

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1034

(02/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Network security

**Guidelines on extensible authentication
protocol based authentication and key
management in a data communication network**

Recommendation ITU-T X.1034



International
Telecommunication
Union
Documents

Document Sharing Hub

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

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1034

Guidelines on extensible authentication protocol based authentication and key management in a data communication network

Summary

The extensible authentication protocol (EAP) is an authentication framework that supports multiple authentication mechanisms between a supplicant and an authentication server in a data communication network. EAP can be used as a basic tool for enabling user authentication and distribution of session keys in a data communication network. Since there are several EAP methods, the application designer should select the optimal EAP method among them.

This revision of Recommendation ITU-T X.1034 describes a framework for EAP-based authentication and key management for securing the lower layer in a communication network. It provides guidance on the selection of EAP methods and describes the mechanism for key management for the lower layer of a data communication network. The framework described in this Recommendation can be applied to protect data communication networks with wireless or wired access networks with a shared medium.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1034	2008-04-06	17
2.0	ITU-T X.1034	2011-02-13	17

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 2012

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Terms and definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	4
5	Conventions	4
6	EAP-based authentication and key management framework	5
	6.1 Introduction	5
	6.2 General features of EAP	6
	6.3 Basic operational procedures for authentication and key management protocols	7
7	EAP protocols.....	7
	7.1 Vulnerabilities in EAP.....	7
	7.2 Set of requirements for EAP.....	8
	7.3 Criteria for evaluating and classifying EAP methods	10
	7.4 EAP method.....	12
	7.5 Evaluation of existing EAP methods.....	12
8	Key management	12
	8.1 Practical threats to a specific wireless access network.....	12
	8.2 General operational phases for key management.....	13
	8.3 Set of requirements for key management.....	14
	8.4 Flow of the key management protocol	16
	8.5 Requirements classification of key management	17
9	Cryptographic key for key management.....	18
	9.1 General policy model	18
	9.2 Possible cryptographic key hierarchy and key derivation	18
	Appendix I – Evaluation of existing EAP methods	20
	Appendix II – AAA protocol	23
	Appendix III – Overview of the existing EAP methods	24
	III.1 Pre-shared secret-based EAP methods	24
	III.2 EAP methods based on public key	25
	III.3 EAP methods that support both shared secret and public key.....	26
	III.4 Tunnel-based EAP methods	26
	Bibliography.....	28

Document ID: 123456789

Recommendation ITU-T X.1034

Guidelines on extensible authentication protocol based authentication and key management in a data communication network

1 Scope

The extensible authentication protocol (EAP) is an authentication framework that supports multiple authentication mechanisms between a supplicant and an authentication server. EAP can work directly over lower layers, e.g., the data link layer, such as the point-to-point protocol (PPP), IEEE 802, CDMA2000, UMTS, or VDSL/ADSL. For example, IEEE 802.1X is a typical transport mechanism for EAP over 802 LANs. The EAP basically performs authentication for a device attached to a LAN, establishing a secure point-to-point connection or preventing access by an unauthorized device. In other words, EAP can be used to authenticate the supplicant wishing to access the network. The AAA function may be used as one of the key functions for lower-layer security of a data communication network. AAA enables transporting the secret key from the authentication server to the authenticator. Thus, defining the requirements of the EAP method and key management protocol, establishing criteria for selecting an optimal EAP method among several existing EAP methods, and defining a suitable framework for EAP and an optimal key management protocol including key derivation methods for lower-layer security in end-to-end data communication are essential. This Recommendation applies mainly to EAP-based authentication and key management protocol for data communication with a wireless access network where communication through the wireless access network should be protected by the key material derived from the key management protocol.

This Recommendation describes a framework for authentication and key management to secure the lower layer in data communication. It also provides guidance on the selection of EAP methods for a data communication network and describes the mechanism for key management and possible key hierarchy for lower-layer security in a data communication network. This Recommendation is to provide complete sets for EAP-based authentication itself but also the key management, from threat analysis to requirements, allowing the network operator to choose an adequate EAP method by using some criteria described for a specific network environment.

2 References

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

- [ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.
- [ITU-T X.1151] Recommendation ITU-T X.1151 (2007), *Guideline on secure password-based authentication protocol with key exchange*.
- [IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*.

- [IETF RFC 4017] IETF RFC 4017 (2005), *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs*.
- [IETF RFC 5216] IETF RFC 5216 (2008), *The EAP-TLS Authentication Protocol*.
- [ISO/IEC 8802-11] ISO/IEC 8802-11:2005/Amd.6:2006, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements*.

3 Terms and definitions

3.1 Terms defined elsewhere

3.1.1 passive attack [ITU-T X.1151]: This refers to an attack that involves listening, i.e., eavesdropping, without modifying or supplementing information.

3.1.2 server-compromised attack [ITU-T X.1151]: This refers to an attack wherein an attacker obtains verifier information from the server and launches a dictionary attack on the password file.

3.1.3 temporal key (TK) [ISO/IEC 8802-11]: This pertains to the keying materials for the encryption and integrity of messages during later data sessions. TK generally resides in the part of PTK.

3.2 Terms defined in this Recommendation

3.2.1 4-way handshake [adapted from IETF RFC 4017]: A 4-way handshake is a process consisting of 4 messages exchanged by two parties, where a pair-wise master key is involved. As a Pair-wise Authentication and Key Management Protocol (AKMP) defined in [ISO/IEC 8802-11], it confirms the mutual possession of a Pair-wise Master Key by two parties and distributes a Group Key.

3.2.2 authentication, authorization, accounting (AAA) [adapted from IETF RFC 4017]: The AAA protocol can be used as transport mechanism for the EAP message; it consists of RADIUS and Diameter. In general, the terms "AAA server" and "backend authentication server" are used interchangeably.

3.2.3 authenticator [adapted from IETF RFC 4017]: The authenticator refers to the endpoint of the link initiating EAP authentication when a supplicant wants to access the network.

3.2.4 backend authentication server [adapted from IETF RFC 4017]: A backend authentication server, i.e., authentication server, pertains to an entity providing authentication service to an authenticator. A typical backend authentication server is the AAA server.

3.2.5 credentials: A set of security-related information comprising keys, keying material and cryptographic algorithm-related parameters that can be used to establish the identity of an entity, or to help that entity communicate securely.

3.2.6 EAP server [adapted from IETF RFC 4017]: This entity executes the EAP authentication method with the supplicant. In case no backend authentication server is used, the EAP server plays the role of the authenticator. In case a backend authentication server is used, that is, if the authenticator operates in pass-through mode, i.e., the authenticator forwards the EAP message without any modification to the supplicant or vice versa, the EAP server is placed on the backend authentication server.

3.2.7 key confirmation: A procedure to prove one entity that another entity established the correct secret keying material as a result of a key establishment.

3.2.8 man-in-the-middle attack [adapted from ITU-T X.1151]: This refers to an attack wherein an attacker intercepts the public key being exchanged by two entities and substitutes his/her own public key to impersonate the recipient, where the attacker can own the public key or take a copy of it while being exchanged. This attack compromises the security of the cryptosystem.

3.2.9 master key (MK): Top-level keying material is shared between the supplicant and the authentication server to derive the master session key. In general, a master key is different from the master session key. This is because the MK represents a positive access decision for a supplicant by the authentication server.

3.2.10 master session key (MSK) [adapted from IETF RFC 4017]: This refers to the keying material derived between the EAP peer and server and exported to the authenticator using the EAP method. MSK is at least 64 octets long. In existing implementations, an AAA server acting as an EAP server transports the MSK to the authenticator. It refers to the privilege given to a supplicant by an authenticator to access the lower layer of a data communication network. In this Recommendation, MSK is used interchangeably with the Pair-wise Master Key (PMK).

3.2.11 mutual authentication [adapted from ITU-T X.1151]: This pertains to a type of authentication wherein the supplicant authenticates the server and the server authenticates the supplicant. Mutual authentication can prevent phishing and pharming attacks.

3.2.12 pair-wise master Key (PMK) [adapted from ISO/IEC 8802-11]: This pertains to the keying material derived between the EAP peer and server and exported to the authenticator using the EAP method. In this Recommendation, the PMK is used interchangeably with the master session key (MSK).

3.2.13 pair-wise transient key (PTK) [adapted from ISO/IEC 8802-11]: This refers to the keying material derived between the EAP peer and authenticator based on the pair-wise master key. This keying material is shared by both the peer and the authenticator.

3.2.14 perfect forward secrecy (PFS) [adapted from ITU-T X.1151]: In the cryptography of a key establishment protocol, this pertains to the condition wherein a compromised long-term private key after a given session does not compromise any earlier session.

3.2.15 server compromised-based dictionary attack [adapted from ITU-T X.1151]: For the password-based EAP method, the attacker is unable to impersonate the supplicant by obtaining a user password even after obtaining the hidden password file. Once the attacker compromises the server, he/she can obtain the hidden password file, i.e., hashed password file, and perform the offline dictionary attack against the hidden password file to obtain the password which can be used to impersonate the supplicant. However, this kind of attack can be prevented by encrypting the hidden password file by the secret key which is stored in the external hardware token or using some sophisticated cryptographic schemes, secret sharing schemes between the server and the hardware token. The resistance to the server compromised-based dictionary can be regarded as a way to mitigate the server-compromised attack. As a conclusion, this capability can be obtained by using a hardware token to store the server's secret materials.

3.2.16 successful authentication [adapted from IETF RFC 4017]: This is referred to as a successful exchange of EAP messages wherein the authentication server decides to allow the supplicant access and the supplicant decides to use such access.

3.2.17 supplicant [adapted from IETF RFC 4017]: This pertains to the endpoint responding to the authenticator. In this Recommendation, the supplicant is used interchangeably with the peer. The peer pertains to the end of the link responding to the authenticator. In [ISO/IEC 8802-11], this end is also known as the supplicant.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AAA	Authentication, Authorization, and Accounting
ADSL	Asymmetric Digital Subscriber Line
CDMA	Code Division Multiple Access
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EMSK	Extended Master Session Key
LAN	Local Area Network
MIC	Message Integrity Code
MK	Master Key
MSK	Master Session Key
MTU	Maximum Transmission Unit
NAS	Network Access Server
PAC	Protected Access Credential
PFS	Perfect Forward Secrecy
PMK	Pair-wise Master Key
PPP	Point-to-Point Protocol
PTK	Pair-wise Transient Key
TCP	Transmission Control Protocol
TEK	Transient Encryption Key
TIK	Transient Integrity protection Key
TK	Transient Key
TLS	Transport Layer Security
SCTP	Stream Control Transmission Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
VDSL	Very High Speed Digital Subscriber Line
3GPP	3rd-Generation Partnership Project
3GPP-2	3rd-Generation Partnership Project 2

5 Conventions

None.

6 EAP-based authentication and key management framework

6.1 Introduction

A supplicant wishing to access the network should be authenticated by the network operator to use the network services or resources of the network operator. Moreover, when the network being accessed uses wireless transmission technology or a wired access network with a shared medium, the supplicant should share the common secret with the network to protect the exchanged message in later sessions against eavesdropping, modifying, or listening. The authentication and key management framework can be used to perform mutual authentication between the supplicant and the authentication server and share the common secret between the supplicant and network access server (NAS) acting as a gateway in the access network as well. This refers to the gateway node enabling the peer to gain access to the network. The function of the authenticator generally resides in the network access server.

There are three entities required for authentication and key management: a supplicant (or peer), an authenticator, and an authentication server. The supplicant functions as an end-user or a supplicant wishing to access the network in the end-user station. The authenticator acts as a policy enforcement point mediating EAP messages between the supplicant and the authentication server. The authentication server acts as a sub-function of the AAA server, authenticating the supplicant, optionally sharing a secret that can be used to derive cryptographic keys, posting the result of authentication of an end-user to the authenticator, and forwarding the shared secret to an authenticator that can be used to derive cryptographic keys between the authenticator and the supplicant to ensure confidentiality and integrity and enable message authentication. The detailed description of a policy model for key management and key derivation is given in clause 9.1.

The path between the supplicant and the authenticator may be the wireless or wired medium used by more than one peer to exchange messages; hence the need for this path to be protected with adequate protection methods. Authentication messages for mutual authentication should be exchanged between the supplicant and authentication server using the EAP transport mechanism via the authenticator. When operating in pass-through mode, the authenticator only relays EAP messages from the supplicant to the authentication server or vice versa. There are many EAP methods that are being used in a variety of applications. Therefore, the network designer should select an adequate EAP method using some criteria for evaluating the existing EAP methods. The type and syntax of an EAP message should also be defined for authentication.

The backend protocol that transfers authentication messages from the authenticator to the authentication server should use the existing AAA protocol. There are two well-known AAA protocols: RADIUS and Diameter. A specific AAA protocol should be selected by defining the criteria for evaluating AAA protocols for authentication.

Authentication and key management generally consists of four operational phases: security capability discovery, EAP authentication, AAA-based key distribution, and key management (see Figure 1). In the security capability phase, a supplicant negotiates on the security capabilities and the various parameters of the protocol to be used with the authenticator. On the other hand, in the EAP phase, the authentication server authenticates a supplicant and derives a master secret shared with the supplicant as a result of the EAP protocol. In an AAA-based key distribution phase, the authentication server transports the master secret to an authenticator to allow authentication to derive various cryptographic keys for a subsequent session between a supplicant and an authenticator. To prevent the use of the same secret key over and over and a security hole as a result of such, fresh cryptographic keys should be used in every session. Finally, in the key management phase, the authenticator exchanges random numbers with the supplicant to obtain a fresh cryptographic key.

In case the authenticator keeps the authentication-related information of a user, the authentication server is not required, i.e., the authentication server can act as part of the authenticator.

