

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1276

(05/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Authentication step-up protocol and metadata Version 1.0

Recommendation ITU-T X.1276

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
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

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

Recommendation ITU-T X.1276

Authentication step-up protocol and metadata Version 1.0

Summary

Electronic identity credential trust elevation methods are used to increase assurance in entity identification using authentication events and related entity information for the purpose of risk mitigation when making access control policy decisions. The goals of this Recommendation are:

- To propose simple trust elevation architectural patterns demonstrating the use of trust elevation in modern access control architectures.
- To describe a common metadata set mechanisms and protocol elements for trust elevation information exchanges.
- To promote the use of trust elevation elements to facilitate standardization among the many technologies and approaches currently in use for credential and authentication risk mitigation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1276	2018-05-14	17	11.1002/1000/13606

Keywords

Access control, authentication, trust elevation.

* 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 2018

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	2
5	Conventions	2
6	Conceptual Models	2
6.1	Trust Elevation Core Model	3
6.2	Trust Elevation Concepts	3
6.3	Use of Authorization Architectures and Models	4
7	Architecture & Design.....	7
7.1	Trust Elevation System Context.....	7
7.2	Assumptions for Trust Elevation Systems	8
7.3	Architecture & Design Factors	8
7.4	Trust Elevation Architecture Components	9
7.5	Other Architecture Components.....	11
8	Implementation Considerations	11
8.1	Orchestration	11
8.2	Enumeration of Authentication Methods	11
8.3	User Enrolment.....	12
9	Trust Elevation Sequence, Metadata and Assertions and Conformance	12
	Appendix I – Trust Elevation Sequence (Example).....	13
I.1	Use Case: Online banking transactions	13
	Appendix II – Metadata and Assertions.....	18
II.1	Component-Component Communications	18
II.2	PDP to TE Method Determiner Request	18
II.3	TE Method Determiner to PDP Response.....	18
	Appendix III – Conformance	19
	Appendix IV – State Models for Assurance Level Evaluation.....	20
IV.1	Evaluation of Assurance Requirements at Transaction Time	20

Document ID: 123456789

Recommendation ITU-T X.1276

Authentication step-up protocol and metadata Version 1.0

1 Scope

Electronic identity credential trust elevation methods are used to increase assurance in entity identification using authentication events and related entity information for the purpose of risk mitigation when making access control policy decisions. The goals of this Recommendation are:

- To propose simple trust elevation architectural patterns demonstrating the use of trust elevation in modern access control architectures.
- To describe a common metadata set, mechanisms and protocol elements for trust elevation information exchanges.
- To promote the use of trust elevation elements to facilitate standardization among the many technologies and approaches currently in use for credential and authentication risk mitigation.

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.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[ITU-T X.1142] Recommendation ITU-T X.1142 (2006), *eXtensible Access Control Markup Language (XACML 2.0)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

3.1.2 authentication assurance [b-ITU-T X.1252]: The degree of confidence reached in the authentication process that the communication partner is the entity that it claims to be or is expected to be.

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

3.1.3 access control [b-ITU-T X.1252]: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.4 trust [b-ITU-T X.1252]: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.

3.1.5 trust framework [b-ITU-T X.1254]: A set of requirements and enforcement mechanisms for parties exchanging identity information.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 trust elevation: The task of increasing the strength of trust by adding factors from the same or different categories of authentication methods that do not have the same vulnerabilities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABAC	Attribute Based Access Control
AL	Authentication Level
BAE	Backend Attribute Exchange Model
LOA	Level of Assurance
PDP	Policy Decision Point
PEP	Policy Evaluation Point
PIP	Policy Information Point
RP	Relying Party
RPT	Requesting Party Token
SAML	Security Assertion Markup Language
TE	Trust Elevation
UMA	User Managed Access
XACML	extensible Access Control Markup Language

5 Conventions

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

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

6 Conceptual models

This clause covers trust elevation conceptual models.

6.1 Trust elevation core model

Figure 1 depicts the core model for trust elevation.

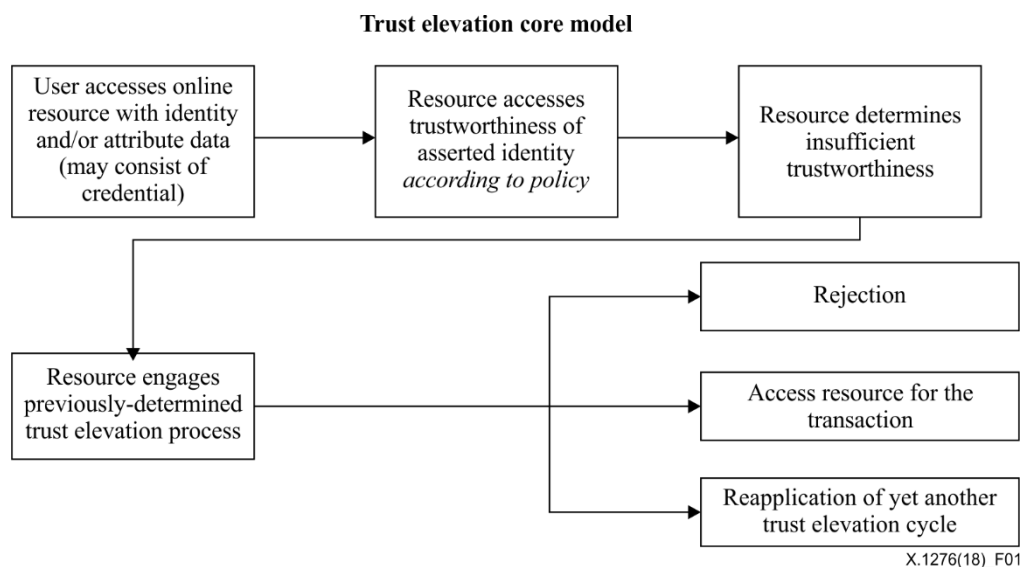


Figure 1 – Trust elevation core model

6.2 Trust elevation concepts

While the flow diagram above is easy to understand, implicit in the core model are several key components and processes, as shown in clause 7.2. The first of these is a component which functions as a policy engine capable of consuming the asserted user data and making a determination as to whether that data satisfies the resource's policy for authentication risk mitigation. The resource manager must have previously performed a risk assessment and adopted a risk mitigation strategy.

The second key component is again an antecedent service generated during the risk assessment and mitigation process. It is composed of a capability to recognize which, if any, risks have been adequately mitigated by the initial transaction, which risks remain to be mitigated and preferred methods for satisfying the remaining needs.

The third key component is a component for evaluating the success of the trust elevation transaction. This could be an iteration of the first component, but it has been broken out in the above graphic to clarify the decision flow.

While these components are necessary to implement the trust elevation of a presented online identity, they require the resource manager to have engaged in prior planning and assessments in order to generate the information necessary to direct the behaviour of the components.

Trust elevation methods are used to increase confidence in entity identification using authentication events and related entity information for the purpose of increased risk mitigation when making access control policy decisions.

Levels of assurance models are structured such that increased risk mitigation results in increased credential or identity assurance level trust. These models require the determination of a given transaction's identity and authentication risk, expressed in terms of level of assurance (LOA) requirements. Policies are designed such that a credential or identity assurance level must meet or exceed the transaction's level of assurance requirement.

Entity identification confidence may be increased by: mitigating an authentication threat not addressed by the original authentication exchange; improved mitigation of the original authentication threat, or examination of contextual or environmental factors to corroborate the existing identification.

The definition of the composition of a particular assurance level scheme, and related policy evaluation criteria, is the responsibility of the parties involved in the transactions. The scheme should be tailored

to the risk tolerance and requirements of the relying party (RP). In other words, it is up to the resource manager to determine when sufficient mitigations of risk have occurred.

6.3 Use of authorization architectures and models

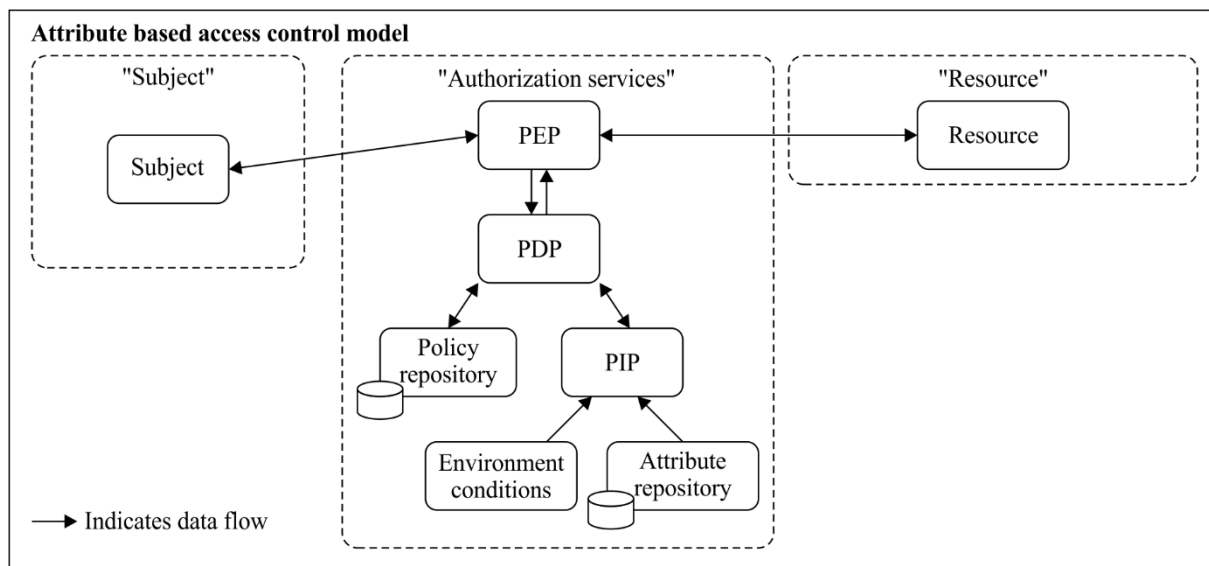
Another way to look at trust elevation is as a type of transaction or access control authorization. From this perspective, evaluation of the current state versus policy requirements results in decisions to 'Permit', 'Deny', or 'Require Elevation'.

The trust elevation core model is compatible with other published authorization models, such as: attribute based access control (ABAC) [ITU-T X.1142].

6.3.1 Attribute based access control model

This clause illustrates how trust elevation (TE) would fit into an attribute based access control model. In [b-NIST SP800-162] the work describes the elements of an attribute based access control model.

As shown in Figure 2, the primary components of authorization services are the policy enforcement point (PEP) which intercepts resource requests; and, the policy decision point (PDP) which checks supplied attributes versus access control policy. The PDP can obtain additional attributes from environmental conditions, policy information point (PIP) and other sources. Based on the policy evaluation, the PDP instructs the PEP to permit or deny access to the resource.



X.1276(18)_F02

Figure 2 – Attribute based access control model

As depicted in Figure 3, when the authorization services determine that trust elevation is required, the trust elevation services take information from "Authentication Services" and "Risk-Based Engine" to evaluate what trust elevation method should be used to achieve the desired result.