

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1254

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Entity authentication assurance framework

Recommendation ITU-T X.1254



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.1254

Entity authentication assurance framework

Summary

This Recommendation defines four levels of entity authentication assurance (i.e., LoA 1 – LoA 4), and the criteria and threats for each of the four levels of entity authentication assurance. Additionally, it:

- specifies a framework for managing the assurance levels;
- provides guidance concerning control technologies that are to be used to mitigate authentication threats, based on a risk assessment;
- provides guidance for mapping the four levels of assurance to other authentication assurance schemas; and
- provides guidance for exchanging the results of authentication that are based on the four levels of assurance.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1254	2012-09-07	17

Copyright International Telecommunication Union/ITU-T
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Full document details: ITU-T X.1254 2012

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.

A similar text is published as ISO/IEC 29115. It differs from this text in four instances: 1) clause 3.1.6: the definition for credential is different and in this Recommendation references the definition in Recommendation ITU-T X.1252; 2) Table 10-1: ISO/IEC 29115 includes an example for impersonation that includes use of an identity for an entity that does not exist; 3) clause 10.2.2.1: ISO/IEC 29115 describes SSL as an example of a protected channel; 4) In this Recommendation, Annex A, *Characteristics of a credential*, is normative.

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 2013

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 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	3
5 Conventions	4
6 Levels of assurance.....	4
6.1 Level of assurance 1 (LoA1)	5
6.2 Level of assurance 2 (LoA2)	5
6.3 Level of assurance 3 (LoA3)	6
6.4 Level of assurance 4 (LoA4)	6
6.5 Selecting the appropriate level of assurance	6
6.6 LoA mapping and interoperability	7
6.7 Exchanging authentication results based on the 4 LoAs	8
7 Actors.....	9
7.1 Entity	9
7.2 Credential service provider.....	9
7.3 Registration authority	9
7.4 Relying party	9
7.5 Verifier	10
7.6 Trusted third party	10
8 Entity authentication assurance framework phases	10
8.1 Enrolment phase	10
8.2 Credential management phase	13
8.3 Entity authentication phase.....	15
9 Management and organizational considerations.....	16
9.1 Service establishment	16
9.2 Legal and contractual compliance	16
9.3 Financial provisions.....	17
9.4 Information security management and audit	17
9.5 External service components.....	17
9.6 Operational infrastructure.....	17
9.7 Measuring operational capabilities.....	17
10 Threats and controls.....	18
10.1 Threats to, and controls for, the enrolment phase	18
10.2 Threats to, and controls for, the credential management phase	20

	Page
10.3 Threats to, and controls for, the authentication phase	25
11 Service assurance criteria	29
Annex A – Characteristics of a credential	30
Appendix I – Privacy and protection of PII	31
Bibliography.....	33

Introduction

Many electronic transactions within or between ICT systems have security requirements which depend upon an understood or specified level of confidence in the identities of the entities involved. Such requirements may include the protection of assets and resources against unauthorized access, for which an access control mechanism might be used, and/or the enforcement of accountability by the maintenance of audit logs of relevant events, as well as for accounting and charging purposes.

Recommendation ITU-T X.1254 provides a framework for entity authentication assurance. Assurance within this Recommendation refers to the confidence placed in all of the processes, management activities and technologies used to establish and manage the identity of an entity for use in authentication transactions.

Technical			Management and organizational
Enrolment phase	• Application and initiation • Identity proofing and identity information verification	• Record-keeping/recording • Registration	• Service establishment • Legal and contractual compliance • Financial provisions • Information security management and audit • External service components • Operational infrastructure • Measuring operational capabilities
Credential management phase	• Credential creation • Credential pre-processing • Credential issuance • Credential activation • Credential storage	• Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement • Record-keeping	
Entity authentication phase	• Authentication • Record-keeping		

X.1254(12)_F01

Figure 1 – Overview of the entity authentication assurance framework

Using four specified levels of assurance (LoAs), this Recommendation provides guidance concerning control technologies, processes and management activities, as well as assurance criteria, that should be used to mitigate authentication threats in order to implement the four LoAs. It also provides guidance for the mapping of other authentication assurance schemes to the specified four levels, as well as guidance for exchanging the results of an authentication transaction. Finally, this Recommendation provides guidance concerning the protection of personally identifiable information (PII) associated with the authentication process.

This Recommendation is intended to be used principally by credential service providers (CSPs) and by others having an interest in their services (e.g., relying parties, assessors and auditors of those services). This entity authentication assurance framework (EAAF) specifies the minimum technical, management and process requirements for four LoAs to ensure equivalence among the credentials issued by various CSPs. It also provides some additional management and organizational considerations that affect entity authentication assurance, but it does not set forth specific criteria for those considerations. Relying parties (RPs) and others may find this Recommendation helpful to gain an understanding of what each LoA provides. Additionally, it may be adopted for use within a trust framework to define technical requirements for LoAs. The EAAF is intended for, but not limited to, session-based and document-centric use cases using various authentication technologies. Both direct and brokered trust scenarios are possible, within either legal/bilateral arrangements or federations.

Recommendation ITU-T X.1254

Entity authentication assurance framework¹

1 Scope

This Recommendation provides a framework for managing entity authentication assurance in a given context. In particular, it:

- specifies four levels of entity authentication assurance;
- specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance;
- provides guidance for mapping other authentication assurance schemes to the four LoAs;
- provides guidance for exchanging the results of authentication that are based on the four LoAs; and
- provides guidance concerning controls that should be used to mitigate authentication threats.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 assertion [b-ITU-T X.1252]: A statement made by an entity without accompanying evidence of its validity.

NOTE – The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this Recommendation, an assertion is considered to be a stronger statement than a claim.

3.1.2 authentication [b-ISO/IEC 18014-2]: Provision of assurance in the identity of an entity.

3.1.3 authentication factor [b-ISO/IEC 19790]: Piece of information and/or process used to authenticate or verify the identity of an entity.

NOTE – Authentication factors are divided into four categories:

- something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);
- something an entity knows (e.g., password, PIN);
- something an entity is (e.g., biometric characteristic);
- something an entity typically does (e.g., behaviour pattern).

¹ Korea (Republic of) has expressed a reservation and will not apply this Recommendation because this Recommendation is in conflict with regulations in Korea, with regard to the required four levels of entity authentication assurance and their criteria for achieving each of the four levels of entity authentication assurance.

3.1.4 claim [b-ITU-T X.1252]: To state as being the case, without being able to give proof.

NOTE – The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this Recommendation, an assertion is considered to be a stronger statement than a claim.

3.1.5 context [b-ITU-T X.1252]: An environment with defined boundary conditions in which entities exist and interact.

3.1.6 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

NOTE – See Appendix I for additional characteristics of a credential.

3.1.7 entity [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in a context.

NOTE – For the purposes of this Recommendation, entity is also used in the specific case for something that is claiming an identity.

3.1.8 identity [b-ISO/IEC 24760]: Set of attributes related to an entity.

NOTE – Within a particular context, an identity can have one or more identifiers to allow an entity to be uniquely recognized within that context.

3.1.9 multifactor authentication [b-ISO/IEC 19790]: Authentication with at least two independent authentication factors.

3.1.10 non-repudiation [b-ITU-T X.1252]: The ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action.

3.1.11 repudiation [b-ITU-T X.1252]: Denial in having participated in all or part of an action by one of the entities involved.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication protocol: A defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

3.2.2 authoritative source: A repository which is recognized as being an accurate and up-to-date source of information.

3.2.3 credential service provider (CSP): A trusted actor that issues and/or manages credentials.

3.2.4 entity authentication assurance (EAA): A degree of confidence reached in the authentication process that the entity is what it is, or is expected to be (this definition is based on the 'authentication assurance' definition given in [b-ITU-T X.1252]).

NOTE – The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented.

3.2.5 identifier: One or more attributes that uniquely characterize an entity in a specific context.

3.2.6 identity information verification: A process of checking identity information and credentials against issuers, data sources or other internal or external resources with respect to authenticity, validity, correctness and binding to the entity.

3.2.7 identity proofing: The process by which the registration authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance.

3.2.8 man-in-the-middle attack: An attack in which an attacker is able to read, insert and modify messages between two parties without their knowledge.

3.2.9 mutual authentication: The authentication of identities of entities which provides both entities with assurance of each other's identity.

3.2.10 phishing: A scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly.

3.2.11 registration authority (RA): A trusted actor that establishes and/or vouches for the identity of an entity to a credential service provider (CSP).

3.2.12 relying party (RP): Actor that relies on an identity assertion or claim.

3.2.13 salt: A non-secret, often random value that is used in a hashing process.

NOTE – It is also referred to as sand.

3.2.14 shared secret: A secret used in authentication that is known only to the entity and the verifier.

3.2.15 time stamp: This is a reliable time variant parameter which denotes a point in time with respect to a common reference.

3.2.16 transaction: A discrete event between an entity and service provider that supports a business or programmatic purpose.

3.2.17 trust framework: A set of requirements and enforcement mechanisms for parties exchanging identity information.

3.2.18 trusted third party (TTP): An authority or its agent, trusted by other actors with respect to specified activities (e.g., security-related activities).

NOTE – A trusted third party is trusted by an entity and/or a verifier for the purposes of authentication.

3.2.19 validity period: The time period during which an identity or credential may be used in one or more transactions.

3.2.20 verification: The process of checking information by comparing the provided information with previously corroborated information.

3.2.21 verifier: The actor that corroborates identity information.

NOTE – The verifier can participate in multiple phases of the EAAF and can perform credential verification and/or identity information verification.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA	Certification Authority
CSP	Credential Service Provider
EAA	Entity Authentication Assurance
EAAF	Entity Authentication Assurance Framework
ICT	Information and Communication Technology
IdM	Identity Management
IP	Internet Protocol
LoA	Level of Assurance
LoAs	Levels of Assurance
MAC	Media Access Control
NPE	Non-Person Entity

PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
RA	Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTP	Trusted Third Party
URL	Uniform Resource Locator

5 Conventions

This Recommendation applies the following verbal forms for the expression of provisions:

- a) "shall" indicates a requirement
- b) "should" indicates a recommendation
- c) "may" indicates a permission
- d) "can" indicates a possibility and a capability.

6 Levels of assurance

This entity authentication assurance framework (EAAF) defines four levels of assurance (LoA) for entity authentication. Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity that uses a particular identity is in fact the entity to which that identity was assigned. For the purposes of this Recommendation, an LoA is a function of the processes, management activities and technical controls that have been implemented by a credential service provider (CSP) for each of the EAAF phases based on the criteria set forth in clause 10. Entity authentication assurance (EAA) is affected by management and organizational considerations, but this Recommendation does not provide explicit normative criteria for these considerations. An entity can be a human or a non-person entity (NPE).

For example, a network's LoA could be a function of the LoAs of all components that make up the network and includes NPEs or endpoint devices (e.g., mobile phones, personal digital assistants (PDAs), set-top boxes, laptops). In some instances, endpoint devices may impersonate legitimate entities. Consequently, the ability to distinguish a trusted device, with some degree of confidence, from a rogue device is fundamental to EAA.

LoA1 is the lowest level of assurance, and LoA4 is the highest level of assurance specified in this Recommendation. Determining which LoA is appropriate in a given situation depends on a variety of factors. The determination of the required LoA is based mainly on risk: the consequences of an authentication error and/or misuse of credentials, the resultant harm and impact, and their likelihood of occurrence. Higher LoAs shall be used for higher perceived risk.

The EAAF provides requirements and implementation guidance for each of the four LoAs. In particular, it provides requirements for the implementation of processes for the following phases:

- a) enrolment (e.g., identity proofing, identity information verification, registration)

- b) credential management (e.g., credential issuance, credential activation)
- c) authentication.

It also provides guidance regarding management and organizational considerations (e.g., legal compliance, information security management) that affect entity authentication assurance.

The LoAs are defined as shown in Table 6-1.

Table 6-1 – Levels of assurance²

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

This framework contains requirements to achieve a desired LoA for each entity authentication assurance framework phase. The overall LoA achieved by an implementation using this framework will be the level of the phase with the lowest LoA.

6.1 Level of assurance 1 (LoA1)

At LoA1, there is minimal confidence in the claimed or asserted identity of the entity, but some confidence that the entity is the same over consecutive authentication events. This LoA is used when minimum risk is associated with erroneous authentication. There is no specific requirement for the authentication mechanism used; only that it provides some minimal assurance. A wide range of available technologies, including the credentials associated with higher LoAs, can satisfy the entity authentication assurance requirements for this LoA. This level does not require use of cryptographic authentication methods (e.g., cryptographic-based challenge-response protocol).

For example, LoA1 may be applicable for authentication in which an entity presents a self-registered username or password to a service provider's website to create a customized page, or transactions involving websites that require registration for access to materials and documentation, such as news or product documentation.

For example, at LoA1, a media access control (MAC) address may satisfy a device authentication requirement. However, there is little confidence that another device will not be able to use the same MAC address.

6.2 Level of assurance 2 (LoA2)

At LoA2, there is some confidence in the claimed or asserted identity of the entity. This LoA is used when moderate risk is associated with erroneous authentication. Single-factor authentication is acceptable. Successful authentication shall be dependent upon the entity proving, through a secure authentication protocol, that the entity has control of the credential. Controls should be in place to reduce the effectiveness of eavesdroppers and online guessing attacks. Controls shall be in place to protect against attacks on stored credentials.

For example, a service provider might operate a website that enables its customers to change their address of record. The transaction in which a beneficiary changes an address of record may be considered an LoA2 authentication transaction, as the transaction may involve a moderate risk of inconvenience. Since official notices regarding payment amounts, account status, and records of

² LoA is a function of the processes, management activities, and technical controls that have been implemented by a CSP for each of the EAAF phases based on the criteria set forth in clause 10.

changes are usually sent to the beneficiary's address of record, the transaction additionally entails moderate risk of unauthorized release of PII. As a result, the service provider should obtain at least some authentication assurance before allowing this transaction to take place.

6.3 Level of assurance 3 (LoA3)

At LoA3, there is high confidence in the claimed or asserted identity of the entity. This LoA is used where substantial risk is associated with erroneous authentication. This LoA shall employ multifactor authentication. Any secret information exchanged in authentication protocols shall be cryptographically protected in transit and at rest (although LoA3 does not require the use of a cryptographic-based challenge-response protocol). There are no requirements concerning the generation or storage of credentials; they may be stored or generated in general purpose computers or in special purpose hardware.

For example, a transaction in which a company submits certain confidential information electronically to a government agency may require an LoA3 authentication transaction. Improper disclosure could result in a substantial risk for financial loss. Other LoA3 transaction examples include online access to accounts that allow the entity to perform certain financial transactions, or use by a third party contractor of a remote system to access potentially sensitive client personal information.

6.4 Level of assurance 4 (LoA4)

At LoA4, there is very high confidence in the claimed or asserted identity of the entity. This LoA is used when high risk is associated with erroneous authentication. LoA4 provides the highest level of entity authentication assurance defined by this Recommendation. LoA4 is similar to LoA3, but it adds the requirements of in-person identity proofing for human entities and the use of tamper-resistant hardware devices for the storage of all secret or private cryptographic keys. Additionally, all PII and other sensitive data included in authentication protocols shall be cryptographically protected in transit and at rest.

For example, services where there is a potential high risk for harm or distress in the case of an authentication failure may require LoA4 protection. The responsible party needs full assurance that the correct entity provided certain critical information, and the responsible party may even be criminally liable for any failure to verify the information. Finally, approval of a transaction involving high risk of financial loss may be an LoA4 transaction.

At LoA4, digital certificates (e.g., ITU-T X.509, card-verifier (CV) certificates) may be used to authenticate NPEs, such as laptops, mobile phones, printers, fax machines and other devices connected to a network. For example, the smartphone enrolment process may require the deployment of digital certificates to the smartphone. Also, in order to prevent unauthorized access to the power grid, digital certificates may be used in the deployment of smart meter technologies.

6.5 Selecting the appropriate level of assurance

Selection of the appropriate LoA should be based on a risk assessment of the transactions or services for which the entities will be authenticated. By mapping impact levels to LoAs, parties to an authentication transaction can determine what LoA they require and can procure services and place reliance on assured identities accordingly. Table 6-2 indicates possible consequences and impacts of authentication failure at the various LoAs.