ATIS-1000030.2008(R2013)

Authentication and Authorization Requirements for Next Generation Network (NGN)

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle – from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000030.2008(R2013), *Authentication and Authorization Requirements for Next Generation Network (NGN)*

Is an American National Standard developed by the **Signaling, Architecture, and Control (SAC)** Subcommittee under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

(R2013)

ATIS-1000030.2008

American National Standard for Telecommunications

Authentication and Authorization Requirements for Next Generation Network (NGN)

Alliance for Telecommunications Industry Solutions

Approved November 20, 2008

American National Standards Institute, Inc.

Abstract

This standard specifies authentication and authorization requirements for Next Generation Network (NGN).

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PTSC which is responsible for the development of this Standard, had the following members:

J. Zebarth, PTSC Chair (Nortel)

M. Dolly, PTSC Vice-Chair (AT&T)

R. Singh, Technical Editor (Telcordia)

M. Dolly, Technical Editor (AT&T)

C. Underkoffler, ATIS Chief Editor

The Signalling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

American National Standard for Telecommunications –

Authentication and Authorization Requirements for Next Generation Network (NGN)

1 Scope

This standard provides authentication and authorization requirements for Next Generation Network (NGN) based on ATIS-1000018, *ATIS NGN Architecture* [ATIS-1000018] and Recommendation Y.2012, Functional Requirements and Architecture of the NGN Release 1 [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. This standard is based on and is aligned with ITU-T Recommendation Y.2702, *Authentication and Authorization Requirements for NGN Release 1* [Y.2702]. The scope of this standard 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 an 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 standard also provides reference models for NGN authentication and authorization.

Notes:

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.

2. In this standard, 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.

3. Authentication of an entity is not intended to indicate positive validation of a person.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

2.1 ATIS References[1]

[ATIS-1000018] ATIS-1000018, *NGN Architecture*.

[ATIS-1000029.2008] ATIS-1000029.2008, *NGN Security Requirements*.

2.2 ITU References[2]

[Y.2012] ITU-T *Recommendation Y.2012, Functional Requirements and Architecture of the NGN Release 1*.

[Y.2201] ITU-T Recommendation Y.2201, *NGN Release 1 Requirements*.

[Y.2701] ITU-T Recommendation Y.2701, *Security Requirements for NGN Release 1*.

[Y.2702] ITU-T Recommendation Y.2702, *Authentication and Authorization Requirements for NGN Release 1*.

[X.800] ITU-T Recommendation X.800, *Security Architecture for Open Systems Interconnection*.

[X.805] ITU-T Recommendation X.805, *Security Architecture for Systems Providing End-to-End Communications*.

[X.810] ITU-T recommendation X.810, *Information Technology – Open System Interconnection – Security Framework for Open Systems: Overview*.

[X.811] ITU-T Recommendation X.811, *Information Technology – Open System Interconnection – Security Frameworks for Open System: Authentication Framework*.

---

1 This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

2 This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

3 Definitions

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.

3.1 ITU-T Recommendation X.800 Definitions

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

Authentication information: Information used to establish the validity of a claimed identity.

Authorization: The granting of rights, which includes the granting of access based on access rights.

Credential: Data that is transferred to establish the claimed identity of an entity.

Data origin authentication: The corroboration that the source of data received is as claimed.

Peer-entity authentication: The corroboration that a peer entity in an association is the one claimed.

3.2 ITU-T Recommendation X.810 Definitions

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

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.

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 ITU-T Recommendation X.811 Definitions

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

Asymmetric authentication method: A method of authentication, in which not all authentication information is shared by both entities.

Authenticated identity: A distinguishing identifier of a principal that has been assured through authentication.

Authentication: The provision of assurance of the claimed identity of an entity.

Authentication certificate: A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.

Authentication exchange: A sequence of one or more transfers of exchange authentication information (AI) for the purposes of performing an authentication.

Authentication information (AI): Information used for authentication purposes.

Authentication initiator: The entity that starts an authentication exchange.

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.

Claim authentication information (claim AI): Information used by a claimant to generate exchange AI needed to authenticate a principal.

Exchange authentication information (exchange AI): Information exchanged between a claimant and a verifier during the process of authenticating a principal.

Principal: An entity whose identity can be authenticated.

Symmetric authentication method: A method of authentication in which both entities share common authentication information.

Verification authentication information (verification AI): Information used by a verifier to verify an identity claimed through exchange AI.

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 ATIS-1000029.2008 Definitions

Terminal equipment border element: Border element providing security functions between customer premises equipment and service provider network.

Border element: Network element providing functions connecting different security and administrative domains.

Corporate Network: A private network that supports multiple users and may be in multiple locations (e.g, an enterprise, a campus).

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.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms.

3GPP	3rd Generation Partnership Project
ACL	Access Control List
AI	Authentication Information
ANI	Application-to-Network Interface
AS	Application Server
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 Telecommunication Service
FE	Functional Entities
GAA	Generic Authentication Architecture
GBA	Generic Bootstrap Architecture
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
ITU-T	International Telecommunication Union – Telecommunication
IWF	Interworking Function
LAP	Liberty Alliance Project
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
OASIS	Organization for the Advancement of Structured Information Standards
OSI	Open System Interconnection
P-CSCF	Proxy Call Session Control Function
PES	PSTN/ISDN Evolution Service
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPII	Protection of Personal 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 Disaster Relief
TE	Terminal Equipment
TE-BE	Terminal Equipment – Border Element
TLS	Transport Layer Security
UAI	User Application 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 document makes use of the basic concepts of authentication described in Recommendation X.811, Information Technology – Open System Interconnection – Security Frameworks for Open System: Authentication Framework [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.

Notes:

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.
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 unambiguous 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.

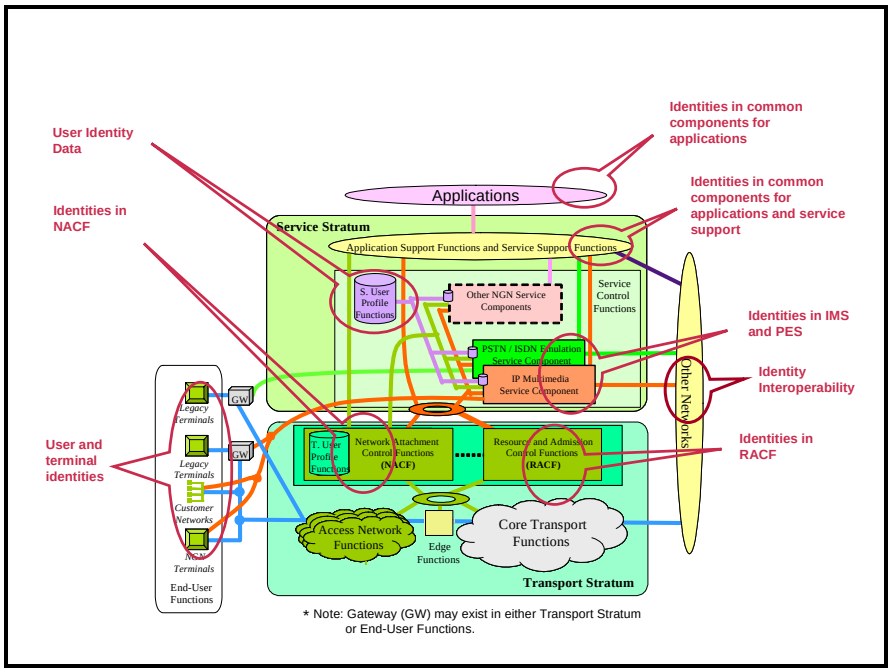


Figure 1 – Example NGN Identifiers

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 deployments.

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 document, 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 (AI) 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.

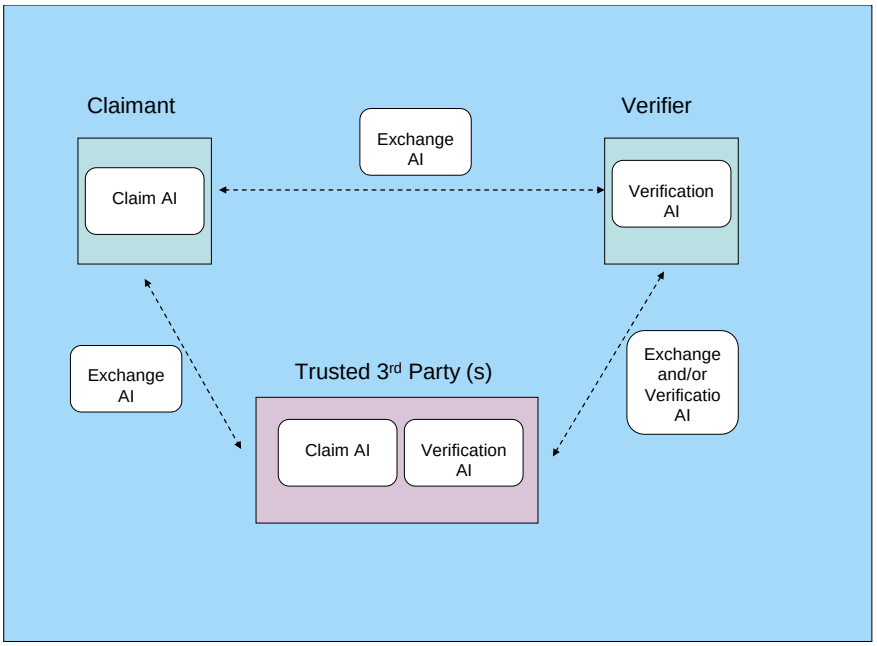


Figure 2– Relationship Between Claimant, Verifier and Trusted Third Party

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 Claimant and Verifier 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 a 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 license, 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 obtaining 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 assessed 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 specialised 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.

A 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 attempting 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 don't 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:

Table 1 - Example Authentication 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

NIST Special Report 800-63 [B31] defines four levels 4 levels for authentication assurance and registration and identity proofing (see Appendix C). NGN providers may choose to adopt the recommendations in [B31].

The NGN provider must access 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 an attribute of an entity identity. Depending on the security policy, the authorization privileges on an entity can be validated though 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 standard. 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 an 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 authorization[3])
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

[3] ETS Authentication may involve additional requirements beyond the basic requirements.

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 standard, the use of the term “user” is not restricted to a person. A user could be a person, groups, companies, or juridical entities.

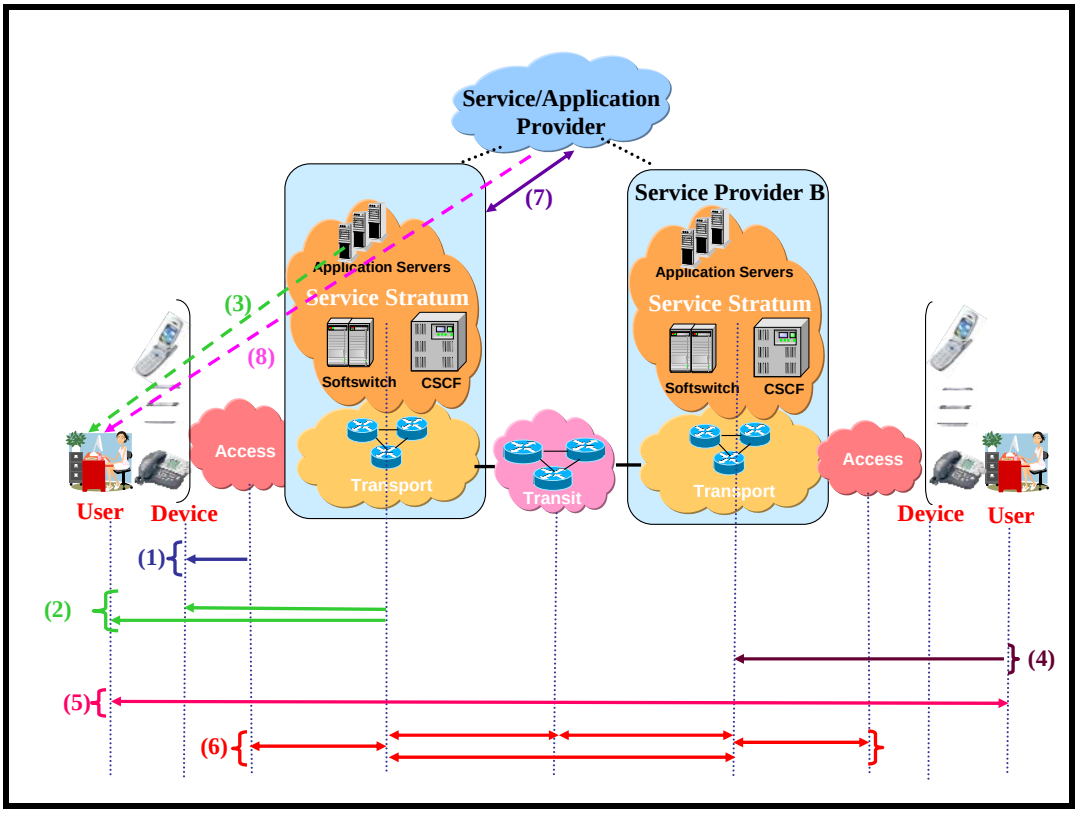


Figure 3 - End-to-end Reference Architectural Model

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 ATIS-1000018

This section describes relationship between the reference model described in this standard and the functional architectural model described in [ATIS-1000018]. Specifically, highlighting:

- The peer authentication relationship in [ATIS-1000018] Figure 1, "NGN architecture overview".
- The functional elements in [ATIS-1000018] Figure 1 intended to perform authentication functions.
- The functional elements in [ATIS-1000018] Figure 1 intended to perform identity management, correlations and binding.
- The functional elements in [ATIS-1000018] Figure 1 intended to enforce access control based on authentication denial.

Figure 4 uses [ATIS-1000018] Figure 1 to illustrate the peering authentication relationships identified in Section 5.5 of this document. The peering authentication relationships are shown with the black double-headed arrows. Not shown is (5), user peer-to-peer authentication and authorization. Note that even when the applications to the user are provided by the NGN provider (i.e., no ANI), there is still an authentication relationship between the end-user and application, and the Service Stratum and the application.

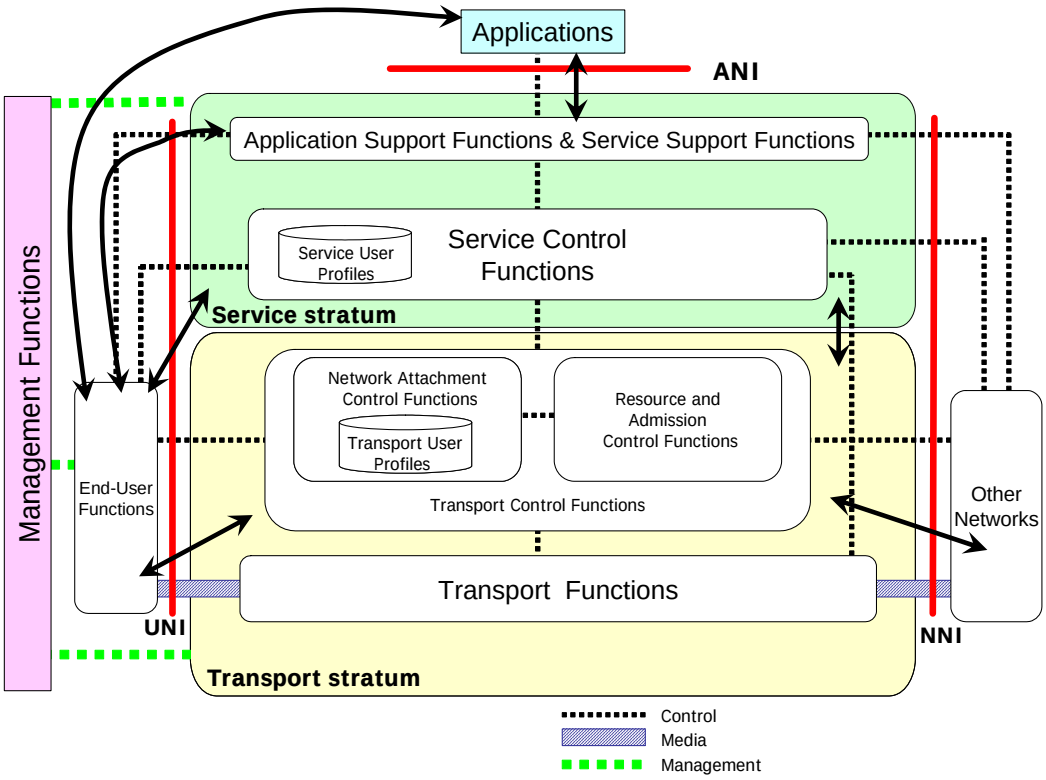


Figure 4 - Authentication Peering References

6 General Requirements

Support of the general identification, authentication and authorization requirements defined in ATIS standard, *NGN Security Requirements* [ATIS-1000029.2008] and ITU-T Recommendation Y.2201, *Requirements for NGN Release 1* [Y.2201] is required by this standard as follows:

(R-1) - The requirements defined in section 7.3.2 (Authentication) of [ATIS-1000029.2008] shall be supported.

(R-2) - The requirements defined in section 5.12 (Identification, Authentication and Authorization) of [Y.2201] shall be supported.

7 Authentication and Authorization of User for Network Access

7.1 Description

Network access authentication and authorization services and capabilities are needed to mitigate threats associated with unauthorized access. Network access authentication and authorization services are needed to verify the identities and to determine whether access should be granted to end user equipment (i.e., Terminal Equipment (TE) and Terminal Equipment – Border Element (TE-BE)) requesting network connectivity to the NGN.

General Assumptions:

a) An end user is not restricted to a person. End users could be a person, groups, companies, or juridical entities.

b) According to [ATIS-1000018], no assumptions are made about the diverse end-user interfaces and end-user networks that may be connected to the NGN access network. All categories of end-user equipment are supported in the NGN, from single-line legacy telephones to complex corporate networks. End-user equipment may be either mobile or fixed.

c) Determination of the network elements that implement the access and authorization services is not in the scope of this standard.

d) Network access and authorization functions may be provided as part of the general Network Attachment Control Function (NACF) described in [ATIS-1000018].

7.2 General Reference Model

Figure 5 shows the reference model for network access/attachment authentication and authorization consisting of the following security domains:

I. Customer Domain – Un-trusted domain containing user equipment owned and operated by the customer, for example:

    a. Legacy TE and TE-BE:

- Legacy TE represents legacy user devices connecting over narrowband access (e.g., analogue and ISDN lines). These TE obtains access to the IP network via a NGN Provider Gateway (e.g., access or media gateway).
- Legacy TE-BE represents user equipment serving as aggregate end points (e.g., enterprise and home network gateways) connecting over narrowband access (e.g., analogue and ISDN lines). These TE-BE obtains access to the IP network via NGN Provider Gateway (e.g., access or media gateway).

b. Legacy TE and TE-BE with Integrated Access Device (IAD)

- Legacy TE with IAD represents legacy user devices connecting over broadband access (e.g., xDSL or Cable). These TE obtains access to the IP network via the IAD in the customer domain.
- Legacy TE-BE represents user equipment serving as aggregate end points (e.g., enterprise and home network gateways) connecting over broadband access (e.g., xDSL and Cable). These user equipment obtain access to the IP network via the IAD in the customer domain.

c. NGN TE and TE-BE:

- NGN TE represents user devices in the customer domain with IP capabilities to support direct connectivity to the IP network (e.g., using xDSLs and Cable broadband access).
- NGN TE-BE represents user equipment serving as aggregate end points (e.g., enterprise and home network gateways) with IP capabilities to support direct connectivity to the IP network.

II. Access NGN Provider Domain: Access network hosted by an NGN Provider (e.g., narrowband, xDSL and Cable). The Access NGN Provider may or may not be the same as the Service NGN Provider. Trust relations between the NGN Providers are governed by Service Level Agreements (SLAs).

III. Service NGN Provider Domain: The Service NGN Provider offers NGN application services to its subscribers. Trust relations between NGN Providers are governed by SLAs.

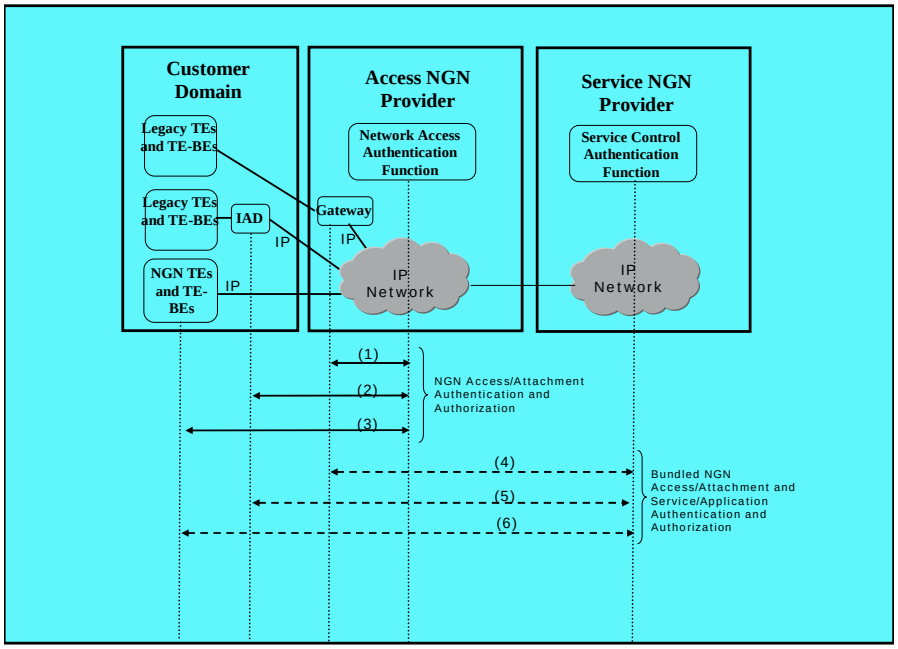


Figure 5 – Reference Model for Network Access/Attachment Authentication and Authorization

Figure 5 shows relationships for network access/attachment identification, authentication and authorization:

(a) Device NGN Access/Attachment Authentication and Authorization – Services and capability to identify, authenticate and authorize user devices access or attachment to the access IP network.

(1). This information flow represent services and capabilities to identify, authenticate and authorized legacy TE and TE-BE for access/attachment to the access IP network. The information flow is between the Gateway (Claimant) in the Access NGN Domain terminating the legacy TE and TE-BE in the Customer Domain and a network element (e.g., Network Access Point) in the Access NGN Domain providing the NGN access/attachment authentication and authorization functions. The NGN access/attachment authentication and authorization functions (Verifier) may to be part of the general NACF described in [ATIS-1000018]. However, where this function is implemented is implementation dependent.

(2). This information flow represents services and capabilities to identify, authenticate and authorize legacy TE and TE-BE with IAD in the Customer Domain for access/attachment to the access IP network. The information flow is between the IAD (Claimant) in the Customer Domain and a network element (e.g., Network Access Point) in the Access NGN Domain providing the NGN access/attachment authentication and authorization. The NGN access/attachment authentication and authorization function (Verifier) may be part of the general NACF described in [ATIS-1000018]. However, where this function is implemented is implementation dependent.

(3). This information flow represents services and capabilities to identify, authenticate and authorize NGN TE and TE-BE with IP capabilities in the Customer Domain for access/attachment to the IP network. The information flow is between the NGN TE or TE-BE (Claimant) in the Customer Domain and a network element (e.g., Network

Access Point) in the Access NGN Domain providing the NGN access/attachment authentication and authorization. The NGN access/attachment authentication and authorization function (Verifier) may to be part of the general NACF described in [ATIS-1000018]. However, where this function is implemented is implementation dependent.

(b) Bundled Device NGN Access/Attachment and Service/Application Authentication and Authorization – Services and capabilities to bundle the Access NGN Provider authentication of the user device with the Service NGN Provider authentication and authorization of the user:

(4). This information flow represents services and capabilities for the Service NGN Provider to implicitly identify and authorize legacy TE and TE-BE. The information flow is between a Gateway (Claimant) in the Access Network Domain and the NGN Provider Domain (Verifier).

(5). This information flow represents services and capabilities for the Service NGN Provider to implicitly identify and authorize legacy TE and TE-BE with IAD. The information flow is between the IAD (Claimant) in the Customer Domain and the Service NGN Provider Domain (Verifier).

(6). This information flow represents services and capabilities for the Service NGN Provider to directly identify, authenticate and authorize NGN TE and TE-BE in the Customer Domain. The information flow is between the NGN TE and TE-BE (Claimant) in the Customer Domain and the Service NGN Provider Domain (Verifier).

Reference Model for Nomadicity

Figure 6 shows the reference model for nomadicity. This reference model is similar to the general reference model, except that in this scenario there is a Visited NGN and Home NGN to take into consideration.

I. Visited NGN Domain: NGN hosted by a Visited NGN Provider. Provides visited network functions for other NGN Provider (i.e., Home Network Provider). Trust relationships are governed by SLAs. The visited network may offer NGN services and may have its' own subscribers.

II. Home NGN Domain: NGN hosted by the Home NGN Provider. The Home NGN Provider offers NGN services to its' subscribers. Trust relationships are governed by SLAs.

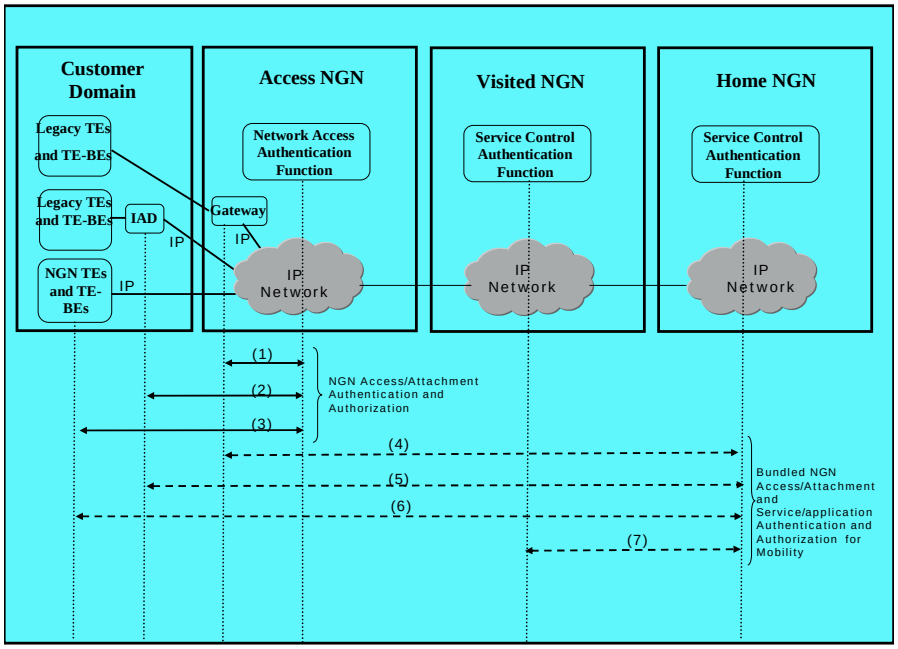


Figure 6 – Reference Model for Nomadicity

The reference model shows information flows between the different domains for bundling the user device authentication and authorization and authentication and authorization of the user for nomadicity. The information flows represents services and capabilities to bundle the Visited NGN Provider authentication and authorization of the user device with the Home NGN Provider authentication and authorization of the user for nomadicity:

(1) – (6). These information flows are the same flows as described for the single service provider scenario in Figure 5.

(7).This information flow represents services and capabilities for a Visited NGN Provider and a Home NGN Provider to exchange identification, authentication and authorization information in support of nomadicity.

7.3 Requirements

7.3.1 General Requirements

The following are general requirements for device network access/attachment identification, authentication and authorization:

(R-3) - It is required that the NGN be able to uniquely identify end user/subscriber devices (e.g., TE and TE-BE) based on NGN provider policy.

(R-4) - It is required that the NGN be capable of identifying, authenticating, and authorizing attachment of the TE and TE-BE at Network Access Points (NAPs).

(R-5) - It is required that network access will only be granted to authorized TE and TE-BE.

(R-6) - For multi-network arrangements, each administrative domain (e.g., Access NGN Provider, Visited NGN Provider, and Home NGN Provider) is required to enforce policies (e.g., SLAs) for identification, authentication, and authorization of TE and TE-BE network access/attachment.

(R-7) - The NGN is required to support capabilities to protect authentication and authorization information (e.g., user profile, subscription information, identity patterns) against unauthorized access, manipulation and corruption.

(R-8) - The NGN is required to support capabilities to provide confidentiality and integrity of protection of messages and information exchanges used for authentication and authorization.

(R-9) - The NGN is required to support capabilities for protection against attacks (e.g., message replay and denial of service attacks) on authentication and authorization functions and capabilities.

(R-10) - It is required that the NGN be capable of detecting and logging unauthorized access attempts (e.g., A system configurable threshold may be set for the number of unauthorized access attempts beyond which an alarm will be generated, logged, and reported to a management system).

7.3.2 Legacy TE and TE-BE

NAPs supporting network access for legacy TE and TE-BE need to support capabilities to identify, authenticate and authorize such access.

(R-11) - Network Access Points (NAPs) supporting legacy TE and TE-BE are required to support capabilities to uniquely identify the fixed line for the attachment or connectivity to the NGN. A Layer 2 address may be used to identify a fixed line (e.g., MAC or link layer address). This function may be provided as part of the general NACF described in [ATIS-1000018].

(R-12) - NAPs supporting legacy TE and TE-BE are required to support capabilities to authenticate and authorize the fixed line for attachment or connectivity to the NGN. Access Control Lists (ACLs) and transport stratum subscription/user profile information may be used to authorize fixed line access to the NGN. These functions may be provided as part of the general NACF described in [ATIS-100018].

(R-13) - NAPs supporting legacy TE and TE-BE are required to support capability to link and bind the identity of a fixed line with the IP address used for NGN access connectivity. This function may be provided as part of the general NACF described in [ATIS-1000018].

7.3.3 Legacy TE and TE-BE with IAD

NAPs supporting network access for legacy TE and TE-BE with IAD in the Customer Domain need to support capabilities to identify, authenticate and authorize such access.

(R-14) - NAPs supporting legacy TE and TE-BE with IAD in the customer domain are required to support capabilities to uniquely identify the fixed line and the IAD for the attachment or connectivity to the NGN. A Layer 2 address may be used to identify a fixed line (e.g., MAC or link layer address) and an IP address for the IAD.

This function may be provided as part of the general network NACF described in [ATIS-100018].

(R-15) - NAPs supporting legacy TE and TE-BE with IAD in the customer domain are required to support capabilities to authenticate and authorize the IAD for attachment or connectivity to the NGN. Only authorized IADs are allowed to obtain attachment or network connectivity to the NGN. Access Control Lists (ACLs) and transport stratum subscription/user profile information may be used to authorize IAD and fixed line access to the NGN. These functions may be provided as part of the general network NACF described in [ATIS-100018].

(R-16) - NAPs supporting legacy TE and TE-BE with IAD in the customer domain are required to support capability to link and bind the identity of a fixed line with the identity of the IAD. This function may be provided as part of the general NACF described in [ATIS-1000018].

7.3.4 NGN TE and TE-BE

NAPs supporting network access for NGN TE and TE-BE need to support capabilities to identify, authenticate and authorize such access to the NGN.

(R-17) - NAPs supporting NGN TE and TE-BE (i.e., direct IP connectivity) are required to support capabilities to uniquely identify user devices within its domain for NGN attachment and connectivity. NGN TE and TE-BE may be uniquely identified by device identities and network addresses (e.g., equipment identities, SIM cards, security token, IP addresses, etc).

(R-18) - NAPs supporting NGN TE and TE-BE (i.e., direct IP connectivity) are required to support capabilities to authenticate and authorize user devices within its domain for NGN attachment and connectivity. The authentication and authorization may be based on transport stratum subscription/user profile information. Only authorized NGN TE and TE-BE are allowed to obtain attachment or network connectivity to the NGN. These functions may be provided as part of the general NACF described in [ATIS-100018].

7.3.5 Bundled User and User Device Authentication and Authorization

Based on risk assessment, authentication and authorization of the user and the user's device combination may be needed to provide a higher level of identity assurance. NGN may support capabilities to bundle authentication functions for NGN access/attachment and access to services/applications based on transport stratum (e.g., user device and network access information) and service stratum (e.g., subscription/user profile) information.

(R-19) - It is required that capabilities to uniquely identify and bind user and user device combination be supported based on NGN provider policy.

(R-20) - It is required that capabilities to authenticate and authorize user and user device combination be supported based on NGN provider policy. Only authorized users and user devices are allowed to obtain attachment/network and access to services/applications.

7.3.6 Bundled User and User Device Authentication and Authorization for Nomadicity

Authentication and authorization of the user and the user's device combination may be supported to provide higher level of identity assurance for nomadicity. Capabilities for exchanging and sharing identification, authentication and authorization information (e.g., user profiles information) among the different administrative domains (i.e., Access NGN Provider, Visited NGN Provider, and Home NGN Provider) for IdM may be supported (see in Section 8.2.2).

(R-21) - It is required that capabilities to uniquely identify user and user device combination for nomadicity be supported based on NGN provider policy.

(R-22) - It is required that capabilities to authenticate and authorize user and user device combination for nomadicity be supported based on NGN provider policy. In cases where the service is independent of the user device, authentication of access information such as fixed line, location or access address may be combined with authentication of the user to provide higher assurance level.

8 Service NGN Provider Authentication and Authorization of User for Access to Service/Application

8.1 Description

Capabilities are needed to mitigate threats associated with unauthorized access to the services and features provided by a NGN Provider. Authentication and authorization services and capabilities are needed to determine whether a user is authorized to receive service or authorized to perform an action based on its privileges. Service/application authentication and authorization is viewed as a NGN Provider authentication of a user and authorization of the user to receive NGN services or to perform an action based on its privileges. Service/application authentication and authorization may involve verifying the identities and authorization of the privileges of the following:

- User
- User Device
- User and Device Combination.

Based on the NGN architecture defined in [ATIS-1000018], service/application authentication and authorization functions will be supported in the Service Stratum using subscription and user profile information.

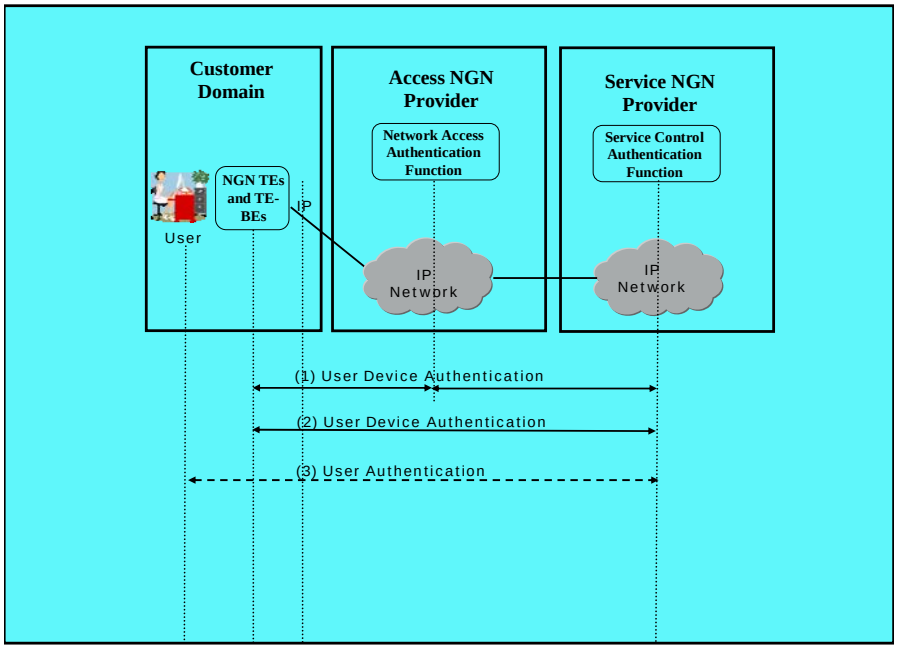


Figure 7 – Reference Model for Service/Application Authentication and Authorization

Figure 7 shows example relationships for Service/Application authorization and authorization in a multi-network provider scenario:

(1). This information flow represents the Service NGN Provider relying on the Access NGN Provider for authentication of a user device through trusts relations.

(2). This information flow represents the Service NGN Provider authentication and authorization of a user device. This case would require the user device to have special identification capabilities (e.g., SIM).

(3). This information flow represents the Service NGN Provider authentication of the user (e.g., user login and provide password or PIN).

8.2 Requirements

8.2.1 General Requirements

The following are general requirements regarding the NGN Provider authentication and authorization of the user:

(R-23) - The NGN is required to support capabilities to identify a user, a user device and a user and device combination, based on subscription and user profile information.

(R-24) - The NGN is required to support capabilities to authenticate and authorize a user, a user device, or a user and user device combination based on subscription and user profile information.

(R-25) - It is required that NGN services only be granted to authorized user, device, or user and device combination.

(R-26) - It is required that the NGN support capabilities to verify and authorize the privileges of a user (e.g., Allowing the user to perform certain actions only if its role or privilege is authorized).

(R-27) - For multi-network arrangements, each administrative domain (e.g., Access NGN Provider, Visited NGN Provider, and Home NGN Provider) is required to enforce policies (e.g., SLAs) for identification, authentication, and authorization of a user, a user device, and a user and device combination.

(R-28) - The NGN is required to support capabilities to provide confidentiality and integrity protection of messages and information exchanges used for authentication and authorization of user, user device, and user and device combination.

(R-29) - The NGN is required to support capabilities to protect against unauthorized access, manipulation and corruption of service authentication and authorization information (e.g., user profile and subscription information).

(R-30) - The NGN is required to support capabilities for protection against attacks (e.g., message replay and denial of service attacks) on service authentication and authorization functions and capabilities.

(R-31) - Capabilities to bundle access network technology specific authentication of user device with the authentication of the user are required to be supported based on NGN Provider policy.

(R-32) - It is required that the NGN be capable of detecting and logging unauthorized access attempts to NGN services or resources (e.g., A system configurable threshold may be set for the number of unauthorized access attempts beyond which an alarm will be generates, logged, and reported to a management system).

(R-33) - It is required that the NGN be capable of detecting and logging access attempts that are unauthorized (e.g., unauthorized user actions).

8.2.2 Authentication Result Sharing for IdM

NGN Provider may need to exchange authentication results among different services and/or applications within its network and externally to other NGN Providers to support Identity Management (IdM) services. This may include assertions and other information relevant to IdM such as (but not limited to):

(a) trust policy

(b) authentication method and information used for the authentication (e.g., authentication keys)

(c) assurance levels

(d) privilege management information (e.g., privileges assigned or validated).

Capabilities for secure exchange of authentication results information (e.g., assertions) and other related information as described above will allow NGN Providers to design service/application platforms with efficient and user friendly authentication and authorization features. For example, authentication result information can be shared

among systems (e.g., application servers) supporting different services and/or applications to allow a NGN Provider to support “single sign on” features and capabilities for user’s convenience. The following requirements are applicable to exchange and sharing of authentication results within a NGN Provider’s network:

(R-34) - The NGN is required to support capabilities to allow the systems and network elements (e.g., application servers) supporting different services and/or applications to exchange and share authentication result information (e.g., assertions, privilege management information, trust policy, and assurance levels) securely based on the NGN provider’s service/application platform specific designs and security policy.

(R-35) - It is required that the communication between different systems or network elements (e.g., application servers) to exchange or share authentication result information be protected against unauthorized access, observation, manipulation or corruption (e.g., confidentiality and integrity protected). This includes protection of any stored information.

In a multi network environment, NGN providers may need to exchange and share authentication results securely with each other based on SLAs. The following requirements are applicable to the exchange and sharing of authentication results between different NGN Providers:

(R-36) - It is required to support capabilities to allow NGN Providers to exchange and share authentication results securely (i.e., across NNI and ANI) based on trust relationships, policies and SLAs between the NGN providers for specific service (e.g., voice, IM/SMS, video, and gaming).

(R-37) - It is required that communication between NGN Providers to exchange and share authentication result information (i.e., across NNIs and ANIs) be protected against unauthorized access, observation, manipulation or corruption (e.g., confidentiality and integrity protected). This includes protection of any stored information. The specific security mechanisms and security practices will be based on trust relationships, policies and SLAs between the NGN Providers for specific service (e.g., voice, IM/SMS, video, and gaming).

(R-38) - It is required to support capabilities to prove authentication method and communicate information about the method(s) that were used to authenticate entities to relying parties such as:

- Method of user's identity verification
- Authentication method (use of digital certificates, signatures, security token, biometric data, SIM, etc.)
- Trust policy
- Authentication assurance levels.

Sharing of authentication information and results are subjected to the compliance with the relevant policies, such as national and regional regulations and legislations for protection of Personally Identifiable Information (PII).

(R-39) - It is required that the NGN Provider ensures the compliance with the relevant policies, such as national and regional regulations and legislations for protection of Personally Identifiable Information (PII). This includes policies formed on the following basic data protection principles:

- Binding of data to a specific purpose,
- No data sharing between applications for different purposes,
- Limitation of data to the minimum needed for a specific purpose,
- Right of persons to have control over their PII.

8.2.3 Service NGN Provider Authentication and Authorization of User for Access to Specific Service/Application

NGN Providers will have to manage user's privileges for access (including user roles and privileges to perform actions) to specific service/application such as:

- Voice services
- Streaming services
- Data and Messaging services
- Emergency Telecommunication Service (ETS) and Telecommunication Disaster Relief (TDR).

Each service may have its own assurance level requirement to validate the identity and privileges of a user, user device or user and device combination based on the risks associated with the likelihood of unauthorized entities obtaining access to the service resource. The necessary assurance level for the authentication and validation of the privileges of a user, user device or user and device combination must be established and implemented for specific service based on the NGN security policy. This would involve support and use of various authentication methods ranging from basic authentication methods using passwords and Personal Identification Numbers (PINs) and more stringent methods using authentication keys such as:

(a) Digital certificates (e.g., X.509 PKI)

(b) Security tokens (hardware and software tokens) and smart cards

(c) Behavioural characteristic data (e.g., keystroke analysis)

(d) Biometric identification data (e.g., voice recognition, fingerprint, iris, or retina identification).

Note: Authentication of an entity is not intended to indicate positive validation of a person.

The ease of use by the user should also be taken into account for authentication and authorization. This is especially true for certain types of services such as ETS and TDR. It is desirable that the authentication process should be user friendly. When considering service specific authentication and authorization, the following requirements in addition to those in the Sections 8.2.1 and 8.2.2 are applicable:

(R-40) - Authentication methods for credentials are required to be supported based on NGN Provider policy. Multi-factor authentication methods are required to be supported and used as appropriate based on NGN Provider policy for identity and privilege assurance.

(R-41) - It is required that it be possible to uniquely identify all users associated with a subscription to an application service, subject to NGN Provider policy. This includes the identification of aggregate end users whose user identities may not be provided to the NGN Provider.[4]

(R-42) - Subject to NGN Provider policy, it is required that it be possible to bind a number of individual users to the same subscription.

(R-43) - Each user/subscriber associated with an application service subscription is required to be uniquely addressable for communication purposes.

(R-44) - Subject to NGN Provider policy, it is required that it be possible for the end-user to access a service simultaneously multiple times and/or from multiple devices.

(R-45) - It is required that it be possible to support multiple subscription profiles for an individual end-user. These multiple subscription profiles are required to be uniquely identifiable.

Subject to NGN Provider policy, periodic authentication of a user may be necessary for high assurance and security.

(R-46) - Subject to NGN Provider policy, it is required that it be possible to periodically re-authenticate the user (e.g., an end user, network element or object) for the duration of an established communication session or transaction.

9 User Authentication and Authorization of NGN Providers

This section provides requirements related to user authenticating and authorization of the network (e.g., user authenticating the identity of the connected NGN network or of the service provider).

9.1 Description

The NGN architecture allows end users to obtain services from multiple NGN Providers. In addition, the Transport NGN Provider (e.g., Access NGN Provider) can be different from the Service NGN Provider. As a result, end users may need to verify the identities of NGN Providers (e.g., access, transport and service providers). Specifically, the following may need to be supported:

- Capabilities to allow an end user to identify, authenticate and authorize the Access NGN Provider for network connectivity (e.g., network access).

[4] An aggregate end point will have two or more aggregate users associated with it. The identity of these users may only be known to the aggregate end point and not the NGN provider.

- Capabilities to allow an end user to identify, authenticate and authorize an Service NGN Provider

9.2 Objectives and Requirements

9.2.1 User Authentication of NGN Provider for Network Attachment

Network Access Points supporting network access for NGN TE and TE-BE should support capabilities to allow the user to identify, authenticate and authorize the network attachment.

(R-47) - Network Access Points (NAPs) supporting NGN TE and TE-BE (i.e., direct IP connectivity) shall support capabilities to allow the end user to uniquely identify the NGN Provider for attachment and connectivity if required by security policy.

(R-48) - Network Access Points (NAPs) supporting NGN TE and TE-BE (i.e., direct IP connectivity) shall support capabilities to allow the user to authenticate and authorize the NGN Provider for attachment and connectivity if required by security policy. These functions may be provided as part of the general Network Attachment Control Function (NACF) described in [ATIS-1000018].

(R-49) - For multi-network arrangements, each administrative domain (i.e., Network Access Provider, Visited NGN Provider, and Home NGN Provider) is required to enforce policies (e.g., SLAs) regarding the identification, authentication, and authorization of the network attachment.

9.2.2 User Authentication of NGN Provider for Obtaining Service

Capabilities to allow an end user to authenticate and authorize an NGN Provider to obtain NGN services may be provided.

(R-50) - The NGN shall supports capabilities to allow an end user to uniquely identify the NGN Provider providing a service or set of services if required by security policy.

(R-51) - The NGN shall supports capabilities to allow an end user to authenticate and authorize the NGN Provider providing service or set of services if required by security policy.

10 NGN Provider Supported User Peer-to-Peer Authentication and Authorization

This section is provided for completeness and is informational.

It is transparent to the NGN Provider that Peer-to-Peer communications are occurring, as the traffic transverses the NGN Provider network only at the transport layer. It should be noted that an NGN Provider may provide the role as an IdP providing IdM services (e.g., capabilities for peer-to-peer authentication) for these communication scenarios.

11 Mutual Network Authentication and Authorization

11.1 Description

Mutual network authentication and authorization are needed to mitigate threats of unauthorized access. Network access authentication and authorization services are needed to verify the identities and to determine whether network transport access, and/or services and capabilities access should be granted. Network access may occur at either the NNI or ANI.

Figure 8 shows the reference model for mutual network authentication and authorization consisting of the following security domains:

I. Access Network Domain: Access network hosted by an access network provider (e.g., narrowband, xDSL and cable). The access network provider may or may not be the same as the NGN Provider. Trust relations between access network provider and NGN Provider are governed by Service Level Agreements (SLAs).

II. Visited NGN Domain: NGN hosted by a visited network provider. Provides visited network functions for other NGN Network Provider (i.e., Home Network Provider). Trust relations are governed by Service Level Agreements (SLAs). The visited may offer NGN services and may have its' own subscribers. In addition, the visited network may have agreements with 3rd Party Application Service Provider. In addition, the visited network may interface with the home network via a transit network, and the trust relationship is governed by SLAs.

III. Home Network Domain: NGN hosted by a home network provider. The home network offers NGN services to its' subscribers. In addition, the home network may have agreements with 3rd Party Application Service Provider via an ANI. Trust relations between visited and home network providers, including any 3rd party provider are governed by service Level Agreements (SLAs). In addition, the home network may interface with a visited or other network via a transit network, where the trust relationships are governed by SLAs.

IV. Transit Network Domain: NGN providing only transport. Trust relationships between the transport network and the adjacent networks, including any 3rd party provider are governed by service Level Agreements (SLAs).

V. Other Network Domain: Either an NGN or non-NGN Provider. Trust relations are governed by Service Level Agreements (SLAs).

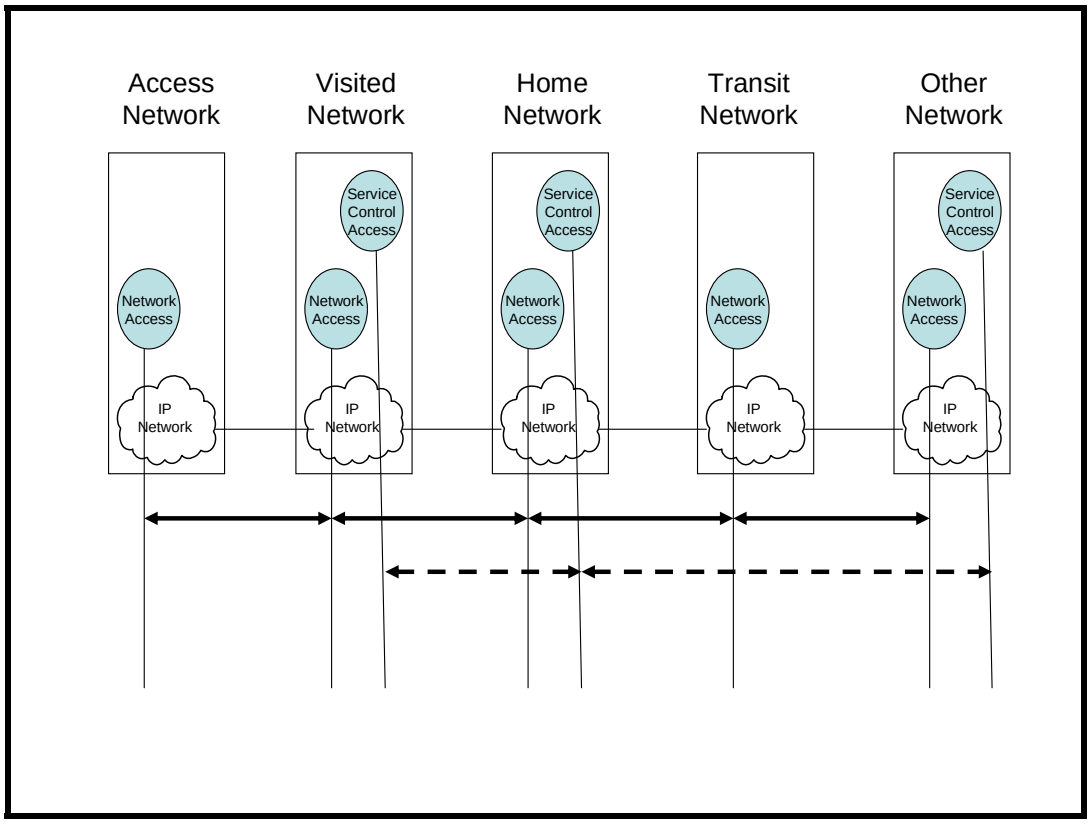


Figure 8 – Mutual Network Authentication

11.1.1 Transport Level Authentication

As shown in Figure 8, transport level authentication is on a hop-by-hop basis, whereby the authentication is always with the adjacent network at the transport. This means that home network does not necessarily need to have an SLA agreement the other network shown in the figure, but rather the transport level relationship is between the home network and the transit network and then between the transit network and the other network.

11.1.2 Service/Application Level Authentication

As shown in Figure 8, service/application level authentication is directly between the service control stratums of the visited, home, and other networks, at a peer-to-peer service/application level. This peer-to-peer relationship is logical and not physical. The physical path is vertical from the service control to network access in one network, then transported directly or via a transit network, and then vertically from the network to service control access in the peer service/application network.

11.2 Mutual Network Authentication Requirements

(R-52) - The NGN is required to support capabilities to uniquely identify adjacent networks at the transport stratum.

(R-53) - The NGN is required to support capabilities to authenticate and authorize access from adjacent networks at the transport stratum.

(R-54) - The NGN is required to support capabilities to uniquely identify, adjacent networks at the service/application stratum.

(R-55) - The NGN is required to support capabilities to authenticate and authorize access from adjacent networks at the service/application stratum.

(R-56) - Each NGN Provider is required to enforce policies for mutual network identification, authentication, and authorization (e.g., using SLAs and trust relationships).

(R-57) - For inter-network communication it is required that it be possible to uniquely identify network elements involved by correlating network element identifiers with identifiers associated with the interconnected NGN Provider.

(R-58) - The NGN is required to support capabilities to protect against unauthorized access, manipulation and corruption of mutual network authentication and authorization information.

(R-59) - The NGN is required to support capabilities for protection against attacks (e.g., message replay and denial of service attacks) on mutual network authentication and authorization functions and capabilities.

(R-60) - It is required that the NGN be capable of detecting and logging unauthorized access attempts from other networks (e.g., A system configurable threshold may be set for the number of unauthorized access attempts beyond which an alarm will be generates, logged, and reported to a management system).

Subject to NGN Provider policy, periodic authentication of an adjacent NGN Provider may be necessary for high assurance and security.

(R-61) - Subject to NGN Provider policy, it is required that it be possible to periodically re-authenticate the interconnecting NGN Provider for the duration of the established communication session or transaction.

12 NGN Provider Authentication and Authorization of 3rd Party Service/Application Provider

12.1 Description

There may be certain scenarios where the provider of an application or service is different from the NGN Provider (i.e., a 3rd party service/application provider). In such scenarios, the NGN Provider would need to authenticate and authorize the 3rd party service/application provider as shown in Figure 9.

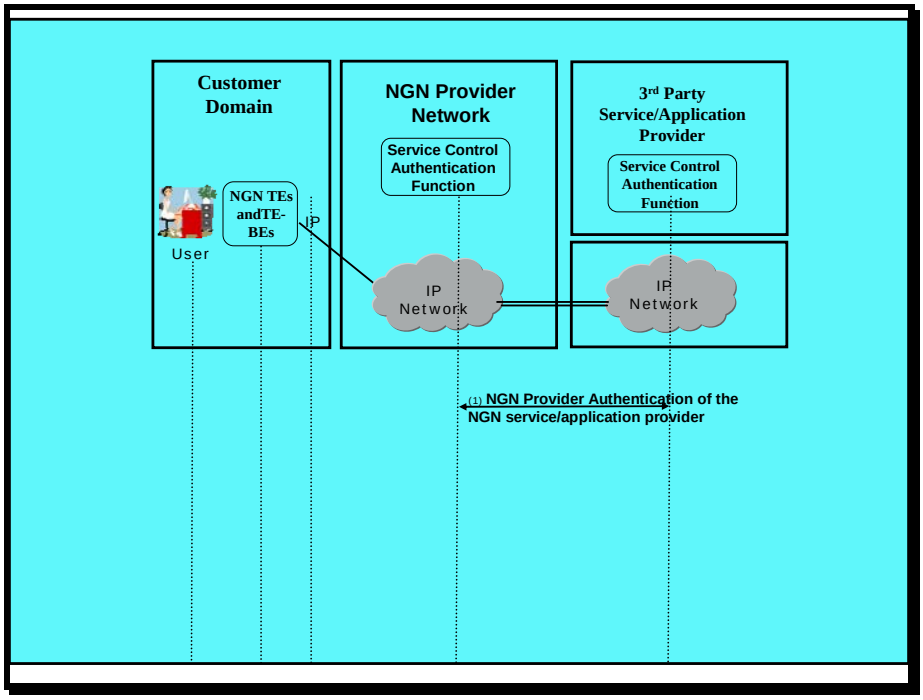


Figure 9 – 3rd Party Service/Application Provider Authentication and Authorization

It should be noted that the user and network authentications described in previous sections occur and are not shown in Figure 9 and the text below.

12.2 Requirements

(R-62) - A 3rd party service/application provider is required to support capabilities to identify itself to an NGN service provider.

(R-63) - A 3rd party service/application provider is required to support capabilities to identify itself to a user.

(R-64) - The NGN is required to support capabilities to uniquely identify 3rd party service/application providers.

(R-65) - The NGN is required to support capabilities to authenticate and authorize 3rd party service/application providers.

(R-66) - NGN Provider and 3rd party service/application providers are required to enforce policies for identification, authentication, and authorization (e.g., using SLAs and trust relationships).

(R-67) - The NGN and 3rd party service/application providers are required to support capabilities to protect against unauthorized access, manipulation and corruption of authentication and authorization information.

(R-68) - The NGN and 3rd party service/application provider are required to support capabilities for protection against attacks (e.g., message replay and denial of service attacks) on authentication and authorization functions and capabilities.

(R-69) - It is required that the NGN be capable of detecting and logging unauthorized access attempts from 3rd party service/application providers (e.g., A

system configurable threshold may be set for the number of unauthorized access attempts beyond which an alarm will be generates, logged, and reported to a management system).

Subject to NGN Provider policy, periodic authentication of an 3rd party service/application provider may be necessary for high assurance and security.

(R-70) - Subject to NGN Provider policy, it is required that it be possible to periodically re-authenticate the 3rd party service/application provider for the duration of an established communication session or transaction.

13 Use of 3rd Party Authentication and Authorization Service

13.1 Description

3rd Party Authentication and authorization service providers may provide:

- Authentication of the user to a service provider;
- Authentication of a service provider to the user;
- Authentication between service providers; and
- Authentication of a service/application provider by either a user or service provider.

In this regard, there will be at least three entities involved when a 3rd party authentication service provider is used. In addition to the 3rd party authentication service provider performing its authentication service function(s) upon request, it is required to authenticate itself to both the requestor and requstee.

13.2 Requirements

The requirements in Section 12.2 are applicable.

14 Authentication and Authorization of Objects

14.1 Description

In addition to authentication and authorization of users, user devices and service providers, there is a need to authenticate objects in general. This includes physical objects such as network elements or systems as well as virtual objects such as:

- applications,
- application process,
- software programs
- signalling, management and bearer messages and data content.

14.2 Requirements

(R-71) - The NGN is required to support capabilities to uniquely identify objects, subject to NGN Provider policy.

(R-72) - The NGN is required to support capabilities to authenticate and authorize objects, subject to NGN Provider policy.

(R-73) - It is required that the NGN support capabilities to verify and authorize the privileges of an object (e.g., allowing the object to perform an action on engage in a process only if its role or privilege is authorized).

(R-74) - NGN Provider is required to enforce policies for identification, authentication, and authorization of objects.

(R-75) - The NGN is required to support capabilities to provide confidentiality and integrity protection of messages and information exchanges used for authentication and authorization of objects.

(R-76) - The NGN is required to support capabilities to protect against unauthorized access, manipulation and corruption of object authentication and authorization information.

(R-77) - The NGN is required to support capabilities for protection against attacks (e.g., message replay and denial of service attacks) on object authentication and authorization functions and capabilities.

(R-78) - It is required that the NGN be capable of detecting and logging unauthorized access attempts from objects (e.g., A system configurable threshold may be set for the number of unauthorized access attempts beyond which an alarm will be generates, logged, and reported to a management system).

(R-79) - It is required that the NGN be capable of detecting and logging privilege attempts that are unauthorized (e.g., unauthorized user actions).

Subject to NGN Provider policy, periodic authentication of an adjacent NGN Provider may be necessary for high assurance and security.

(R-80) - Subject to NGN Provider policy, it is required that it be possible to periodically re-authenticate the associated object for the duration of the related established communication session or transaction.

Annex A

(informative)

A: Use of ITU-T Recommendation X.1141, Security Assertion Markup Language (SAML) 2.0

This Appendix provides example use cases for conveying authentication results while supporting privacy use of SAML for Service/Application Authentication.

When the authentication results need to be exchanged among the trusted services and/or applications which can be 3rd party provider's, Security Assertion Markup Language (SAML) 2.0 may be used. SAML 2.0 is an open specification standardized by the Organization for the Advancement of Structured Information Standards (OASIS). SAML can be used specifically for the following cases:

- Single Sign On: when different services and applications allow their users Single Sign On for users' convenience without exchanging all user information among them.
- Account Federation: when different services and applications link their accounts for the same user.

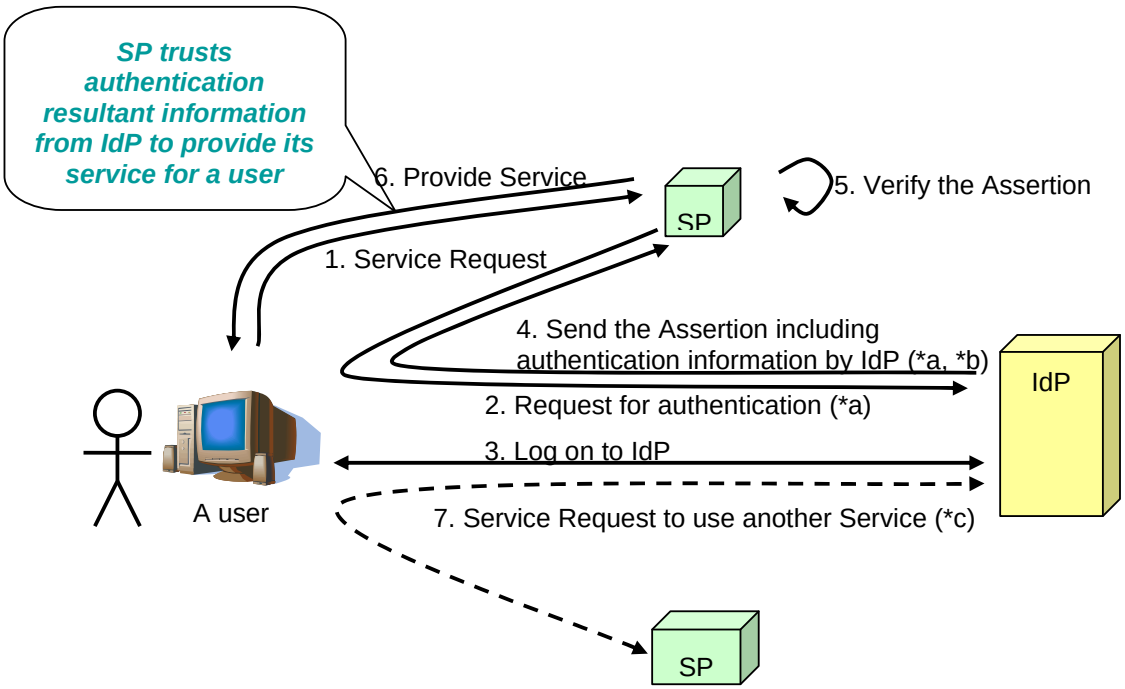
A.1 Service/Application Authentication Procedures

When the authentication results need to be exchanged among the trusted services and/or applications which can be 3rd party provider's, Security Assertion Markup Language (SAML) 2.0 may be used. SAML 2.0 is an open specification standardized by the Organization for the Advancement of Structured Information Standards (OASIS). SAML can be used specifically for the following cases:

- Single Sign On: when different services and applications allow their users Single Sign On for users' convenience without exchanging all user information among them.
- Account Federation: when different services and applications link their accounts for the same user.

A.2 Service/Application Authentication – Call Flow Examples

Figure 10 shows a typical example of Single Sign On with federation using SAML 2.0.



(*a) 2 and 4 are communication (e.g. HTTP-redirect) via a user agent (e.g. Web browser)

(*b)The Assertion can contain attribute information and authorization decision when necessary.

(*c) The same flow as from 1. through 6., excluding logging in to IdP. (In other words, a user only needs to log on to IdP once to be authenticated)

Figure 10 - SSO Call Flow Example using SAML2.0

Recommendation X.1141, Security Assertion Markup Language, SAML 2.0 [B-29] defines the terms shown on the Figure 10 as follows:

- Identity Provider (IdP)

  A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.

- Service Provider

  A role donned by a system entity where the system entity provides services to principals or other system entities.

- Assertion

A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource.

A.3 Security of Service/Application Authentication Procedures and Mechanisms

SAML2.0 itself has features such as Anonymous Federation and Pseudonyms to protect security as well as privacy. Anonymous Federation provides a transient nameID for service provider. Pseudonyms allow Users can be identified to a Service Provider during Single Sign On using pair-wise pseudonyms that preserve privacy while enabling a persistent relationship to be maintained with the user. SAML2.0 also SAML V2.0 permits attribute statements, name identifiers, or entire assertions to be encrypted. This feature ensures that end to end confidentiality of these elements may be supported as needed.

Annex B

(informative)

B: 3GPP Generic Bootstrapping Architecture (GBA)

The Generic Bootstrapping Architecture (GBA) specifies access-independent bootstrapping procedure. It provides a framework for mutual authentication of the End-Users and Network Application Function (NAF).

The GBA is an authentication system that includes three parties:

- An end-user who is trying to obtain network services using User Equipment (UE)
- Application server (called Network Application Function or NAF)
- A trusted entity (called Bootstrapping Server Function or BSF), which is involved in authentication and key exchange between two other entities.

The basics of the GBA authentication process are illustrated by the reference model and described below. The following acronyms are used:

BSF Bootstrapping Server Function

HSS Home Subscriber System

NAF Network Application Function

SLF Subscriber Locator Function

UE User Equipment

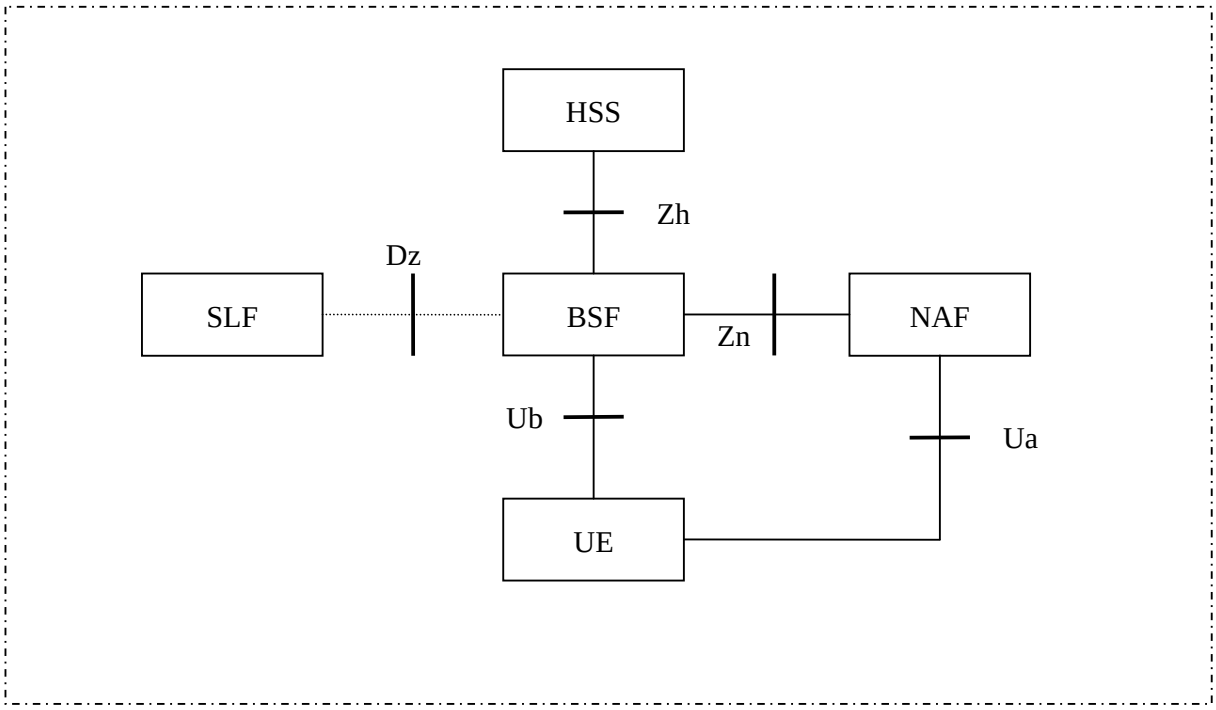


Figure 11 – Simple network model for bootstrapping from ETSI TS 133 220[B-1]

These are the basic steps of the GBA procedure:

1. NAF requests authentication and negotiates the use of GBA over Ua reference point.

2. The BSF client that runs on the UE initiates bootstrapping procedurre over the reference point Ub. The BSF fetches authentication information and the GBA user security settings from the HSS over Zh. The UE and the BSF mutually authenticate using http Digest AKA. The procedure results in the UE receiving bootstrapping transaction identifier (B-TID) from the BSF and establishing a shared key (Ks) between the UE and the BSF.

3. UE derives Ks_NAF from Ks and sends B-TID (along with the application-specific data) to the NAF.

4. The NAF sends B-TID to the BSF over Zn reference point.

5. The BSF based on B-TID determines the Ks that should be used, derives Ks_NAF from it and sends Ks_NAF to the NAF.

6. Finally, UE and NAF can authenticate each other using the shared key Ks_NAF. The exact authentication procedure depends on the protocol between the UE and NAF. For instance, GBA specifies that HTTP-based applications can use either HTTP Digest authentication (RFC2617) or TLS pre-shared key ciphersuites (RFC4279).

Note: The BSF queries the SLF over the Dz reference point to obtain the name of the HSS containing the subscriber-specific data. The SLF is not needed when the BSF is configured to use a pre-defined HSS.

Mapping of the GBA entities to the NGN entities specified in Y.2012, *Functional requirements and architecture of the NGN of Release 1.*

- NAF - corresponds to *Applications* entity of the Y.2012 Figure 3: NGN generalized functional architecture.
- BSF – can be included in T-11 Authentication & Authorization FE. That is T-11 can be augmented and enabled with the capabilities of the BSF server.
- HSS corresponds to S-5 Service User Profile FE
- SLF corresponds to S-4 Subscription Locator FE
- UE corresponds to the End-User Function

Annex C

(informative)

C: NIST Special Report 800-63

This Appendix provides a summary of NIST Special Report 800-63 which specifies 4 levels for authentication assurance and registration and identity proofing.

Summary of NIST Special Report 800-63

Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce. This recommendation provides technical guidance to agencies to allow an individual person to remotely authenticate his/her identity to a Federal IT system. This guidance addresses only traditional, widely implemented methods for remote authentication based on secrets. With these methods, the individual to be authenticated proves that he or she knows or possesses some secret information. NIST expects to explore other means of remote authentication (for example using biometrics, or by extensive knowledge of private, but not truly secret, personal information) and may develop additional guidance on the use of these methods for remote authentication.

This technical guidance supplements OMB guidance, E-Authentication Guidance for Federal Agencies, [OMB 04-04] that defines four levels of authentication Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. The OMB guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

After completing a risk assessment and mapping the identified risks to the required assurance level, agencies can select appropriate technology that, at a minimum, meets the technical requirements for the required level of assurance. In particular, the document states specific technical requirements for each of the four levels of assurance in the following areas:

- Tokens (typically a cryptographic key or password) for proving identity,
- Identity proofing, registration and the delivery of credentials which bind an identity to a token,
- Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be,

- Assertion mechanisms used to communicate the results of a remote authentication to other parties.

A summary of the technical requirements for each of the four levels is provided below.

Level 1 - Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 2 – Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 3 - Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 4 – Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

Annex D

(informative)

D: Identity Management (IdM) Call Flow Examples

D.1 Overview

The example flows in this appendix are from 3GPP TR 33.980, Technical Report on 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA) (Release 7) [B-30].

The flows provide the details of possible interworking methods between the Security Assertion Markup Language v2.0, SAML v2.0 (or alternatively the Liberty Alliance Identity Federation Framework, ID-FF), the Identity Web Services Framework (ID-WSF) , the Security Assertion Markup Language (SAML) and a component of GAA called the Generic Bootstrapping Architecture (GBA). This Appendix is informative and only applies if ID-WSF and GBA or SAML v2.0 and GBA are used in combination.

D.2 Call Flow Examples

These flows only apply if Liberty Alliance and GBA or SAML v2.0 and GBA are used in combination.

D.2.1 SSO scenario: ID-FF with <lib:AuthnResponse> transfer

D.2.1.1 HTTPS with conventional TLS

In this scenario the UE is not Liberty Alliance Project (LAP) aware. All protocol elements are taken from within ID Federation Framework [B-7] and complemented by the GAA-specific details from [B-2]. First the steps are outlined that are needed when utilizing HTTPS deploying conventional TLS [B-24] according to [B-2], clause 5.3:

1) The UE contacts the SP to gain access to a service provided by the SP by sending an HTTP Request. This request will contain the GBA-based authentication support indication (cf. step 3), as this is required for the redirection of the request according to step 3.

2) On receipt of the HTTP request from UE, the SP obtains the identity provider and sends a redirect HTTP Response with < lib:AuthnRequest> to UE. The means by which the identity provider address is obtained is implementation-dependent and up to the service provider.

3) The UE in turn contacts the IdP under the URL given in the Location header field and the UE must access the NAF/IdP URL with an HTTP Request with <lib:AuthnRequest> information [B-12].

The UE will indicate to the NAF/IdP that GBA-based authentication is supported by adding a constant string to the "User-Agent" HTTP header as a product token as specified in IETF RFC 2616 [B-12]. This constant string will be set according to step 2 of clause 5.3 of TS 33.222 [B-2].

If a bootstrapped security association between UE and IdP exists, then UE and IdP/NAF share the keys to protect reference point Ua and the UE possesses all necessary data to perform HTTP Digest Authentication from previous messages. In this case step 3 is combined with the request in step 5, and step 4 is omitted.

4) As the IdP is collocated with the NAF, the HTTP Digest authentication is conducted in the accordance to 3GPP TS 33.222 [B-2] and a HTTP response with Unauthorized status and WWW-Authenticate header field is sent to the UE. The method and details of this authentication are defined by TS 33.222 [2] and not in [B-7].

   If the UE does not contain a valid bootstrapping session or the freshness of the key material is not sufficient for the IdP, then the UE will execute a new bootstrapping procedure with the BSF. This is transparent to the SP.

5) The UE returns the Authorization data, using the B-TID as a username and the Ks_(ext/int)_NAF as password to the IdP. The UE may include further LAP related user data.

   If the IdP is collocated with the NAF, then this happens as outlined in TS 33.222 [B-2]. The USS might contain Liberty specific information.

6) The <lib:AuthnRequest> is processed. The IdP responds with an <lib:AuthnResponse> in the HTTP Response redirect URL [B-12]. The IdP may include further LAP-related data.

7) The UE contacts the SP again using this URL and HTTP Request with <lib:AuthnResponse>.

8) The SP answers with a HTTP Response.

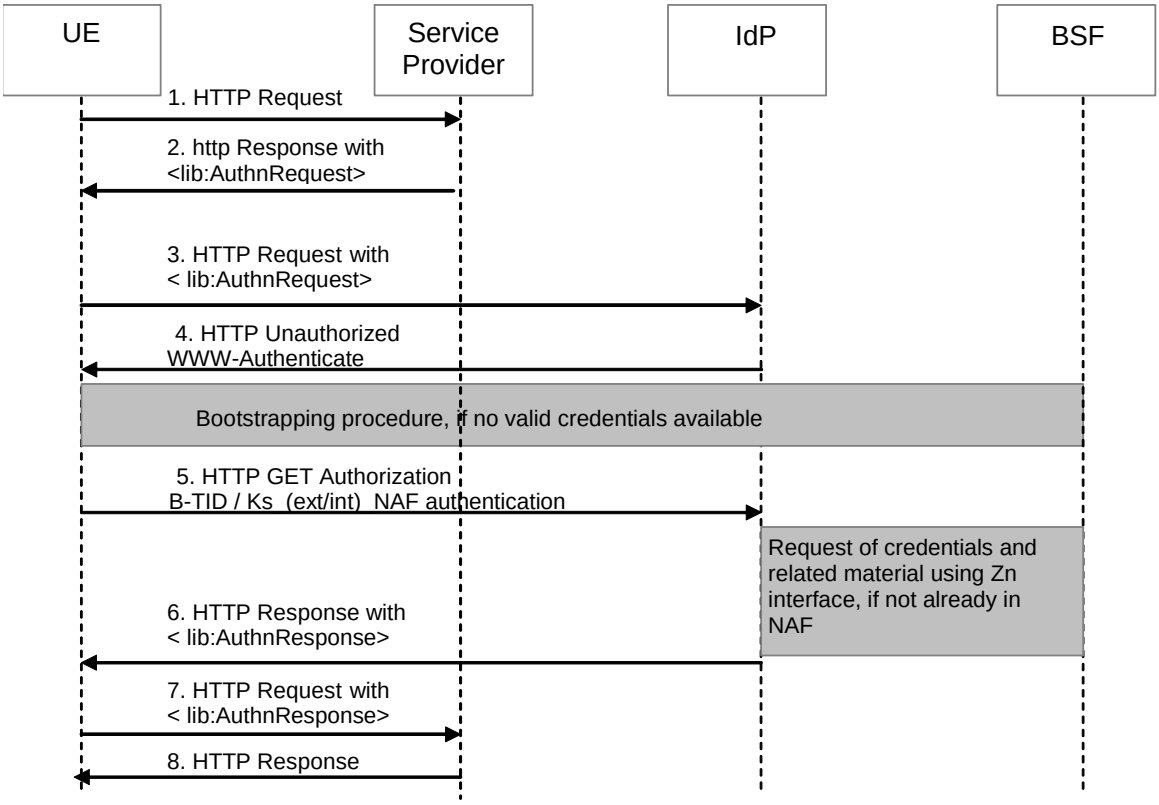


Figure 12: Message flow for SSO with <lib:AuthnResponse> and conventional TLS with GBA

NOTE 1: As the IdP is collocated with the NAF i.e. Ua is chosen for authentication as outlined in TS 33.222 [B-2], then each request over Ua is authenticated by itself, as each request carries the full Authorization Header. There is no difference between first request and follow-up requests.

NOTE 2: LAP ID-FF specification [B-7] defines also a POST-based communication between UE and IdP besides a GET-based request with a query string. This is in conformance with TS 33.222 [B-2], as there only a HTTP request is specified without any explicit method stated.

NOTE 3: The SP may use the GBA-based authentication support indication received in step 1 to select an appropriate identity provider address.

D.2.1.2 HTTPS with PSK TLS

When HTTPS with Pre-shared Keys (PSK) TLS according to TS 33.222 [B-2], clause 5.4, is utilized, then the steps are the following:

1) The UE contacts the SP to gain access to a service provided by the SP by sending an HTTP Request. This request will contain the GBA-based authentication support indication (cf. step 3 of clause D.2.1.1), as the UE may be forced by the IdP/NAF to use conventional TLS, even if the UE offers the usage of PSK TLS.

2) On receipt of the HTTP request from UE, the SP obtains the identity provider and sends a redirect HTTP Response with < lib:AuthnRequest> in the URL to the UE. The means by which the identity provider address is obtained is implementation-dependent and up to the service provider.

3) The UE starts to set up a PSK TLS tunnel to the IdP/NAF as specified in clause 5.4 in TS 33.222 [B-2]. This is in preparation of sending the redirected request to the

IdP/NAF (cf. step 4). During TLS tunnel setup the UE indicates possibility to use PSK TLS, and the IdP/NAF may select to use PSK TLS with GBA.

The UE recognizes from the TLS ciphersuite selected by IdP/NAF if the IdP/NAF will use PSK TLS.

If a bootstrapped security association between UE and IdP/NAF exists, then UE and IdP/NAF share the keys to protect reference point Ua. Thus the UE possesses all necessary data to set up the PSK TLS tunnel according to TS 33.222 [B-2] and the next step can be approached immediately without executing a bootstrapping procedure.

If no bootstrapped security association between UE and IdP/NAF exists, but the UE does contain a valid bootstrapping key Ks, then the UE establishes a PSK TLS tunnel with the IdP/NAF based on the related Ks_(ext)_NAF.

If the UE does not contain a valid bootstrapping session or the freshness of the key material is not sufficient for the IdP/NAF, then the UE will execute a new bootstrapping procedure with the BSF. This is transparent to the SP.

4) The UE accesses the IdP/NAF URL with the HTTP GET Request with <lib:AuthnRequest> information [12] within the established PSK TLS tunnel.

5) The IdP extracts the <lib:AuthnRequest>, processes it, uses the UE authentication done during the PSK TLS tunnel establishment, and sends a redirect HTTP Response to the UE, which redirects the UE back to the SP. The URL may contain a SAML artefact or a <lib:AuthnResponse>.

6) The SP extracts the SAML artefact or the <lib:AuthnResponse>, processes it and answers with a HTTP Response.

7) The SP answers with a HTTP Response.

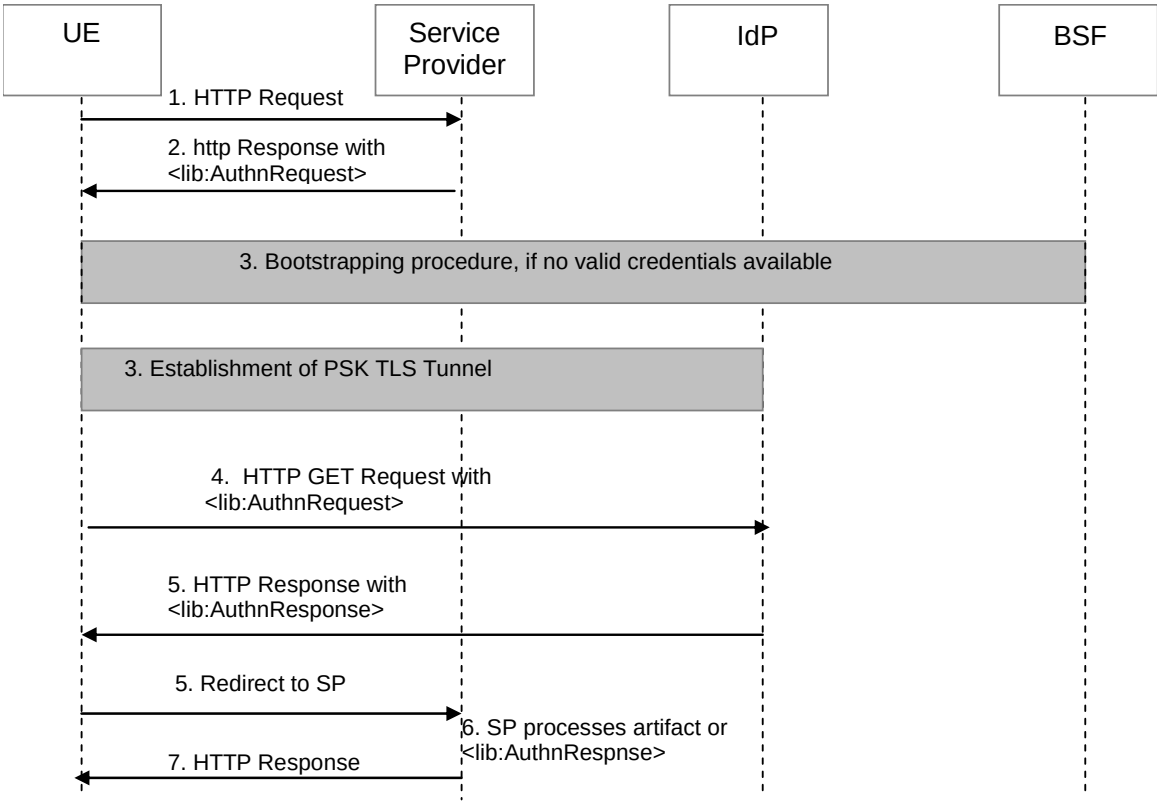


Figure 13: Message flow for SSO with <lib:AuthnResponse> and usage of PSK TLS with GBA

NOTE: The notes given in clause D.2.1.1are also applicable for usage of PSK TLS as defined in this clause.

D.2.2 SSO scenario: ID-FF with artefact transfer

This scenario is similar to the scenario given in clause D.2.1, with the extension that the service provider is able to contact the IdP directly.

NOTE: As the basic message flow is the same for artefact and for <lib:AuthnResponse> usage, the same differences between usage of conventional TLS and PSK TLS as in clause D.2.1 apply to this clause also. Message flows given in this clause refer to conventional TLS, Analogous usage of PSK TLS is also possible.

The IdP must support an additional interface to SP, to allow the SP retrieval of the authentication assertion. This interface is not completely separated from GBA, as this authentication information may include GBA related information, e.g. user identity, pseudonym and further information from GUSS, restrictions based on GBA, etc.

1) The UE contacts the SP to gain access to a service provided by the SP by sending an HTTP Request. This request will contain the GBA-based authentication support indication (cf. step 3), as this is required for the redirection of the request according to step 3.

2) On receipt of the HTTP request from UE, the SP obtains the identity provider and sends a redirect HTTP Response with < lib:AuthnRequest> to UE. The means by which the identity provider address is obtained is implementation-dependent and up to the service provider.

3) The UE in turn contacts the IdP under the URL given in the Location header field and the UE must access the NAF/IdP URL with an HTTP Request with <lib:AuthnRequest> information [B-12].

   The UE will indicate to the NAF/IdP that GBA-based authentication is supported by adding a constant string to the "User-Agent" HTTP header as a product token as specified in IETF RFC 2616 [B-12]. This constant string will be set according to step 2 of clause 5.3 of TS 33.222 [B-2].

   If a bootstrapped security association between UE and IdP/NAF exists, then UE and IdP/NAF share the keys to protect reference point Ua and the UE possesses all necessary data to perform HTTP Digest Authentication from previous messages. In this case step 3 is combined with the request in step 5, and step 4 is omitted.

4) If the UE is not yet authenticated with the IdP, then the authentication has to take place here, as defined in TS 33.222 [B-2]. The method and details of this authentication are not defined by Liberty Alliance in [B-7]. The IdP sends a HTTP response with Unauthorized status to the UE as defined in TS 33.222 [B-2].

   If there is no valid NAF specific key material in the NAF, or the freshness of the key material is not to the satisfaction of the NAF or IdP, then the bootstrapping procedure has to be performed as defined in TS33.220 [B-1]. This is transparent to the SP.

5) The UE answers with a HTTP GET request with Authorization header field containing as a username the B-TID and as a password the Ks_(ext/int)_NAF. The UE may include further LAP related user data.

   The IdP/NAF can request the credentials and related material, if it does not have it stored already. The received USS may contain further Liberty specific information.

6) The IdP responds with a SAML artefact in the HTTP Response redirect URL [B-12]. The IdP may include further LAP related data.

7) The UE contacts the SP again using this URL and HTTP Request with the SAML artefact.

8) The SP sends an HTTP Request with the SAML artefact to the IdP. The request contains a <samlp:Request> SOAP Request message to the identity provider's SOAP endpoint, requesting the assertion by providing the SAML assertion artefact in the < samlp:AssertionArtefact> element as specified in [B-12]

9) The IdP can now construct or find the requested assertion and responds with a <samlp:Response> SOAP Response message with the requested <saml:Assertion> or an status code as defined [B-13]. The IdP sends the authentication assertion that corresponds to the artefact.

10) The SP processes the SOAP message with the <saml:Assertion> returned in the <samlp:Response>, verifies the signature on the <saml:Assertion> and processes the message as defined in [B-12] and then answers with a HTTP Response.

The SAML authentication assertion should have a lifetime equal to or less than the B-TID.

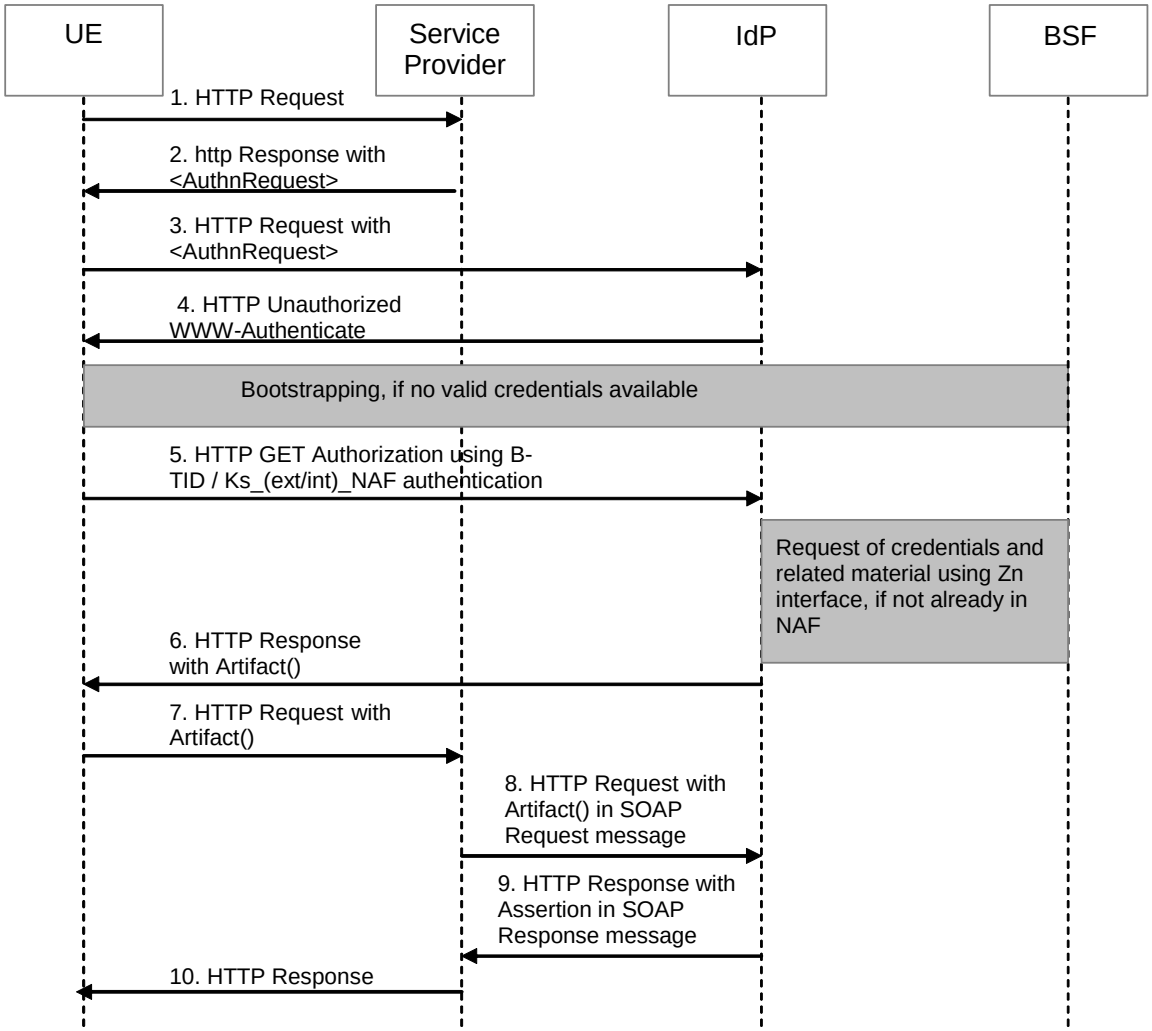


Figure 14: Message flow for SSO with Artefact transfer and usage of GBA

D.2.3 SSO scenario: ID-WSF Authentication Service

In this scenario the UE is LAP enabled, i.e. a LUAD (Liberty enabled User Agent or Device as defined in Liberty ID-WSF Profiles for Liberty enabled User Agents and Devices specification [B-16]). The protocol elements used are taken from ID–WSF Authentication Service [B-8], and the interaction of UE with IdP comprises two consecutive protocol runs. The active LUAD client contacts the NAF/IdP first before accessing the service provided by the SP.

1. The UE authenticates with the Authentication Service (AS) of the IdP and retrieves a security token, which entitles the UE to invoke some services.

2. The UE invokes the Single-Sign-On Service (SSOS) of the IdP using the security token. In this step the UE receives the authentication assertion (authentication and authorisation information) to be used at the SP.

3. The UE presents the authentication assertion to the SP acting as a WSP for web service access.

In case the WSP providing the web service to the user is part of the domain of the IdP operator, the LUAD client may also contact the WSP directly with the security token. In this case the SSOS contact may be left out.

Mapping of the three steps to GBA is done in the following way:

- The first step is mapped to the communication between user (LUAD) and AS as specified within LAP [B-8]. The authentication protocol is embedded in the SASL protocol. The Ub run must be executed by the UE if necessary. This is not based on LAP protocols [B-6], [B-7] or [B-8], but only on GBA protocols [B-1].
- The second and third steps are completely as defined in LAP (no connection to GBA). The only dependency on GBA is in the content of the SAML authentication assertion depending partly on GBA results (protocol parameters, e.g. execution time, and user-specific parameters, e.g. taken from USS).

  The following gives a message flow for the SSO scenario of the ID-WSF authentication service with response transfer. This can also applies when the SSOS also offers an ID-WSF authentication service, in which case the SSOS is collocated with the AS.

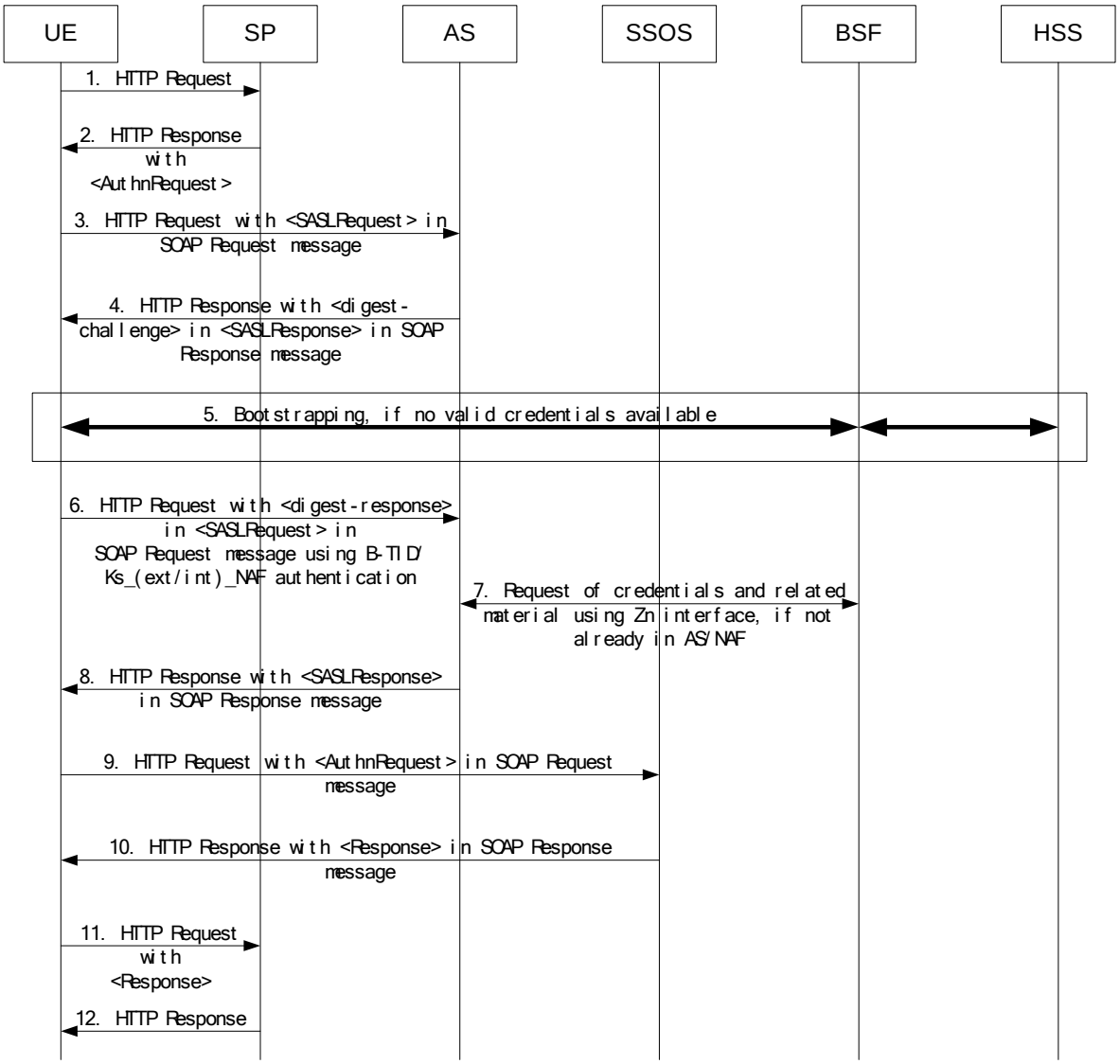


Figure 15: Message flow for ID-WSF AS and SSO with Response transfer and usage of GBA

1. The UE contacts the SP to gain access to a service provided by the SP by sending an HTTP request.
2. On receipt of the HTTP request from the UE, the SP obtains the AS address and sends a redirect HTTP response to the UE. The HTTP response may or may not contain an < lib:AuthnRequest> header according to the application or deployment model. The means by which the AS's address is obtained is implementation-dependent.
3. The UE (LUAD-WSC) sends an HTTP request to the AS. The request contains a soap-bound <SASLRequest> header, where the "mechanism" parameter is filled with a list of one-or-more client-supported SASL mechanism names.

   The UE will indicate to the NAF/AS that GBA-based authentication is supported by adding a constant string to the "User-Agent" HTTP header as a product token as

specified in IETF RFC 2616 [B-12]. This constant string will be set according to step 2 of clause 5.3 of TS 33.222[B-2].

If a bootstrapped security association between UE and NAF/AS exists, then UE and NAF/AS share the keys to protect reference point Ua and the UE may perform a subsequent authentication procedure if the SASL profile allows. In this case step 3 is combined with the request in step 6, and step 4 and step 5 are omitted.

4 The AS sends a HTTP response to the UE. The response contains a soap-bound <SASLResponse> header, where the "serverMechanism" parameter is filled with a selected SASL mechanism name (i.e. DIGEST authentication) from the client-supported SASL mechanism list and in this case the <SASLResponse> header also contains a <digest-challenge> parameter. The method and details of this parameter are compliant to RFC2831.

5 If the UE does not contain a valid bootstrapping session or the freshness of the key material is not sufficient for the AS, then the UE will execute a new bootstrapping procedure with the BSF and obtain a shared key Ks_(ext/int)_NAF. This is transparent to the SP.

6 The UE re-sends a HTTP request to the AS. The request contains a soap-bound <SASLRequest> header, where the "mechanism" parameter is filled with the returned SASL mechanism in step 4 and in this case the <SASLRequest> header also contains a <digest-response> parameter, where the authorization data is computed using the B-TID as a username and the Ks_(ext/int)_NAF as the password. The method and details of this parameter are compliant to RFC2831. The UE may include further LAP related user data.

7 As the AS is collocated with the NAF, the AS requests Ks_(ext/int)_NAF and other materials from the BSF using the Zn interface if they are not available yet.

8 The AS processes the <digest-response> parameter in the <SASLRequest> header. Then the AS responds with a soap-bound <SASLResponse> header in the HTTP Response. The <SASLResponse> header contains an ID-WSF EPR (EndpointReference) parameter which refers to the SSOS instance and the Service type URI is set according to [B-8] to identify the ID-WSF SSOS. The <SASLResponse> header also contains some necessary credentials for the UE to invoke the SSOS. The AS may include further LAP-related data.

9 The UE sends a HTTP request to the SSOS. The request contains a soap-bound <samlp2:AuthnRequest> header, where the ProtocolBinding attribute is set according to [B-8] to identify the SAML protocol binding to be used .The request also contains a <wsse:security> header which includes the returned credentials in step 8.The UE may have to construct the <samlp2:AuthnRequest> header by itself if it does not receive such a header in step 2 according to the application or deployment model.

10 The <samlp2:AuthnRequest> is processed. The SSOS responds with an <samlp2: Response> header in the HTTP Response redirect URL [B-12]. The <samlp2: Response> header contains a <saml2:Assertion> parameter . The SSOS may include further LAP-related data.

11 The UE contacts the SP again using this URL and HTTP Request with <samlp2: Response >.

12 The SP answers with a HTTP Response.

NOTE: If the IdP is co-hosted with the BSF, then the first step could be mapped to Ub reference point of GBA [B-4]. The second step could be mapped to Ua interface of GBA.

Despite having this formal analogy of executing two consecutive protocol runs required by both protocol worlds, it seems that a simple mapping is not possible. The syntax and semantic of the information elements transferred between GBA and LAP protocols differ substantially.

D.2.4 SSO scenario: SAML v2.0 with <samlp:Response> transfer

D.2.4.1 HTTPS with TLS

This scenario is a version of the scenario in clause D.2.1.1 with the difference that all protocol elements are taken from within SAML v2.0 [B-28] implementing the Web Browser SSO Profile from [B-13]. Hence all the steps described there apply here as well, after replacing <lib:AuthnRequest> with <samlp:AuthnRequest> and <lib:AuthnResponse> with <samlp:Response>. The steps are not repeated here, only an adapted version of Figure 12 is included.

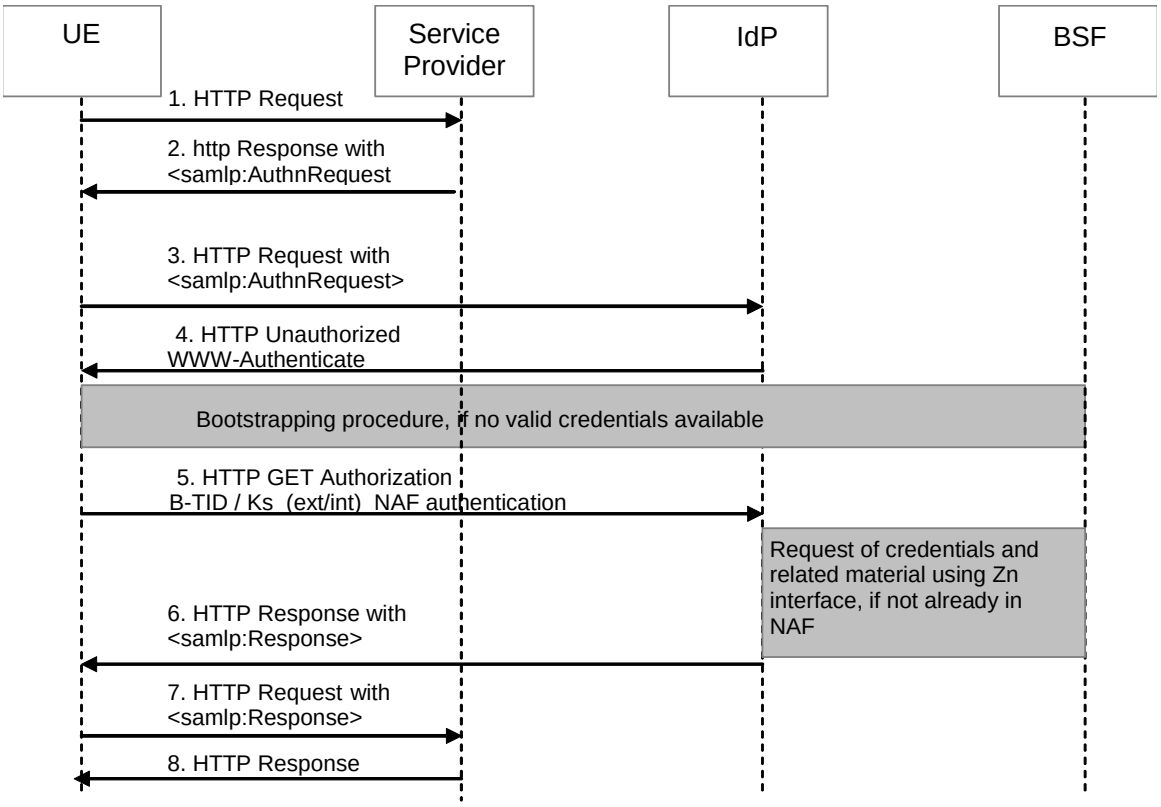


Figure 16: Message flow for SSO with <samlp:Response> and TLS with GBA

D.2.4.2 HTTPS with PSK TLS

This scenario is a version of the scenario in clause D.2.1.2 with the difference that all protocol elements are taken from within SAML v2.0 [B-28] implementing the Web Browser SSO Profile from [B-13]. Hence all the steps described there apply here as well, after replacing <lib:AuthnRequest> with <samlp:AuthnRequest> and <lib:AuthnResponse> with <samlp:Response>. The steps are not repeated here, only an adapted version of Figure 13 is included.

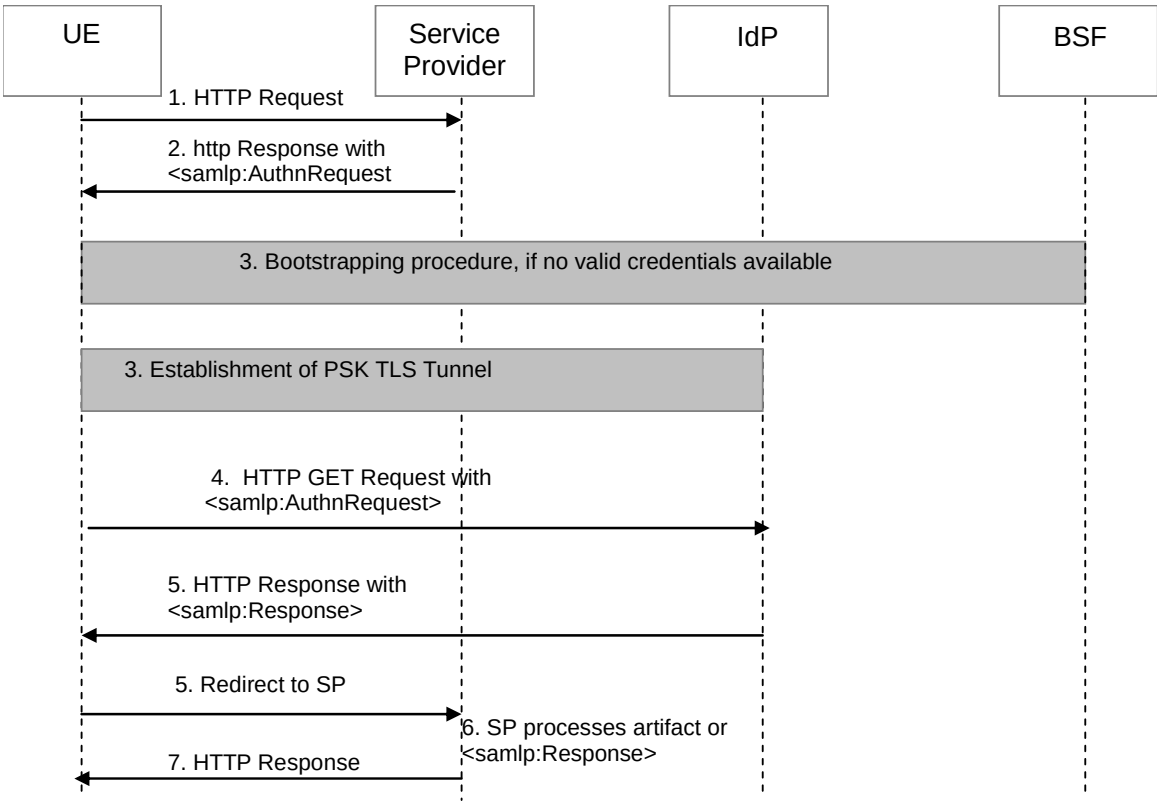


Figure 17: Message flow for SSO with <samlp:Response> and usage of PSK TLS with GBA

D.2.5 SSO scenario: SAML v2.0 with artefact transfer (resolution)

This scenario is a version of the scenario in clause D.2.2 with the difference that all protocol elements are taken from within SAML v2.0 [B-28] implementing the Web Browser SSO Profile from [B-13]. Hence all the steps described there apply here as well, after replacing <lib:AuthnRequest> with <samlp:AuthnRequest>. The steps are not repeated here, only the adapted version of Figure 14 is included.

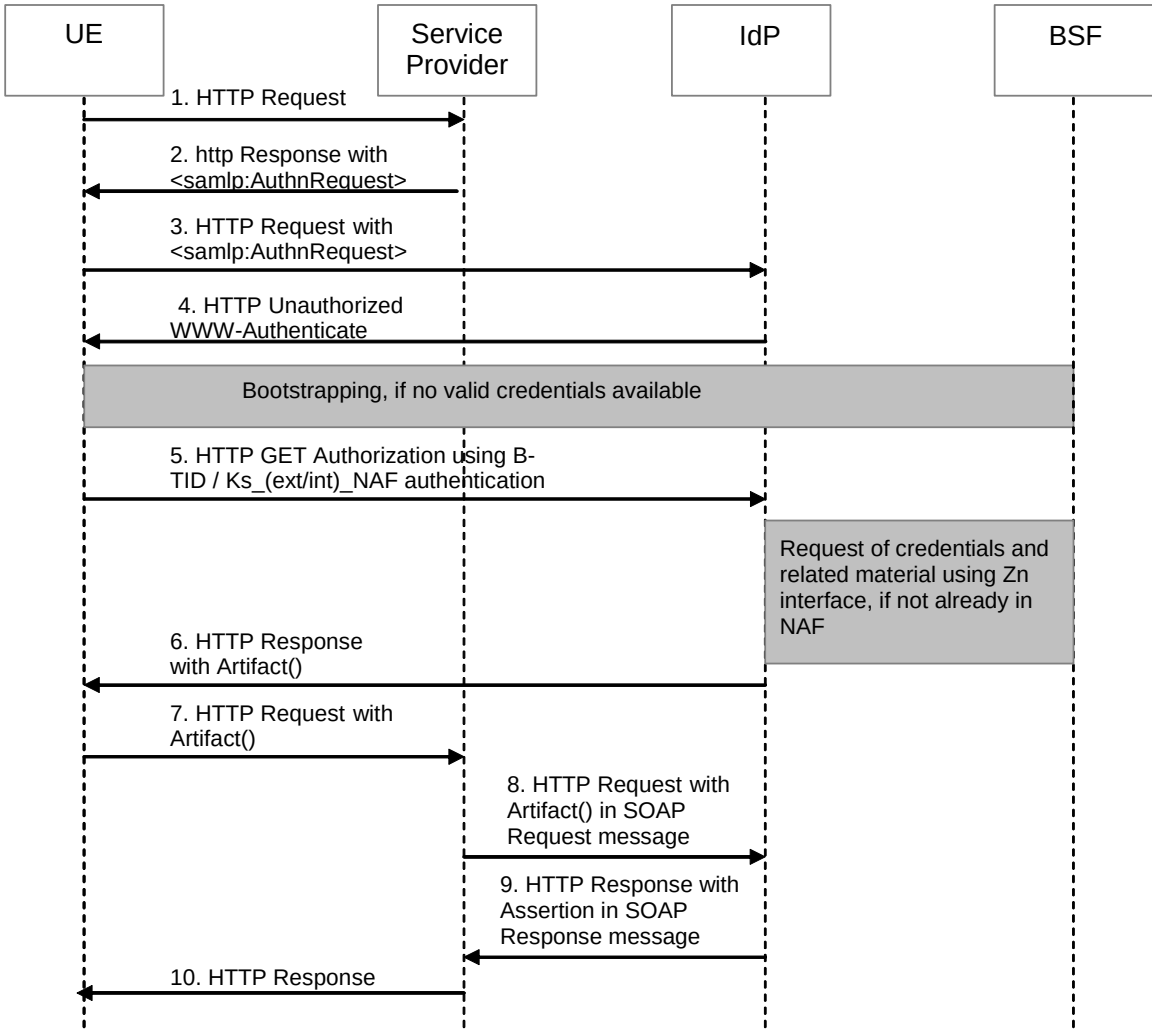


Figure 18: Message flow for SSO with Artefact resolution (SAML v2.0) and usage of GBA

Annex E

(informative)

E: Informative References

[B-1] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".[5]

[B-2] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)". [5]

[B-3] 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for subscriber certificates". [5]

[B-4] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details". [5]

[B-5] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3". [5]

[B-6] Liberty Alliance Project, ID-WSF v2.0: "Liberty ID-WSF Security Mechanisms".[6]

[B-7] Liberty Alliance Project, ID-FF v1.2: "Liberty ID-FF Architecture Overview".[6]

[B-8] Liberty Alliance Project, ID-WSF v2.0 "Liberty ID-WSF Authentication Service Specification and Single Sign-On Service".[6]

[B-9] Liberty Alliance Project, ID-WSF v2.0: "Liberty ID-WSF SOAP Binding Specification".[6]

[B-10] Liberty Alliance Project, ID-WSF v2.0: "Liberty ID-WSF Discovery Service Specification".[6]

[B-11] Organization for the Advancement of Structured Information Standards (OASIS), SAML v2 Core "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0".[7]

[B-12] Liberty Alliance Project, ID-FF v1.2: "Liberty ID-FF Bindings and Profiles Specification".[6]

[B-13] Organization for the Advancement of Structured Information Standards (OASIS), "Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0".[7]

[B-14] Liberty Alliance Project, ID-WSF v1.2: "Security Mechanisms".[6]

[B-15] Liberty Alliance Project Support Documents: "Authentication Context Specification" v2.0. [6]

---

[5] This document is available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

[6] This document is available from The Liberty Alliance Project at < http://projectliberty.org/.

[7] This document is available from OASIS at http://www.oasis-open.org/

[B-16] Liberty Alliance Project, ID-WSF "Profiles for Liberty enabled User Agents and Devices".[6]

[B-17] IETF RFC 2222 (1997), "Simple Authentication and Security Layer (SASL)".[8]

[B-18] IETF RFC 2831 (2000), "Using Digest Authentication as a SASL Mechanism".[8]

[B-19] IETF RFC 2617 (1999), "HTTP Authentication: Basic and Digest Access Authentication".[8]

[B-20] Liberty Alliance Project Support Documents: "Liberty Reverse HTTP Binding for SOAP Specification" v1.1. [6]

[B-21] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".[5]

[B-22] IETF RFC 3546 (2003-06), "Transport Layer Security (TLS) Extensions".[8]

[B-23] Liberty Alliance Project, ID-SIS: "Liberty Alliance ID-SIS 1.0 Specifications".[6]

[B-24] IETF RFC 2246 (1999-01), "The TLS Protocol Version 1.0[8]

[B-25] IETF RFC 4279 (2005-12), "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)". [8]

[B-26] Liberty Alliance Project, ID-FF v1.2: "Liberty ID-FF Protocols and Schema Specification".

[B-27] Organization for the Advancement of Structured Information Standards (OASIS), "Authentication Contexts for the OASIS Security Assertion Markup Language (SAML) V2.0".[7]

[B-28] Organization for the Advancement of Structured Information Standards (OASIS), SAML v2 Core "Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0".[7]

B-29] ITU-T Recommendation X.1141 Security Assertion Markup Language (SAML 2.0)[10]

[B-30] 3GPP TR 33.980, Technical Report on 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA) (Release 7). [5]

[B-31] NIST Special Publication 800-63: Electronic Authentication Guidelines.[9]

[B-32] M-04-04: E-Authentication Guidance for Federal Agencies.

[B-33] IETF RFC 4412, “Communication Resource Priority for the Session Initiation Protocol”. [8]

[B-34] ITU-T Recommendation E.107, Emergency Telecommunications Service (ETS) and Interconnection Framework for National Implementations of ETS.[10]

---

[8] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[9] This document is available at the National Institute of Standards and Technology (NIST), Computer Security at Resource Center (CSRC)
< http://csrc.nist.gov/publications/ >.

[10] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[X.509] ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection – The Directory Public-key and Attribute Certificate Frameworks. [8]