International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1159

(11/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Security protocols

Delegated non-repudiation architecture based on ITU-T X.813

Recommendation ITU-T X.1159

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
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.1159

Delegated non-repudiation architecture based on ITU-T X.813

Summary

Non-repudiation is the ability to prevent entities from denying that they have sent or received electronic transaction data in a telecommunication network. Recommendation ITU-T X.1159 provides a delegated non-repudiation architecture based on Recommendation ITU-T X.813 to generate non-repudiation evidence by a trusted third party (TTP) instead of a user.

Recommendation ITU-T X.813 defines six non-repudiation mechanisms: a TTP security token, security tokens and tamper-resistant modules, a digital signature, time stamping, an in-line TTP and a notary. This Recommendation complies with these six mechanisms, and the non-repudiation service can use a combination of these mechanisms to satisfy the security requirements of the application service.

In this Recommendation, a right and/or user's signing key for a non-repudiation generation delegates to a TTP, which is a central signing authority, and the central signing authority generates and verifies non-repudiation evidence using the delegated user's signing/validation key or the central signing authority's secret key/validation key. The delegated non-repudiation model in this Recommendation is capable of responding to key loss and theft, is safe in an open network, such as a mobile and cloud network, and provides convenient non-repudiation service.

This Recommendation describes the delegated non-repudiation service models and operations for each of the service models. The architecture also defines the security requirements of the delegated non-repudiation service. In this delegated non-repudiation service model, there are two types of service models that use the central signing authority's secret key and the delegated signing key.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1159	2014-11-13	17	11.1002/1000/12342

Keywords

Central signing authority, delegated non-repudiation service, non-repudiation architecture.

---

* 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.1159

Delegated non-repudiation architecture based on ITU-T X.813

1 Scope

This Recommendation provides an enhanced non-repudiation model based on [ITU-T X.813] in support of application services. The user can authenticate and generate non-repudiation evidence for the transaction of data by a trusted third party (TTP), which is the central signing authority. The recommended architecture provides an integration of the authentication token to access the central signing authority. The architecture also integrates multiple service providers to provide a non-repudiation service for a single authenticated device. The model will provide non-repudiation services for any type of device including the mobile device. Although this architecture requires the use of strong authentication, this is out of the scope of this Recommendation. Furthermore, issuing and managing a signing key are out of the scope of this Recommendation.

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.813] Recommendation ITU-T X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication token [b-ITU-T X.509]: Information conveyed during a strong authentication exchange, which can be used to authenticate its sender.

3.1.2 evidence [ITU-T X.813]: Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute.

3.1.3 evidence subject [ITU-T X.813]: The entity whose involvement in an event or action is established by evidence.

3.1.4 evidence verifier [ITU-T X.813]: An entity that verifies non-repudiation evidence.

3.1.5 in-line TTP [b-ITU-T X.842]: A TTP positioned directly in the communication path between the entities that can facilitate secure exchanges between these entities.

3.1.6 non-repudiation token [b-ITU-T X.1156]: This token is the unforgeable evidence for the non-repudiation service.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication service provider: The entity is a trusted third party (TTP) that issues the authentication device and/or user's signing key and verifies the transaction-based authentication information.

3.2.2 central signing authority: The entity is a trusted third party (TTP) that stores and manages the user's delegated signing key and generates the non-repudiation evidence on behalf of the user.

3.2.3 delegated signing key: The signing key that is used in generating non-repudiation evidence by a trusted third party (TTP).

3.2.4 delegation information: The information that is derived by the user's signing key for a delegated non-repudiation service.

3.2.5 delegation warrant: The information that assumes that the user gave the central signing authority the authority to generate a non-repudiation evidence.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASP Authentication Service Provider

DB DataBase

HSM Hardware Security Module

LDAP Lightweight Directory Access Protocol

NRD Non-Repudiation of Delivery

NRE Non-Repudiation Evidence

NRO Non-Repudiation of Origin

OCSP Online Certificate Status Protocol

OTP One-Time Password

PKI Public Key Infrastructure

RET REsulT

SM Service Model

SP Service Provider

TTP Trusted Third Party

5 Conventions

The keywords "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 keywords "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 keywords "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 Delegated non-repudiation architecture

6.1 Introduction

[ITU-T X.813] defines six non-repudiation mechanisms that use: a TTP security token, security tokens and tamper-resistant modules, a digital signature, time stamping, an in-line TTP, and a notary. The non-repudiation service can use a combination of these mechanisms and services to satisfy the security requirements of the application.

This Recommendation defines a delegated non-repudiation architecture based on [ITU-T X.813] which can provide a non-repudiation service by TTP safely and conveniently. The delegated non-repudiation model can protect against key loss or theft because the architecture stores the user's signing key safely and can generate and verify non-repudiation evidence (NRE) for the transaction of data by a TTP. In addition, the delegated non-repudiation model can apply a mobile and/or a cloud service.

A non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. The evidence generation requestor requests the evidence generator to generate evidence for an event or action, see [ITU-T X.813]. In this Recommendation, the evidence generation requestor is a user, and the evidence generator is a central signing authority.

A delegated non-repudiation service permits an entity to delegate its evidence generation right to the TTP, called a central signing authority, and a central signing authority will generate the evidence on behalf of the user. In [ITU-T X.813], the evidence generator will generate the evidence using its own key, but in the delegated non-repudiation service, the evidence generator, called the central signing authority, will generate the evidence using either its own key or the delegated user's signing key.

The delegated non-repudiation service provides non-repudiation of origin (NRO) and/or non-repudiation of delivery (NRD).

Figure 1 illustrates the concept of the delegated non-repudiation architecture, which shows the interactions of the different entities for the delegated non-repudiation service.

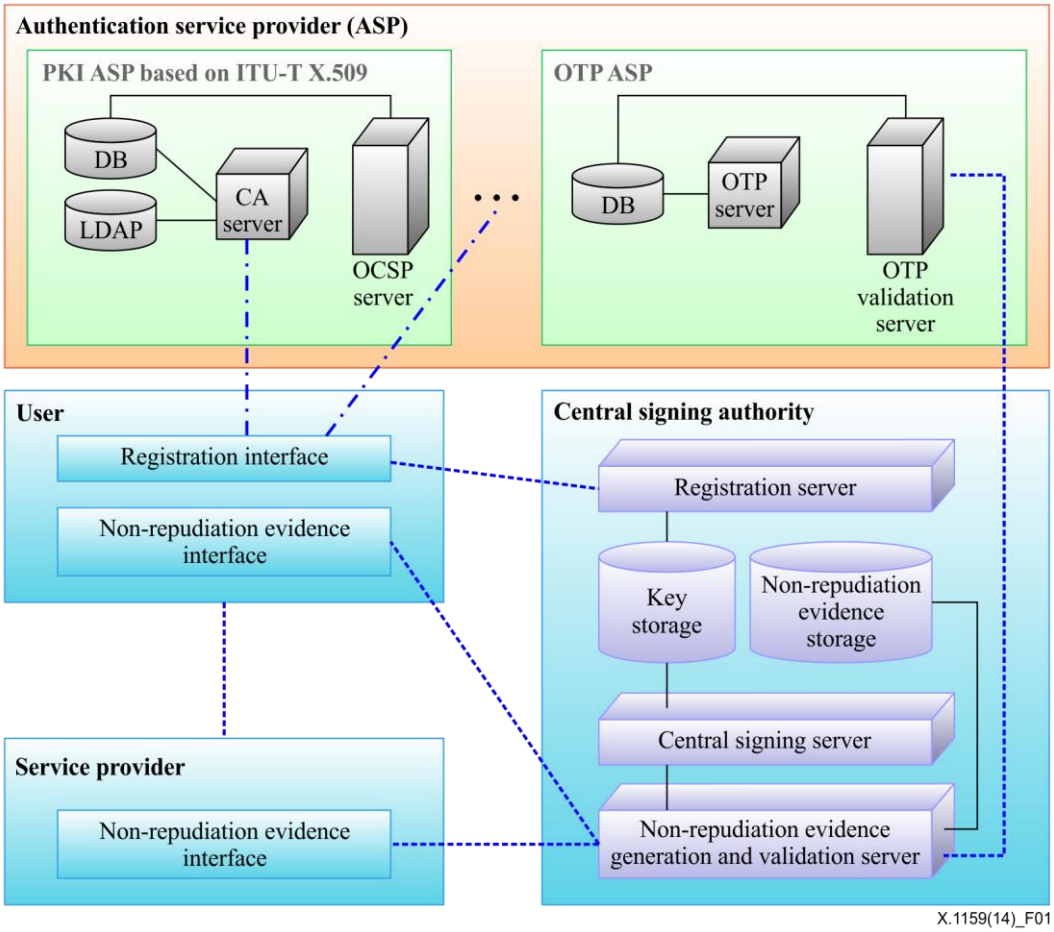

Figure 1 – Concept of delegated non-repudiation architecture

For the delegated non-repudiation service, the user pre-issues a signing key and/or an authentication token through the authentication service provider (ASP). Using the registration interface, the user can register the non-repudiation service to a central signing authority. In this operation, a central signing authority verifies the user's identification and registers a pre-issued authentication token to access a central signing authority. If necessary, the user can register the delegated signing key to a central signing authority in this operation. Using the registration server, a central signing authority registers the user's delegated signing key and stores it securely in the key storage. If the user or the service provider needs to provide the non-repudiation service, they may request from a central signing authority to generate the non-repudiation evidence through the non-repudiation evidence interface. A central signing authority validates the user's transaction-based authentication data before the generation of non-repudiation evidence. The non-repudiation evidence, concatenated with the result of validation, is stored securely in a non-repudiation token storage. In a non-repudiation evidence generation and validation server, the central signing authority can generate and validate the non-repudiation evidence. For the generation of the non-repudiation evidence, a signature is generated by a central signing server which is only for the access to a key storage. The central signing authority generates the non-repudiation evidence and sends it to the requestor. Also the central signing authority can store it in non-repudiation evidence storage.

6.2 Entities

The delegated non-repudiation architecture consists of four entities as follows:

1) user;

2) service provider (SP);

3) central signing authority;

4) authentication service provider (ASP).

6.2.1 Roles of user

A user is the evidence subject and can request evidence generation for proof as the originator of data. A user registers the delegated non-repudiation service with a central signing authority and can be provided with the service by a central signing authority. If necessary, the user registers the user's delegated signing key with a central signing authority. For delegated non-repudiation service, the user's signing key and authentication token are required to be pre-issued. The user is the subject that approves the transaction by verifying the received non-repudiation evidence for delivery.

6.2.2 Roles of service provider

A service provider is the evidence subject and can request evidence generation for proof of data delivered. A service provider registers the delegated non-repudiation service with a central signing authority and can be provided with the service by a central signing authority. The service provider is the subject that approves the transactions by verifying the received non-repudiation evidence of origin.

6.2.3 Roles of central signing authority

A central signing authority is an in-line TTP and the subject that generates and verifies non-repudiation evidence using the delegated user's signing/validation key or the central signing authority's secret key/validation key.

The user's delegated signing key is required to be stored in a physically secure device such as a hardware security module (HSM) to prevent unauthorized access, and the non-repudiation evidence is required to be generated with the involvement of the user. The central signing authority is required to validate the user's delegated signing key before generating non-repudiation evidence using the user's delegated signing key, and the non-repudiation evidence must include trusted time information.

6.2.4 Roles of authentication service provider

The ASP is a TTP and the subject that issues the user's signing key and/or user's authentication token. The ASP also provides an authentication service for a user and the user's transaction-based authentication information.

6.3 Operations of the delegated non-repudiation service

The operations of the delegated non-repudiation service consist of a registration of the delegated non-repudiation service, the generation of non-repudiation evidence and the verification of non-repudiation evidence.

In the registration of the delegated non-repudiation service, a central signing authority proves the user's identification and registers a pre-issued authentication token to access a central signing authority. If necessary, a user can register the delegated signing key with a central signing authority. Furthermore, the central signing authority registers the user's delegated signing key and stores it securely in a key storage.

6.3.1 Registration of the delegated non-repudiation service

This is a process where a user or a service provider registers the delegated non-repudiation service with a central signing authority. The central signing authority proves the requestor's identification and registers the requestor's authentication token to access the central signing authority. The central signing authority also registers the delegation warrant. If necessary, a requestor can register the delegated signing key with the central signing authority. The central signing authority also registers the requestor's delegated signing key and stores it securely in a key storage.

In general, when a non-repudiation service is provided through delegation of a user's signing key to a TTP, the user and the TTP share the same signing key, which results in limitations of the non-repudiation service between the objects. Because the delegated signing key is the same as the user's original signing key, the non-repudiation evidence generated by a central signing authority is indistinguishable from the non-repudiation evidence generated by the user. Consequently, in this case, the service cannot provide the non-repudiation between the user and a central signing authority. If the user fully trusts the TTP, the service may be applicable. Otherwise, a delegated signing key for a non-repudiation generation is required to be distinguishable from the user's original signing key. In the delegated non-repudiation service model, the requestor derives the delegated information from the requestor's signing key and then sends the delegated information to a central signing authority. A central signing authority derives the requestor's delegated signing key from the received delegated information by the requestor and from a central signing authority's secret key.

The delegated non-repudiation service is required to provide the management of a delegated signing key such as renewal and revocation. Furthermore, the requestor's pre-issued authentication token is required to provide the function to generate transaction-based authentication information.

6.3.2 Generation of the non-repudiation evidence

This is a process in which a central signing authority generates the non-repudiation evidence using its own secret key or registers a delegated signing key.

A user or service provider makes a request to a central signing authority to generate non-repudiation evidence of origin or delivery with transaction-based authentication information. This information is generated using symmetric or asymmetric cryptographic techniques such as message authentication codes (MACs), digital signature, etc., using a secret key issued by the ASP. For example, if transaction based authentication information is generated using a one-time password (OTP)-based cryptographic technique (see [b-ITU-T X.1153]), the generation function can use an OTP generation function. The central signing authority validates a requestor's transaction-based authentication information through an ASP. If the authentication result is valid, the central signing authority generates the non-repudiation evidence using its own key or the delegated signing key. A central signing authority is required to verify the non-repudiation generation key before generating the non-repudiation evidence.

[ITU-T X.813] defines the non-repudiation evidence format as follows:

Candidate inputs include:

– the non-repudiation policy;
– the distinguishing identifier of the evidence subject;
– the distinguishing identifier of the non-repudiation service requester;
– the data or a digital fingerprint of the data;
– the distinguishing identifier of the TTP that will be used to generate the digital signature, the security token or other evidence.

Candidate outputs include:

– evidence (e.g., a digital signature or a security token);
– the distinguishing identifier of the TTP that generated the digital signature, the security token or other evidence.

6.3.3 Verification of non-repudiation evidence

This is a process in which a central signing authority verifies the non-repudiation evidence. In clause 6.3.2, non-repudiation evidence can be generated using the central signing authority's own key or the registered delegated signing key. If the non-repudiation evidence is generated using a central signing authority's secret key, the central signing authority verifies the non-repudiation evidence

using its own secret key. On the other hand, if the non-repudiation evidence is generated using delegated signing key, the central signing authority verifies the non-repudiation evidence using the delegated verification key. A central signing authority is required to verify both the delegated verification key and the central signing authority's secret key before verifying the non-repudiation evidence.

7 Requirements for a delegated non-repudiation service

7.1 Unforgeability

Only a central signing authority is required to generate the valid non-repudiation evidence and the non-repudiation evidence is existentially unforgeable. The non-repudiation evidence generated by a central signing authority for a transaction, *tm,* cannot generate the same evidence when the same transaction, *tm,* is conducted by another entity. Furthermore, a central signing authority is required to check a status of evidence generation key (e.g., revoked) before generating the non-repudiation evidence.

7.2 Prevention of misuse

A central signing authority is required to generate the valid non-repudiation evidence on behalf of a user.

7.3 Verifiability

A central signing authority is required to provide enough verification for the non-repudiation evidence. In addition, the verifier can be convinced of the user's delegation for the non-repudiation evidence.

7.4 Identifiability

The non-repudiation evidence is required to include the identifiers of the corresponding user, the service provider, the central signing authority and of the types of the generating key.

8 Delegated non-repudiation service models

In the delegated non-repudiation service model, there are two types of service models that use the central signing authority's secret key and the delegated signing key.

For a delegated non-repudiation service, the user can give a central signing authority the authority and/or user's signing key to generate non-repudiation evidence. If the user gives a central signing authority only the authority to generate non-repudiation evidence; in the first service model, the central signing authority can generate the non-repudiation evidence using its own secret key. This service model is described in clause 8.1. The second service model, where the user gives a central signing authority the authority and the user's signing key to generate non-repudiation evidence, a central signing authority can generate the non-repudiation evidence using the user's delegated signing key. This service model is described in clause 8.2. Each service model provides NRO and NRD. For example, an originator of the transactions may request a service for NRO and a recipient may request a service for NRD.

8.1 Delegated non-repudiation service model using a central signing authority's secret key

This service model does not need the registration operation of the user's signing key. The central signing authority generates the non-repudiation evidence using its own secret key. A central signing authority can generate non-repudiation evidence using symmetric or asymmetric algorithms.

8.1.1 Non-repudiation evidence of origin

Figure 2 illustrates the service model for delegated non-repudiation of origin using a central signing authority's secret key.

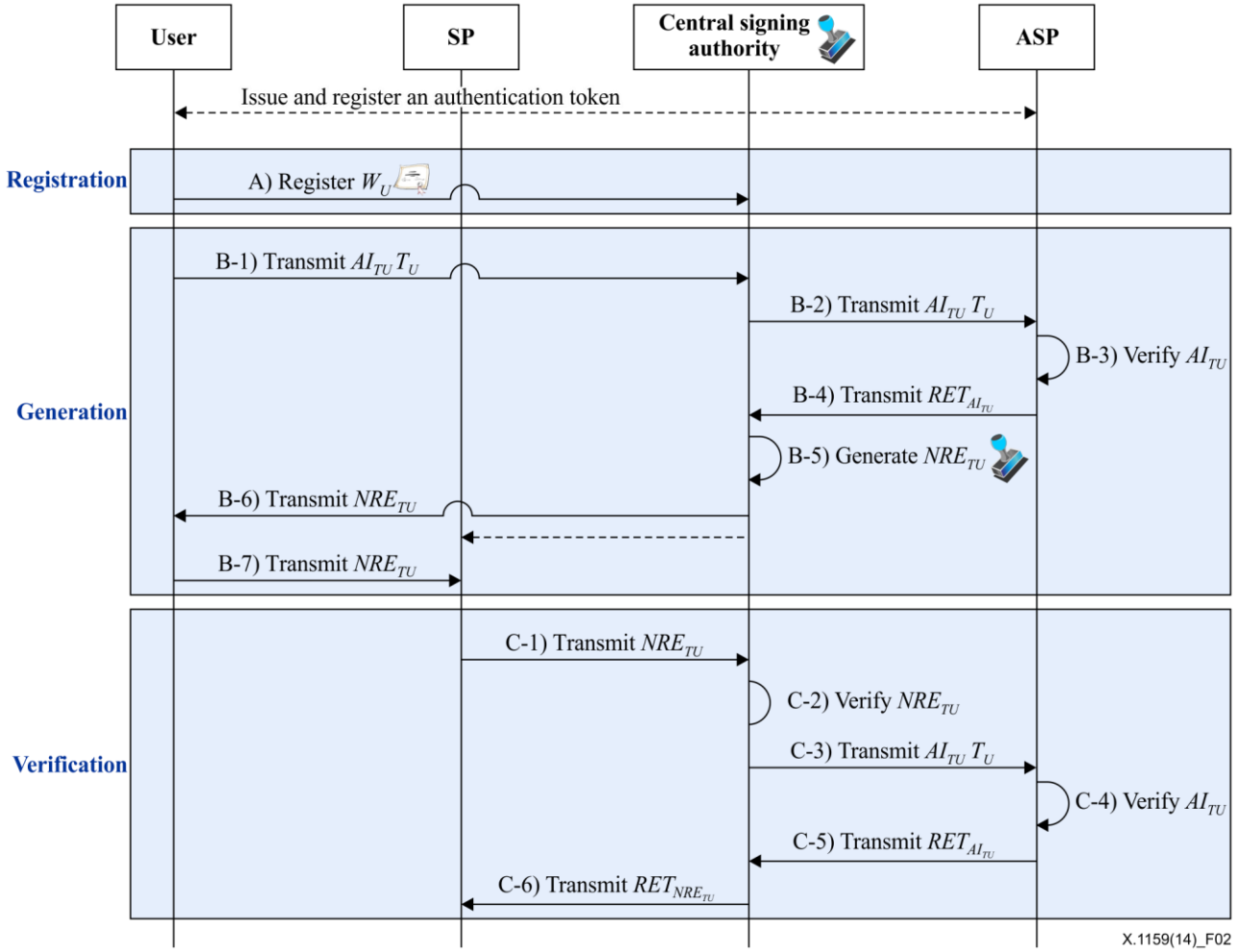

Figure 2 – Service model for delegated non-repudiation of origin using a central signing authority's secret key

Step A: Registration

For the delegated non-repudiation service, the user pre-issues a signing key and/or an authentication token through an ASP. In this step, the user registers a delegation warrant, W_U, where it is assumed that the user gives a central signing authority the authority to generate non-repudiation evidence.

Step B: Generation for non-repudiation evidence of origin

When the service provider requests from the user the non-repudiation evidence of origin, the user, in turn, requests from a central signing authority to generate the non-repudiation evidence. For this request, the user transmits the transaction-based authentication information (AI_{TU}) to a central signing authority. The central signing authority uses the ASP to verify the user's transaction-based authentication information AI_{TU} and then generates the non-repudiation evidence NRE_{TU} using its own secret key. Additionally, a central signing authority transmits NRE_{TU} to the user and securely stores NRE_{TU} and AI_{TU} transmitted by the user, and the verification result of AI_{TU} RET_{AITU}. The user transmits NRE_{TU} to the service provider.

Step C: Verification for non-repudiation evidence of origin

When the service provider requests from a central signing authority to verify NRE_{TU}, a central signing authority verifies NRE_{TU} and AI_{TU}. A central signing authority then transmits the result for verification of NRE_{TU} to the service provider. If a central signing authority transmits the non-repudiation evidence of origin to the service provider directly in step B, the service provider cannot necessarily verify the evidence.

8.1.2 Non-repudiation evidence of delivery

Figure 3 illustrates the service model for delegated non-repudiation of delivery using a central signing authority's secret key.

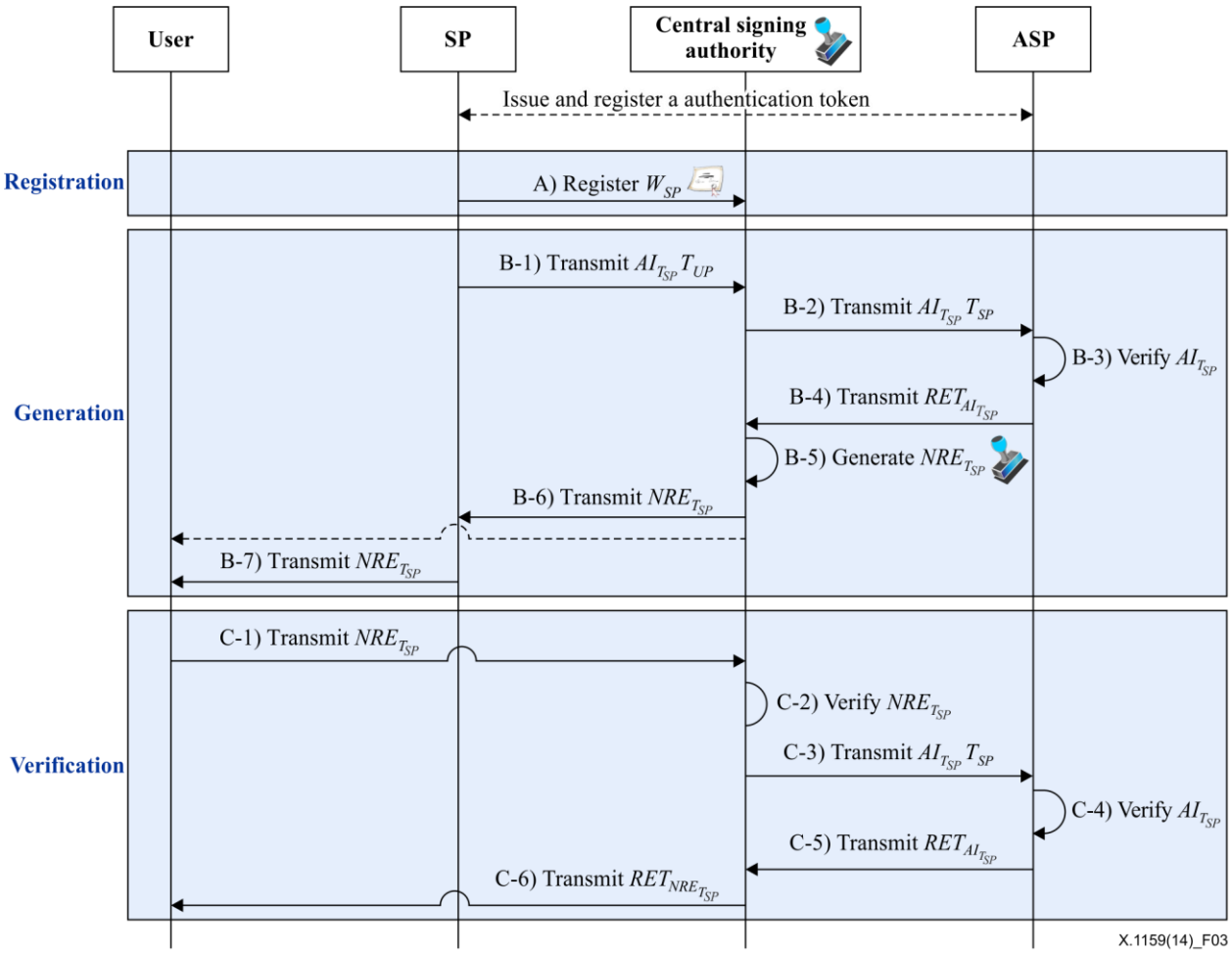

Figure 3 – Service model for delegated non-repudiation of delivery using a central signing authority's secret key

Step A: Registration

For the delegated non-repudiation service, the service provider pre-issues a signing key and/or an authentication token through an authentication service provider. In this step, the service provider registers a delegation warrant, W_U, where it is assumed that the service provider gives a central signing authority the authority to generate non-repudiation evidence.

Step B: Generation for non-repudiation evidence of delivery

When the user requests from the service provider the non-repudiation evidence of delivery, the service provider requests a central signing authority to generate the non-repudiation evidence. For this request, the service provider transmits the transaction-based authentication information, AI_{TSP}, to a

central signing authority. The central signing authority uses the ASP to verify the user's transaction-based authentication information AI_{TSP} and then generates the non-repudiation evidence NRE_{TSP} using its own secret key. The central signing authority also transmits NRE_{TSP} to the service provider and securely stores NRE_{TSP}, AI_{TSP} transmitted by the service provider and the verification result of AI_{TSP} RET_{AITSP}. The service provider transmits NRE_{TSP} to the user.

Step C: Verification for non-repudiation evidence of delivery

When the user requests from a central signing authority to verify NRE_{TSP}, a central signing authority verifies NRE_{TSP} and AI_{TSP}. The central signing authority also transmits NRE_{TSP} for delivery to the user directly in step B, since the user cannot necessarily verify the evidence.

8.2 Delegated non-repudiation service model using delegated signing key

This service model needs the registration operation of the user's signing key for delegated non-repudiation service. If the user fully trusts a central signing authority, the user delegates its original signing key to a central signing authority. Otherwise, a delegated signing key for a non-repudiation generation is required to be distinguishable from the user's original signing key. In the delegated non-repudiation service model, the user derives the delegated information from the user's signing key and then sends the delegated information to a central signing authority. The central signing authority derives the user's delegated signing key from the received delegated information by the user and the central signing authority's signing key. These models provide not only a general non-repudiation service but also a non-repudiation service between the user and the central signing authority because only the central signing authority can generate a valid delegation non-repudiation evidence using the user's delegation signing key, whereas the other cannot generate a valid one. To validate the non-repudiation evidence, the non-repudiation evidence validator needs the user and the central signing authority's validation key. The central signing authority generates the non-repudiation evidence using the delegated signing key.

8.2.1 Non-repudiation evidence of origin

Figure 4 illustrates the service model for delegated non-repudiation of origin using delegated signing key.

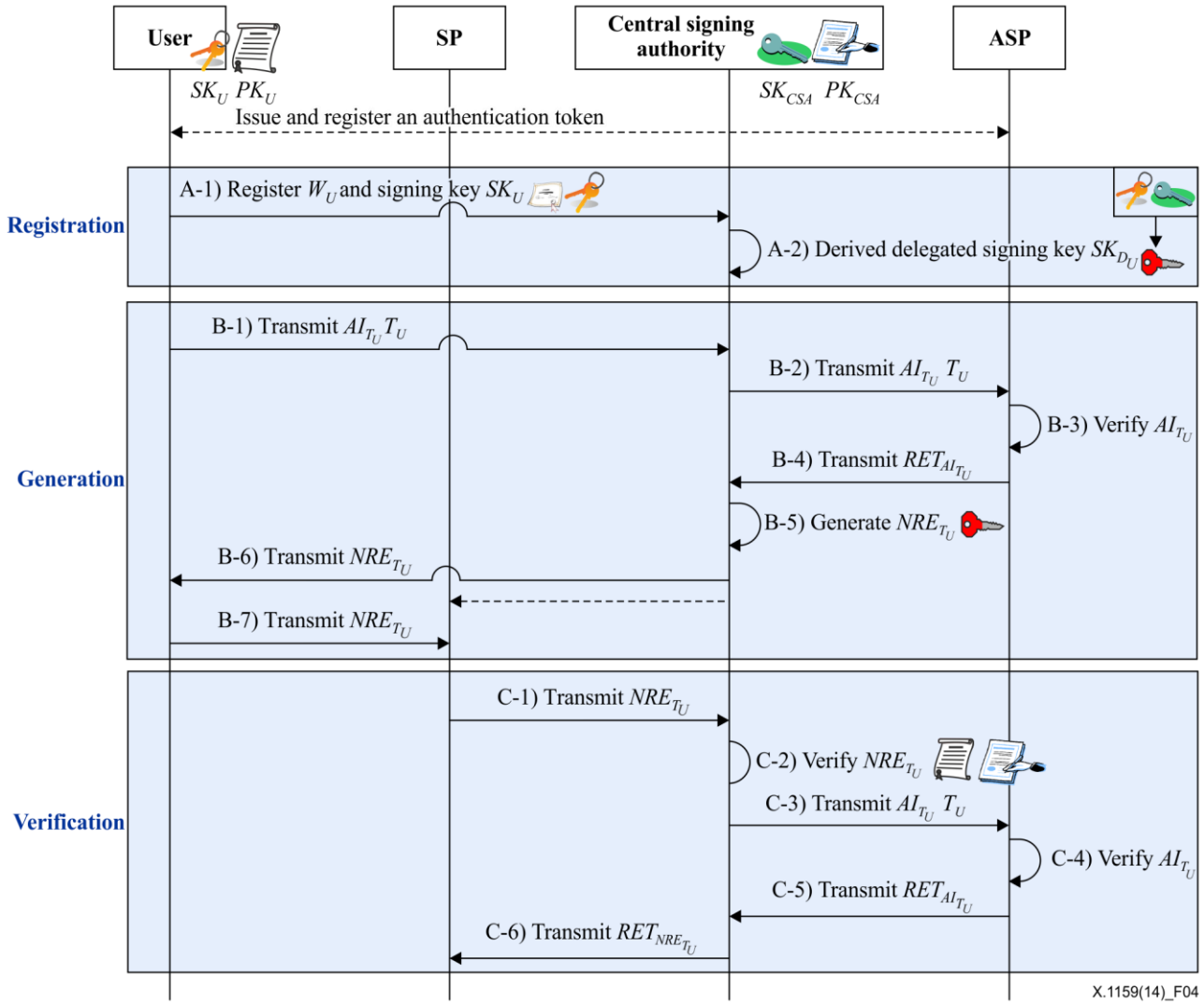

Figure 4 – Service model for delegated non-repudiation of origin using delegated signing key

Step A: Registration

For the delegated non-repudiation service, the user pre-issues a signing key and/or an authentication token through an authentication service provider. In this step, the user registers a delegation warrant, W_U, where it is assumed that the user gives a central signing authority the authority to generate non-repudiation evidence. The user also derives delegated information from the user's signing key and then transmits the delegated information, SK_U, to a central signing authority. The central signing authority derives the user's delegated signing key from the received delegated information by the user and the central signing authority's signing key.

Step B: Generation for non-repudiation evidence of origin

When the service provider requests from the user the non-repudiation evidence of origin, the user, in turn, requests a central signing authority to generate the non-repudiation evidence. For this request, the user transmits the transaction-based authentication information (AI_{TU}) to central signing authority. The central signing authority uses the ASP to verify the user's transaction-based authentication information AI_{TU} and then generates the non-repudiation evidence NRE_{TU} using the derived delegated user's signing key. The central signing authority also transmits NRE_{TU} to the user and securely stores NRE_{TU} and AI_{TU} transmitted by the user and the verification result of AI_{TU} RET_{AITU}. The user transmits the NRE_{TU} to the service provider.

Step C: Verification for non-repudiation evidence of origin

When the service provider requests from a central signing authority to verify NRE_{TU}, it verifies NRE_{TU} (using the user and the central signing authority's verification key) and AI_{TU}. The central signing authority also transmits the verification result of NRE_{TU} to the service provider. If the central signing authority transmits NRE_{TU} to the service provider directly in step B, the service provider cannot necessarily verify the evidence.

8.2.2 Non-repudiation evidence of delivery

Figure 5 illustrates the service model for delegated non-repudiation of delivery using delegated signing key.

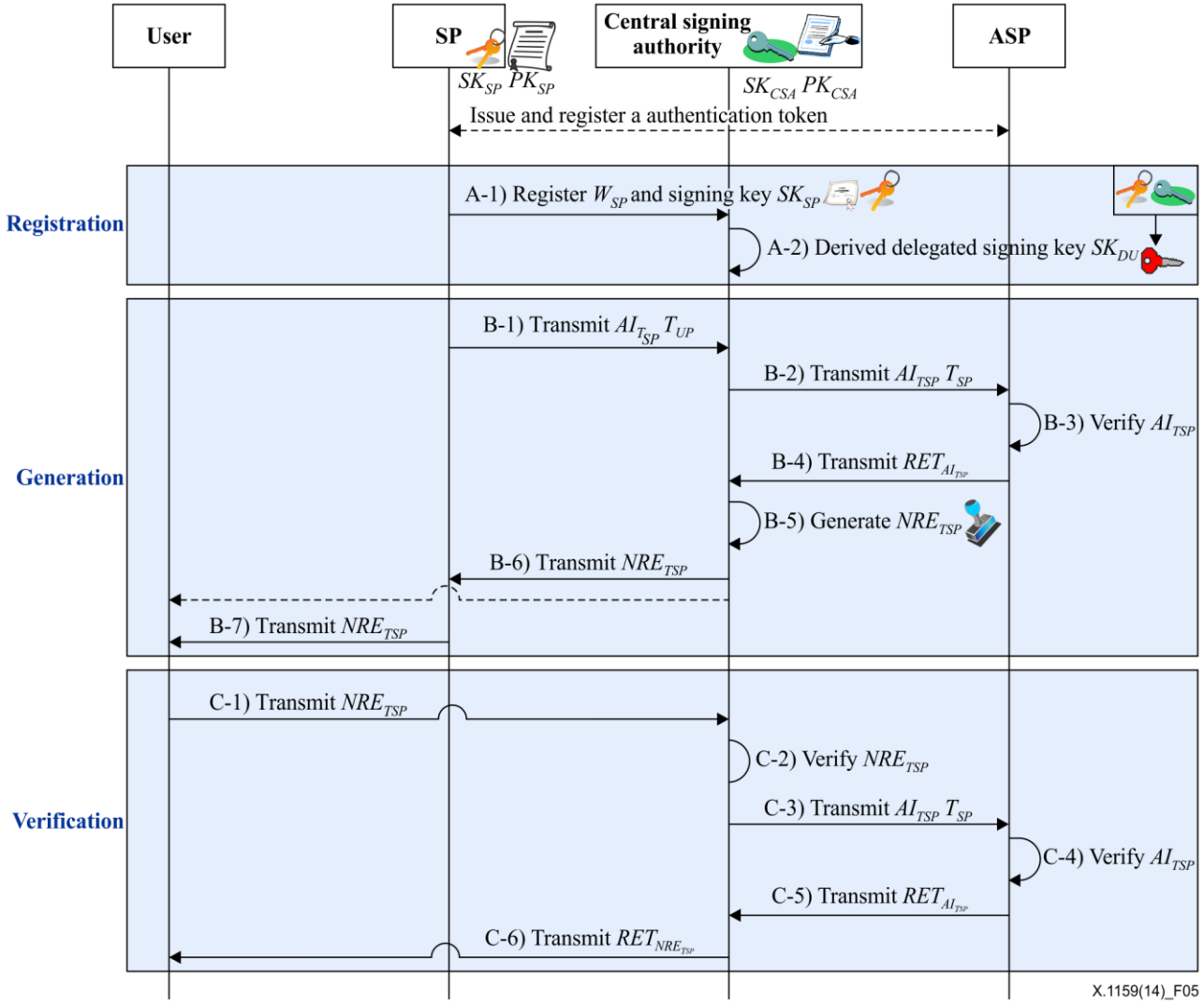

Figure 5 – Service model for delegated non-repudiation of delivery using delegated signing key

Step A: Registration

For the delegated non-repudiation service, the service pre-issues a signing key and/or an authentication token through an authentication service provider. In this step, the service registers a delegation warrant, W_U, where it is assumed that the service provider gives a central signing authority the authority to generate non-repudiation evidence. The service provider also derives delegated information from the service provider's signing key, and then transmits the delegated information, SK_{SP}, to a central signing authority. The central signing authority derives the service provider's

delegated signing key from the received delegated information by the service provider and the central signing authority's signing key.

Step B: Generation for non-repudiation evidence of delivery

When the user requests from the service provider the non-repudiation evidence of delivery, the service provider requests a central signing authority to generate the non-repudiation evidence. For this request, the service provider transmits the transaction-based authentication information, AI_{TSP}, to a central signing authority. The central signing authority uses the ASP to verify the user's transaction-based authentication information AI_{TSP} and then generates the non-repudiation evidence NRE_{TSP} using the derived delegated signing key. The central signing authority also transmits NRE_{TSP} to the service provider and securely stores NRE_{TSP}, AI_{TSP} transmitted by the service provider, and the verification result of AI_{TSP} RET_{AITSP}. The service provider transmits NRE_{TSP} to the user.

Step C: Verification for non-repudiation evidence of delivery

When the user requests from a central signing authority to verify NRE_{TSP}, a central signing authority verifies NRE_{TSP} and AI_{TSP}. If the central signing authority transmits NRE_{TSP} to the user directly in step B, the user cannot necessarily verify the evidence.

8.3 Security considerations for delegated non-repudiation service models

The security considerations for delegated non-repudiation service models (SMs) are shown in Table 1 which gives considerations in order to satisfy the requirements for each service model. SM1 refers to the delegated non-repudiation service model using the central signing authority's secret key in clause 8.1, and SM2 refers to the delegated non-repudiation service model that uses the delegated signing key in clause 8.2.

Table 1 – Security considerations for delegated non-repudiation service models

	SM1	SM2
R1-Unforgeability	– The secret key which generates non-repudiation evidence is known only to a central signing authority and is required to be securely stored.	– A delegated signing key which generates non-repudiation evidence is required to be distinguishable from the user's original signing key.
R2-Prevention of misuse	– Generation (only by a user) and verification (only by ASP) of transaction-based authentication information is prohibited from intervening with the central signing authority. – The central signing authority is required to verify transaction-based authentication information by the ASP before generating non-repudiation evidence. Furthermore, the central signing authority is required to securely store the transaction-based authentication, the result of validation, and the non-repudiation evidence.	

Table 1 – Security considerations for delegated non-repudiation service models

<table>
<tr><th></th><th>SM1</th><th>SM2</th></tr>
<tr><td rowspan="2">R3-Verifiability</td><td>– Even if the central signing authority's secret key has changed (e.g., updating, reissuing of key), the central signing authority is required to provide verification methods for generation of non-repudiation evidence using the new key as well as the old key.</td><td>– Even if the delegated signing key has changed (e.g., updating, reissuing of key for user and/or the central signing authority), the central signing authority is required to provide verification methods for generation of non-repudiation evidence using the new key as well as the old key.</td></tr>
<tr><td colspan="2">– The non-repudiation evidence is required to involve an explicit unforgeable warrant which includes the fact that the user gave the central signing authority the authority and/or the user's signing key for generation of non-repudiation evidence. The warrant can also be identified by anyone to verify the non-repudiation evidence.</td></tr>
<tr><td>R4-Identifiability</td><td>-</td><td>– The non-repudiation evidence is required to provide the identifier to indicate whether the delegated signing key is the user's original key or a derived key from the user's key and the central signing authority's key.</td></tr>
</table>

Bibliography

[b-ITU-T X.509] Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8:2014, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.842] Recommendation ITU-T X.842 (2000) | ISO/IEC TR 14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services*.

[b-ITU-T X.1153] Recommendation ITU-T X.1153 (2011), *Management framework of a one time password-based authentication service*.

[b-ITU-T X.1156] Recommendation ITU-T X.1156 (2013), *Non-repudiation framework based on a one-time password*.

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, 2015