International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2703

(01/2009)

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

Next Generation Networks – Security

The application of AAA service in NGN

Recommendation ITU-T Y.2703

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	**Y.2700–Y.2799**
Generalized mobility	Y.2800–Y.2899

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

Recommendation ITU-T Y.2703

The application of AAA service in NGN

Summary

Recommendation ITU-T Y.2703 provides an application of authentication, authorization and accounting (AAA) for NGN release 1.

Source

Recommendation ITU-T Y.2703 was approved on 23 January 2009 by ITU-T Study Group 13 (2009-2012) under the WTSA Resolution 1 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T Y.2703

The application of AAA service in NGN

1 Scope

This Recommendation describes an application for authentication, authorization and accounting (AAA) for next generation networks (NGNs) based on [b-ITU-T Y.2201]: NGN release 1 requirements, [b-ITU-T Y.2012]: Functional requirements and architecture of the NGN release 1 (FRA), [b-ITU-T Y.2701]: Security requirements for NGN release 1, and [b-ITU-T Y.2702]: NGN authentication. This Recommendation applies to the authentication, authorization and accounting process in accessing an NGN using the AAA client and AAA server. In particular, this Recommendation addresses the accounting function only from the standpoint of its contribution to security accounting.

The scope of this Recommendation is:

1) The enrolment process.
2) Authentication functions and procedures.
3) Authorization functions and procedures.
4) Security-accounting functions and procedures.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation makes use of the following terms defined elsewhere:

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

3.1.2 authentication certificate [b-ITU-T X.811]: A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.

3.1.3 authentication information [b-ITU-T X.811]: Information used for authentication purposes.

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

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

3.1.6 security audit trail [b-ITU-T X.800]: Data collected and potentially used to facilitate a security audit.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 security accounting: The role that tracks security-related actions or events that can be included as resources in the security audit function.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AAA Authentication, Authorization and Accounting

AM-FE Access Management Functional Entity

ANI Application-to-Network Interface

EAP Extensible Authentication Protocol

ID Identity – as defined by the network, service, or entity being accessed

NAS Network Access Server

NGN Next Generation Network

NNI Network-to-Network Interface

NP Network Provider

OAMP Operations, Administration, Maintenance, and Provision

RACF Resource Access Control Function

SCTP Stream Control Transport Protocol

SR Service Resource

TAA-FE Transport Authentication and Authorization Functional Entity

TE Terminal Equipment

TUP-FE Transport User Profile Functional Entity

UNI User-to-Network Interface

5 Conventions

None.

6 General concepts for the AAA service

This clause deals with the basic concepts of AAA.

6.1 Overview

The authentication, authorization and accounting service provides the functions by which a user's identity is verified (authentication), is given access to the services (authorization) and a means by which consumption of resources is measured (accounting).

6.2 The AAA process

The individual processes within the AAA framework are as follows:

Authentication validates the end user's identity prior to permitting network access. The end user presents a set of credentials such as a username/password combination, a security key, a certificate or biometric data (for example, fingerprints). These credentials are normally agreed during the enrolment process. Verification of the credentials leads to the authorization process.

Authorization defines the privileges and services the end user is allowed once network access is granted. This might include providing an IP address or invoking a filter to determine which applications or protocols are supported. Authentication and authorization are performed together in an AAA-managed environment.

Accounting provides the methodology for collecting information about the end user's resource consumption which can then be processed for billing, auditing, and capacity-planning purposes. Certain accounting data is relevant to the development of a security audit trail.

These three processes are centralized into a set of functions which together provide access control.

6.3 AAA procedure

The AAA service system is composed of an AAA server and an AAA client.

The AAA server has access to a database of user profiles and configuration data. It communicates with AAA clients residing on network components such as NAS (network access server) and routers, to provide distributed AAA services.

The AAA service scenarios are summarized in the following steps:

- The end user connects to the point-of entry device and requests access to the network.
- The AAA client forwards the end user's identity/authentication credentials to the AAA server.
- The AAA server authenticates the user based on the credentials. If authentication is successful, the server then determines which service(s) are authorized and returns an accept or reject response and other relevant data to the AAA client.
- The AAA client notifies the end user that access to specified resources has been granted or denied.

The AAA client sends an accounting message to the AAA server during connection set-up and termination for record collection and storage.

7 Application model for authentication and authorization in NGN

This Recommendation is based on security requirements for NGN in [b-ITU-T Y.2701] and the NGN authentication reference model in [b-ITU-T Y.2702]. The NGN authentication reference model (Figure 7-1) depicts eight authentication reference points; three of which are considered/taken into account by this Recommendation:

They are:

(1) access of user to network;

(2) access of user to network provided service;

(4) access of service provider to receiving user.

Reference points (1) and (4) refer to transport of user traffic and may be viewed as depending on "horizontal" access control at the transport control level, whereas reference points (2) and (8) may be viewed as depending on control data between the transport and service control layers and therefore as being "vertical." This relationship is displayed in Figure 7-2.

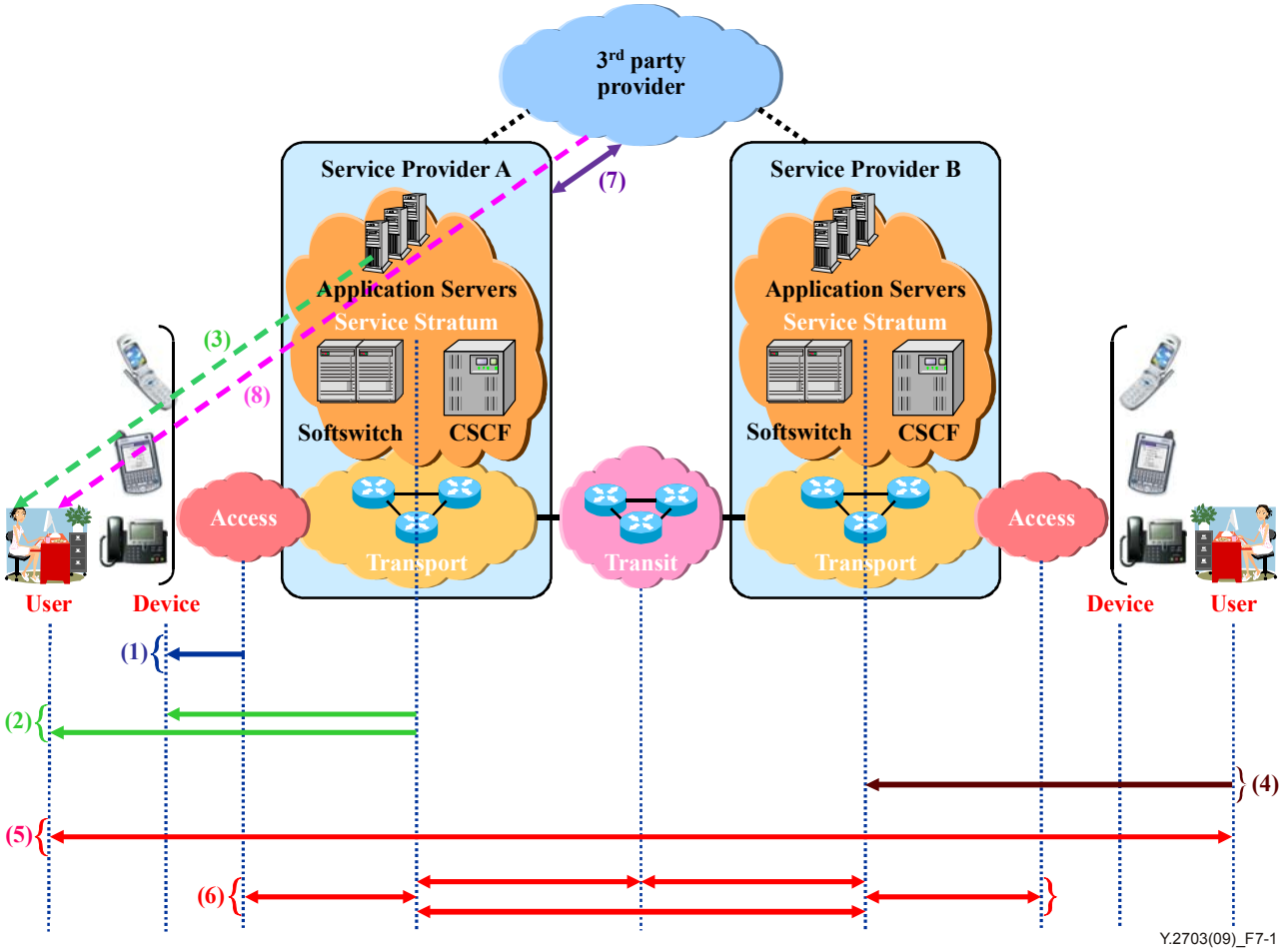

Figure 7-1 – End-to-end reference architectural model (Y.2702 NGN authentication)

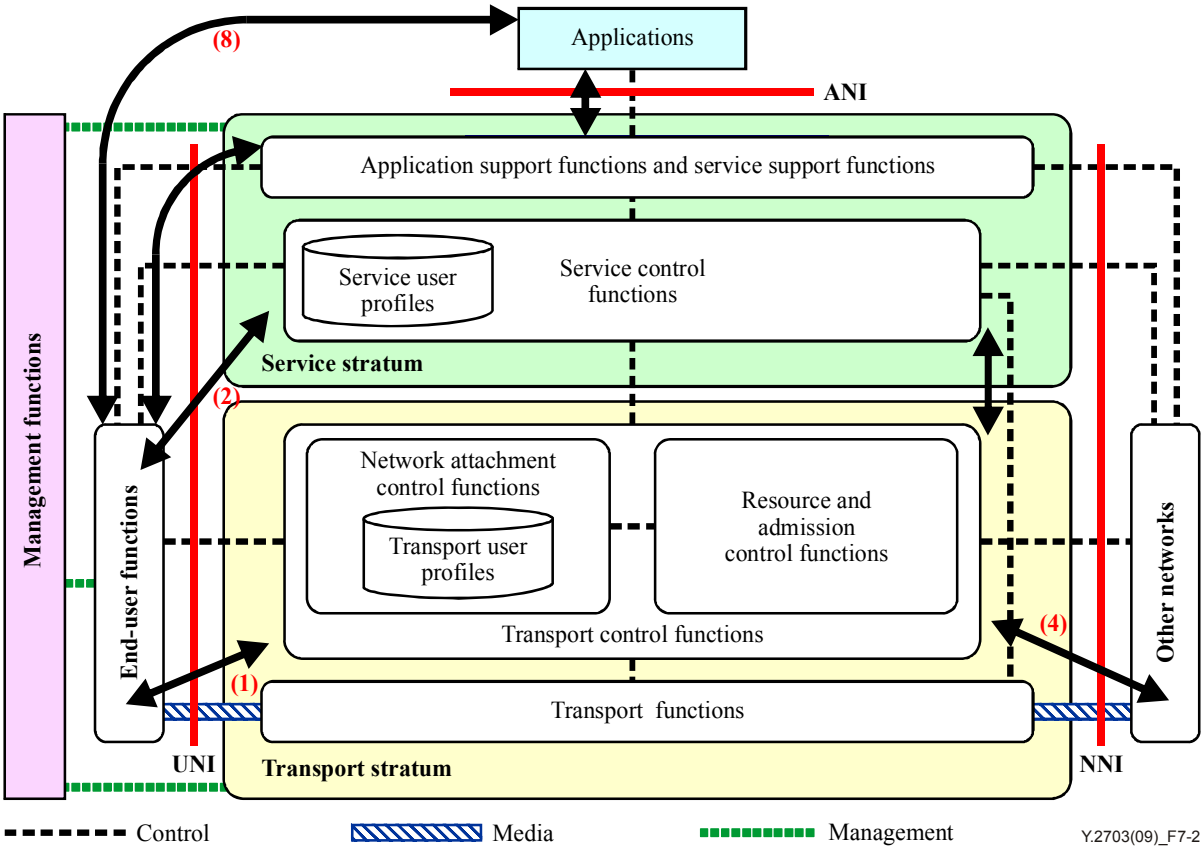

Figure 7-2 – NGN architecture and AAA related domains (Y.2702 NGN authentication)

8 AAA architecture in NGN

This clause describes the relationship between the AAA reference model and the functional architectural model described in [b-ITU-T Y.2012].

8.1 User to network access

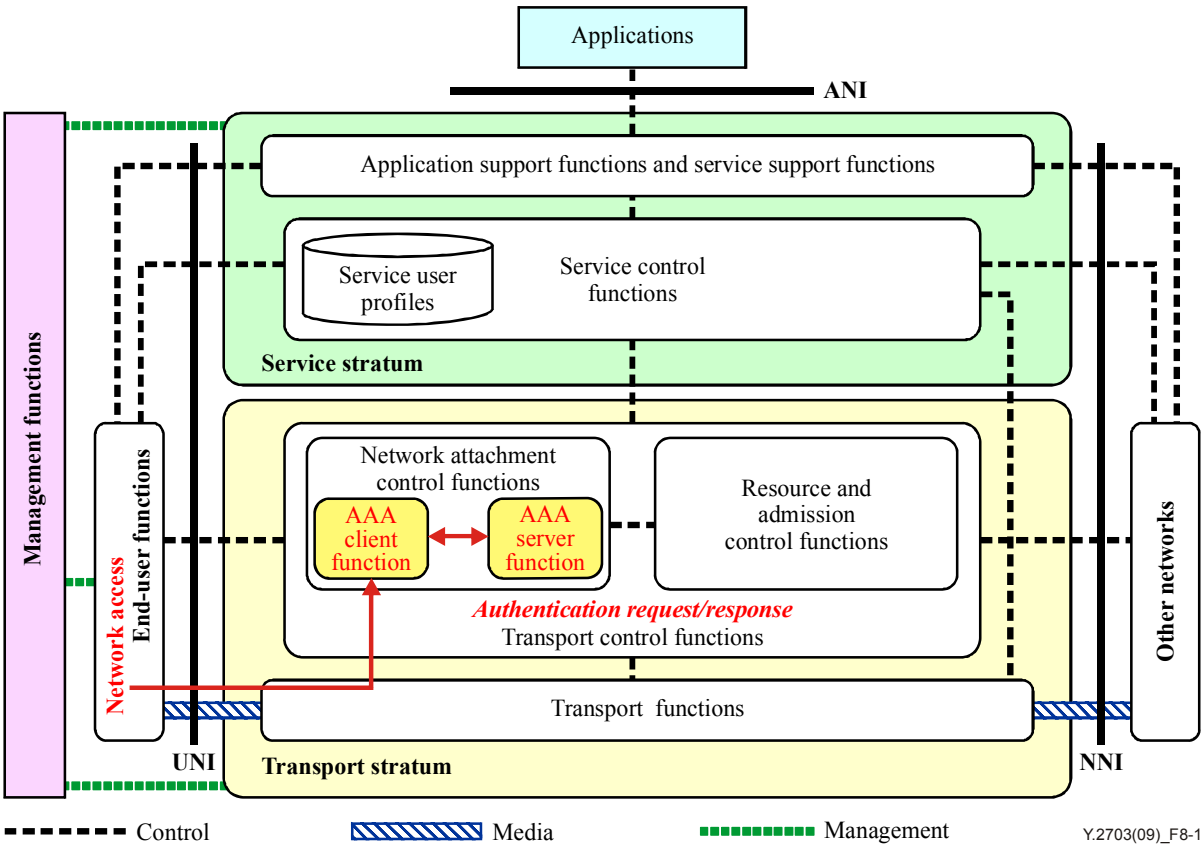

Figure 8-1 – Authentication and authorization of a user for network access

Figure 8-1 shows the application of AAA for user to network access (i.e., an application of type-1 in Figure 7-1 above).

Once an entity in the transport control functions (typically, T-14 AM-FE) detects the connection request from a user terminal, it starts acting as an AAA client. It requests the entities in the transport control functions which play the role of AAA server (such as T-11 TAA-FE, and T-12 TUP-FE), for authentication of the user and authorization for the use of NGN resources. The protocols such as RADIUS or Diameter can be used for this request and response procedure. Based on the request from an AAA client, an AAA server authenticates the user by explicit (e.g., EAP) or implicit (e.g., access-line authentication) procedures. After successful authorization of a user depending upon the user profile (usually managed by TUP-FE), the AAA server requests RACF for reservation and allocation of NGN resources for that user. Once it is granted, the AAA server notifies the AAA client of permission to connect that user equipment.

8.2 User to network service attachment

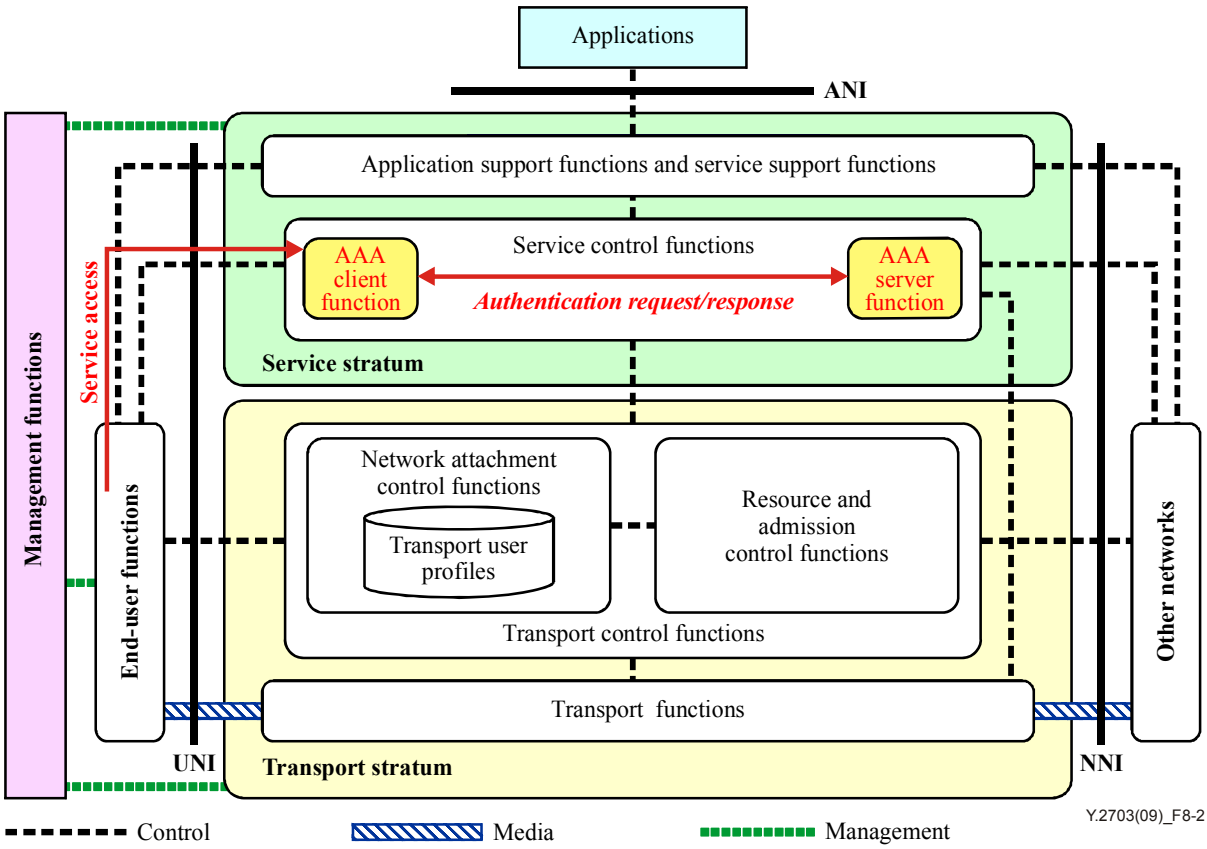

Figure 8-2 – Authentication and authorization of user for service access

Figure 8-2 shows the application of AAA for user to service access (i.e., an application of type-2 in Figure 7-1 above).

Similarly to the previous case shown by Figure 8-1, an AAA client in service control functions (typically, S-1 S-CES-FE) detects the connection request from a user terminal. It requests an AAA server (such as S-5 SUP-FE, or S-6 SAA-FE), for authentication and authorization for the requested service. A service based on the service request is either provided or rejected depending upon the result of authentication and authorization.

Once the user is connected to the network or the service, each AAA client notifies its AAA server of the information on NGN resources consumed by the user to help an AAA server collect accounting information associated with the user.

8.3 Authentication and authorization of user for access to 3rd party service

Third-party services accessed through the ANI are not addressed in NGN release 1. Therefore, the authentication and authorization of user for access to third-party services is out of scope of this Recommendation. This Recommendation does not depict the reference model for third-party services. However, a use-case illustrating authentication and authorization of a 3rd party service is described in Appendix III.

9 Enrolment

A prerequisite for AAA is identification of the entity to be authenticated, e.g., the user or device. The credentials that identify the entity are established through an enrolment process which establishes the unique identity of a user/device. The credentials are used in the authentication process whenever access to service(s) is sought. The enrolment process may include acceptance of terms and conditions as well as financial arrangements. Although the initial verification of identity and credentials is referred to as enrolment, subsequent access to services and credential checks are known as registration. Precise arrangements for enrolment will depend on provider policies, nature of services, etc.

10 Authentication

This Recommendation uses the basic concepts of authentication described in [b-ITU-T X.811]. Network and service access authentication services and capabilities are needed to mitigate threats associated with attempts to gain unauthorized access. Additional information on digital certificate is in Appendix II.

10.1 Authentication entities

The term "claimant" is used to describe an entity which requests authentication. A claimant includes the functions necessary for engaging in authentication exchanges.

The AAA client provides a specialized function that is part of the access path between the claimant and the verifying entity on each access request and enforces the decision made by the verifier.

In the AAA managed environment, the AAA server is the verifying entity and issues an authentication certificate to the claimant upon successful authentication.

10.2 Procedure for authentication

In a AAA managed environment, the AAA server provides the authentication service for the user. It identifies the entity requesting access sufficiently to determine which services can be authorized for access and charged for. An authentication certificate may be issued by the AAA server.

10.2.1 Successful authentications

The following steps and Figure 10-1 provide an example of the message flow for a successful authentication.

Step 1. An entity requests the AAA client for access.

Step 2. The AAA client requests the AAA server for authentication of the entity.

Step 3. The AAA server requests the AAA client for the credentials of the entity to start the authentication.

Step 4. The AAA client requests the entity for the credential(s) required for authentication.

Step 5. The entity, now a claimant, sends the requested credential(s) to the AAA client.

Step 6. The AAA client forwards the required credential(s) to the AAA server for authentication.

Step 7. The AAA server verifies the received credential(s) against the claimant's user profile.

Step 8. If the credentials could be verified, the AAA server proceeds to the authorization process without notifying the AAA client or claimant.

Step 9. After the authorization process, the AAA server sends an allow access message to the AAA client.

Step 10. The AAA client forwards the allow access message to the claimant.

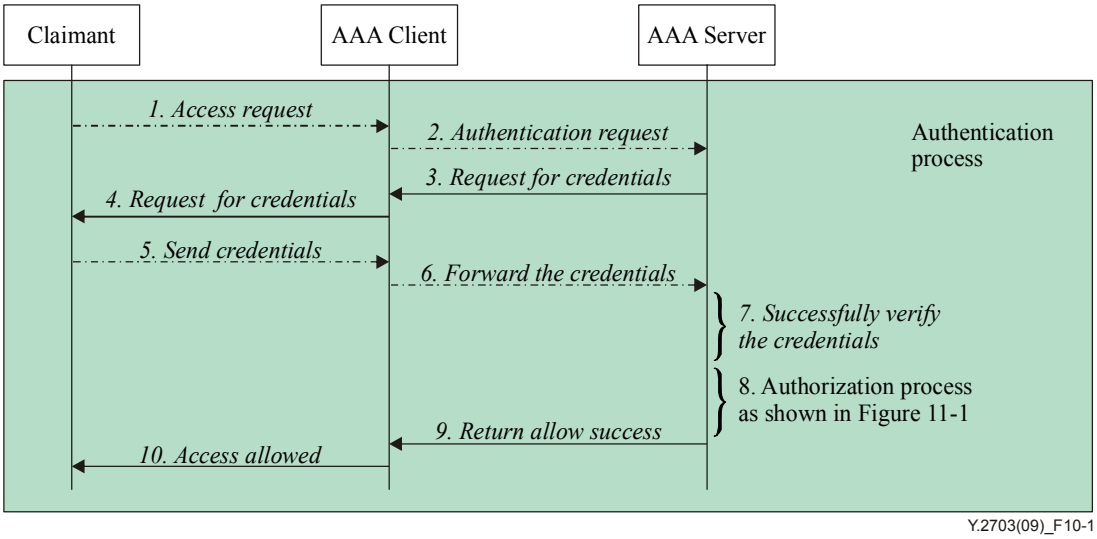

Figure 10-1 – Message flows for successful authentication

10.2.2 Unsuccessful authentications

The following steps and Figure 10-2 provide an example of the message flow for an unsuccessful authentication.

Step 1. An entity requests the AAA client for access.

Step 2. The AAA client requests the AAA server for authentication of the entity.

Step 3. The AAA server requests the AAA client for the credentials of the entity to start the authentication.

Step 4. The AAA client requests the entity for credential(s) required for authentication.

Step 5. The entity, now a claimant, sends the requested credential(s) to the AAA client.

Step 6. The AAA client forwards the required credential(s) to the AAA server for authentication.

Step 7. The AAA server verifies the received credential(s) against the claimant's user profile.

Step 8. If the credentials could not be verified, the AAA server sends a deny access message to the AAA client.

Step 9. The AAA client forwards the deny access message to the claimant.

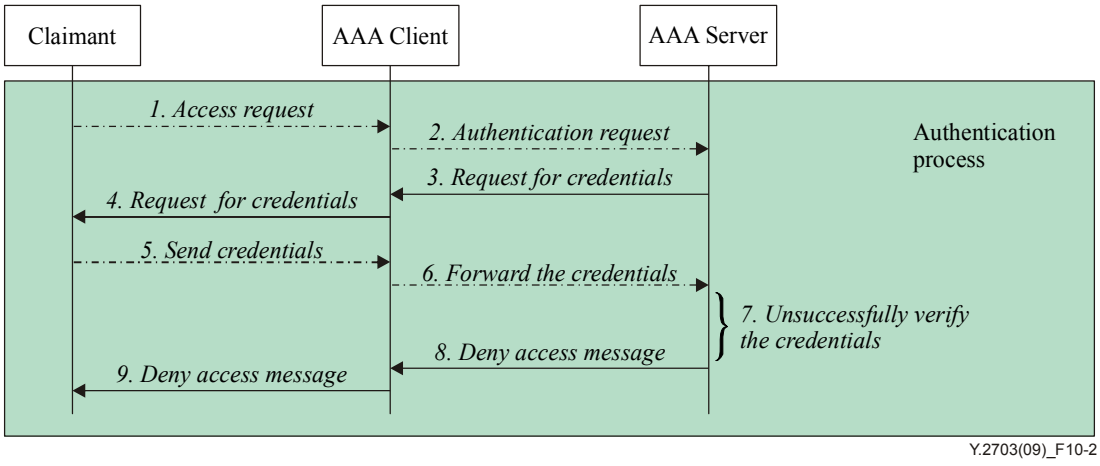

Figure 10-2 – Message flows for unsuccessful authentication

11 Authorization

Authorization is defined as the act of determining whether a particular privilege can be granted to the presenter of a particular credential. The privilege can be the right of access to service resource (SR) and may include reading, writing or modifying resources depending on the policy. The authorization process follows authentication and approves or denies access to NGN service depending on the results of the previous authentication steps and policy.

11.1 Authorization aspects for NGN

The purpose of authorization is to provide and control access to authorized services for the authenticated user. In NGN, the AAA server communicates with network elements containing enrolled entities access privileges.

This Recommendation treats authentication and authorization as associated processes, normally conducted sequentially for enrolled entities each time access is requested. However, a provider's policy may permit an entity to request immediate access/usage rights without re-authentication or enrolment. This case is not addressed.

Authorization of the user for service is accomplished by the AAA server communicating and receiving authorization information from the appropriate network elements. On completion of the authorization process by the AAA server, acknowledgement information is forwarded to the user requesting the service.

Receipt of the acknowledgement information constitutes the successful completion of the authentication and authorization set of processes, and the accessing entity is considered to be connected to the network or authorized SR.

11.2 Authorization entities

The authorization process is performed automatically by the AAA server following authentication without involvement of the accessing entity. The AAA server provides a specialized function that makes the authorization decisions by applying access control policy rules.

11.3 Procedure for authorization

The procedure for the authorization process is as depicted in Figure 11-1:

Step A. Upon the successful authentication of the entity, the AAA server identifies the services and resources available to and accessible for the claimant.

Step B. Once Step A is completed, the AAA server advises the transport and service control functions to assign/allocate authorized services and resources to the claimant's use.

Step C. The AAA server sends an allow access message to the AAA client.

Step D. The AAA client forwards the allow access message to the claimant.

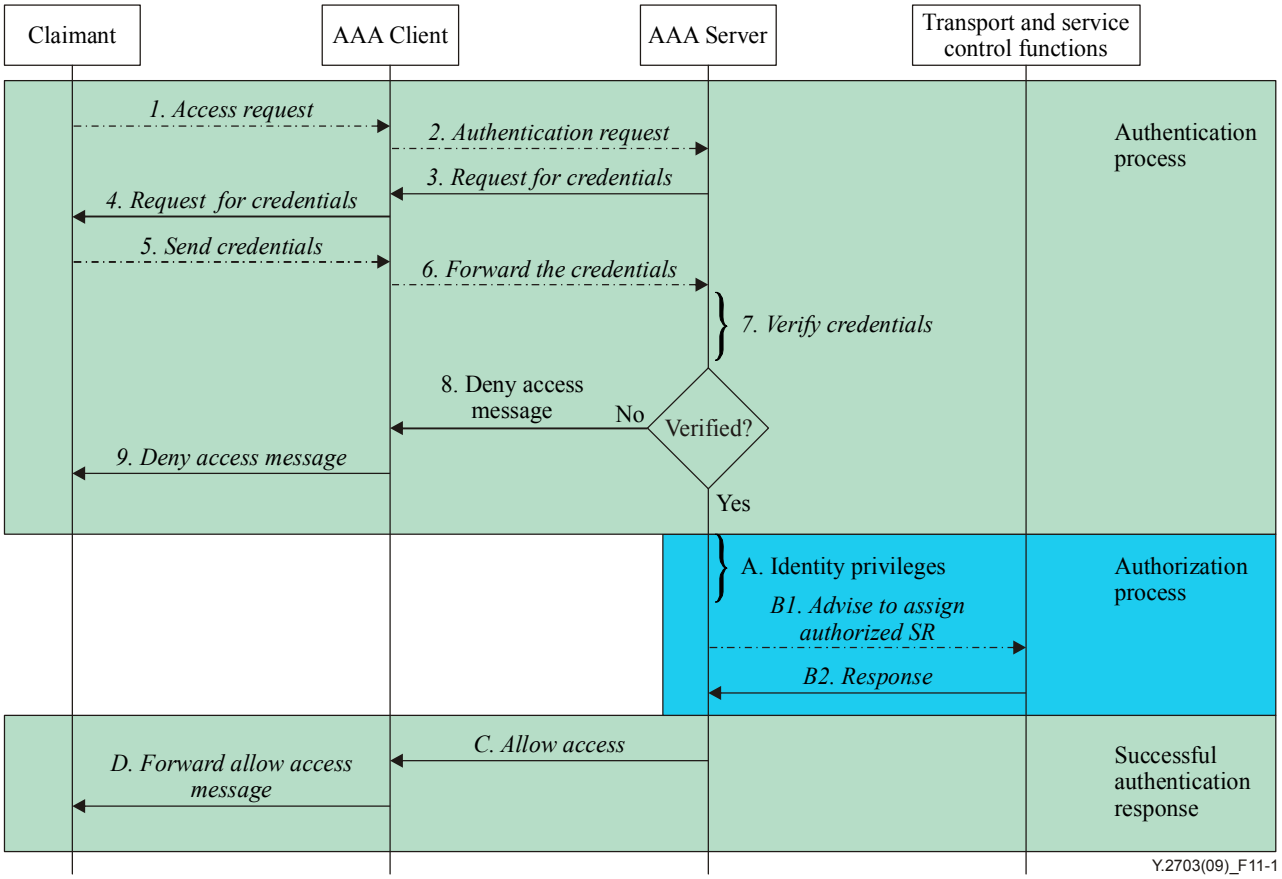

Figure 11-1 – Message flows for the authorization process

12 Accounting

The final "A" in "AAA" stands for accounting. Accounting in the AAA context includes a security element which can be used in association with other security event data to support an accounting function.

12.1 Security accounting

Accounting of security events uses that subset of the accounting function which provides accounting data that is then used in developing a security audit trail for use by the security auditing function. The extent of the security audit trail depends on the security auditing needs and policy identified by the NGN provider for that particular context, e.g., start and end times of successful and unsuccessful network or service access, the service accessed, and identity information of the accessing entity (for successful authentications). The actual audit function is outside the scope of this Recommendation. The procedure of security accounting is as in Figure 12-1.

12.2 Functions for security accounting

The security accounting is a service area that performs functions such as:

1) Capture: is responsible for acquiring detectable data from an event and providing information as relevant to the security context. Data to be captured may include:
   - the results of authentication;
   - information related to revocation of authentication and/or certificate;
   - information on authentication assurance;
   - other information relating to the process of authentication.

2) Storage: keeps the representations that the capture function produces.

3) Review: seeks to accurately describe the event by: verifying the accuracy of what was captured, discerning facts by examining what was captured.

4) Report: takes information from the review function and delivers it to an audit function.

5) Audit: verifies the correctness of a security accounting report or the conformance to usage policy and security guidelines. The audit function may require the ability to alert immediately.

It should be noted that only capture is an AAA function with storage, review, report and audit being management functions. These are out of scope for this Recommendation.

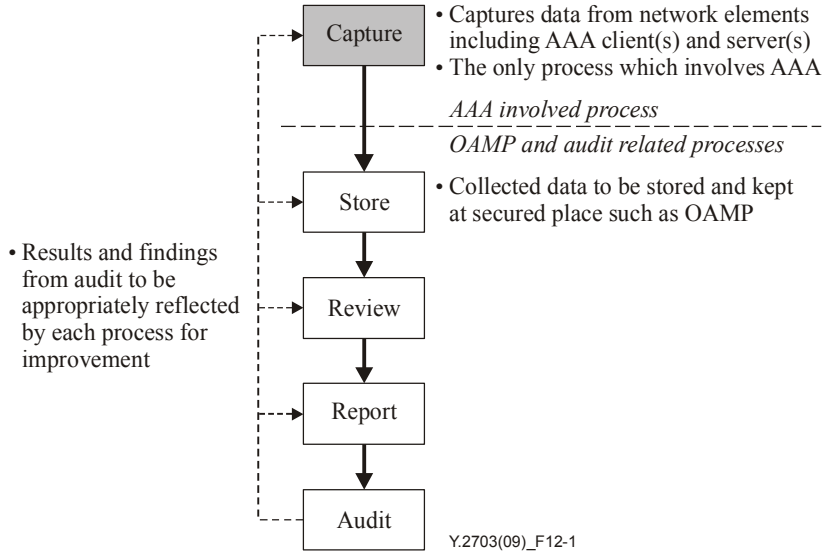

Figure 12-1 – Security accounting process example

Appendix I

Authentication protocol for AAA in NGN

(This appendix does not form an integral part of this Recommendation)

This appendix deals with the EAP protocol that is transported over data link layers, and AAA protocols which provide AAA framework at the various applications.

I.1 EAP protocol for AAA service in NGN

The EAP protocol defines an authentication framework which supports various authentication methods. The EAP runs on the peer and authentication server via the authenticator. The EAP is directly transported over data link layers such as IEEE 802 and PPP (point-to-point protocol).

However, due to the feature of link dependency, the EAP protocol requires the lower layer such as EAPoL, IEEE 802.1X, and IEEE 802.11i. Figure I.1 describes the EAP multiplexing model. The EAP method layer includes the authentication algorithm. The EAP peer and authenticator have a respective functionality as an authentication client and authenticator. The EAP layer performs the delivery of the EAP messages. The lower layer transmits or receives the EAP frames between the peer and the authenticator. Since the link layer consists of various link protocols, the EAP requires various lower layers for each link protocol.

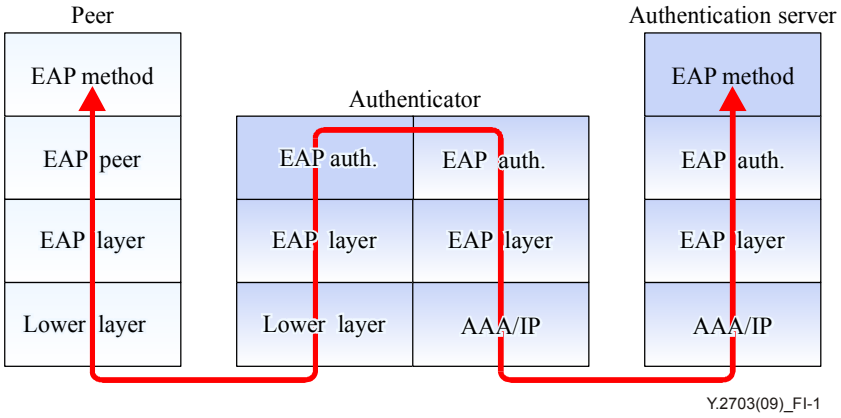

Figure I.1 – EAP forwarding model

The EAP requires lower layer for reliable message delivery, error detection, and ordering messages as follows:

- Since the EAP does not know that the peer receives the message from the authenticator, the EAP requires the reliable channel between the peer and the authenticator.
- The EAP does not assure that the EAP messages are delivered to the destination without error. The EAP needs an error detection function from the lower layer.
- The EAP messages might be changed in order or duplicated by any reason. Thus, the EAP requires duplication detection and ordering for guaranteeing correct operations.
- The lower layer does not know whether the upper layer includes authentication protocol or not. The EAP requires an indication of the authentication protocol.

I.2 AAA protocols

AAA protocols such as RADIUS were initially deployed to provide dial-up PPP and terminal server access. Diameter protocol was developed with the growth of the Internet and the introduction of new access technologies. Table I.1 shows the comparison of AAA protocols.

Table I.1 – Comparison of AAA protocols

	RADIUS	DIAMETER
Network size	Small	Large
Transport	UDP	SCTP/TCP
Encryption	Password only	Entire packet
Authentication/Authorization	Combination	Combination
Standard	IETF	IETF
Protocol architecture	C/S	P2P
Scalability	Low	High

In case of RADIUS protocol, managing dispersed serial line and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are by definition a link to the outside world, they require careful attention to security, authorization and accounting. This can be best achieved by managing a single "database" of users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user.

The base Diameter protocol may be used by itself for accounting applications, but for use in authentication and authorization, it is always extended for a particular application.

Appendix II

X.509 digital certificates as credentials

(This appendix does not form an integral part of this Recommendation)

A common method for providing authentication assurance is the use of digital certificates as described in [b-ITU-T X.509] and [b-ITU-T X.811]. The certificate defined by [b-ITU-T X.509], which is widely used, contains the following data types.

– ***version*** is the version of the encoded certificate. If the extensions component is present in the certificate, version shall be v3. If the issuerUniqueIdentifier or subjectUniqueIdentifier component is present, version shall be v2 or v3.

– ***serialNumber*** is an integer assigned by the CA to each certificate. The value of serialNumber shall be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate).

– ***signature*** contains the algorithm identifier for the algorithm and hash function used by the CA in signing the certificate (e.g., md5WithRSAEncryption, sha-1WithRSAEncryption, id-dsa-with-sha1, etc.).

– ***issuer*** identifies the entity that has signed and issued the certificate.

– ***validity*** is the time interval during which the CA warrants that it will maintain information about the status of the certificate.

– ***subject*** identifies the entity associated with the public-key found in the subject public key field.

– ***subjectPublicKeyInfo*** is used to carry the public key being certified and to identify the algorithm which this public key is an instance of (e.g., rsaEncryption, dhpublicnumber, id-dsa, etc.).

– ***issuerUniqueIdentifier*** is used to uniquely identify an issuer in case of name reuse.

– ***subjectUniqueIdentifier*** is used to uniquely identify a subject in case of name reuse.

– ***extensions field*** allows addition of new fields to the structure.

Appendix III

Authentication and authorization use-case

(This appendix does not form an integral part of this Recommendation)

The use-case using the AAA service in this appendix is based on the reference model provided in [b-ITU-T Y.2702].

III.1 Authentication and authorization of user for network access

Network access authentication and authorization services are needed to verify the identities and to determine whether access should be granted to the end user equipment.

III.1.1 Device access/attachment to NGN authentication and authorization

In this case, there are 3 types of NGN device access/attachment, authentication and authorization. These services and capabilities identify, authenticate and authorize user devices access or attachment to the access IP network:

– identify, authenticate and authorized legacy TE and TE-BE for access/attachment to the access IP network ((1) of Figure III.1);

– identify, authenticate and authorize legacy TE and TE-BE with IAD in the customer domain for access/attachment to the access IP network ((2) of Figure III.1);

– identify, authenticate and authorize NGN TE and TE-BE with IP capabilities in the customer domain for access/attachment to the IP network ((3) of Figure III.1).

The AAA client provides the authentication service for the device and network provider: it automatically allows the device to access the network provider, as necessary.

The procedure of identification depicted in (1) of Figure III.1 is as follows:

Step 1: The gateway (claimant) requests network access/attachment from the AAA client

Step 2: The AAA client requests the identification of the gateway from AAA server (verifier) which identifies the gateway

Step 3: The AAA server sends the results of identification to the AAA client

Step 4: The AAA client forwards the results to the gateway, where the AAA client stores the access list of the gateway

In case of (2) and (3), IAD and NGN TE is claimant respectively. The remaining process is identical to the procedure of (1).

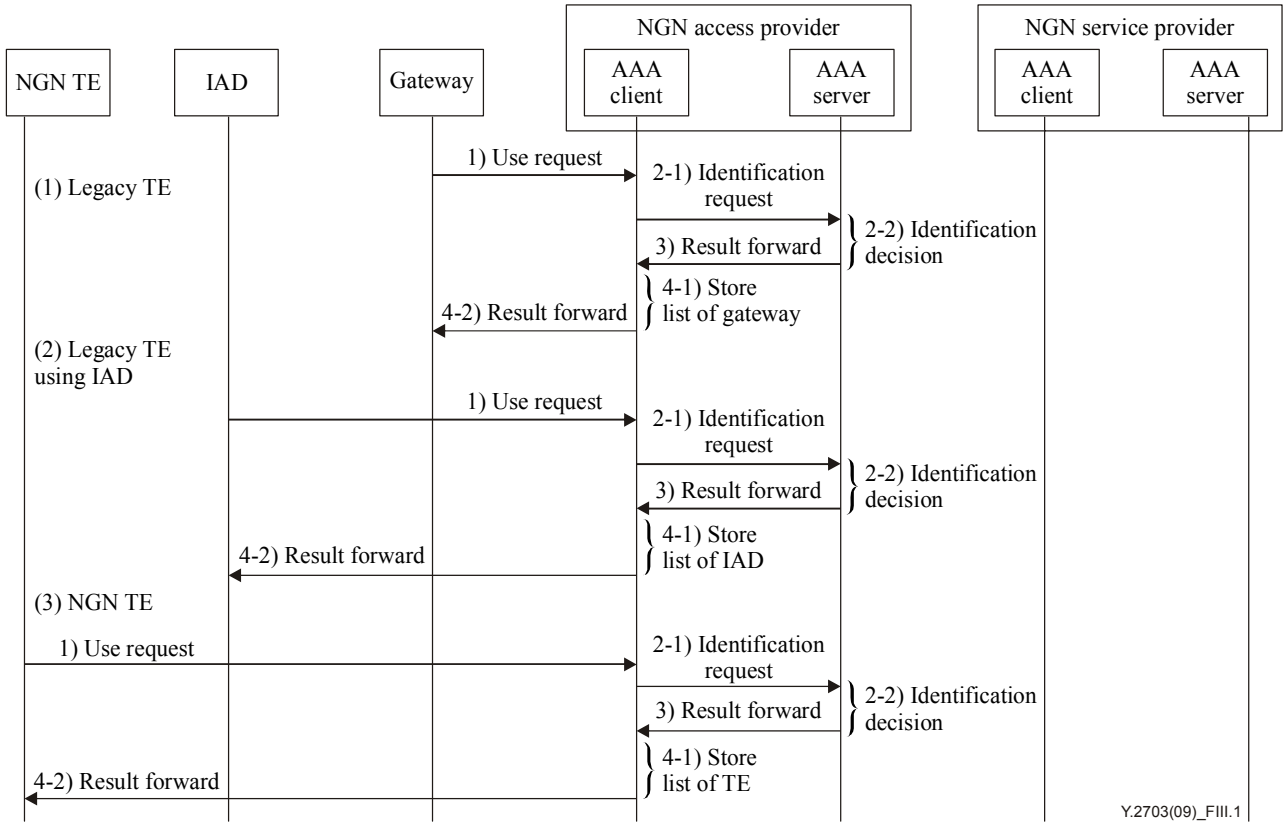

Figure III.1 – Procedure of identification for a device to access NGN network

III.1.2 Bundled device access/attachment to NGN and service/application authentication and authorization

In this case, there are 3 types of NGN access/attachment, authentication and authorization. These services and capabilities bundle the NGN access provider authentication of the user device with that of the NGN service provider as follows:

– services and capabilities for the NGN service provider to implicitly identify and authorize legacy TE and TE-BE ((1) of Figure III.2);

– services and capabilities for the NGN service provider to implicitly identify and authorize legacy TE and TE-BE with IAD ((2) of Figure III.2);

– services and capabilities for the NGN service provider to directly identify, authenticate and authorize NGN TE and TE-BE in the customer domain ((3) of Figure III.2).

The AAA client provides the authentication service for the device and service/application provider: it automatically allows the device to access the service/application provider, as necessary.

The procedure of the identification depicted in (1) of Figure III.2 is as follows:

Step 1: The gateway (claimant) requests the use of service/application from the AAA client

Step 2: The AAA client requests the identification of the gateway from the AAA server (verifier) in the access network domain, where the AAA server identifies the gateway

Step 3: The AAA server sends the results of the identification to the AAA client and the AAA server in the NGN service provider domain simultaneously

Step 4: The AAA client forwards the results to the gateway, where the AAA client stores the access list of the gateway

The procedure of the identification depicted in (2) of Figure III.2 is as follows:

Step 1: The IAD (claimant) requests the use of service/application from the AAA client.

Step 2: The AAA client requests the identification of the IAD from the AAA client in the NGN service provider domain, where the AAA server (verifier) in the NGN service provider domain identifies the IAD.

Step 3: The AAA server sends the results of the identification to the AAA client.

Step 4: The AAA client forwards the results to IAD, where the AAA client stores the access list of IAD.

In case of (3), NGN TE is claimant. The remaining process is identical to the procedure of (2).

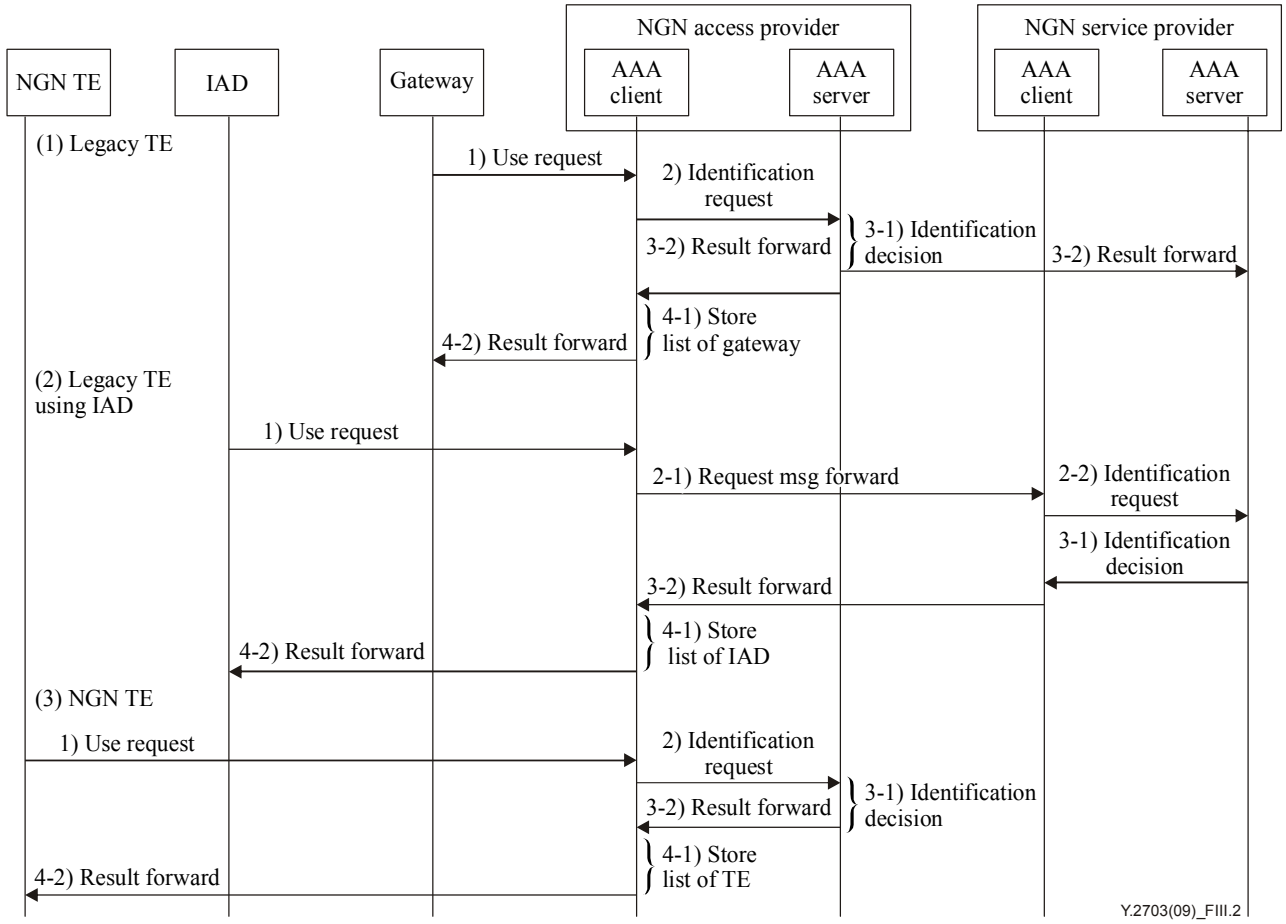

Figure III.2 – Procedure of identification for a device to use service/application provider

III.2 NGN service provider authentication and authorization of user for access to service/application

In this case, there are 3 types in service/application authentication and authorization in a multi-network provider:

– NGN service provider indirect authentication of a user device through trust relations with the NGN access provider ((1) of Figure III.3);

– NGN service provider direct authentication and authorization of a user device. ((2) of Figure III-3);

– NGN service provider direct authentication of the user ((3) of Figure III.3).

The AAA client provides the authentication service for the user and service/application provider: it automatically allows the user to access the service/application provider, as necessary.

The procedure of the identification depicted in (1) of Figure III.3 is as follows:

Step 1: The TE (claimant) requests the use of service/application from the AAA client.

Step 2: The AAA client requests the identification of the device from the AAA server (verifier) in the access network domain, where the AAA server identifies the device.

Step 3: The AAA server sends the results of the identification to the AAA client and the AAA server in the NGN service provider domain simultaneously.

Step 4: The AAA client forwards the results to the gateway, where the AAA client stores the access list of the device.

The procedure of the identification depicted in (2) of Figure III.3 is as follows:

Step 1: The TE (claimant) requests the use of service/application from the AAA client in the NGN service provider domain.

Step 2: The AAA client requests the identification of the device from the AAA server (verifier) in the NGN service provider domain, where the AAA server identifies the device.

Step 3: The AAA server sends the results of the identification to the AAA client.

Step 4: The AAA client forwards the results to the device, where the AAA client stores the access list of the device.

The procedure of the authentication depicted in (3) of Figure III.3 is as follows:

Step 1: The user (claimant) requests the use of service/application from the AAA client in the NGN service provider domain.

Step 2: The AAA client requests the authentication of the user from the AAA server (verifier) in the NGN service provider domain that authenticates the user.

Step 3: The AAA server sends the results of the authentication to the AAA client.

Step 4: The AAA client forwards the results to the user, where the AAA client stores the access list of the user.

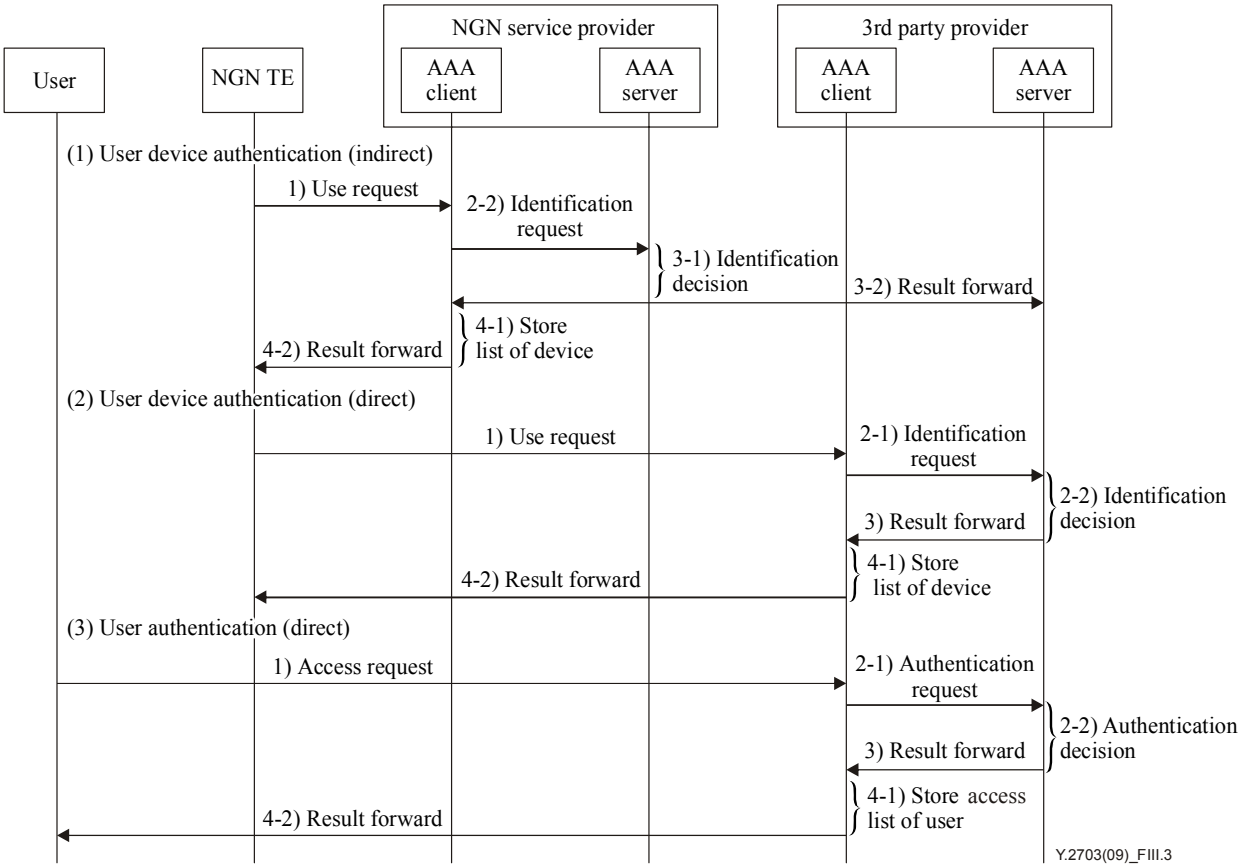

Figure III.3 – Procedure of NGN service provider authentication and authorization of user

III.3 User authentication and authorization of NGN providers

In this case, there are 2 types in user authentication and authorization of the network:

– User authentication of NGN provider for network attachment ((1) of Figure III.4).

– User authentication of NGN provider for obtaining the service ((2) of Figure III.4).

The AAA client provides the authentication service for the user authentication and authorization of the network: it automatically allows the user to access the network provider, as necessary.

The procedure of the identification depicted in (1) of Figure III.4 is as follows:

Step 1: The user (claimant) requests authentication of the NAP (network access points) from the 3rd party verifier.

Step 2: The 3rd party verifier forwards AI (authentication information) to the NAP.

Step 3: Exchange AI between 3rd party verifier and the NAP.

Step 4: The 3rd party verifier forwards the results to the user, where the 3rd party verifier verifies.

The procedure of the identification depicted in (2) of Figure III.4 is as follows:

Step 1: The user (claimant) requests authentication of network from the 3rd party verifier.

Step 2: The 3rd party verifier forwards the request of the user to the AAA client, where the AAA client requests AI from the AAA server.

Step 3: The AAA server sends AI to the AAA client and exchanges AI between the 3rd party verifier and the AAA client.

Step 4: The 3rd party verifier forwards the results to the user, where the 3rd party verifier verifies.

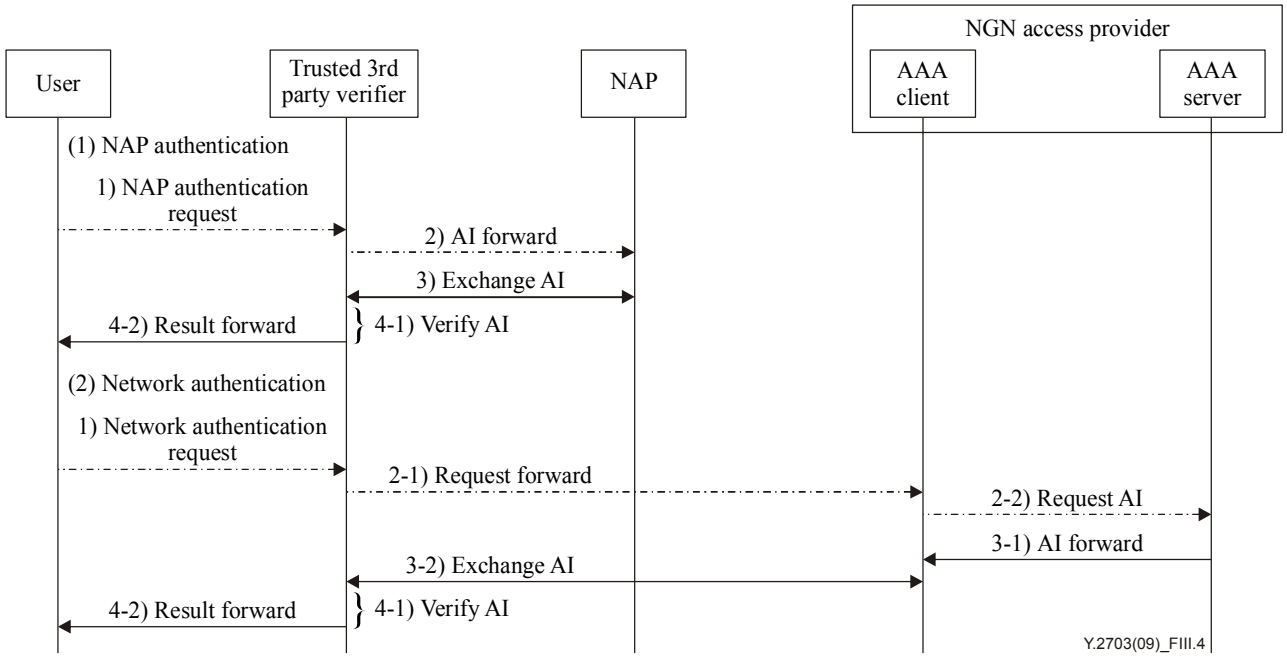

Figure III.4 – Procedure of user authentication and authorization of NGN providers

III.4 NGN provider authentication and authorization of 3rd party service/application provider

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). The NGN provider would need to authenticate and authorize the 3rd party service/application provider.

The AAA client provides the authentication service for the NGN provider authentication and authorization of the 3rd party service/application provider.

The procedure of the identification depicted in Figure III.5 is as follows:

Step 1: The AAA client (claimant) in the NGN provider requests an authentication from the 3rd party service/application provider to the 3rd party verifier.

Step 2: The 3rd party verifier forwards the request of the user to the AAA client in the 3rd party service/application provider and the AAA client requests AI from the AAA server.

Step 3: The AAA server forwards AI to the AAA client and exchanges AI between the 3rd party verifier and the AAA client.

Step 4: The 3rd party verifier forwards the results to the AAA client in the NGN provider, where the 3rd party verifier verifies and the AAA server stores the result.

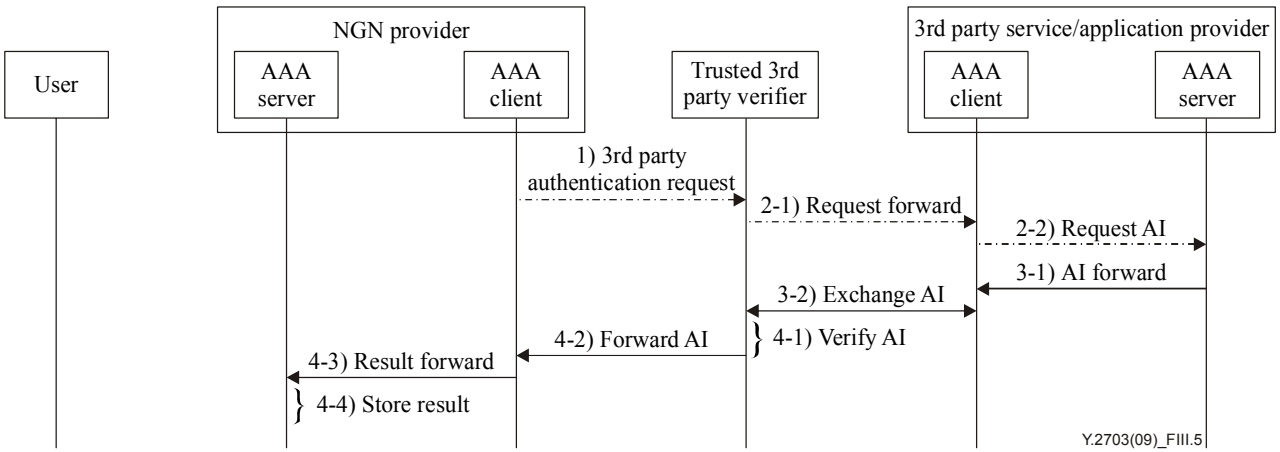

Figure III.5 – Procedure of NGN provider authentication and authorization of 3rd party service/application provider

III.5 Use of 3rd party authentication and authorization service

Service providers may provide third party authentication and authorization. In this case, there are 2 types in use of 3rd party authentication and authorization service:

– Authentication of the user to a service provider ((1) of Figure III.6).

– Authentication of a service provider to the user ((2) of Figure III.6).

III.5.1 Authentication of the user to a service provider

The AAA client provides the authentication service for the user authentication and authorization to a service provider: it automatically allows the user to access a 3rd party service/application provider, as necessary.

The procedure of the identification depicted in Figure III.6 is as follows:

Step 1: The user (claimant) requests network access from the AAA client.

Step 2: The AAA client requests qualification from the user to the AAA server in the 3rd party service/application provider, where the AAA server (verifier) authenticates the user.

Step 3: The AAA server sends the results of authentication to the AAA client.

Step 4: The AAA client forwards the results to the user, where the AAA client stores the access list of the user.

Step 5: If granted, the user can access the specified resource of the network.

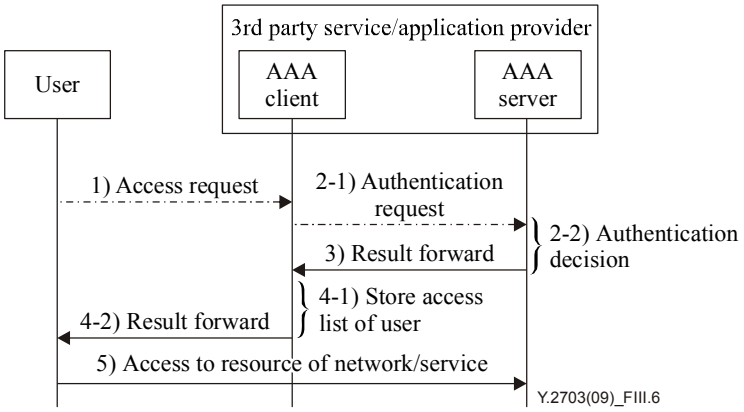

Figure III.6 – Procedure of use of 3rd party authentication and authorization service

III.5.2 Authentication of a service provider to the user

The AAA client provides the authentication service for authentication of a service provider to the user. The procedure of the identification depicted in Figure III.7 is as follows:

Step 1: The user (claimant) in custom domain requests authentication from the 3rd party service/application provider to the 3rd party verifier

Step 2: The 3rd party verifier forwards the request of the user to the AAA client in the 3rd party service/application provider, and the AAA client requests AI from the AAA server

Step 3: The AAA server forwards the AI to the AAA client and exchanges AI between the 3rd party verifier and the AAA client

Step 4: The 3rd party verifier forwards the results to the AAA client in the NGN provider, where the 3rd party verifier verifies and stores the result

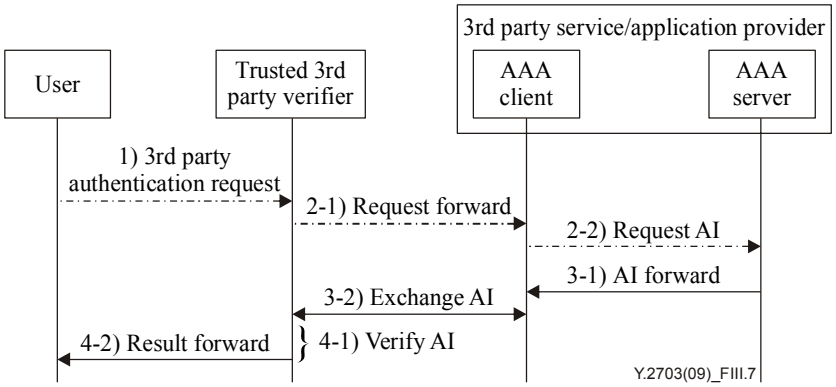

Figure III.7 – Procedure of use of 3rd party authentication and authorization service

Bibliography

[b-ITU-T M.3410] Recommendation ITU-T M.3410 (2008), *Guidelines and requirements for security management systems to support telecommunications management*.

[b-ITU-T Q.3201] Recommendation ITU-T Q.3201 (2007), *EAP-based security signalling protocol architecture for network attachment*.

[b-ITU-T Q.3202.1] Recommendation ITU-T Q.3202.1 (2008), *Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[b-ITU-T X.812] Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

[b-ITU-T X.816] Recommendation ITU-T X.816 (1995) | ISO/IEC 10181-7:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for next generation networks*.

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

[b-ITU-T Y.2233] Recommendation ITU-T Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009