International Telecommunication Union

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

International Telecommunication Union

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

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.					

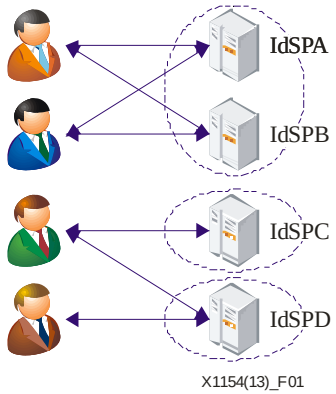

Figure 1 – Example of multiple grouping of IdSPs from the view-point of trust relationship with users

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)

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
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.					

7.1.1 Model T-1

Model T-1 is the model when one IdSP provides a single factor authentication, and when an IdSP, a service provider and one or more terminals are connected with each other via the network.

When the service provider receives a service request from the terminal, the service provider requests the IdSP to authenticate the user. The IdSP, which receives the authentication request from the service provider, authenticates the user by a single factor authentication method. If the authentication results received from the IdSP indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is not able to provide a combined authentication. Therefore, this model is out of scope in this Recommendation.

7.1.2 Model T-2

Model T-2 is the model when one IdSP provides a combined authentication (multiple, multi-method or multifactor authentication), and when an IdSP, a service provider and one or more terminals are connected with each other via the network.

When the service provider receives a service request from the terminal, the service provider requests the IdSP to authenticate the user. The IdSP, which receives the authentication request from the service provider, authenticates the user by a combined authentication method. If the authentication results received from the IdSP indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide any type of a combined authentication method, though it depends on the type of the authentication method provided by an IdSP.

7.1.3 Model T-3

Model T-3 is the model when multiple IdSPs provide the same single factor authentication method, and when multiple IdSPs, a service provider and one or more terminals are connected with each other via the network. Specifically, in model T-3, all users have trust relationships with all IdSPs.

When the service provider receives a service request from the terminal, the service provider selects multiple IdSPs to satisfy the required authentication assurance and requests the selected IdSPs to authenticate the user respectively. If all authentication results received from the IdSPs indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide a multiple authentication method.

It is noted that this model is able to provide a single factor authentication if the authentication method provided by one IdSP satisfies the required authentication assurance. However, the single factor authentication on this model is out of the scope of this Recommendation.

7.1.4 Model T-4

Model T-4 is the model when multiple IdSPs provide the same combined authentication method, and when multiple IdSPs, a service provider and one or more terminals are connected with each other via the network. Specifically, in model T-4, all users have trust relationships with all IdSPs.

When the service provider receives a service request from the terminal, the service provider selects one or multiple IdSPs that satisfy the required authentication assurance and requests the selected IdSP(s) to authenticate the user respectively. If all authentication results received from the IdSP(s) indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide any type of combined authentication though it depends on the type of combined authentication provided by an IdSP and/or the selection of IdSPs. (Multiple multifactor authentications and multiple multi-method authentications might be performed.)

7.1.5 Model T-5

Model T-5 is the model when multiple IdSPs provide single authentication methods, which are of different types but use the same factor, and when multiple IdSPs, a service provider and one or more terminals are connected with each other via the network. Specifically, in model T-5, all users have trust relationships with all IdSPs.

When the service provider receives a service request from the terminal, the service provider selects the multiple IdSPs to satisfy the required authentication assurance and requests the selected IdSPs to authenticate the user respectively. If all authentication results received from the IdSPs indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide multiple authentication or multi-method authentication. It is noted that the performed authentication method depends on the combination of IdSPs.

This model is also able to provide a single factor authentication if the authentication method provided by one IdSP satisfies the required authentication assurance. However, the single factor authentication on this model is out of the scope of this Recommendation.

7.1.6 Model T-6

Model T-6 is the model when multiple IdSPs provide combined authentication methods, which are of different types but use the same factor (i.e., multiple or multi-method authentication methods are provided), and when multiple IdSPs, a service provider and one or more terminals are connected with each other via the network. Specifically, in model T-6, all users have trust relationships with all IdSPs.

When the service provider receives a service request from the terminal, the service provider selects one or multiple IdSPs to satisfy the required authentication assurance and requests the selected IdSP(s) to authenticate the user respectively. If all authentication results received from the IdSP(s) indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide multiple authentications or multi-method authentications, though it depends on the selection and combination of IdSPs.

7.1.7 Model T-7

Model T-7 is the model when multiple IdSPs provide single authentication methods, which use different factors, and when multiple IdSPs, a service provider and one or more terminals are connected with each other via the network. Specifically, in model T-7, all users have trust relationships with all IdSPs.

When the service provider receives a service request from the terminal, the service provider selects the multiple IdSPs to satisfy the required authentication assurance and requests the selected IdSPs to authenticate the user respectively. If all authentication results received from the IdSPs indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide any type of combined authentication. It is noted that the performed authentication method depends on the selection of IdSPs.

This model is also able to provide a single factor authentication if the authentication method provided by one IdSP satisfies the required authentication assurance. However, the single factor authentication on this model is out of the scope of this Recommendation.

7.1.8 Model T-8

Model T-8 is the model when multiple IdSPs provide combined authentication methods, which use different factors, and when multiple IdSPs, a service provider and one or more terminals are connected with each other via the network. Specifically, in model T-8, all users have trust relationships with all IdSPs.

When the service provider receives a service request from the terminal, the service provider selects one or multiple IdSPs to satisfy the required authentication assurance and requests the selected IdSP(s) to authenticate the user respectively. If all authentication results received from the IdSP(s) indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide any type of combined authentication method.

7.1.9 Model T-9

Model T-9 is the model when multiple IdSPs provide the same single factor authentication method, and when multiple IdSPs, a service provider and more terminals are connected with each other via the network. Specifically, in model T-9, one or more users do not have trust relationships with all IdSPs.

NOTE – This model is able to exist with an IdSP that does not have a trust relationship with any users in this model. However, a model which contains such an IdSP is out of the scope of this Recommendation.

When the service provider receives a service request from the terminal, the service provider selects the multiple IdSPs to satisfy the required authentication assurance from a group of IdSPs, which have trust relationships with the user, and requests the selected IdSPs to authenticate the user respectively. If all authentication results received from the IdSPs indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide a multiple authentication method.

It is noted that this model is able to provide a single factor authentication if the authentication method provided by one IdSP satisfies the required authentication assurance. However, the single factor authentication on this model is out of the scope of this Recommendation.

7.1.10 Model T-10

Model T-10 is the model when multiple IdSPs provide the same combined authentication method, and when multiple IdSPs, a service provider and more terminals are connected with each other via

the network. Specifically, in model T-10, one or more users do not have trust relationships with all IdSPs.

NOTE – Model T-10 exists where the IdSP does not have a trust relationship with any users. However, this model which contains such an IdSP is out of the scope of this Recommendation.

When the service provider receives a service request from the terminal, the service provider selects one or multiple IdSPs that satisfy the required authentication assurance and requests the selected IdSP(s) to authenticate the user respectively. If all authentication results received from the IdSP(s) indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide any type of combined authentication, though it depends on the type of combined authentication provided by an IdSP and/or the selection of IdSPs. Multiple multifactor authentications and multiple multi-method authentications might be performed.

7.1.11 Model T-11

Model T-11 is the model when multiple IdSPs provide single authentication methods, which are of different types but use the same factor, and when multiple IdSPs, a service provider and more terminals are connected with each other via the network. Specifically, in model T-11, one or more users do not have trust relationships with all IdSPs.

NOTE – Model T-11 exists where the IdSP does not have a trust relationship with any users. However, this model which contains such an IdSP is out of the scope of this Recommendation.

When the service provider receives a service request from the terminal, the service provider selects the multiple IdSPs to satisfy the required authentication assurance from a group of IdSPs, which have trust relationships with the user, and requests the selected IdSPs to authenticate the user respectively. If all authentication results received from the IdSPs indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide multiple authentication or multi-method authentication. It is noted that the performed authentication method depends on the combination of IdSPs.

This model is also able to provide a single factor authentication if the authentication method provided by one IdSP satisfies the required authentication assurance. However, the single factor authentication on this model is out of scope of this Recommendation.

7.1.12 Model T-12

Model T-12 is the model when multiple IdSPs provide combined authentication methods, which are of different types but use the same factor (i.e., multiple or multi-method authentication methods are provided), and when multiple IdSPs, a service provider and more terminals are connected with each other via the network. Specifically, in model T-12, one or more users do not have trust relationships with all IdSPs.

NOTE – Model T-12 exists where the IdSP does not have a trust relationship with any users. However, this model which contains such an IdSP is out of the scope of this Recommendation.

When the service provider receives a service request from the terminal, the service provider selects one or multiple IdSPs to satisfy the required authentication assurance from a group of IdSPs, which have trust relationships with the user, and requests the selected IdSP(s) to authenticate the user respectively. If all authentication results received from the IdSP(s) indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide multiple authentication or multi-method authentication, though it depends on the selection and combination of IdSPs.

7.1.13 Model T-13

Model T-13 is the model when multiple IdSPs provide single authentication methods, which use different factors, and when multiple IdSPs, a service provider and more terminals are connected with each other via the network. Specifically, in model T-13, one or more users do not have trust relationships with all IdSPs.

NOTE – Model T-13 exists where the IdSP does not have a trust relationship with any users. However, this model which contains such an IdSP is out of the scope of this Recommendation.

When the service provider receives a service request from the terminal, the service provider selects the multiple IdSPs to satisfy the required authentication assurance from a group of IdSPs, which have a trust relationship with the user, and requests the selected IdSPs to authenticate the user respectively. If all authentication results received from the IdSPs indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide any type of multiple authentications. It is noted that the performed authentication method depends on the selection of IdSPs.

This model is also able to provide a single factor authentication if the authentication method provided by one IdSP satisfies the required authentication assurance. However, the single factor authentication on this model is out of the scope of this Recommendation.

7.1.14 Model T-14

Model T-14 is the model when multiple IdSPs provide combined authentication methods, which use different factors, and when multiple IdSPs, a service provider and more terminals are connected with each other via the network. Specifically, in model T-14, one or more users do not have trust relationships with all IdSPs.

NOTE – Model T-14 exists where the IdSP does not have a trust relationship with any users. However, this model which contains such an IdSP is out of the scope of this Recommendation.

When the service provider receives a service request from the terminal, the service provider selects one or multiple IdSPs to satisfy the required authentication assurance from a group of IdSPs, which have a trust relationship with the user, and requests the selected IdSP(s) to authenticate the user respectively. If all authentication results received from the IdSP(s) indicate that the user has been authenticated successfully, the service provider provides its service to the terminal.

This model is able to provide any type of combined authentication methods.

7.2 Entity authentication life cycle model

The entity authentication life cycle model is the state transition model in the entity authentication phase which is defined in [ITU-T X.1254].

There are two model types: the life cycle model from the user's view-point and the life cycle model from the SP's view-point.

7.2.1 Life cycle model from the user's view-point

Through the authentication process of the life cycle model from the user's view-point, the authentication status consists of four instances: "no authentication", "identified", "verified" and "logged out" (Figure 2).

The initial authentication status is "no authentication".

When the user sends an authentication request and is identified by the IdSP, the status changes from "no authentication" to "identified".

Once the user has been authenticated by the IdSP, the status changes from "identified" to "verified".

Furthermore, if the user sends a logout request or if some time has elapsed after the user was authenticated when the status is "verified", the status changes from "verified" to "logged out".

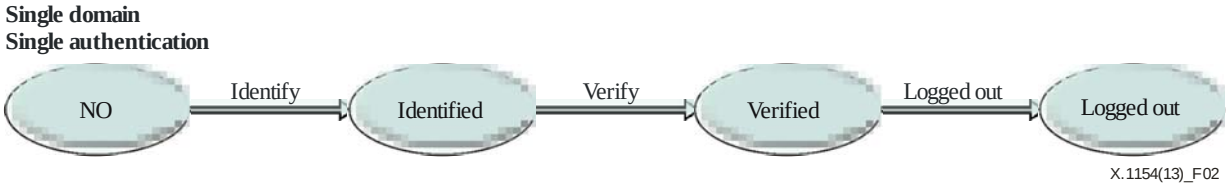

Figure 2 – State transition of single factor authentication

In the case of combined authentication, the status transition from "identified" to "verified" is different (Figure 3).

Through the combined authentication process, the IdSP or the service provider manages the current authentication assurance of the user.

When the user is authenticated by a single factor authentication successfully, the current authentication assurance is updated and evaluated if it satisfies the required authentication assurance.

If the current authentication assurance satisfies the required authentication assurance, the status changes from "identified" to "verified".

Furthermore, if the user sends a logout request or if some time has elapsed after the user was authenticated when the status is "verified", the status changes from "verified" to "logged out".

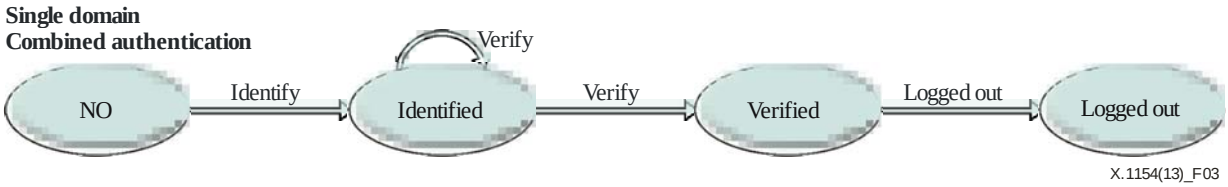

Figure 3 – State transition of combined authentication in single domain

The status transition is shown in Figure 4 in the case of combined authentication in multiple domains which have different authentication assurance requirements in models T-4, T-6 and T-8.

Although the status transition in the first domain is the same as in Figure 3, the status transition in other domains is different.

When the status in the first domain is "verified for 1st domain" and the user sends an authentication request to the second domain, the status in the second domain changes to "insufficient for 2nd domain" if the user is identified in the second domain. If the current authentication assurance of the user satisfies the required authentication assurance in the second domain, the status changes from "insufficient for 2nd domain" to "verified for 2nd domain".

Otherwise, the user is authenticated by the IdSP (or the service provider) and the current authentication assurance is updated and evaluated if it satisfies the required authentication assurance. Furthermore, if the user sends a logout request to any domain, the status in all domains changes from "verified" to "logged out".

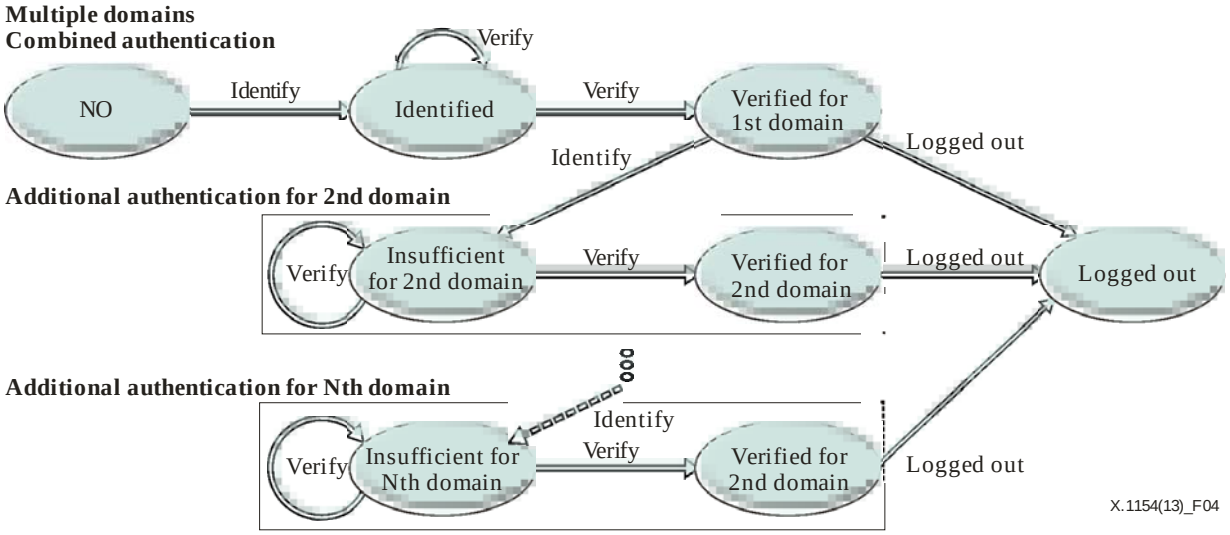

Figure 4 – State transition of combined authentication in multiple domains with different assurance requirements

The status transition is shown in Figure 5 in the case of combined authentication in multiple domains with federation. This is the same as the case of combined authentication in multiple domains that have different authentication assurance requirements in model T-4, T-6 and T-8.

The status transition in the first domain is the same as in Figures 3 and 4.

When the status in the first domain is "verified" and the user sends an authentication request to the second domain, the status does not change, however the user is identified in the second domain.

Furthermore, if the user sends a logout request to any domain, the status in all domains changes from "verified" to "logged out".

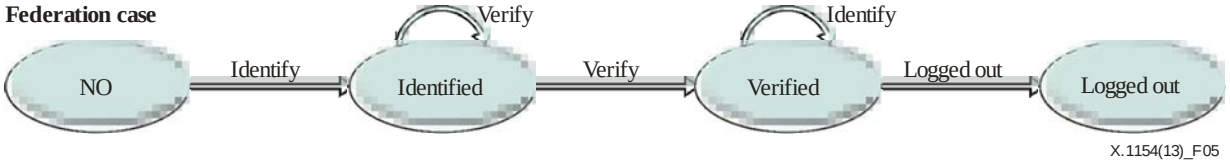

Figure 5 – State transition of combined authentication in multiple domains with federation

7.2.2 Life cycle model from the service provider's view-point

Through the authentication process of the life cycle model from the SP's view-point, the authentication status also consists of four instances: "no authentication", "identified", "verified" and "logged out" (Figure 6).

The initial authentication status is "no authentication".

When the SP receives an authentication request and identifies who the user is, the status changes from "no authentication" to "identified". After this stage, the status changes from "identified" to "verified" if the user is authenticated by the IdSP.

Furthermore, if the SP receives a logout request from the user or some time has elapsed after the user was authenticated, when the status is "verified", the status changes from "verified" to "logged out".

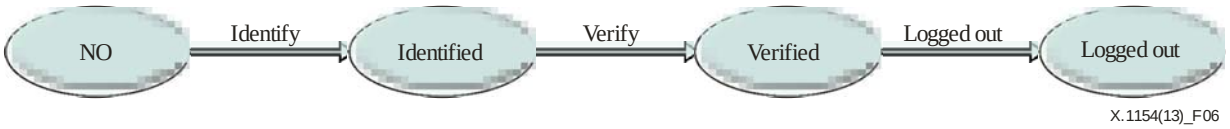

Figure 6 – State transition of single factor authentication

In the case of combined authentication, the status transition from "identified" to "verified" is different.

Through the combined authentication process, the IdSP or the service provider manages the current authentication assurance of the user.

When the user is successfully authenticated by the IdSP, the current authentication assurance is updated and evaluated if it satisfies the required authentication assurance.

If the current authentication assurance satisfies the required authentication assurance, the status changes from "identified" to "verified".

Furthermore, if the user sends a logout request or some time has elapsed after the user was authenticated when the status is "verified", the status changes from "verified" to "logged out".

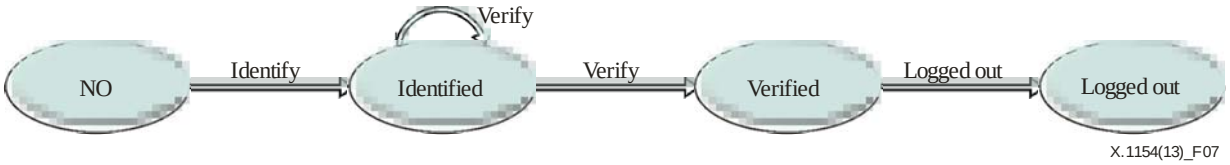

Figure 7 – State transition of combined authentication

From the view-point of the SP, there is no difference from the case of combined authentication even if the user accesses multiple domains and federated domains.

8 Operations in multiple IdSP environments

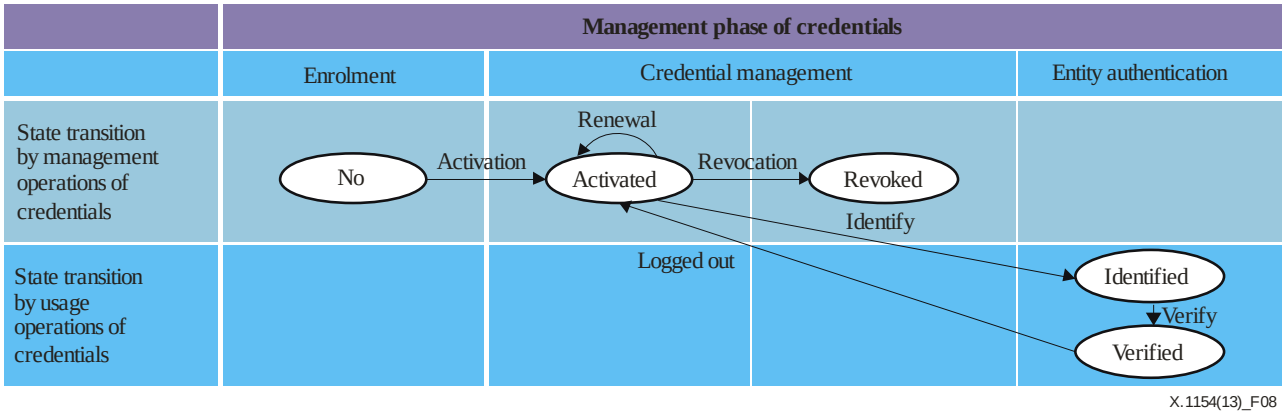

Figure 8 – Operations for the user

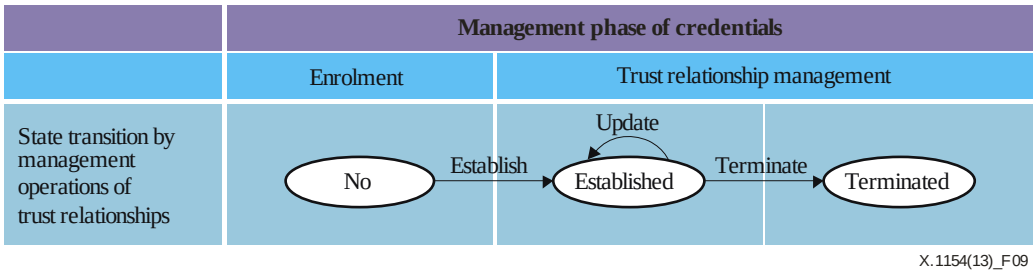

Figure 9 – Operations for the service provider

In the models shown in clause 7, the following types of IdSP operations are described:

1) management operations of credentials (Figure 8),

2) usage operations of credentials (Figure 8),

3) management operations of trust relationships with service providers (Figure 9).

8.1 Credential management operations

Credential management operations are operations for the user to manage the life cycle of a credential as follows:

1) Activate

   The activate operation performs the credential activation process, which is defined in [ITU-T X.1254], to specify the user's credential.

2) Renewal

   The renewal operation performs the credential renewal process, which is defined in [ITU-T X.1254], to specify the user's credential.

3) Revoke

   The revoke operation processes the credential revocation process, which is defined in [ITU-T X.1254] to specify the user's credential.

8.2 Usage operations of credentials

If the credential is activated, usage operations can be performed. Usage operations of credentials are operations for the identification/verification of the user and for the expiry of the assertion which was initially issued by the operation to verify the user.

1) Identify

   The identify operation identifies the user.

   This operation is used in the entity authentication phase.

2) Verify

   The verify operation verifies if the communication peer is the user it claims to be based on the presented credential. Once the communication peer is verified, an assertion is issued to the communication peer.

   This operation is used in the entity authentication phase.

3) Logged out

   The assertion expires after the logged out operation.

   This operation is used in the use phase.

8.3 Management operations of trust relationships with service providers

Management operations of trust relationships with service providers are operations for service providers to create and delete the trust relationship with service providers.

1) Establish

   The establish operation creates a new trust relationship with a certain service provider.

   This operation is used in the trust relationship enrolment phase.

2) Update

   The update operation renews the existing trust relationship with a certain service provider.

   This operation is used in the trust relationship management phase.

3) Terminate

   The terminate operation destroys the specified trust relationship with a particular service provider.

   This operation is used in the trust relationship management phase.

9 General framework of combined authentication on multiple identity service provider environments

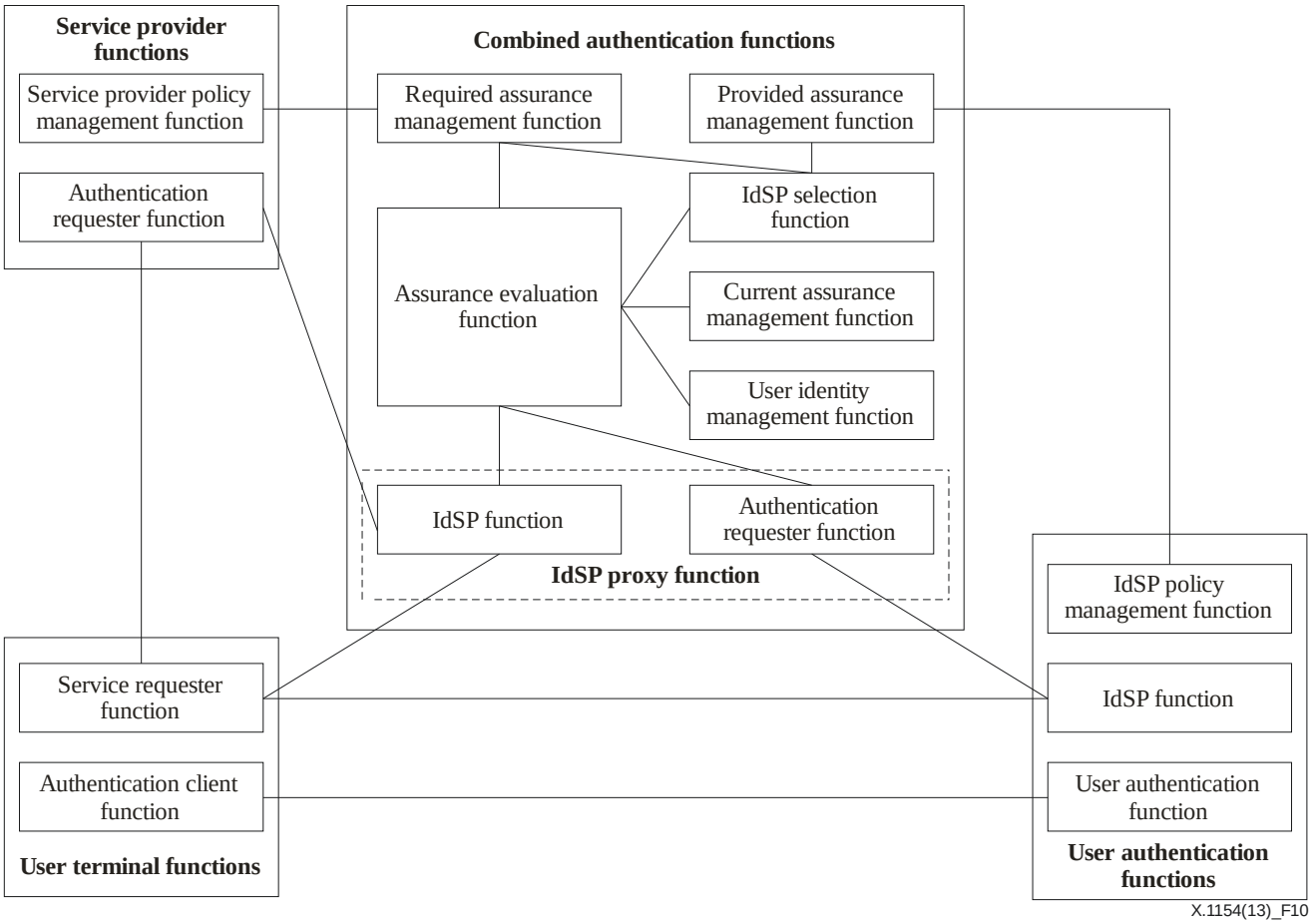

Figure 10 – Model of general framework of combined authentication on multiple identity service provider environments

In Figure 10, the framework of combined authentication contains four logical function blocks: user authentication functions, service provider functions, user terminal functions, and combined authentication functions.

9.1 Logical components

9.1.1 User authentication functions

User authentication functions contain three functions: user authentication function, IdSP function, and IdSP policy management function.

The user authentication function is a function to perform the verify operation and to authenticate a user.

The IdSP function is a function to receive an authentication request from (an authentication requester function of) the combined authentication functions and to perform the identify operation. Furthermore, the IdSP function is to receive a logout request and perform a logged out operation.

The IdSP policy management function is a function to manage an IdSP's authentication policy which contains a type of authentication method and an authentication assurance level provided by the user authentication function.

9.1.2 Service provider functions

Service provider functions contain two functions: authentication requester function and service provider policy management function.

The authentication requester function is a function to send an authentication request to (the IdSP function of) the combined authentication functions.

The service provider policy management function is a function to manage the service provider's authentication policy which contains an authentication assurance level requested to provide a service.

9.1.3 User terminal functions

User terminal functions contain two functions: service requester function and authentication client function.

The service requester function is a function to send a service request to (an authentication requester function of) the service provider functions.

The authentication client function is a function to communicate with (a user authentication function of) a single factor authentication function to authenticate the user.

9.1.4 Combined authentication functions

Combined authentication functions contain eight functions: IdSP function, authentication requester function, required assurance management function, provided assurance management function, current assurance management function, user identity management function, assurance evaluation function and IdSP selection function.

The IdSP function is a function to receive an authentication request from (an authentication requester function of) the service provider functions and perform the identify operation. Furthermore, the IdSP function receives a service termination request and performs the log out operation.

The authentication requester function is a function to send an authentication request or a logout request to (the IdSP function of) the single factor authentication functions.

The required assurance management function is a function to manage an authentication assurance level requested by each service provider function via the establish/update/terminate operations.

The provided assurance management function is a function to manage a type of authentication method and an authentication assurance level provided by each single factor authentication function via the establish/update/terminate operations.

The current assurance management function is a function to manage a current authentication assurance level of each user.

The user identity management function is a function to manage the identity information of each user via the create/update/revoke function.

The assurance evaluation function is a function to verify the result of user authentication supplied by the IdSP function of the single factor authentication functions, to evaluate the current assurance level of the user and to check whether the current assurance level of the user satisfies the required assurance level of the service provider.

The IdSP selection function is a function to select one or multiple single factor authentication functions for the user to satisfy the required assurance level of the service provider.

It is noted that some existing identity management (IdM) frameworks can use another function, identify the service bridge provider function, instead of the IdSP function and authentication requester function.

9.2 Behaviours

9.2.1 Service request

Figure 11 shows the basic behaviour of a service request in the general framework of combined authentication in multiple identity service provider environments.

(1) A service requester function sends a service request to the authentication requester function in the service provider functions.

(2) When the authentication requester function in the service provider functions receives the service request, it sends an authentication request to the IdSP function in the combined authentication functions, if the authentication requester function judges that the user terminal function is required to be authenticated to provide the application service.

(3) When the IdSP function receives the service request, it sends the authentication request to the assurance evaluation function.

(4) The assurance evaluation function retrieves a current assurance level of the user terminal from the current assurance management function and sends an IdSP selection request with the current assurance of the user terminal to an IdSP selection function.

(5) The IdSP selection function retrieves a required assurance level of the service provider and provides an assurance level of each IdSP from the required assurance management and the provided assurance management functions, respectively. Then, the IdSP selects an IdSP from a list of available IdSPs and sends the name to the assurance evaluation function.

(6) The assurance evaluation function retrieves an identifier of the user terminal in the selected IdSP from a user identity management function, if needed, and sends an authentication request to the authentication requester function. Furthermore, the authentication requester function sends an authentication request to the IdSP function in the selected IdSP functions.

(7) The IdSP function sends the authentication request to the authentication function. Additionally, the authentication function performs user authentication with the authentication client on the user terminal functions.

(8) The authentication function returns the authentication result to the assurance evaluation function via the IdSP function in the IdSP functions and via the authentication requester function in the combined authentication functions.

(9) The assurance evaluation function evaluates and updates the current assurance of the user terminal.

(10) If the current assurance level of the user terminal is not enough to provide the service (i.e., less than the required assurance), the assurance evaluation function requests again an IdSP selection request from the IdSP selection function. Then, steps (5)-(9) are repeated.

(11) If the current assurance of the user terminal is enough to provide the service in (10), the assurance evaluation function sends an authentication result to the IdSP function.

(12) The IdSP function creates an assertion and sends it to the authentication requester in the service provider functions.

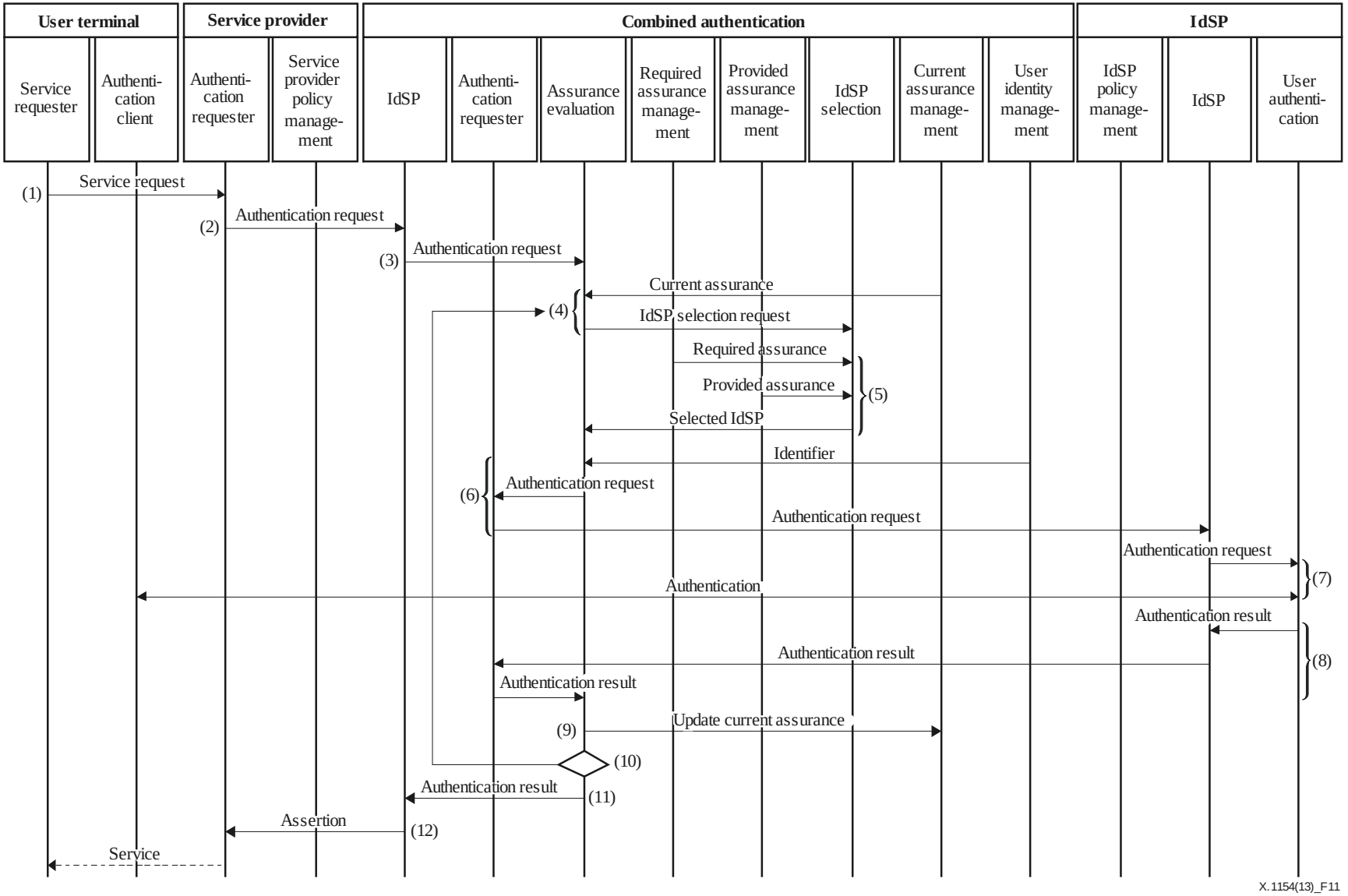

Figure 11 – Basic behaviour of service request on the general framework of combined authentication in multiple identity service provider environments

9.2.2 Service terminate

Figure 12 shows a basic behaviour of service termination in the general framework of combined authentication in multiple identity service provider environments.

(1) A service requester function sends a service termination request to the authentication requester function in service provider functions.

(2) When the authentication requester function in the service provider functions receives the service termination request, it sends a logout request to the IdSP function in the combined authentication functions.

(3) When the IdSP function receives the logout request, it sends the termination request to the assurance evaluation function.

(4) The assurance evaluation function retrieves a list of IdSPs which the user terminal logs in and sends a logout request to all of the listed IdSP functions via the authentication requester function.

(5) The IdSP function returns a logout result.

(6) When the assurance evaluation function receives the logout result, the current assurance is updated.

(7) If the assurance evaluation function receives all the logout results, it returns the termination result to the IdSP function.

(8) The IdSP function returns the logout result to the authentication requester function.

(9) The authentication requester function returns the service termination result to the service requester.

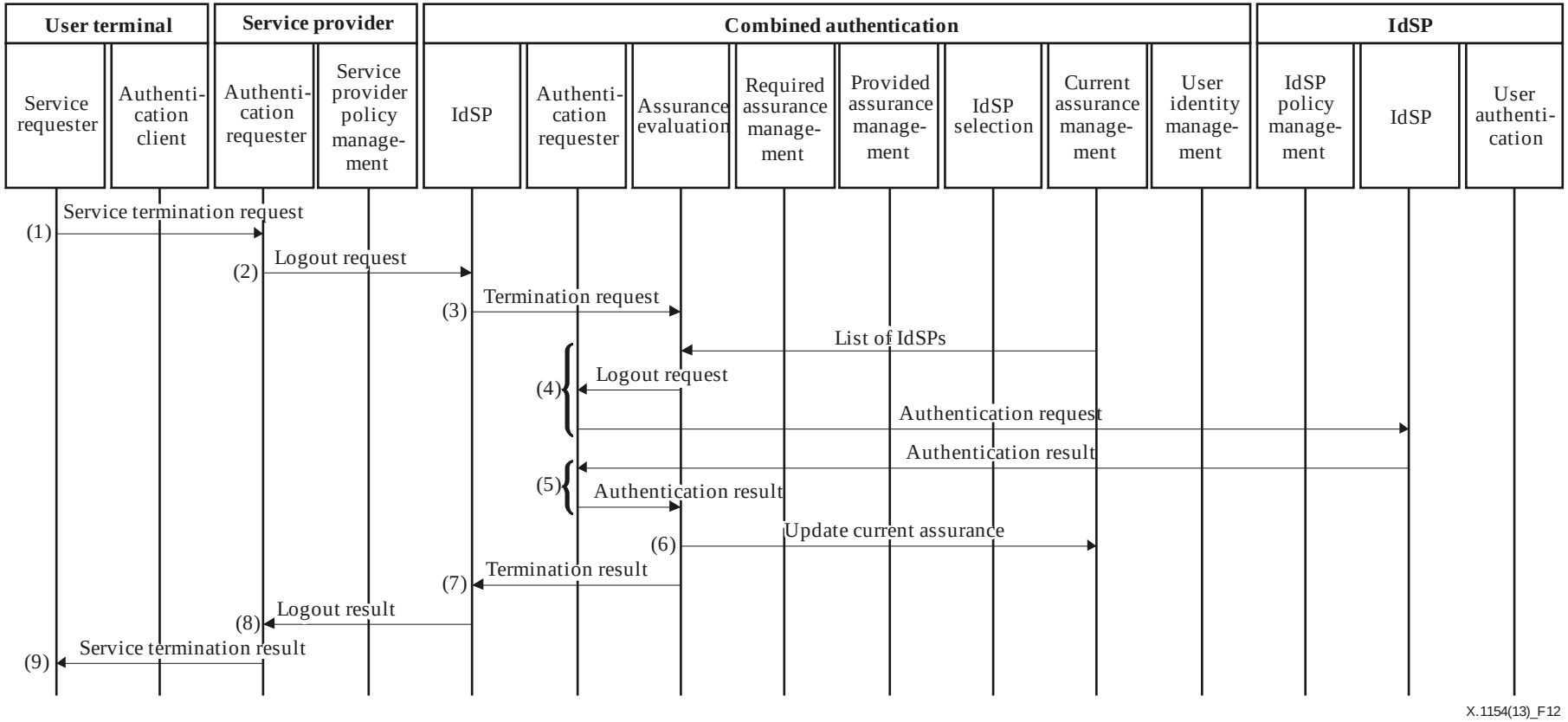

Figure 12 – Basic behaviour of service termination in the general framework of combined authentication in multiple identity service provider environments

9.2.3 Management of the required assurance of the service provider functions

For the management of the required assurance of the service provider functions in the combined authentication functions, a required assurance is sent from the service provider policy management function to the required assurance management function via the establish/update/terminate operations.

9.2.4 Management of provided assurance of the IdSP functions

For the management of the provided assurance of the IdSP functions in the combined authentication functions, a required assurance is sent from the IdSP policy management function to the provided assurance management function via the establish/update/terminate operations.

Annex A

Considerations for combined authentication

(This annex forms an integral part of this Recommendation.)

A.1 Achieving estimated authentication assurance

As combined authentication is an authentication that uses multiple credentials, different credentials are required to be used to achieve an estimated authentication assurance. In other words, a simple combination of multiple authentication methods or IdSPs will lead to a total failure of the assurance level if the same credential is used.

To achieve an estimated authentication assurance, a process is required to verify if the credentials used in the combined authentication are different or not. The verification process is recommended to be performed before updating the current authentication assurance.

In the model where a combined authentication function and user authentication functions are implemented in one entity (for example, one IdSP provides a combined authentication), it is easy for the verification process to be performed in the IdSP. Furthermore, the verification process could be performed when the create/update operation is executed.

On the other hand, in the model where a combined authentication function and user authentication functions are implemented in one entity (for example the SP uses multiple IdSPs providing a single factor authentication), additional data exchange between the combined authentication function and user authentication function is required for the verification process. Specifically, a function to send the data to identify the credential is required in the user authentication function. Furthermore, a function to confirm that a different credential is used by comparing each data received from the user authentication functions is required in the combined authentication function.

In the case of applying the authentication method using public key infrastructure (PKI), the function in the user authentication function can be sending a public key as the data that indicates the credential and the function in the combined authentication function can compare these data directly.

However, in the case of applying the authentication method using a shared secret (e.g., a password), the function in the user authentication function is prohibited from sending the shared secret itself as the data that indicates the credential.

A.2 Selection of IdSP(s)

It is required that the IdSP selection function discovers and selects suitable IdSP(s) when the service provider receives a service request from the terminal.

To select the suitable IdSP, the required assurance management function and the provided assurance management function are required to be implemented securely.

In addition, the current assurance management function is required to be implemented securely in the IdSP (in the model where one IdSP provides a combined authentication function) or SP (in the model that the SP provides in the combined authentication function).

Further on, the assurance evaluation function is required to retrieve the current authentication assurance, the required authentication assurance and the provided authentication assurance securely.

A.3 Effective authentication assurance

In some cases, effective authentication assurance may be less than the estimated authentication assurance because the authentication assurance changes as a result of being influenced by various environmental factors.

In such a case, a function to send the effective authentication assurance to the SP is required in the IdSP. Further on, a function is required in the SP to update and evaluate the current authentication assurance of the user based on the effective authentication assurance.

A.4 Security considerations for multifactor authentication

There are two types of multifactor authentications: one is the multifactor authentication using a single credential for verification, and the second type uses multiple credentials for verification.

The first type of authentication is based on a public key certificate stored in the smart card or is based on a one-time password using a hardware device.

The second type of authentication is based on a combination of a one-time password and biometric factors.

The first type of multifactor authentication is required to use tamper-resistant hardware to store credentials.

A.5 Security considerations for multi-method authentication

In the case of multi-method authentication, it is required for each credential not to be derived (or guessed) by other credentials.

A.6 Security considerations for multiple authentication

In the case of multiple authentications, it is required for each credential not to be derived (or guessed) by other credentials.

Appendix I

Relationship with related standards

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

I.1 Relationship with [ITU-T X.1141]

Figure I.1 shows the relationship between the model described in this Recommendation and the one described in clause 10 and the security assertion markup language (SAML 2.0) of [ITU-T X.1141]. Grey boxes are functions defined in SAML.

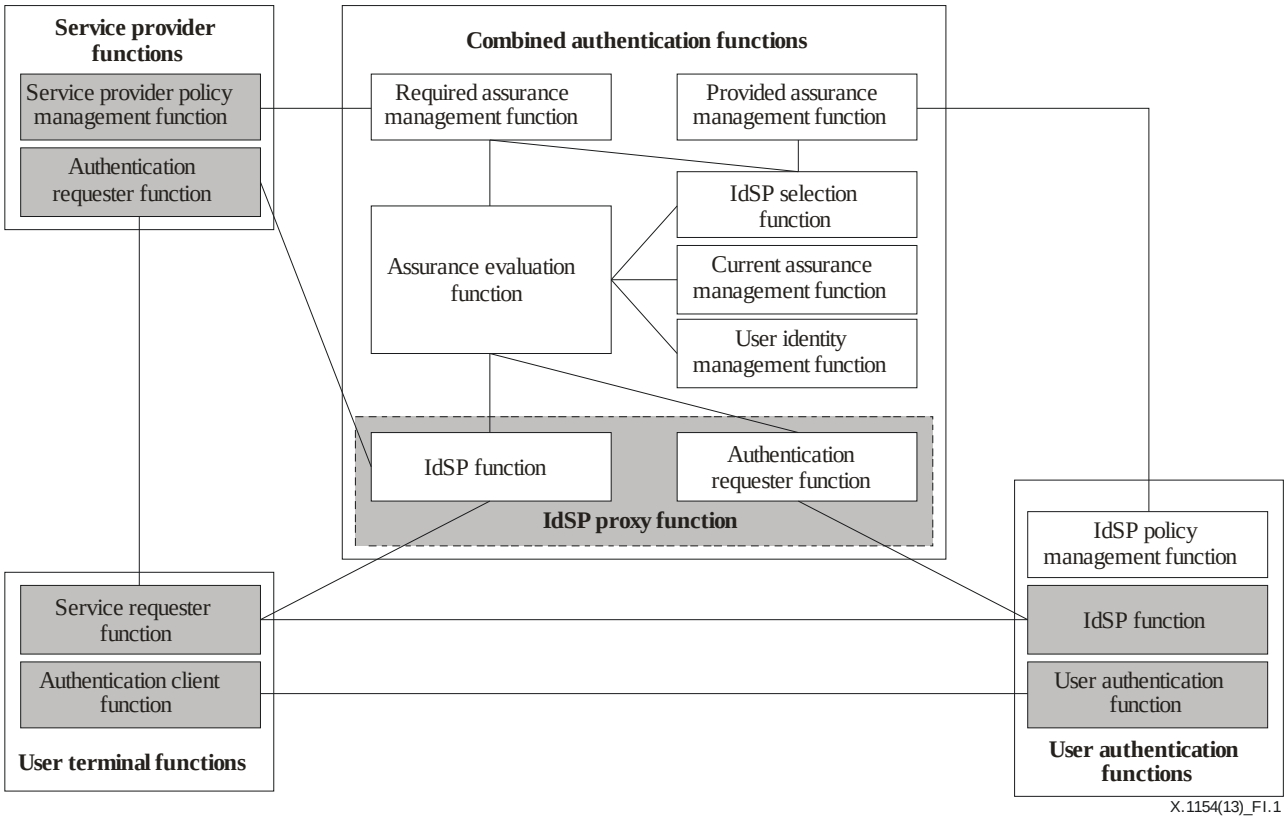

Figure I.1 – Relationship with [ITU-T X.1141]

I.2 Relationship with [ITU-T X.1254]

The framework in this Recommendation is to provide combined authentication using multiple IdSPs. It means that the framework in this Recommendation is one instance to implement the authentication phase, which is described in [ITU-T X.1254], in multiple IdSP environments.

Bibliography

[b-ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1084] Recommendation ITU-T X.1084 (2008), *Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems*.

[b-ITU-T X.1086] Recommendation ITU-T X.1086 (2008), *Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security*.

[b-ITU-T X.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure (TAI)*.

[b-ITU-T X.1151] Recommendation ITU-T X.1151 (2007), *Guideline on secure password-based authentication protocol with key exchange*.

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013