

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.1154

(04/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Security protocols

General framework of combined authentication on multiple identity service provider environments

Recommendation ITU-T X.1154

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.1154

General framework of combined authentication on multiple identity service provider environments

Summary

Recently, many application services, especially financial services, require more reliable or combined authentication methods such as multifactor authentication due to the increase in identity (ID) theft. For example, one-time password authentication and other new authentication methods are used instead of traditional password-based authentication.

The combinations of authentication methods provide multiple identity service providers (IdSPs) the ability to enhance the assurance of authentication. Recommendation ITU-T X.1154 provides the general framework of combined authentication in multiple IdSP environments for a service provider. In this Recommendation, three types of combined authentication methods are considered: multifactor authentication, multi-method authentication and multiple authentications.

The framework in this Recommendation describes models, basic operations and security requirements for each model component and each message between the model components to maintain an overall level of authentication assurance in situations of a combination of multiple IdSPs.

In addition, the framework also describes models, basic operations and security requirements to support the authentication service that manages a combination of multiple IdSPs.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1154	2013-04-26	17

Keywords

Combined authentication, entity authentication, multifactor authentication.

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 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	3
6	Types of combined authentication.....	3
7	Authentication models on multiple IdSP environments	4
7.1	Basic models with regard to service provider	4
7.2	Entity authentication life cycle model	10
8	Operations in multiple IdSP environments.....	13
8.1	Credential management operations	14
8.2	Usage operations of credentials.....	14
8.3	Management operations of trust relationships with service providers	15
9	General framework of combined authentication on multiple identity service provider environments.....	15
9.1	Logical components.....	16
9.2	Behaviours.....	17
Annex A – Considerations for combined authentication		23
A.1	Achieving estimated authentication assurance	23
A.2	Selection of IdSP(s).....	23
A.3	Effective authentication assurance	23
A.4	Security considerations for multifactor authentication.....	24
A.5	Security considerations for multi-method authentication.....	24
A.6	Security considerations for multiple authentication	24
Appendix I – Relationship with related standards		25
I.1	Relationship with [ITU-T X.1141].....	25
I.2	Relationship with [ITU-T X.1254].....	25
Bibliography.....		26

Introduction

Recently, many application services, especially financial services, require more reliable or combined authentication methods such as multifactor authentication due to the increase in identity (ID) theft. For example, one-time password authentication and other new authentication methods are used instead of traditional password-based authentication.

ITU-T Recommendations related to authentication for secure application service, see [b-ITU-T X.509] and [ITU-T X.1141], are standardized as authentication frameworks. These ITU-T Recommendations basically consider that one service provider and/or one user belongs to one security domain provided by one IdSP even if the service provider and the user belong to different security domains. To achieve enhancement of authentication, IdSP requires the implementation of stronger authentication methods (for example, methods in [b-ITU-T X.1151], [b-ITU-T X.1084], [b-ITU-T X.1086] and [b-ITU-T X.1089]).

On the other hand, it often occurs that one user retrieves several identities from several IdSPs and one service provider establishes trust relationships with several IdSPs. In these multiple IdSP environments, there may be an alternative way for enhancement of authentication when the service provider uses multiple IdSPs to authenticate the user.

Moreover, even if the service provider (SP) implements stronger authentication, identity service bridge provider may be used to combine multiple IdSPs.

However, because each IdSP is operated by different providers, a simple combination of multiple IdSPs may lead to the collapse of the overall authentication level.

Therefore, the general framework is required to describe models, basic operations and security requirements for each model component and each message between the model components to maintain an overall level of authentication assurance in situations of a combination of multiple IdSPs.

In addition, the requirement of stronger/more reliable authentication increases the complexity of implementation and/or management of the authentication system. As a result, the authentication service that manages a combination of multiple IdSPs is used to authenticate the user on behalf of the application service. This authentication service is required to manage a combination of multiple IdSPs that satisfy the authentication policies of each application service.

The framework is also required to describe models, basic operations and security requirements to support the authentication service.

Recommendation ITU-T X.1154

General framework of combined authentication on multiple identity service provider environments

1 Scope

This Recommendation provides the general framework of combined authentication in multiple identity service provider (IdSP) environments for the service provider to achieve combined authentication such as multifactor authentication.

The framework in this Recommendation describes models, basic operations and security requirements for each model component and each message between the model components to maintain an overall level of authentication assurance in situations of a combination of multiple IdSPs.

In addition, the framework also describes models, basic operations and security requirements to support the authentication service that manages a combination of multiple IdSPs.

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

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.

3.1.2 assurance level [b-ITU-T X.1252]: A level of confidence in the binding between an entity and the presented identity information.

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

3.1.4 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.

3.1.5 end user [ITU-T X.1141]: A natural person who makes use of resources for application purposes.

3.1.6 identifier [b-ITU-T X.1252]: One or more attributes used to identify an entity within a context.

3.1.7 identity [b-ITU-T X.1252]: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

NOTE – Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.

3.1.8 identity service bridge provider [b-ITU-T X.1252]: An identity service provider that acts as a trusted intermediary among other identity service providers.

3.1.9 identity service provider (IdSP) [b-ITU-T X.1252]: An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

3.1.10 relying party [ITU-T X.1141]: A system entity that decides to take an action based on information from another system entity. For example, an SAML relying party depends on receiving assertions from an asserting party (a SAML authority) about a subject.

3.1.11 service provider [ITU-T X.1141]: A role donned by a system entity where the system entity provides services to principals or other system entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication factor: A type of credential; there are three types of authentication factors: ownership factor, knowledge factor and biometric factor.

3.2.2 biometric factor: An authentication factor verifying something the user is or does.

3.2.3 combined authentication: An authentication that uses multiple credentials.

3.2.4 current assurance level: A level of authentication assurance of a certain entity at the current point in time.

3.2.5 knowledge factor: An authentication factor verifying something the user knows.

3.2.6 multifactor authentication: An authentication that uses multiple credentials from two or more of the three categories of authentication factors.

3.2.7 multi-method authentication: An authentication that uses multiple credentials from different authentication methods.

3.2.8 multiple authentication: An authentication that uses multiple credentials from the same authentication methods.

3.2.9 ownership factor: An authentication factor verifying something the user has.

3.2.10 provided assurance level: An assurance level that certain identity service providers (IdSPs) will provide when the IdSP authenticates the user.

3.2.11 required assurance level: An assurance level that a certain service provider will require to provide its own service.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ID	Identity
IdM	Identity Management
IdSP	Identity Service Provider
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SP	Service Provider

5 Conventions

In this Recommendation:

The words "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The words "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The words "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The words "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Types of combined authentication

In this Recommendation, the following three types of combined authentication methods are considered:

- Multifactor authentication that uses multiple credentials from two or more of the three categories of authentication factors. For example, (1) authentication by a public key certificate stored in the smart card, (2) authentication by one-time password authentication that uses a hardware device, and (3) authentication by the combination of one-time password authentication and biometric authentication are examples of multifactor authentication.
- Multi-method authentication that uses multiple credentials from different authentication methods. For example, (1) authentication by a combination of one-time password authentication and passphrase authentication, and (2) authentication by a combination of fingerprint authentication and finger vein authentication are examples of multi-method authentication.
- Multiple authentications that use multiple credentials from the same authentication methods. For example, (1) double password authentication, and (2) fingerprint authentication using multiple fingers are examples of multiple authentication.

The difference between the above three authentication methods is the combination of credentials. Additionally, the "authentication factor" provides a categorization of credentials. Moreover, there are three types of authentication factors: ownership factor, knowledge factor and biometric factor.

- Ownership factor is an authentication factor verifying something the user has. Some examples are the smart card, the security token, software token, fixed line phones and mobile phones.
- Knowledge factor is an authentication factor verifying something the user knows. Some examples include a password, a passphrase and personal identification number (PIN).
- Biometric factor is an authentication factor verifying something the user is or does. Fingerprints, finger veins and iris are such examples.

7 Authentication models on multiple IdSP environments

7.1 Basic models with regard to service provider

To consider the authentication model from the view-point of the service provider, the following factors should be considered for authentication models when a user receives an application service:

- The authentication method provided by IdSP is a single factor authentication or a combined authentication.
- The model contains single IdSP or plural IdSPs. If the model contains plural IdSPs, those IdSPs provide the same method or different methods. If plural IdSPs provide different methods, these methods are different factors or the same factor.

Therefore, to achieve combined authentication, there are eight types of functional models, according to the number of SPs and IdSPs, and one type of combined authentication (Table 1). In addition, if there are multiple users in multiple IdSP environments, one user may not have a trust relationship with all IdSPs. In other words, IdSPs can be grouped from the view of a set of users who have a trust relationship with them (Figure 1). In this case, the following factor is also considered.

- IdSPs are classified into one group or multiple groups from the view-point of a trust relationship with the users.

If IdSPs are classified into one group, models T-3 to T-8 in Table 1 can be applied.

If IdSPs are classified into more than two groups, models T-9 to T-14 can be considered (see Table 2).

Table 1 – Basic authentication models (if IdSPs are categorized into one group)

	# of IdSP	# of types of authentication method	Type of provided authentication method by one IdSP	# of groups of IdSPs	Provided authentication method by combination of IdSPs
T-1	One	One	Single factor	One	None
T-2			Combined	One	Combined (Note 1)
T-3	Multiple	One	Single factor	One	Multiple
T-4			Combined	One	Combined (Note 1)
T-5		Multiple (different methods)	Single factor	One	Multiple, multi-method (Note 2)
T-6			Combined (multiple or multi-method)	One	Multiple, multi-method (Note 3)
T-7		Multiple (different factors)	Single factor	One	Multiple, multi-method, multifactor (Note 2)
T-8			Combined	One	Combined (Note 3)

Table 1 – Basic authentication models (if IdSPs are categorized into one group)

	# of IdSP	# of types of authentication method	Type of provided authentication method by one IdSP	# of groups of IdSPs	Provided authentication method by combination of IdSPs
NOTE 1 – All three types of combined authentication can be provided. However, the provided authentication method depends on the type of authentication provided by an IdSP. NOTE 2 – All three types of combined authentication can be provided. However, the provided authentication method depends on the selection of IdSPs. NOTE 3 – All three types of combined authentication can be provided. However, the provided authentication method depends not only on the types of authentication provided by IdSPs but also on the selection of IdSPs.					

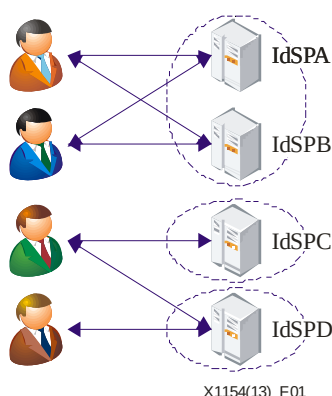


Figure 1 – Example of multiple grouping of IdSPs from the view-point of trust relationship with users

Table 2 – Basic authentication models (if IdSPs are categorized into several groups)

	# of IdSP	# of types of authentication method	Type of provided authentication method by one IdSP	# of groups of IdSPs	Provided authentication method by combination of IdSPs
T-9	Multiple	One	Single factor	Multiple	Multiple
T-10			Combined	Multiple	Combined (Note 1)
T-11		Multiple (different methods)	Single factor	Multiple	Multiple, multi-method (Note 2)
T-12			Combined (multiple or multi-method)	One	Multiple, multi-method (Note 3)
T-13		Multiple (different factors)	Single factor	Multiple	Multiple, multi-method, multifactor (Note 2)
T-14			Combined	Multiple	Combined (Note 3)