

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.1254

(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Entity authentication assurance framework

Recommendation ITU-T X.1254

ITU-T

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

Recommendation ITU-T X.1254

Entity authentication assurance framework

Summary

Recommendation ITU-T X.1254 specifies three entity authentication assurance levels (AALs), and criteria for and threats to each of them.

Additionally, it:

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

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1254	2012-09-07	17	11.1002/1000/11608
2.0	ITU-T X.1254	2020-09-03	17	11.1002/1000/14260

Keywords

AAL, assurance, authentication, authentication assurance level, identity management, IdM, level of assurance, LoA.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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 2021

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	Digital authentication process flow	4
	6.1 General	4
	6.2 Digital identity assurance	5
	6.3 Roles	6
	6.4 Authentication processes components.....	7
7	Apply risk management to the authentication assurance framework	8
	7.1 General	8
	7.2 Authentication risk	8
8	Threat categories, risks and controls	9
	8.1 Assurance levels	9
	8.2 Authenticator compromise	11
	8.3 Transaction compromise	13
	8.4 Verifier impersonation.....	14
	8.5 Subscriber impersonation	15
	8.6 Authentication service compromise, risks and controls	20
	8.7 Privacy, risks and controls.....	21
	Appendix I – An example of strong authentication using [b-ITU-T X.1278]	23
	I.1 Introduction	23
	I.2 Threat categories	23
	I.3 [b-ITU-T X.1278] enables "high-assurance strong authentication"	23
	I.4 Old authentication with passwords.....	24
	I.5 New authentication with [b-ITU-T X.1278]	25
	I.1 Interoperability and certification	25
	Bibliography.....	27

Introduction

A digital identity is the unique representation of an entity engaged in an online transaction. Assurance – or confidence – that the digital identity with which one is interacting is consistent with the claimed identity, lies at the heart of online trust, security and access control. Three types of assurance are identified to contribute to establishing trust in a digital identity: identity assurance; authentication assurance; and federation assurance.

This Recommendation provides a framework for authentication assurance. For the purposes of this Recommendation, authentication is the process by which a claimed identity is verified for the purpose of conducting an online transaction. For services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the user accessing the service today is the same as that which accessed the service previously.

The framework established in this Recommendation provides online service providers – relying parties (RPs) and credential service providers (CSPs) – with a systematic approach to understanding their risks and identifying controls to help mitigate them. It is designed to facilitate the methodical selection of controls and risk mitigation strategies using a three-step process:

1. identification of roles and services to determine threat categories;
2. application of a targeted risk management process to determine the strength of controls required; and,
3. identification of which technologies – protocols, credential types, etc. – are employed to further refine controls.

A threat-based model

This Recommendation is designed to facilitate the methodical selection of controls and risk mitigation strategies. A preliminary step in being able to select appropriate controls and mitigation strategies is the identification of the types of risks and threats associated with the role(s) and services of an online service provider. See Figure 0-1.



Figure 0-1 – Services, risks, and controls

This framework is organized on the basis of risks and threat categories that provide online service providers with a functional link between risk assessment processes, and control and risk mitigation activities.

Identity service providers may provide all, some or only one of the functional components of these digital identity phases. As such, it is appropriate to assess risks and address controls and risk mitigation approaches on a similar componentized approach to the digital transaction lifecycle. This Recommendation addresses risks and controls to the credential management and authentication phases of this lifecycle. Other documents (e.g., [b-ISO/IEC TS 29003]) address the risks and controls for the enrolment and identity proofing activities, as well as organizational and management controls. It is anticipated that these documents, and others, will be aligned to represent a coordinated set of core identity management standards (as illustrated in Figure 0-2) that, when used in combination, provide the processes, risks, and controls for the digital identity transaction lifecycle.

This Recommendation also presents a catalogue of privacy threats, considerations and mitigating controls that are specific to its scope (authentication and credential management). This Recommendation does not include privacy considerations with respect to identity proofing or enrolment.

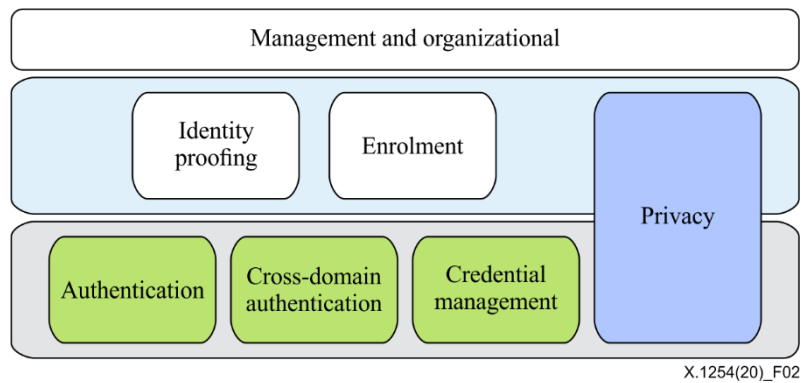


Figure 0-2 – Core aligned identity management standards

Relationship to the previous version of this Recommendation

The first edition of this Recommendation [ITU-T X.1254 (2012)] presented the lifecycle for digital identity transactions through three phases: enrolment and identity proofing; credential management; and entity authentication. The industry has evolved since 2012 and new concepts and approaches have emerged, such as password-free authentication and step-up authentication. As such, the industry has moved from the concept of a level of assurance (LoA) as a single ordinal that drives implementation-specific requirements. Instead, by combining appropriate business and privacy risk management side-by-side with mission need, implementers will select identity assurance levels (IALs), authentication assurance levels (AALs) and federation assurance levels (FALs) as distinct options. This Recommendation focuses on AALs. IALs and FALs lie outside the scope of this Recommendation.

Recommendation ITU-T X.1254

Entity authentication assurance framework

1 Scope

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

- establishes three entity authentication assurance levels (AALs);
- gives guidelines for understanding these entity AALs;
- specifies criteria and guidelines for achieving identified levels of EAA;
- provides guidance for comparing and mapping across authentication assurance schemes;
- provides guidance for exchanging the results of authentication that are based on specific assurance levels; and
- provides guidance concerning controls that should be used to mitigate authentication threats, based on a risk assessment.

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 of the claimed 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); or
- something an entity typically does (e.g., behaviour pattern).

3.1.4 authentication protocol [b-ISO/IEC 29115]: Defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

3.1.5 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.

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

3.1.7 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.

3.1.8 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 of something that is claiming an identity.

3.1.9 identity; partial identity [b-ISO/IEC 24760-1]: 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.

3.1.10 identity information verification [b-ISO/IEC 29115]: 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.

3.1.11 identity proofing [b-ISO/IEC 29115]: Process by which the registration authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance.

3.1.12 man-in-the-middle attack [b-ISO/IEC 29115]: Attack in which an attacker is able to read, insert and modify messages between two parties without their knowledge.

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

3.1.14 mutual authentication [b-ISO/IEC 29115]: Authentication of identities of entities which provides both entities with assurance of each other's identity.

3.1.15 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.

3.1.16 phishing [b-ISO/IEC 29115]: Scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly.

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

3.1.18 risk assessment [b-ISO/IEC 27000]: Overall process of risk identification, risk analysis and risk evaluation.

3.1.19 shared secret [b-ISO/IEC 29115]: Secret used in authentication that is known only to the entity and the verifier.

3.1.20 transaction [b-ISO/IEC 29115]: Discrete event between an entity and service provider that supports a business or programmatic purpose.

3.1.21 verification [b-ISO/IEC 29115]: Process of checking information by comparing the provided information with previously corroborated information.

3.1.22 verifier [b-ISO/IEC 29115]: Actor that corroborates identity information.

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

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

NOTE – This definition is based on that in [b-ISO/IEC 29115].

3.2.2 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.

NOTE 1 – The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented.

NOTE 2 – This definition is based on that of authentication assurance given in [b-ITU-T X.1252].

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

NOTE – This definition is based on that in [b-ITU-T X.1252].

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

NOTE – This definition is based on that in [b-ISO/IEC 29115].

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

NOTE – This definition is based on that in [b-ISO/IEC 29115].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAL	Authentication Assurance Level
CSP	Credential Service Provider
EAA	Entity Authentication Assurance
FAL	Federation Assurance Level
FIDO	Fast Identity On-line
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol-Secure
IAL	Identity Assurance Level
IdM	Identity Management
IDP	Identity Provider
LoA	Level of Assurance
MAC	Media Access Control
MITM	Man-In-The-Middle
MITB	Man-In-The-Browser
OAuth	Open Authentication
OpenID	Open Identity
OTP	One-Time Password
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
RA	Registration Authority



RP	Relying Party
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
URL	Uniform Resource Locator

5 Conventions

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

- "shall" indicates a requirement;
- "should" indicates a recommendation;
- "may" indicates a permission;
- "can" indicates a possibility or a capability.

6 Digital authentication process flow

6.1 General

Digital identity is the unique representation of an entity engaged in an online transaction. In its simplest form, digital authentication involves verification, to some degree of confidence, of an entity's claimed identity for the purpose of granting it access to an online service. A registered entity attempts to authenticate an online service by demonstrating possession of an authenticator, also known as a credential, with which they were issued at the time of registration. The online service – also known as a relying party (RP) in the transaction – then makes an attempt to verify the validity of the authenticator with the identity provider (IDP) or the credential service provider (CSP) or verifier. The entity is granted access to the online service after its credential has been verified by the CSP or verifier.

Figure 6-1 illustrates the following digital authentication process flow:

- an entity accesses an online service of an RP;
- the RP redirects the entity to the CSP for authentication;
- the CSP verifies the entity's possession of the registered authenticator(s);
- the CSP sends an authentication assertion to the RP to assert the entity's authentication status;
- an authenticated session is established between the entity and the RP.

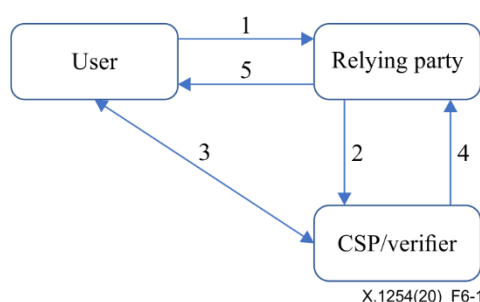


Figure 6-1 – Digital authentication process flow

Illustrating the digital authentication process flow in this manner provides a methodology for understanding the risks associated with the various roles and functions involved in digital authentication.