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 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/.

Table of Contents

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.

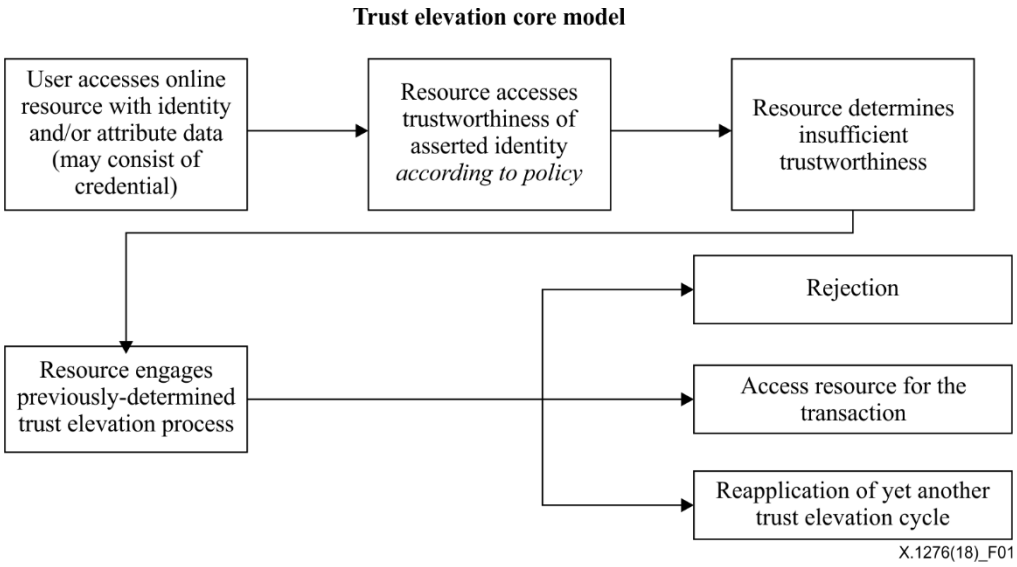


Figure 1 – Trust elevation core model

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.

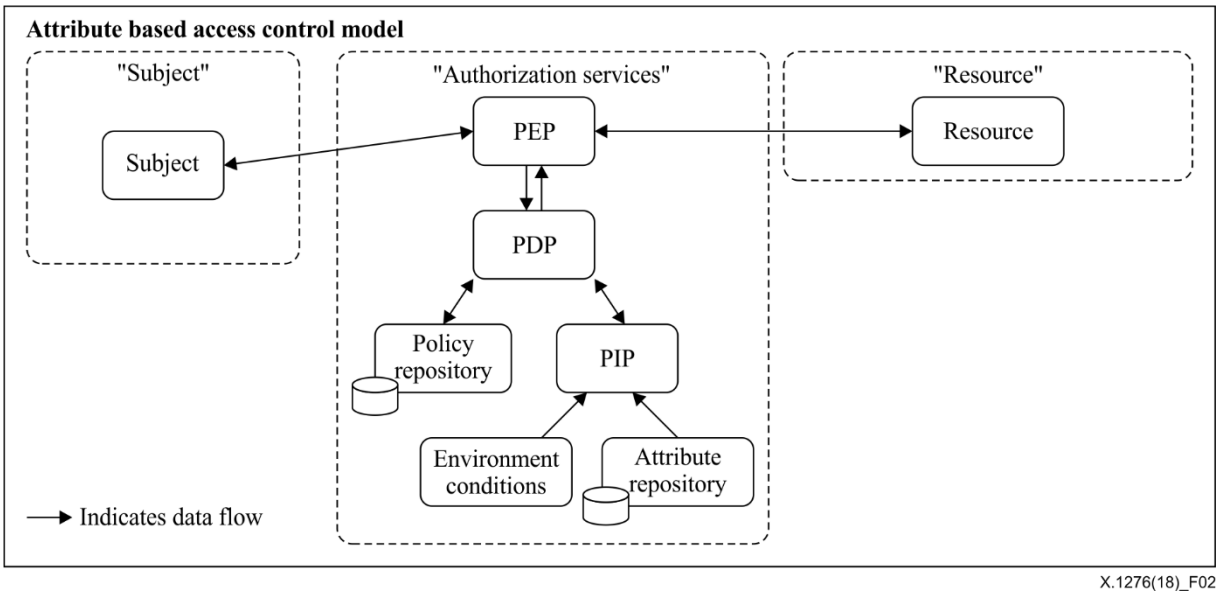


Figure 2 – Attribute based access control model

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.

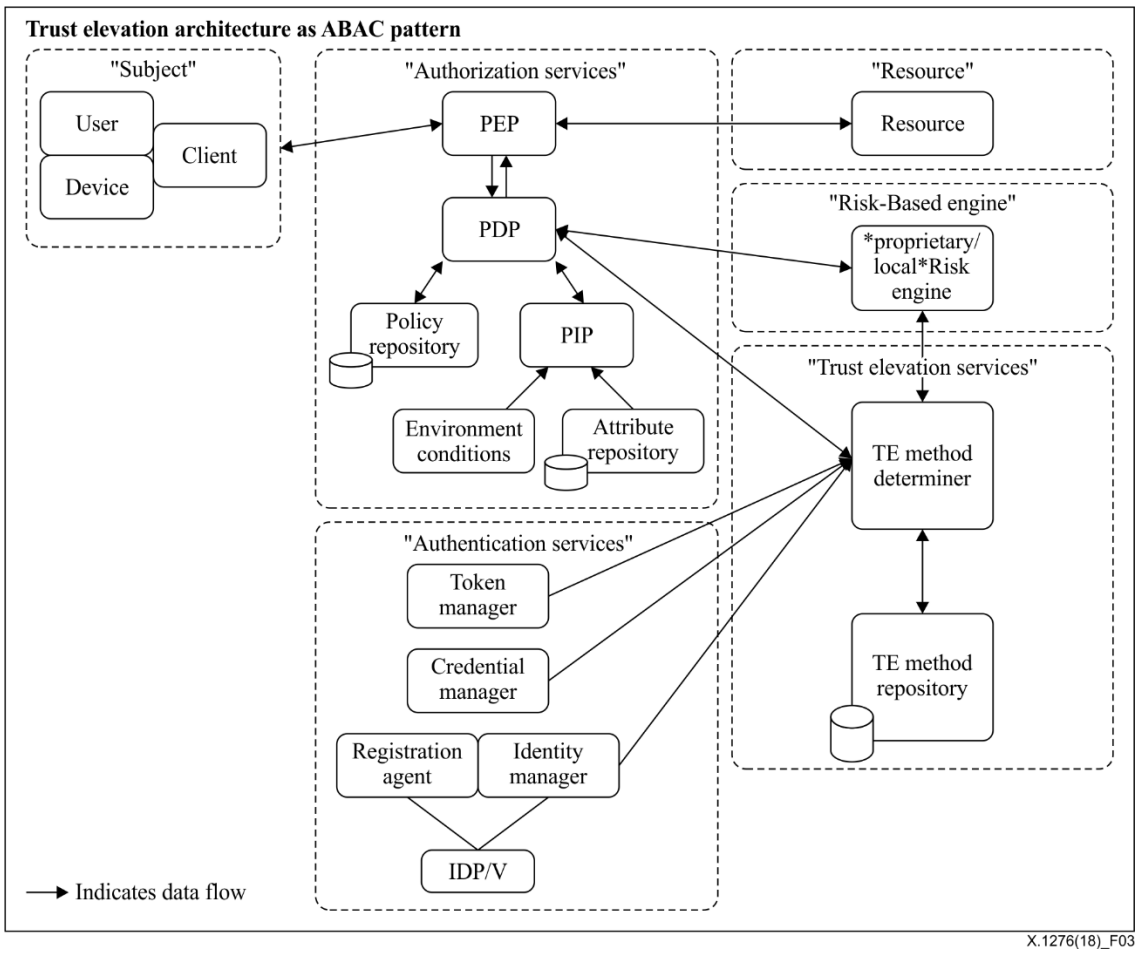


Figure 3 – Trust elevation architecture as ABAC pattern

6.3.2 User managed access authorization model

NOTE – This clause is non normative.

The user-managed access protocol (UMA) defines a mechanism for a policy enforcement point – known as the resource server – to delegate authorization of a requesting party to a policy decision point – known as the authorization server – using elements of the OAuth 2.0 authorization framework.

To gain access to a protected resource, an UMA client (web or mobile application operating on behalf of a requesting party) must present a valid access token, called a requesting party token (RPT), to the resource server. The RPT must be valid and associated with sufficient authorization data, issued through a trust elevation process, before the resource server can grant access.

The authorization server, guided by policies set by the owner of the protected resource, elevates trust by testing whether the requesting party meets the policies. As part of this process, it could demand that the requesting party (or the client on their behalf) provide claims, such as identity information or even promises to adhere to constraints set by the resource owner, such as an embargo on information release until a certain date.

A policy that the authorization server can consider is what mechanism was used to authenticate the person. UMA does not require the use of any particular authentication protocol, but works especially well with OpenID Connect.

The OpenID Connect Core specification defines two claims in the ID Token format called `acr` and `amr`, which provide details about what type of authentication was performed. Their values can be defined by a domain, a federation, a global registry, or some other trust framework. An UMA authorization server can test a requesting party against policies to evaluate the sufficiency of the authentication mechanism as provided in values of these claims.

In the event that the mechanism was not sufficient, the authorization server can indicate the reason for the authorization failure and what type of credentials would satisfy the policy. At this point, the client can request re-authentication from the OpenID Provider and ultimately re-request the RPT token. This flow would constitute trust elevation by step-up authentication.

6.3.3 XACML authorization model

The extensible access control markup language (XACML) standard defines a reference architecture for ABAC, a language for expressing access control rules and policies, and a protocol for generating and processing access control requests and returning responses.

Access to resources is mediated by a PEP, which relies on decisions from a PDP. When a user attempts to access a protected resource, the PEP assembles a request, which provides attributes about the user, the resource, the environment, and the action requested. The PEP communicates the request to the PDP, which evaluates it according to pre-defined policies.

To perform trust elevation, the access control policy can specify how users must be authenticated, including parameters such as authentication method, credentials accepted, and levels of assurance. Trust elevation in this context means enhancing authentication and/or authorization by means of requiring additional attributes.

Consider the following example: a user requests access to a protected resource. The access control policy governing the resource requires multi-factor authentication using a strongly vetted identity credential by means of setting the MustBePresent attribute to TRUE. The PEP controlling access to the resource has only hitherto validated the user identity by means of a lower assurance username/password combination. When the PEP initially formulates the request, it bases the user identity attribute on the previous username/password authentication event. When the PDP receives the request, it evaluates the request according to the appropriate policy, based on the resource. Since MustBePresent = TRUE, the PDP renders an "Indeterminate" decision, with a status code of "urn:oasis:names:tc:xacml:1.0:status:missing-attribute". Upon receiving this "Indeterminate" with MissingAttribute status decision from the PDP, the PEP may resubmit a request after acquiring the proper attributes. In this case, the proper attributes could only be gathered through a step-up authentication event. This sequence constitutes a sample trust elevation event.

Alternatively, security administrators and resource owners may devise a series of Boolean attributes to test for authentication methods used, i.e.,:

– subject-id-authenticated-by-password
– subject-id-authenticated-by-smart-card
– subject-id-authenticated-by-biometric-iris-scan
– subject-id-authenticated-by-biometric-fingerprint
– subject-id-authenticated-by-two-factors
– subject-id-authenticated-by-three-factors.

This would allow policy authors to specify which methods are acceptable by testing for a TRUE result among the list they define as meeting security requirements.

Lastly, the Obligation element of XACML could be used to perform trust elevation. Any rule that permits access and specifies the authentication level required would add an obligation stating the minimum required authentication level, e.g.,

> if "User authorized" then Permit. FulfillOn=Permit -> authenticated-by-two-factors-obligation.

In this case, the PEP does not need any special attributes. It makes a normal authorization request. If the response is Deny or NotApplicable, then the authentication level is irrelevant because the user is not allowed access. If the response is Permit without any authentication level obligations, then access

is allowed even at the lowest authentication level. If the response is Permit with specific authentication level obligations, then the PEP must perform step-up authentication to the authentication level of the highest level of the obligations it received. If the highest level is satisfied, then any lower levels are satisfied. If that step-up fails or cannot be attempted, then access is denied. If step-up succeeds then access is allowed without needing an additional authorization request.

6.3.4 SAML backend attribute exchange (BAE) model

The security assertion markup language (SAML) standard [ITU-T X.1141] defines a means for representing authentication events between different trusting security domains. A SAML assertion may contain a variety of attributes about the requesting subject and the conditions of the authentication event. Subject and Issuer attributes generally relate the name of the subject and the name of the organization with which the subject is associated in the AuthenticationStatement element. The AuthenticationStatement also contains an AuthenticationContext attribute, which details how the subject was authenticated in the context of the current assertion.

SAML-aware relying party applications can request additional attributes via the AttributeQuery element. Moreover, SAML authorities can request full attribute evaluations via the AuthzDecisionQuery element. Relying parties may specify acceptable authentication methods and credentials by using the RequestedAuthnContext element, and can force a fresh authentication event by setting ForceAuthn to true.

Trust elevation can be exemplified in the following scenario using SAML: a user attempts to access content protected by a SAML-aware relying party (RP) application. The user posts a SAML assertion containing Subject/Issuer attributes and indicates a low-level assurance authentication event to the RP. The RP's access control policy requires additional attributes and a higher strength credential and authentication event. The RP initiates a SAML authentication request to the user's home domain. This forces a step-up authentication event and retrieval of additional attributes, as required by the attribute contract. As with the XACML model, trust elevation means enhancing authentication and/or authorization by means of requiring additional attributes.

7 Architecture and design

This clause provide the architecture and design of trust elevation.

7.1 Trust elevation system context

The participants, authentication methods, communication protocols and authorization methods of the trust elevation system MUST be agreed upon among the participants.

If new participants and/or methods are introduced to the trust elevation system, appropriate onboarding processes MUST be used.

The lack of generally agreed-upon criteria and evaluations of an authentication method's efficacy to counter threats, mitigate impacts or reduce negative occurrence frequency, as well as local extrinsic concerns makes dynamic addition of new authentication methods problematic. A trust elevation system may consider a password-based authenticator to be sufficient for identification whereas another trust elevation system may require additional fraud detection infrastructure to realize the same degree of sufficiency.

The trust elevation system MUST use business rules and technologies related to authentication and authorization for performing trusted transactions that are shared among participants. A trust elevation system could refer to: federated systems; systems controlled by a single governing entity; or a single system.

7.2 Assumptions for trust elevation systems

There are several assumptions that help to set the context for trust evaluation systems:

– The resource manager MUST have a defined set of requirements for authentication and/or authorization control. The requirements MAY include combinations of static rules and dynamic risk evaluations.
– In the case of federated services, the federation agreement MUST define the available identification and authentication methods and their relationship to discrete 'levels' of assurance that map to risk mitigation or compensating controls.
– Authentication methods MUST be described sufficiently to allow creation of sets of compatible methods that cover identifiable risks or threats to allow implementers to choose independent authentication factors.

7.3 Architecture and design factors

There are many potential factors that influence the design specific trust elevation architectures. The nature and impact of the factors is determined by local requirements.

7.3.1 Definition of 'Elevation' or 'Step-Up'

The semantics of combining authentication methods to increase risk mitigation MUST be dependent on local definition of authentication method characteristics within a trust elevation system.

The risk models of the resource manager and/or federation that comprise the trust elevation system MUST be considered when defining how combinations of methods modify risk mitigation.

For example, in a federation repetition of a password authentication to re-confirm the authenticator may change the risk mitigation from 'Low' to 'Medium'. In a different federation, the same risk mitigation change might require a second authentication method which is different from the first one used.

The full range of permitted combinations and their effect on risk mitigation SHOULD be defined for the local entities.

7.3.2 Use of shared definitions

As with authentication method combinations, the specification of each permitted authentication method MUST be shared within a trust elevation system.

NOTE – If a fingerprint template biometric is to be used, common specification of sampling mechanics, template calculation and comparison algorithms is essential. Variance in specification within a trust elevation system will result in different semantic meaning when combining authentication methods.

7.3.3 Authentication state tracking

Authentication state per subject MAY need to be kept.

The trust elevation system MAY need to know which authentication methods have been attempted in prior transaction attempts in order to select a different authentication method or factor to be attempted next.

Tracking state per subject and transaction attempt may prove to be a complex undertaking unless care is taken when designing elevation policy.

7.3.4 Location of policy decisions

The architecture and design SHOULD be able to accommodate local, remote and distributed policy evaluation. Policy evaluation for trust elevation purposes may occur within a single system, or may occur in several different systems and then combined.

A mechanism for calculating the combined result of the policy evaluation MUST be designed.

7.3.5 Consideration of time or quality degradation

When designing the state model for the authorization system, time-related degradation of information quality or authenticator validity SHOULD be considered. The degradation COULD be defined as nil, or according to a specified time function.

7.3.6 Responsiveness to threat environment

The effect of changes in the threat environment might cause changes of calculated assurance levels. Designers SHOULD determine if and how to respond to changes to the threat environment.

If a system component is observed to be under active attack, the authorization system SHOULD require increased assurance levels through use of additional authentication methods.

7.4 Trust elevation architecture components

The following architecture diagram in Figure 4 shows trust elevation system components and other components related to trust elevation systems and their core functions. The dashed line boxes represent the boundary for each major component. The solid line boxes represent the functions within the major components. In other authorization model representations, the functions may have different names and may possibly appear within different major component boundaries.

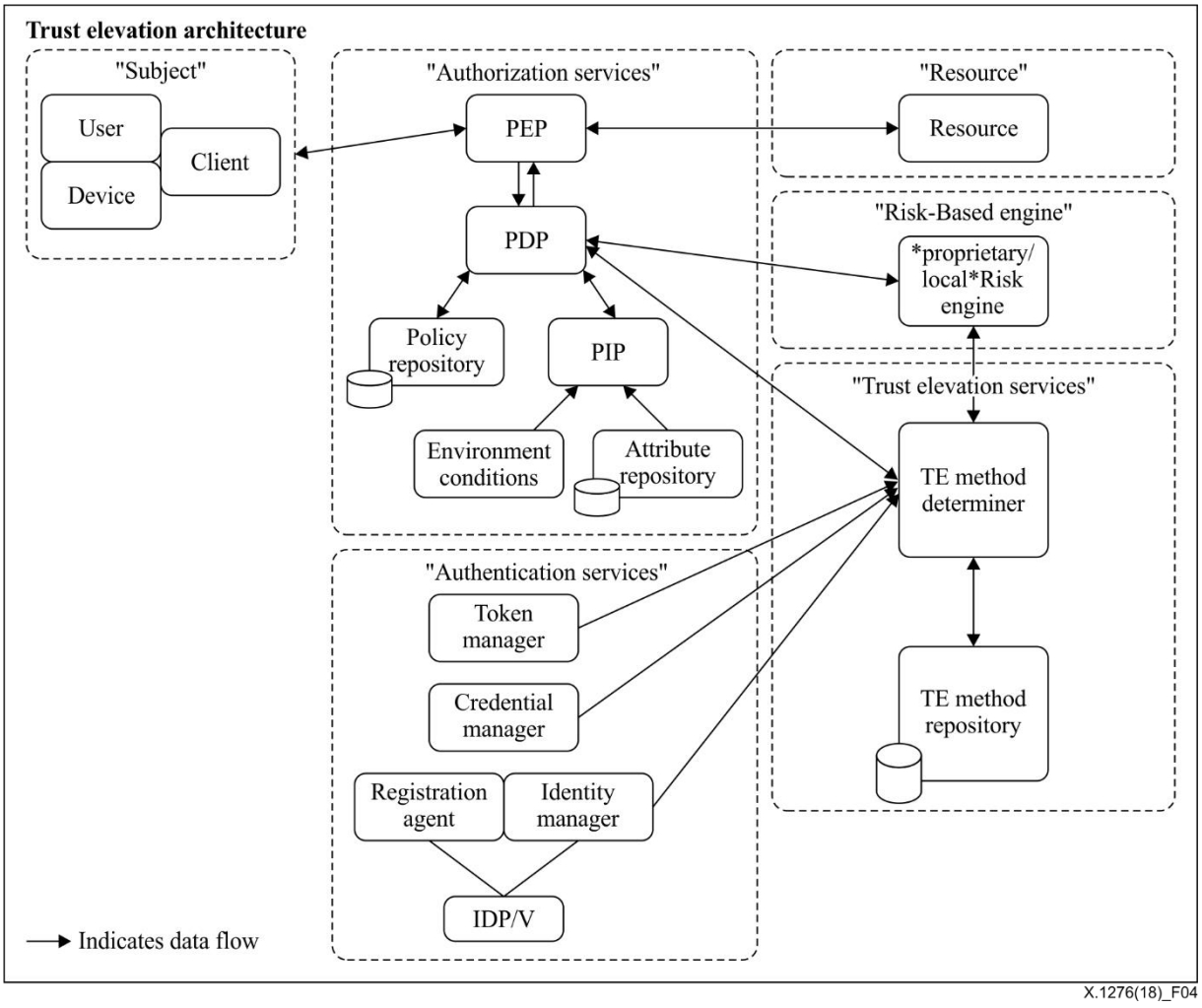


Figure 4 – Trust elevation architecture

7.4.1 Trust elevation services component

The trust elevation services component is comprised of the trust elevation method determiner and the trust elevation method repository.

When the authorization services component determines that the subject is not permitted to access the resources due to insufficient identification and authentication assurance, the trust elevation services component is used to select an additional authentication method or methods which would allow the subject to access the resources.

The trust elevation services component enables the authorization services to ask the subject to retry access using different or additional authenticators.

The trust elevation services are aware of the methods and authenticators previously used by the subject to attempt access. This enables mitigation of identification threats different from the initial authentication methods and authenticators, without having to hard code all combinations of authenticators that could be used.

For example, if the initial authenticator used username/password (a 'known' factor), the trust elevation services would not recommend that authenticator if asked for another single factor authenticator: it might return a 'have' or 'are' factor authentication method, or a 'known' factor authentication method that is not username/password.

7.4.1.1 Trust elevation method determiner

The trust elevation method determiner makes trust elevation policy decisions.

It receives requests from the authorization services component that MUST include current authentication state information of the subject and the desired level of assurance.

The trust elevation method determiner uses policies stored in the trust elevation method repository to determine which, if any, authentication methods could be used to achieve the desired level of assurance.

The trust elevation policy MUST map the combinations of authenticators to the desired assurance levels.

Given the desired assurance level, the trust elevation method determiner MUST be able to evaluate trust elevation policy to identify the list of authentication methods that could be used to achieve the desired assurance level.

The current authentication state information MAY include data about: authenticators presented to the authorization services component; authentication methods that were used by the subject to achieve the current authentication state; and, the current LOA of the subject.

If the authentication capabilities of subjects (user, device or client) are dynamic or dependent on device, user or software abilities and features, the method determiner MAY need information about the specific capabilities of the specific subject in order to avoid unnecessary round trips to the subject.

7.4.1.2 Trust elevation method repository

The trust elevation method repository contains information necessary to the functions of the trust elevation method determiner.

The trust elevation method repository MUST contain information about the implemented authentication methods and their characteristics. These characteristics are used in the trust elevation policy when the concepts of 'stronger' authenticators or 'more' assurance are represented.

If the trust elevation system uses authentication factors to determine authenticator strength, it COULD treat a single factor authenticator as weaker than a two-factor authenticator. In this case the characteristics SHOULD include details of which authentication factors are used.

7.5 Other architecture components

These components interact with trust elevation systems but are not part of the trust elevation systems.

7.5.1 Authorization services component

The authorization services component MUST be capable of requesting and processing trust elevation information. Trust elevation services may be treated as an information source or a remote policy engine.

The authorization services component may need additional functionality to handle and track multiple access attempts by the subject as the subject responds to elevation requests.

7.5.2 Risk-based engine component

If a risk-based engine component exists, it represents systems that may be used by the resource manager to detect, measure and respond to threats in the operational environment. Detection of increased online attacks could cause the resource manager to require a greater degree of identification or authentication for access to resources.

8 Implementation considerations

This clause provides implementation considerations.

8.1 Orchestration

Orchestration of trust elevation systems interaction with access control system components is required.

The access control components MUST be capable of requesting additional authentication or information from the subject.

Since the trust elevation services component determines which authentication methods are required after the first round of policy evaluation, all components in the access control service MUST be able to handle the extra requests.

8.2 Enumeration of authentication methods

The implemented authentication methods MUST be enumerated and details stored in the trust elevation repository.

The details that SHOULD be captured are identified in Deliverable 2, comprised of threats eliminated and risks mitigated. The detailed information will enable analysts to design trust elevation sequences that use complementary authentication methods to strengthen risk mitigation.

8.2.1 Subject component

Authentication methods recorded in the trust elevation method repository MAY involve any combination of user, device and client.

As the subject might interact with the authorization services at different points in time with different user, device or client elements, authentication methods MUST NOT make assumptions about the relationships between the subject, user, device or client.

NOTE – The same user attempting access from a different device that has an identical device model has lower assurance than use of the originally registered device. Authentication methods involving the device need to be able to differentiate between those devices.

8.2.2 Effect of device capability changes

Devices may have different authentication method capabilities at enrolment versus at the time of the transaction. Device hardware used for authentication SHOULD NOT be assumed to be available or functioning.

8.3 User enrolment

Enrolment is a key phase to support the execution of trust elevation. At enrolment time, the trust elevation system MUST identify, record and possibly provision authentication methods. These authentication methods COULD include user, device, geo-location, network location and environmental elements.

9 Trust elevation sequence, metadata and assertions and conformance

Appendix I provide an example of a trust elevation sequence.

Appendix II provides examples of metadata and assertions.

Appendix III provides conformance guidelines.

Appendix IV provides state models for assurance level evaluation.

Appendix I

Trust elevation sequence (example)

(This appendix does not form an integral part of this Recommendation.)

The specific structure and content of the policy table and methods table are defined within the trust elevation system, driven by the relying party's authentication policies.

In this simple example, a static mapping of a relying party defined transaction risk levels to pre-defined authentication strengths encoded as "Authentication Levels" (AL) is shown. The relying party defines which authentication level transitions are required for each transaction risk level.

The policies are based on the 'authentication factors' approach to risk mitigation. The relying party policy sets out the permitted combinations of authentication factors required to move from one authentication level to another authentication level.

Note that all transitions for all risk levels are not necessarily defined. The policy table only shows valid policies for this relying party within this trust system. If a particular transition is not defined, it is deemed to be invalid.

I.1 Use case: Online banking transactions

I.1.1 Description

A bank customer (subject) initially logs on to the bank site (through a browser or mobile app) to view their account balance. Then, they decide to perform a higher risk transaction that requires a higher level of authentication: a funds transfer of $X.

I.1.2 Pre-conditions

– Subject has an existing relationship with the bank (i.e., is an account holder).

– Subject has previously registered their authentication methods (e.g., password, device, biometric).

– There are three authentication levels defined by the bank (the relying party).

I.1.2.1 Transaction risk levels

Transaction designation	Transaction name	Transaction risk level
T1	Check account balance	Low
T2	Transfer funds out	Med

I.1.2.2 Policy table

The policy table is defined during system design by the relying party.

NOTE – Authentication policies are set by the relying party.

Transaction risk level	Initial strength	Desired strength	Authentication needed*	Policy designation
Low	AL0	AL1	One factor, either what you know or have	P1
Med	AL0	AL2	Two factors, any class	P2
	AL1	AL2	One factor, different than used for AL1 authentication	P3

Transaction risk level	Initial strength	Desired strength	Authentication needed*	Policy designation
High	AL0	AL3	Three factors	P4
	AL1	AL3	Two factors, any class, different than used for AL1 authentication	P5
	AL2	AL3	One factor, different than used for AL1 OR AL2 authentication	P6

Where AL0 represents a "user not logged in" state.

I.1.2.3 Methods table

The methods table enumerates the authentication methods available in the trust system.

Method designation	Method description	Class(es)	Single factor (SF) strength	Threats addressed*
M1	PIN (>=4 char)	Know	1	
M2	Password (>=8char)	Know	1	
M3	Device ID	Have	1	
M4	Crypto key (TLS protocol)	Have	2	
M5	Biometric – face	Are	NA	
M6	Biometric – fingerprint	Are	NA	
M7	PIN + Device ID	K+H	2	
M8	Crypto key + face	H+A	3	

NOTE – *For the benefit of relying party operators setting up policies.

I.1.3 Process flows

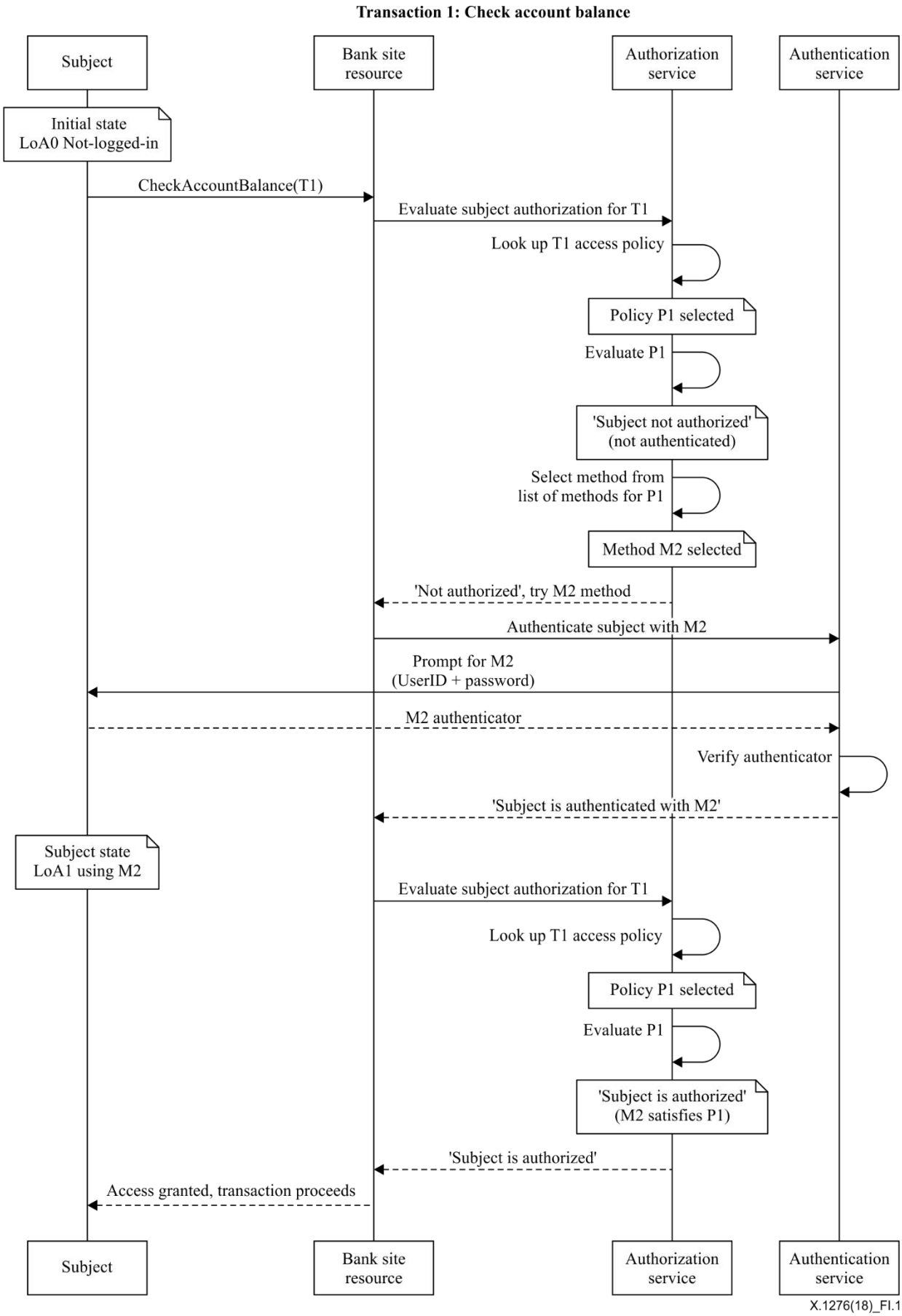
I.1.3.1 Transaction 1: Check account balance

NOTE – In the process flow the PEP is not shown and is assumed to be part of the resource.

```
Title Transaction 1: Check Account Balance
Note over Subject: Initial State \nLoA0 Not-logged-in
Subject->Bank Site\nResource: CheckAccountBalance(T1)
Bank Site\nResource->Authorization\nService: Evaluate Subject authorization for T1
Authorization\nService-> Authorization\nService: Look up T1 Access Policy
Note over Authorization\nService: Policy P1 selected
Authorization\nService-> Authorization\nService: Evaluate P1
Note over Authorization\nService: 'Subject Not Authorized'\n(Not Authenticated)
Authorization\nService-> Authorization\nService: Select Method from \nlist of
Methods for P1
note over Authorization\nService: Method M2 selected
Authorization\nService-->Bank Site\nResource: 'Not Authorized', Try M2 Method
Bank Site\nResource-> Authentication\nService: Authenticate Subject with M2
Authentication\nService->Subject: Prompt for M2 \n (UserID + Password)
Subject--> Authentication\nService: M2 Authenticator
Authentication\nService-> Authentication\nService: Verify Authenticator
Authentication\nService--> Bank Site\nResource: 'Subject is Authenticated with M2'
Note over Subject: Subject State \nLoA1 using M2
Bank Site\nResource-> Authorization\nService: Evaluate Subject authorization for
T1
Authorization\nService-> Authorization\nService: Look up T1 Access Policy
note over Authorization\nService: Policy P1 selected
```

I.1.3.2 Transaction 1: Sequence

NOTE – In the process flow the PEP is not shown and is assumed to be part of the resource.



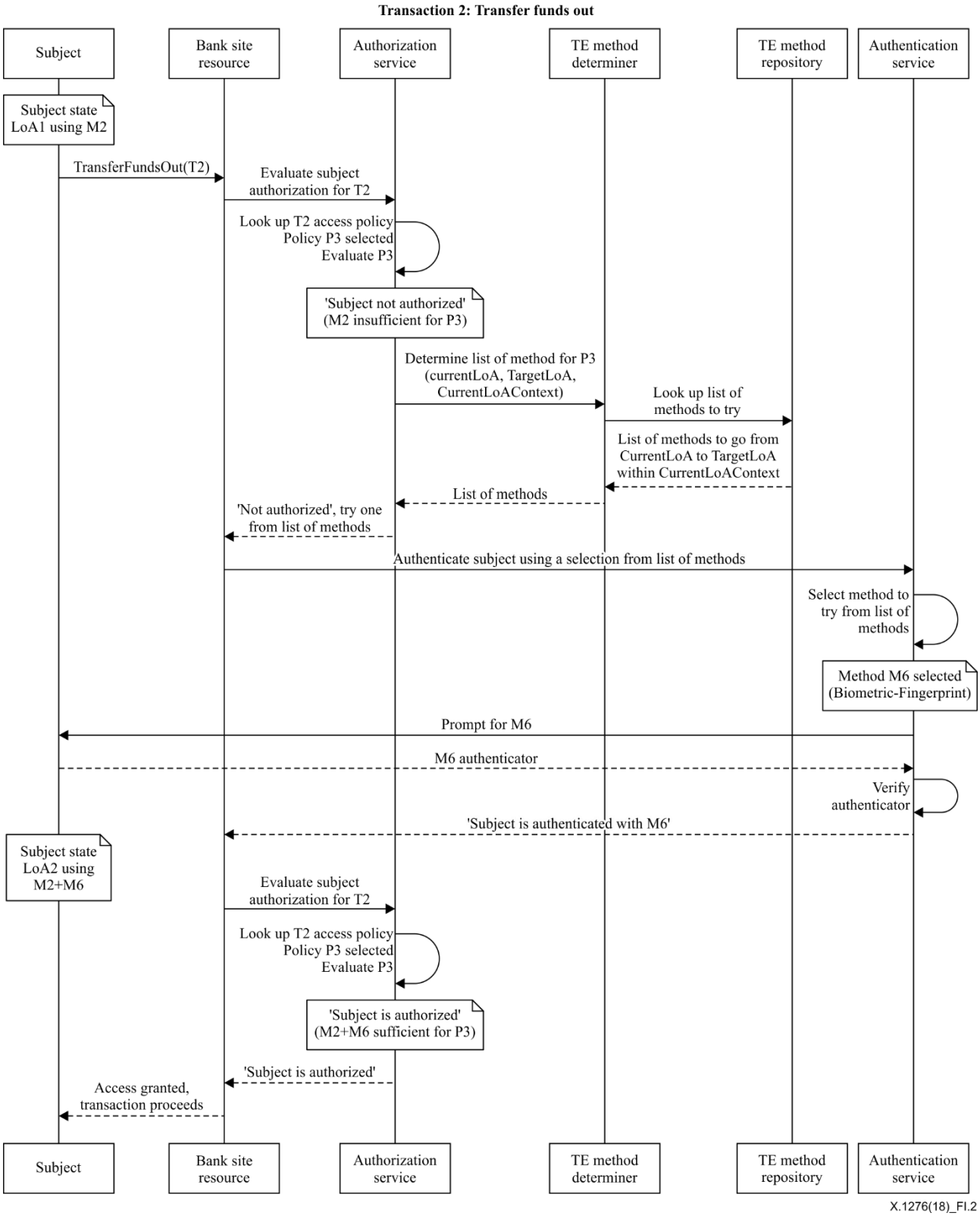
I.1.3.3 Transaction 2: Transfer funds out

NOTE – In the process flow the PEP is not shown and is assumed to be part of the resource.

```
Title Transaction 2: Transfer Funds Out
Note over Subject: Subject State \nLoA1 Using M2
Subject->Bank Site\nResource: TransferFundsOut(T2)
Bank Site\nResource->Authorization\nService: Evaluate Subject authorization for T2
Authorization\nService-> Authorization\nService: Look up T2 Access Policy\nPolicy
P3 selected\nEvaluate P3
Note over Authorization\nService: 'Subject Not Authorized'\n(M2 Insufficient for
P3)
Authorization\nService->TE Method\nDeterminer: Determine List of Methods for
P3\n{CurrentLoA, TargetLoA, CurrentLoAContext}
TE Method\nDeterminer->TE Method\nRepository: Look Up List of Methods to try
TE Method\nRepository-->TE Method\nDeterminer: List of Methods\nto go from
CurrentLoA to TargetLoA\nwithin CurrentLoAContext
TE Method\nDeterminer-->Authorization\nService: List of Methods
Authorization\nService-->Bank Site\nResource: 'Not Authorized',\nTry one from List
of Methods
Bank Site\nResource-> Authentication\nService: Authenticate Subject using a
selection from List of Methods
Authentication\nService-> Authentication\nService: Select Method to try from
\nlist of Methods
note over Authentication\nService: Method M6 selected\n(Biometric-Fingerprint)
Authentication\nService->Subject: Prompt for M6
Subject--> Authentication\nService: M6 Authenticator
Authentication\nService-> Authentication\nService: Verify Authenticator
Authentication\nService--> Bank Site\nResource: 'Subject is Authenticated with M6'
Note over Subject: Subject State \nLoA2 using M2+M6
Bank Site\nResource->Authorization\nService: Evaluate Subject authorization for T2
Authorization\nService-> Authorization\nService: Look up T2 Access Policy\nPolicy
P3 selected\nEvaluate P3
Note over Authorization\nService: 'Subject Is Authorized'\n(M2+M6 Sufficient for
P3)
Authorization\nService-->Bank Site\nResource: 'Subject is Authorized'
Bank Site\nResource-->Subject: Access Granted, Transaction Proceeds
```

I.1.3.4 Transaction 2: Sequence

NOTE – In the process flow the PEP is not shown and is assumed to be part of the resource.



Appendix II

Metadata and assertions

(This appendix does not form an integral part of this Recommendation.)

II.1 Component-component communications

Content of authorization service (PDP) to trust elevation method determiner request:

– Current authentication level.

– Method(s) that were used to achieve current authentication level.

– Target authentication level.

Content of trust elevation method determiner to authorization service (PDP) response:

– List of methods that could be used to achieve target authentication level.

Content of authorization service (PDP)-Authentication service request:

– Subject ID.

– List of methods to choose from.

II.2 PDP to TE method determiner request

The fragments below are examples showing the kinds of information to exchange between components.

```
<trustel:MethodTypeRequest>
    <trustel:CurrentLoA>....</trustel:CurrentLoA>      //current Authentication Level in numerical value
    <trustel:TargetLoA>...</trustel:TargetLoA>  //Target Authentication Level in numerical value
    <trustel:CurrentLoAContext>
         <trustel:Method>...</trustel:Method> //could be "|" delimited array of methods
         <trustel:AuthnDeviceSig>..</trustel:AuthnDeviceSig>  //Device Fingerprint
         <trustel:AuthnLocation>...</trustel:AuthnLocation>   //Device location
         <trustel:AuthnIP>...</trustel:AuthnIP>  //IP of the device
         <trustel:AuthnTime>...</trustel:AuthnTime>     //time of request
    </trustel:CurrentLoAContext>
</trustel:MethodTypeRequest>
```

II.3 TE method determiner to PDP response

```
<trustel:MethodTypeResponse>
    <trustel:Method>...</trustel:Method>  //could be "|" delimited array of methods
</trustel:MethodTypeResponse>
```

Appendix III

Conformance

(This appendix does not form an integral part of this Recommendation.)

In order to conform to this specification, the trust elevation system under consideration:

1) Must be designed and use an architecture that conforms to the normative statements in clause 6.
2) Must be implemented in conformance with the normative statements in clause 7.

Appendix IV

State models for assurance level evaluation

(This appendix does not form an integral part of this Recommendation.)

IV.1 Evaluation of assurance requirements at transaction time

One of the core assumptions of trust elevation is that a subject attempting a transaction is unable to meet the policy requirements for identification certainty unless an elevation event occurs.

An important concept is that measured assurance levels change over time due to many factors. At the instant of authorization policy evaluation, the current state of identity attribute assurance level and authenticator assurance level are compared to the transaction's assurance level requirement. If the measured assurance levels are greater or equal to the requirement, the transaction proceeds.

Figures IV.1 to IV.3 show that the assurance level of the identity information attributes established via the identity proofing and verification processes are separate and unlinked to the assurance level of the authentication event (which includes credential and authenticator details). This approach is consistent with ITU-T X.1254 LOA calculation method.

IV.1.1 Up-front policy evaluation of proofing and authenticator levels

Figure IV.1 illustrates a scenario where the levels of identity attribute assurance and authenticator assurance are determined in advance and do not degrade over time.

The vertical dashed lines represent the potential points in time of the transaction event. The identity attribute assurance and authenticator assurance levels are compared to the transaction assurance level requirement. If both values are greater than the requirement, the transaction can proceed (check mark). If one or both are lower, the transaction cannot proceed (X mark) and is either rejected or directed to a trust elevation event.

Trust elevation in this scenario combines authentication factors to step up combined authenticator assurance to meet or exceed the transaction requirement.

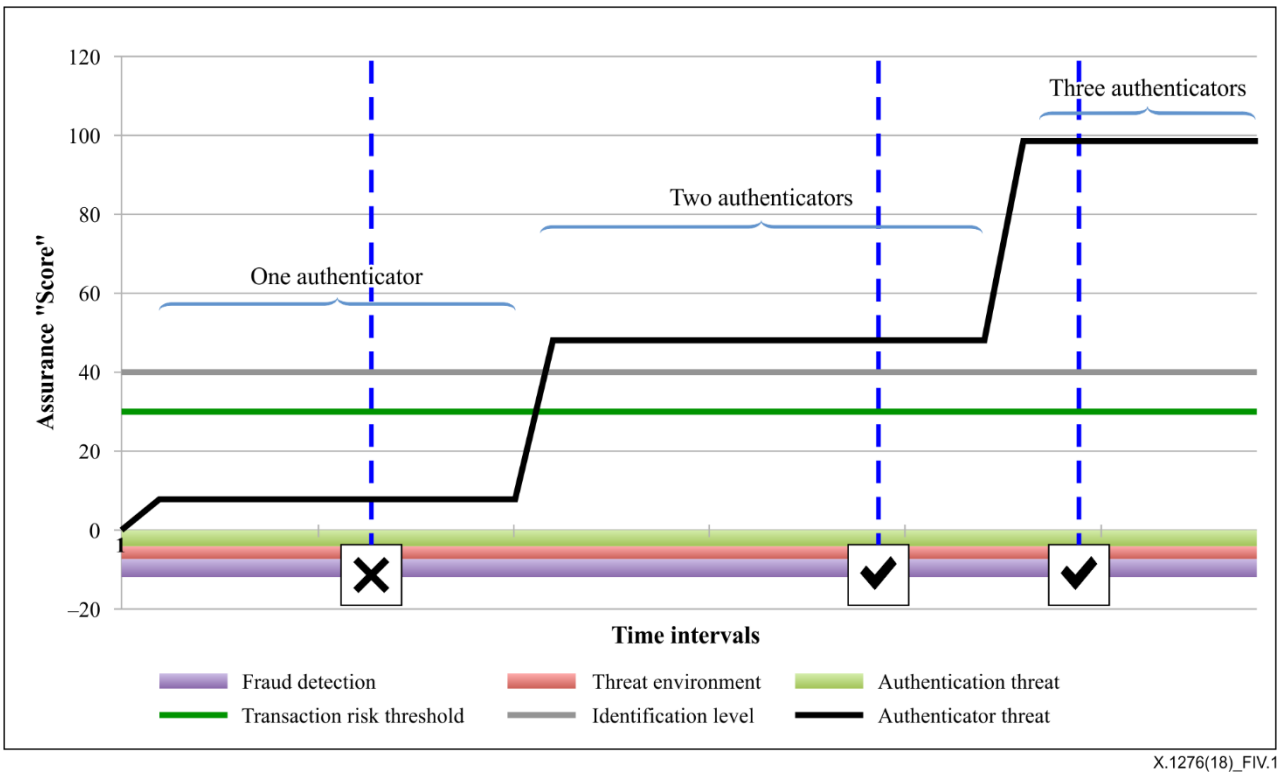


Figure IV.1 – Conceptual model: Identity attribute proofing level and authenticator assurance level (All with no degradation)

NOTES:

– The 'Assurance Score' is a simple numerical representation of the degree of certainty for illustrative purposes. 'Assurance Level 3' has been arbitrarily defined as '30' on the scale.

– The grey line represents the assurance level resulting from the identity proofing and verification process; established at subject registration time by the registration agent.

– The black line represents the authenticator assurance level resulting from the authentication event. It takes credential, authentication secrets and authenticator generation factors into account.

– The green line represents the resource owner defined assurance score/level required for the transaction. It is based on the resource owner's risk determination methods. In this example, the transaction requirement is '30' or 'LOA3'.

– The black line initially shows the effect of a single authenticator, then two authenticators, then three authenticators.

IV.1.2 Time-based degradation of authenticator assurance levels

The assurance level of the authenticator is important. Figure IV.2 illustrates a scenario where the authenticator assurance level changes over time due to time-based degradation of the credential, secrets and authenticator generation processes.

The vertical dashed lines represent the potential points in time of the transaction event. The identity attribute assurance and authenticator assurance levels are compared to the transaction assurance level requirement. If both values are greater than the requirement, the transaction can proceed (check mark). If one or both are lower, the transaction cannot proceed (X mark) and is either rejected or directed to a trust elevation event.

The scenario shows that due to rapid degradation of authenticator assurance for most time periods, trust elevation to three authenticators is needed for the transaction policy.

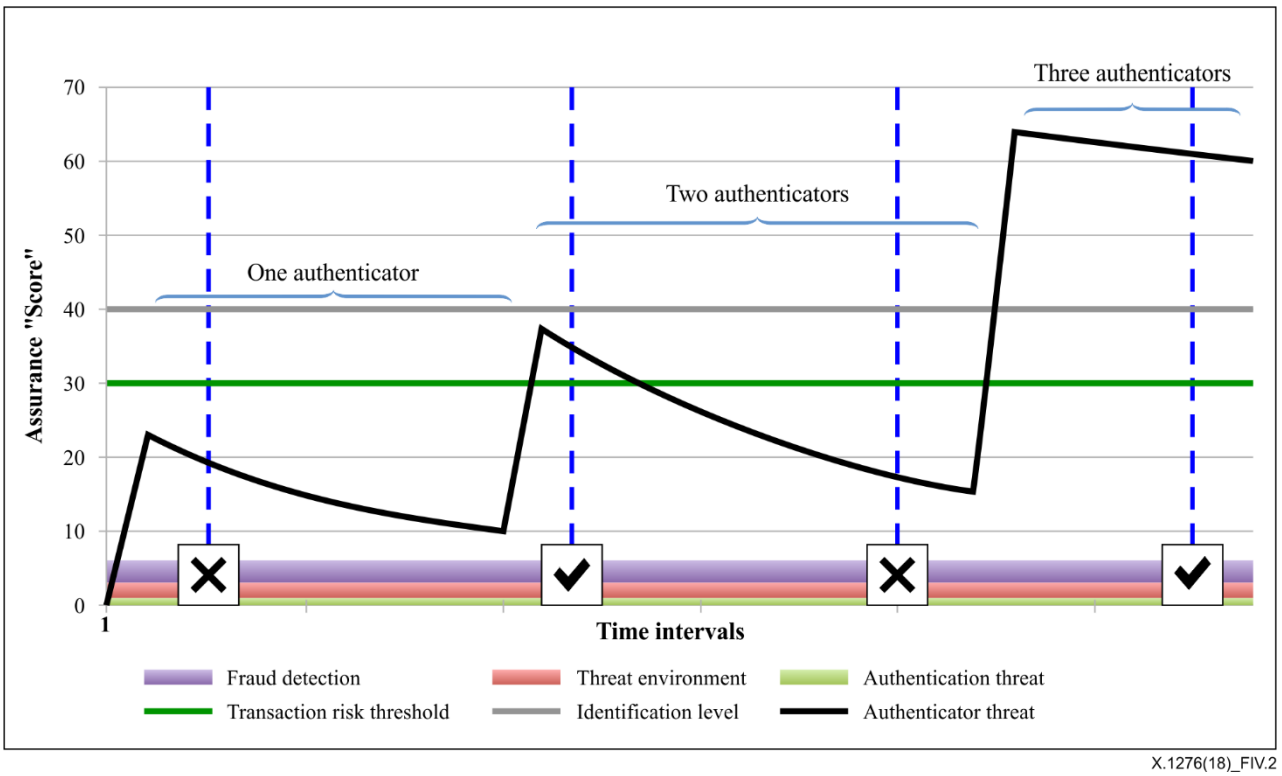


Figure IV.2 – Conceptual model: Identity attribute proofing level and authenticator assurance level (Authenticator quality degrades over time)

IV.1.3 Threat environment effects on effective authenticator level

Figure IV.3 illustrates a more complex example in which the overall threat level affects the authenticator assurance level. A simplistic calculation is used where increasing threat environment, increasing detected fraud and decreased system security subtract directly from the authenticator assurance score.

This mimics the effect that a risk-based authentication system or risk engine might have on transaction assurance requirement evaluation.

As in the previous illustrations, the vertical dashed lines represent the potential points in time of the transaction event.

Where the increased threat level causes the effective authenticator assurance level to dip below the green transaction requirement line, trust elevation could be used to achieve the minimums necessary. Note that in the 'Two Authenticators' region, the transaction could proceed or fail depending on the magnitude of the threat levels. If the transaction fails, the relying party could choose to retry at a later time, or request additional authenticators.

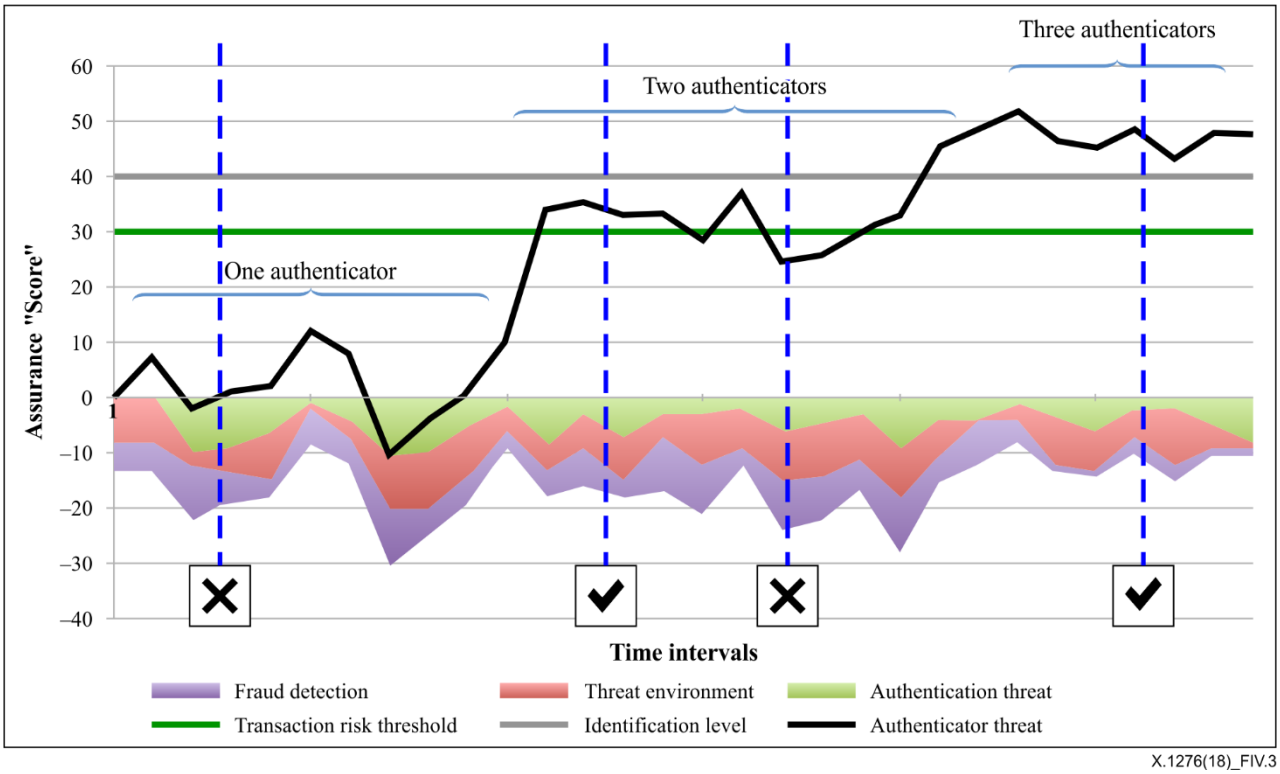


Figure IV.3 – Conceptual model: Identity attribute proofing level and authenticator assurance level (Threat environment fluctuations)

Bibliography

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

[b-NIST SP 800-162] NIST, Special Publication 800-162, (2014), *Guide to Attribute Based Access Control (ABAC) Definition and Considerations.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018