

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1124

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Authentication architecture for mobile end-to-end communication

Recommendation ITU-T X.1124

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

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

Recommendation ITU-T X.1124

Authentication architecture for mobile end-to-end communication

Summary

Recommendation ITU-T X.1124 describes a service layer authentication architecture for mobile end-to-end data communication between mobile users and various service providers in the network. The generic negotiation mechanisms and authentication procedures specified in this Recommendation support both those entities that have miscellaneous authentication capabilities and those entities that have differentiated security requirements. The authentication addressed in this Recommendation is used for service providers and requesters and is independent of network access authentication of the mobile users.

Source

Recommendation ITU-T X.1124 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 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/>.

© ITU 2008

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

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	5
5	Conventions	6
6	Overview	6
6.1	Use case description	6
6.2	Security considerations.....	7
7	Security architecture	8
7.1	Authentication model	8
7.2	Network elements	9
7.3	Reference points	11
7.4	Requirements for authentication information.....	12
7.5	Key structure	13
8	Authentication procedures	14
8.1	Authentication procedures overview	14
8.2	Entity initial authentication procedure	17
8.3	Entity re-authentication procedure	20
8.4	Authentication inquiring procedure with key generation.....	21
8.5	Mutual authentication procedure between SS and SP	25
9	Overall authentication procedures	25
	Appendix I – Some examples of entity authentication procedure	26
I.1	HTTP digest AKA used in 3GPP	26
I.2	HTTP digest AKA used in 3GPP2	27
I.3	TLS-Cert based authentication mechanism.....	28
I.4	Authentication procedure based on public key certificate authentication mechanism.....	29
I.5	Authentication procedure based on a biometric authentication mechanism ..	31
	Appendix II – Examples of mutual authentication between SS and SP	33
II.1	Standardized cases.....	33
II.2	Other possible cases	33
	Appendix III – Key lifetime.....	35
	Appendix IV – Mapping of the reference points to those in 3GPP/3GPP2.....	36
	Bibliography.....	37



Recommendation ITU-T X.1124

Authentication architecture for mobile end-to-end communication

1 Scope

This Recommendation describes service layer authentication architecture in mobile end-to-end data communication between mobile users and various service providers in the network.

This Recommendation applies to three types of entities: mobile terminals in compliance with different mobile communication standards, service authentication-related network elements, and application servers in various networks including mobile networks and open networks. This Recommendation applies to three types of services: the services that are operated by mobile network operators (including the services operated by a visited network, e.g., when a user in a 3rd Generation Partnership Project (3GPP) network uses the service in a 3rd Generation Partnership Project 2 (3GPP2) network); the services provided by application servers on open networks such as the Internet for mobile terminals (e.g., web services and e-mail services); and the services provided by certain powerful mobile users acting as customized service brokers for other mobile users.

This Recommendation provides generic negotiation mechanisms and authentication procedures to support both those entities that have miscellaneous authentication capabilities and those that have differentiated security requirements. The authentication addressed herein is used for service providers and requesters and it is independent of network access authentication of the mobile users. This Recommendation builds upon the work of other standard bodies and consortia to define a more generalized authentication architecture for mobile environments.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- | | |
|----------------|--|
| [ITU-T M.3016] | Recommendation ITU-T M.3016 (1998), <i>TMN Security Overview</i> . |
| [ITU-T X.509] | Recommendation ITU-T X.509 (2000) ISO/IEC 9594-8:2001, <i>Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks</i> . |
| [ITU-T X.800] | Recommendation ITU-T X.800 (1991), <i>Security architecture for Open Systems Interconnection for CCITT applications</i> . |
| [ITU-T X.805] | Recommendation ITU-T X.805 (2003), <i>Security architecture for systems providing end-to-end communications</i> . |
| [ITU-T X.810] | Recommendation ITU-T X.810 (1995) ISO/IEC 10181-1:1996, <i>Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview</i> . |
| [ITU-T X.1121] | Recommendation ITU-T X.1121 (2004), <i>Framework of security technologies for mobile end-to-end data communications</i> . |
| [ITU-T X.1122] | Recommendation ITU-T X.1122 (2004), <i>Guideline for implementing secure mobile systems based on PKI</i> . |

[IETF RFC 4120] IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5)*.
<<http://www.ietf.org/rfc/rfc4120.txt>>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application server [ITU-T X.1121]: An entity that connects to an open network for data communication with mobile terminals.

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

3.1.3 authentication information [ITU-T X.800]: Information used to establish the validity of a claimed identity.

3.1.4 certificate repository [ITU-T X.1122]: Database in which the certificates, CRL and other PKI-related information are stored and which is accessible online.

3.1.5 confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

3.1.6 denial of service [ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.7 eavesdropping [ITU-T M.3016]: A breach of confidentiality by monitoring communication.

3.1.8 masquerade [ITU-T X.800]: The pretence by an entity to be a different entity. For instance, an authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity that has those privileges. Types include replay, relay and compromise of claim authentication information.

3.1.9 mobile network [ITU-T X.1121]: A network that provides wireless network access points to mobile terminals.

3.1.10 mobile terminal [ITU-T X.1121]: An entity that has wireless network access function and connects to a mobile network for data communication with application servers or other mobile terminals.

3.1.11 mobile user [ITU-T X.1121]: An entity (person) that uses and operates the mobile terminal for receiving various services from application service providers.

3.1.12 replay [ITU-T X.800]: A message, or part of a message, is repeated to produce unauthorized effect. For example, a valid message containing authentication information may be replayed by another entity in order to authenticate itself (as something that it is not).

3.1.13 trusted third party (TTP) [ITU-T X.810]: A security authority or its agent, trusted by other entities with respect to security-related operations.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication capability information: Authentication mechanisms supported by a service subscriber or a service provider.

3.2.2 authentication mode: An identifier that specifies authentication mechanisms between a service subscriber (SS) and an entity authentication centre (EAC), a service provider (SP) and an

EAC, and authentication inquiring/derived key generation mechanism/mutual authentication mechanisms between an SS and an SP.

3.2.3 authentication negotiation procedure: A procedure that happens during the authentication procedure in which, according to the local policy, the EAC must choose an authentication mode from the authentication mechanisms supported by service providers/service subscribers and the network.

3.2.4 authentication procedure: The process of authentication between a service entity and the EAC, and authentication between two service entities, i.e., an SS and an SP. Generally, a whole authentication procedure comprises three independent integral sub-procedures: initial authentication between service entity and EAC; authentication inquiring and key generation/transportation/negotiation; and mutual authentication between service entities.

3.2.5 challenge/response: A method of protecting against replay attack. For example, if entity A wants to obtain a new message from entity B, it can first send a challenge in the form of a nonce (e.g., a cryptographic value that is used only once) to B. A then receives a response from B, based on the nonce that proves B was the intended recipient.

3.2.6 derived key: A key, indicated by K_{sp} , that is generated during the authentication inquiring and key generation/transportation/negotiation procedure. The key is shared by an SS and an SP, and it is generally derived using shared keying material K_s , which is the shared key between the EAC and the SS, and the identity information of service entities. It can be the base of mutual authentication between SS and SP, and be used to derive a following session key K_t to protect service communication between the SS and the SP. The length and lifetime of a derived key will be set according to parameters such as service type and security degree. Generally, the algorithm to derive the derived key has a default value.

3.2.7 entity authentication centre (EAC): A central network element defined in the authentication architecture, which accomplishes authentication negotiation and mutual authentication with service entities, establishes shared keying material between service entities, enquires or responds to the inquiring of authentication status of service entities, and helps to generate the derived key for the SS and SP, etc. The function of the EAC may contain other functions, e.g., the bootstrapping function in 3GPP and 3GPP2, the Kerberos server's function, or a certificate verification function.

3.2.8 entity subscription database (ESD): A database-type network element defined in the authentication architecture, which stores service entity's subscription information and authentication information binding with an entity's identifier. In addition, the ESD may have the function to compute necessary authentication data or to achieve such authentication data from another network element, e.g., similar to the function of the authentication centre in 3GPP. The ESD may contain a certificate repository, where the certificates of mobile terminals and network elements in mobile network are stored, and a certificate revocation list (CRL) to perform public key crypto functions.

3.2.9 home network: The mobile network to which the SS subscribes.

3.2.10 interim authentication check identifier (IAC-ID): A temporary identifier for an SP assigned by the EAC during the initial entity authentication of the service provider with the EAC. The identifier can be a local index of the shared keying material between the EAC and the SP. It has a lifetime that is also set by the EAC. When the SP queries the authentication status of a service subscriber from the EAC, its IAC-ID is used to establish its identity.

3.2.11 interim service request identifier (ISR-ID): A temporary identifier for an SS assigned by the EAC during the initial entity authentication of a service subscriber with the EAC. When an SS requests service from a service provider, its ISR-ID is used to establish the SS's identity. It can also act as an index of shared keying material between the EAC and the SS.

3.2.12 policy: A set of rules defined locally by a network element or other network management authority.

NOTE – There could be various policies regarding the enforcement or implementation of this Recommendation.

3.2.13 private entity identifier (PID): A permanent identifier that represents the real identity of an SS. It should be defined to be unique and can be used by the network operator to authenticate, account and manage the SS. The private information of the SS can only be obtained by the EAC and the ESD. An example of a PID is the international mobile subscriber identity (IMSI) in a 3rd Generation Partnership Project (3GPP) network.

3.2.14 public entity identifier (UID): The identifier of an SP that is used for public access of the SP by the EAC and the SS.

3.2.15 service authentication proxy (SAP): A network element that is deployed to transmit the authentication information between the visited SP and the SS's home EAC when an SS uses the service provided by an SP in the visited network which has had a subscription relationship with the SS's home network.

3.2.16 service entity: A service subscriber or a service provider.

3.2.17 service provider (SP): A network entity that is capable of providing services for mobile users. It may be an application server in an operator network or in open network. It may also be a mobile user that has the facilities to provide services to other mobile users.

3.2.18 service subscriber (SS): A network entity that is capable of requesting subscribed services from an SP. Generally, the SS is a mobile user but it may also be an application server that acts as a retailer to obtain service resources for mobile users.

3.2.19 security degree: An identifier (e.g., number) that represents a set of security parameters including at least one authentication mechanism, the crypto algorithms and related parameters to reflect the security requirement of a certain service. It is defined to profile the security requirement of each service.

3.2.20 service type: The particular kind or category of service provided by the SP and consumed by the SS. There are several kinds of service and each service belongs to one service type, e.g., in 3GPP, there are service types of unspecific service, PKI-Portal, presence and MBMS, etc.

3.2.21 shared keying material: Key data which is generated during mutual authentication procedure of the SS (or SP) and the EAC, and which is used to protect the security communication of the reference point connecting the EAC and the SS (or SP). The shared keying material between the SS and the EAC is denoted by K_s and the shared keying material between the SP and the EAC is denoted by K_p . Its key length, generation algorithm and lifetime are set according to some other parameters, such as service type and security degree.

3.2.22 subscription information: The information that reflects the subscribing relationship among an SS, an SP and the relying mobile network. Subscription information between a service subscriber and its home network contains the subscriber's private entity identifier (e.g., PID), the basic key material (e.g., a shared secret or a public-key certificate) and its lifetime, entity service permission flag (i.e., whether it is allowed to request a specific service), the supported authentication mechanism(s) (e.g., HTTP authentication and key agreement, Diffie-Hellman based authentication mechanisms, a biometric authentication mechanism, etc.), and the authentication inquiring and key generation mechanism (e.g., GBA, Kerberos, Mediation), etc. Subscription information between a service provider and a mobile network contains the provider's identity information and public entity identifier (e.g., UID) according to the service, optionally the basic key material (e.g., a shared secret or a public-key certificate) and its lifetime, entity service permission flag (e.g., whether it is allowed to provide a specific service), the supported authentication

mechanisms (e.g., certificate-based TLS authentication mechanism, PSK-TLS, IPSec), and the authentication inquiring and key generation mechanism (e.g., GBA, Kerberos, Mediation), etc.

3.2.23 user universal identification module (UUIIM): The logical entity in the mobile terminal containing the permanent keys and the functions required to perform the mobile user authentication to the mobile network. For example, UUIIM can be one or more IMSI/USIM applications in 3GPP. UUIIM is technically equivalent to UICC in 3GPP specifications or UIM in 3GPP2 specifications.

3.2.24 visited network: A mobile network, to which an SS does not subscribe, which has a roaming relationship with the SS's home network. A visited network can also provide services for the SS.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
AKA	Authentication and Key Agreement
AS	Application Server
CAVE	Cellular Authentication and Voice Encryption
CK	Cipher Key
CRL	Certificate Revocation List
EAC	Entity Authentication Centre
ESD	Entity Subscription Database
GBA	Generic Bootstrapping Architecture
HTTP	HyperText Transfer Protocol
IAC-ID	Interim Authentication Check Identifier
IMSI	International Mobile Subscriber Identity
IK	Integrity Key
IKE	Internet Key Exchange
IMPI	Internet Protocol Multimedia Private Identity
IPSec	Internet Protocol Security
ISIM	Internet Protocol Multimedia Services Identity Module
ISR-ID	Interim Service Request Identifier
Ks	shared Key between SS and EAC
Ksp	shared Key between SS and SP
Kt	denote Key for session communication
MBMS	Multimedia Broadcast/Multicast Service
MN	Mobile Node
MTK	MBMS Traffic Key
NAF	Network Application Function

NAI	Network Access Identifier
PID	Private Entity Identifier
PKI	Public-Key Infrastructure
PSK-TLS	Pre-Shared Key Ciphersuites for Transport Layer Security
RES	a 3GPP authentication parameter
SAP	Service Authentication Proxy
SGT	Service Granted Ticket
SIM	Subscriber Identity Module
SP	Service Provider
SS	Service Subscriber
TLS	Transport Layer Security
TLS-Cert	Transport Layer Security based on Certificate
TLS-PSK	Transport Layer Security based on Pre-Shared Key
TTP	Trusted Third Party
UE	User Equipment
UICC	Universal Integrated Circuit Card
UID	Public Entity Identifier
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module
UUIM	User Universal Identification Module
XRES	a 3GPP authentication parameter

5 Conventions

None.

6 Overview

6.1 Use case description

When providing certain services to a mobile user, most of the application servers must first establish a mutual trust relationship with the user (e.g., the relationship between a mobile user and an authentication proxy, a mobile user and a PKI system, or a mobile user and an application server). It is through mutual authentication that the trust relationship between a mobile user and an application server is established. With the development of the mobile network, there are more and more types of service, and the service provider can be not only a network operator, but also a third-party service provider, or even a mobile user. That is, some mobile users cannot only use the services provided by a mobile operator, but can also provide some services for other users.

This Recommendation defines three types of service provider (SP): mobile operators; third-party service providers; and mobile users. The service subscriber (SS) can be a mobile user or a third party application server (AS).

In order to establish a mutual trust relationship between various types of service entity it is necessary to have a common authentication architecture that is applicable to different standards for mobile networks. This Recommendation defines a common architecture to meet this requirement.

NOTE – The service entities may be located in the same network or different networks, e.g., one service entity may be in 3GPP network, and another in 3GPP2 network.

6.2 Security considerations

In the authentication architecture, the following security threats are considered, which are derived from the security threats defined in [ITU-T X.805]:

- Eavesdropping: Intruders obtain transmitted data without authorization by monitoring the transmission media. This is the most common type of interception attack method. In mobile communication, this threat results from the open nature of the wireless interface. Intruders can acquire authentication information and identity information by intercepting the radio signals and decoding the transmissions.
- Masquerade: The pretence by an entity to be a different entity. Intruders impersonate a legitimate user to access a resource to obtain a benefit or for other unauthorized purposes. Masquerading as a legitimate user is easier in mobile communication than in wired communication. With a masquerade attack, an intruder fools the system into believing he/she is a legitimate user, thereby gaining access to system services and confidential information.
- Unauthorized message manipulation: Intruders may modify, insert, replay or delete authentication data on radio interface, including both accidental and deliberate manipulation.
- Replay attack: Intruders can copy or relay intercepted messages but may not be able to decrypt them. The re-transmission of such messages can be used to gain unauthorized access to a network or resources.
- Denial of service attack: The prevention of authorized access to resources or the delaying of time-critical operations. For example, an intruder may prevent user authentication data from being transmitted on the radio interface by physical means or by inducing protocol failures.

In this architecture the following security requirements are considered:

- Entity identity confidentiality: The property that the permanent identity (e.g., international mobile subscriber identity, i.e., IMSI in 3GPP) of a user to whom a service is delivered cannot be compromised by eavesdropping on the radio access link. To achieve these objectives, the service entity (i.e., an SS or SP) is normally identified by a temporary identity allocated by the network. To avoid entity traceability, which may lead to compromise of entity identity confidentiality, the entity should not be identified for a long period by means of the same temporary identity.
- Entity authentication: The entity authentication process contains service entity authentication and EAC authentication, i.e., the EAC validates the identity of the entity and the service entity validates that the EAC is legitimate.

In order to achieve these objectives, before obtaining service, the service subscriber must perform an entity authentication procedure that includes the following two steps. The first step is authentication between the service entity and the EAC, i.e., the service entity and the EAC validate identities mutually. The second step is authentication between entities: the service entities validate identities mutually. The authentication procedure between the service entity and the EAC is specified in clauses 8.2 and 8.3. The authentication between service entities is specified in clauses 8.4 and 8.5.

The service entity and the EAC make an agreement on their shared key and securely negotiate the derived key generation algorithm used subsequently.

The negotiation of the shared keying material is accomplished in an authentication procedure between the entity and the EAC (see clause 8.2). The negotiation of the derived key generation algorithm depends on the security requirement of the service requested by the entity (see clause 8.4).

7 Security architecture

7.1 Authentication model

Figure 1 shows an authentication reference model for mobile end-to-end data communication.

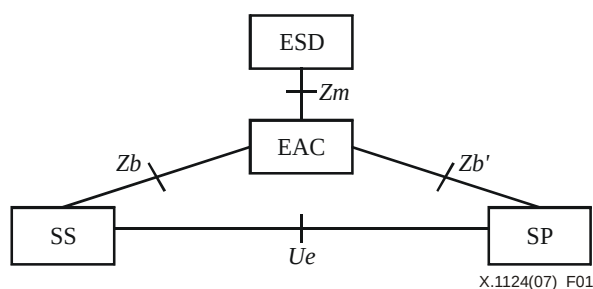


Figure 1 – Authentication model in mobile end-to-end data communication

Figure 1 shows the relationship between service entities (SS and SP), the entity subscription database (ESD) and the entity authentication centre (EAC) in the operator's network.

If the SS wants to use the service provided by the SP in the visited network, which has a subscription relationship with the SS's home network, then a service authentication proxy (SAP) must transmit the authentication information between the visited SP and the SS's home EAC. Figure 2 shows an authentication reference model for mobile end-to-end data communication.

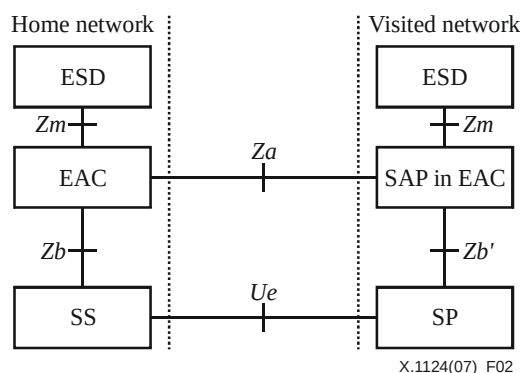


Figure 2 – Authentication model for accessing service in visited network

When the visited network has an EAC, the SAP may be co-located with the EAC. When the visited network has not deployed an EAC, it needs at least an SAP which is a proxy of the visited EAC. The SP can communicate with the home EAC via the SAP.