to describe the entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in an authentication exchange to request verification of a claimed identity.

An entity involved in mutual authentication will assume both claimant and verifier roles.

The term "trusted third party" is used to describe a security authority or its agent, trusted by other entities with respect to security-related activities. In the context of this Recommendation, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

NOTE – A claimant or verifier may span multiple functional components, possibly residing in different open systems.

5.1.4 Authentication information

The types of authentication information described in this standard are:

- exchange authentication information (exchange AI);
- claim authentication information (claim AI);
- verification authentication information (verification AI).

The term "authentication exchange" is used to describe a sequence of one or more transfers of exchange AI for the purposes of performing an authentication.

Figure 2 illustrates the relationship among a claimant, a verifier, and a trusted third party. Figure 2 also illustrates the three types of authentication information that may make up an authentication exchange

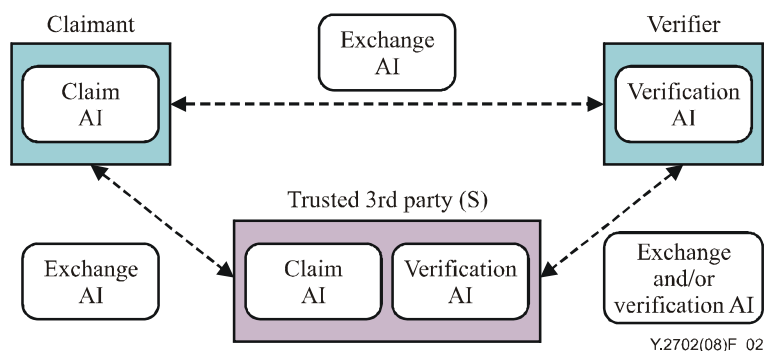


Figure 2 – Relationship between claimant, verifier and trusted third party

In some cases, in order to generate exchange AI, a claimant may need to interact with a trusted third party. Similarly, in order to verify exchange AI, a verifier may need to interact with a trusted third party. In these cases the trusted third party may hold verification AI related to a principal.

It is also possible that a trusted third party is used in the transfer of exchange AI. Depending on the exchange, the third party may take on the role of a claimant relative to the verifier.

The entities may also need to hold authentication information to be used in authenticating the trusted third party.

5.1.5 Multi-factor authentication

Multi-factor authentication involves validating the authenticity of the identity of a principal by verifying multiple identifiers and attributes associated with the principal. Generally, multifactor authentication can be organized based on the following grouping of authentication attributes:

- 1) something you are (e.g., physical or behavioural characteristics of an end user or customer's characteristic or attribute that is being compared such as typing patterns, voice recognition);

- 2) something you have (e.g., a driver's licence, or a security token);
- 3) something you know (e.g., a password, pin number, security image).

The most common example of a single-factor authentication key is a password (something you know). Sometimes passwords, by themselves, do not provide sufficient confidence in the identity of an entity, and stronger forms of authentication, involving other authentication keys, would be required for access to certain NGN resources, applications and services. This would depend on the risks associated with the likelihood of unauthorized entities obtain access to the NGN resources, applications and services.

The authentication factors and keys should be selected based on the risks to be addressed. Specifically the impacts of unauthorized entities obtaining access to NGN resources, applications and services would have to be accessed to determine the required authentication. Example electronic authentication keys are:

- passwords,
- hardware tokens,
- software tokens,
- one-time password device tokens.

The use of passwords for authentication is widely established. The "password" is a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings or images that the subscriber memorizes and must identify when presented along with other similar images. However, password systems are susceptible to many attacks. Additional protections for the communication channel can be used to protect the password, but this still does not prevent all attacks.

Hardware tokens are specialized hardware devices that protect secrets (normally cryptographic keys) and perform cryptographic operations. Authentication is accomplished by proving possession of the device and control of the key. The cryptographic operations support authentication of both parties and the protection of the communication channel used for the authentication exchange.

Software tokens are essentially software implementations of hardware tokens and share many of the advantages of hardware tokens (e.g., a cryptographic key that is typically stored on disk or some other media). The soft token key can be encrypted under a key derived from some activation data. Typically, the activation data is a password known only to the user, so a password is required to activate the token. Authentication is accomplished by proving possession and control of the key. As with hardware tokens, software tokens support authentication of both parties and protection of the communication channel used for the authentication exchange.

One-time password device token is a personal hardware device that generates "one time" passwords for use in authentication. One-time password systems rely on a series of passwords generated using special algorithms. Each password of the series is called a one-time password as it is distinct from the others generated and can only be used once. A wide variety of one-time password systems exist that provide varying protection against attacks.

5.2 Authentication threats

Authentication factors and keys can be attacked as follows:

- 1) "Something you are" – replicating the customer's characteristic or attribute that is being compared (for example, fingerprints, typing patterns).
- 2) "Something you have" – obtaining or copying what the customer has.
- 3) "Something you know" – discovering what the customer knows.

In general, authentication threats can be divided into threats that involve attacks against the authentication protocol, and other attacks that may reveal either token values, or compromise confidential information.

Using multiple authentication factors improves security because multiple methods must be subverted. Using a hardware device (something you have) that is not easily copied also reduces the scope of an attack, as it is expected that the owner will notice the loss of the device. Authentication keys based on software or hardware tokens may be combined with activation data (e.g., a password) to implement two-factor authentication so that the authentication is not reliant on possession of the token alone.

A customer may subvert the authentication system by deliberately divulging their one-factor authentication key to an accomplice and then denying it later, with the aim of repudiating subsequent successful authentications. The use of multiple authentication factors makes such a denial less credible and may deter such attacks.

5.2.1 Authentication protocol threats

Example authentication protocol threats include:

- 1) Eavesdroppers:
 - eavesdroppers observing authentication protocol message exchanges for later analysis;
 - eavesdroppers generally attempt to obtain tokens to pose as claimants.
- 2) Impostors:
 - impostor claimants posing as subscribers to the verifiers to test guessed tokens or obtain other information about a specific subscriber;
 - impostor verifiers posing as verifiers to legitimate subscriber claimants to obtain tokens that can then be used to impersonate subscribers to legitimate verifiers;
 - impostor relying parties posing as the relying party system to verifiers to obtain sensitive user information.
- 3) Hijackers:
 - hijackers who take over an authenticated session and pose as subscribers to relying parties to obtain sensitive information or input invalid information;
 - hijackers who take over an authenticated session and pose as relying parties to verifiers to obtain sensitive information or output invalid information.

These attacks may be mitigated in the following ways:

- Requiring an element of freshness for each authentication to counters replay attacks.
- Eavesdropper and session hijacking attacks may be countered by using cryptography to protect the signalling channel (channel encryption) used for the authentication exchange (for example, TLS in anonymous mode).
- Man-in-the-middle and verifier impersonation attacks can be resisted, in a limited way, by using similar protections as with eavesdropper and session hijacking attacks. Combining the encryption with additional cryptographic techniques improves protection against these attacks (for example, using a mutual handshake exchange based around cryptography – such as TLS in authenticated mode – with cryptographic keys being held by the customer and the verifier achieves 'strong' mutual authentication).
- Encryption provides only limited resistance to man-in-the-middle and verifier impersonation attacks, as security of the exchange can be compromised without breaking the encryption. For example, a customer may be deceived into accepting an authentication exchange as being from the verifier when it is not. Cryptographic-based mutual authentication techniques can be used between the customer and the verifier.

5.2.2 Authentication token threats

If an attacker can gain control of a token, they will be able to masquerade as the token's owner. Threats to tokens can be categorized into attacks on authentication keys as follows:

- Something you have may be stolen from the owner or cloned by the attacker. For example, an attacker who gains access to the owner's computer might copy a software token. A hardware token might be stolen or duplicated.
- Something you know may be disclosed to an attacker. The attacker might guess a password or PIN. Where the token is a shared secret, the attacker could gain access to the verifier and obtain the secret value. An attacker may install malicious software (e.g., a keyboard logger) to capture this information. In addition, an attacker may determine the secret through off-line attacks on network traffic from an authentication attempt.
- Something you are may be replicated. An attacker may obtain a copy of the token owner's identification and construct a replica.

There are several strategies to mitigate these threats:

- Multiple factors raise the threshold for attacks. If an attacker needs to steal a cryptographic token and guess a password, the work factor may be too high.
- Physical security mechanisms may be employed to protect a stolen token from duplication. Physical security mechanisms can provide tamper evidence, detection, and response.
- Complex passwords may reduce the likelihood of a successful guessing attack. By requiring use of long passwords that do not appear in common dictionaries, attackers may be forced to try every possible password.
- System and network security controls may be employed to prevent an attacker from gaining access to a system or installing malicious software.

5.2.3 Other authentication threats

Attacks are not limited to the authentication protocol itself. Other attacks include:

- malicious code attacks that may compromise authentication tokens;
- intrusion attacks that obtain credentials or tokens by penetrating the subscriber/claimant, certification authority or verifier system;
- insider threats that may compromise authentication tokens;
- out-of-band attacks that obtain tokens in some other manner, such as social engineering to get a subscriber to reveal his password to the attacker, or "shoulder-surfing";
- attacks that fool claimants into using an insecure protocol, when they think that they are using a secure protocol, or trick them into overriding security controls (for example, by accepting server certificates that cannot be validated);
- intentional repudiation by subscribers who deliberately compromise their tokens.

Education and advice for the customer are methods to combat malicious code and social engineering attacks. Auditing and anomaly detection are commonly used to counter customer fraud attacks. Using multiple authentication keys can deter customer fraud attacks. Insider attacks may be countered through personnel vetting, auditing, and (where appropriate) using separation of duties and dual control.

5.3 Authentication assurance

To protect NGN resources, applications and services, NGN providers must determine the required level of assurance in the authentication used for network access and application/service transactions.

Each NGN provider should establish and implement a process for authentication assurance. The authentication assurance process will involve a method to categorize confidence (i.e., confidence in the identity information electronically presented to a service provider) in the authentication mechanisms and the information provided for authentication.

The authentication assurance process will establish and use relative and discrete levels of assurance to quantify confidence in the authentication process. For example, "n" levels of authentication assurance could be used. Level 0 could represent the lowest assurance level and level "n" the highest. The "n" levels will be used to define the level of assurance in terms of the likely consequence (e.g., the nature of the potential impacts) of an authentication error based on the assumption that all identifiers used in authentication are not equal or necessarily have the same authentication value.

The following is an example authentication assurance method:

Example authentication method

Assurance level	Relative confidence
Level 0	No confidence in the asserted identity validity (e.g., use of access list controls)
Level 1	Some confidence in the asserted identity validity
Level 2	High confidence in the asserted identity validity
—	—
Level n	Highest degree of confidence in the asserted identity validity

The NGN provider must assess the potential risks associated with the consequences of authentication errors or to determine the appropriate level of assurance in an entity (e.g., end user's) identity. Authentication errors with potentially worse consequences will require higher levels of assurance.

The risk from an authentication error is a function of two factors:

- a) potential harm or impact;
- b) the likelihood of such harm or impact.

Categories of harm and impact, not limiting, include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- NGN provider or customer liability
- Harm to NGN provider infrastructure, resource, applications, services or public interests
- Harm to public and government interest (e.g., critical communications such as ETS and TDR)
- Unauthorized release of sensitive information
- Harm to personal safety services
- Civil or criminal violations

5.4 Authorization and privilege management

Authentication on its own is not sufficient in determining what the authenticated entity is authorized to do once access is granted. Authentication must be combined with authorization and privilege management mechanisms and approaches to provide access control to NGN services and resources. For example, assignment of roles and privileges to end-users/subscribers to control access to services and applications and to management interfaces to manage their subscription and profiles. Another example is role-based access control (RBAC) for control of OAM&P access.

Authorization or privilege can be viewed as an attribute of an entity identity. Depending on the security policy, the authorization privileges on an entity can be validated through authentication.

5.5 End-to-end reference architectural model

This clause describes the end-to-end reference model used to organize and group the authentication requirements in this Recommendation. The reference model depicts:

- 1) Authentication and authorization of user for network access (e.g., authentication and authorization of an end user device, a home network gateway, or an enterprise gateway to obtain access or attachment to the network).
- 2) Service provider authentication and authorization of user for access to service/application (e.g., authentication and authorization of a user, a device or a combined user/device where the authentication and authorization apply to NGN service/application access).
- 3) Service provider authentication and authorization of user for access to specific service/application (e.g., ETS and TDR specific authentication and authorization¹).
- 4) User authentication and authorization of network (e.g., user authenticating the identity of the connected NGN network or of the service provider).
- 5) User peer-to-peer authentication and authorization (e.g., authentication and authorization of the called user (or terminating entity), authentication and authorization of the originating entity, or data origin authentication as network functions).
- 6) Mutual network authentication and authorization (e.g., authentication and authorization across NNI interface at the transport level, or service/application level).
- 7) Authentication and authorization of service/application provider.
- 8) Use of 3rd party authentication service.

Figure 3 illustrates the authentication reference points outlined above.

In this Recommendation, the use of the term "user" is not restricted to a person. A user could be a person, groups, companies, or juridical entities.

¹ ETS authentication may involve additional requirements beyond the basic requirements.

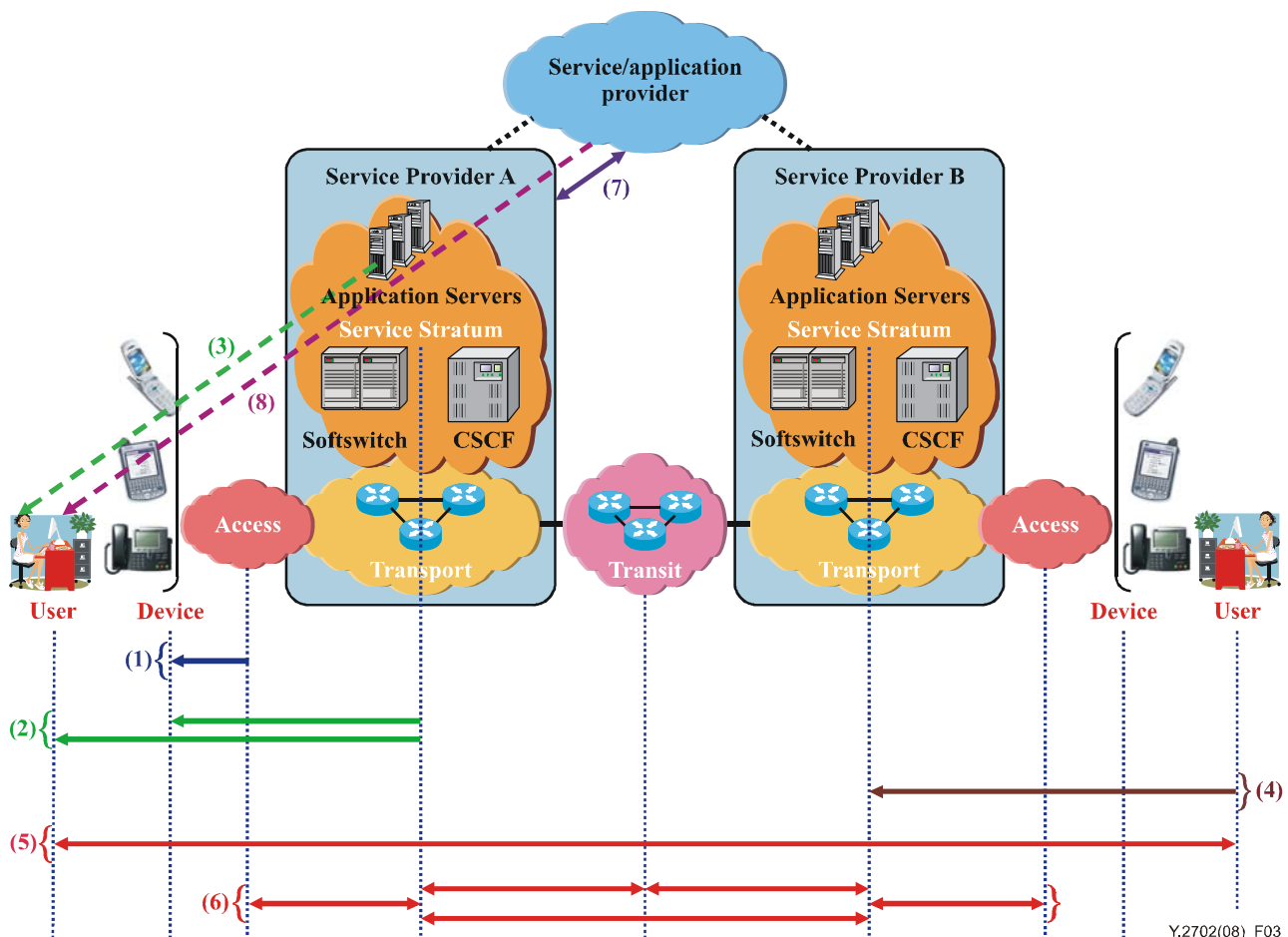


Figure 3 – End-to-end reference architectural model

As shown in Figure 3, authentication and authorization occurs both at the transport level and the service application level. In addition, there may be a binding or bundling of authentication that may occur. An example is when the service provider may bind/bundle the authentication of the user and the user's device in order to provide higher level of authentication assurance. For the most part horizontal authentication is achieved on a hop by hop basis. The main exception to this is user to user authentication, which is end to end. With exception of the user authenticating and authorizing the network, the relationships require mutual authentication.

5.6 Relationship with NGN architecture specified in [ITU-T Y.2012]

This clause describes relationship between the reference model described in this Recommendation and the functional architectural model described in [ITU-T Y.2012]. Specifically, highlighting:

- The peer authentication relationship in Figure 1 of [ITU-T Y.2012], "NGN architecture overview".
- The functional elements in Figure 1 of [ITU-T Y.2012] intended to perform authentication functions.
- The functional elements in Figure 1 of [ITU-T Y.2012] intended to perform identity management, correlations and binding.
- The functional elements in Figure 1 of [ITU-T Y.2012] intended to enforce access control based on authentication denial.