Draft Recommendation ITU-T X.sap-9

Delegated non-repudiation architecture based on X.813

Summary

The non-repudiation is to prevent entities from denying that they have sent or received electronic transaction data in the telecommunication network. This proposed Recommendation will create an enhanced non-repudiation model based on X.813 in support of application services.

The proposed architecture can generate and verify the non-repudiation evidence for the transaction data by trusted third parity (TTP) that is the central sign authority (CSA).

The proposed architecture integrates multiple authentication devices to access the trusted third party that is the central signing authority (CSA). It also integrates multiple service providers to provide a non-repudiation service with a single authenticated device. The delegated non-repudiation architecture provides the ability to manage user authentication centrally. The service providers can provide the service of a user authentication and non-repudiation without additional construction of authentication systems.

This Recommendation describes the delegated non-repudiation service models and operations for each of the service models. This architecture also defines the security requirements of the delegated non-repudiation service.

1. Scope

This Recommendation will create an enhanced non-repudiation model based on X.813 in support of application services. The user can authenticate and generate non-repudiation evidence for the transaction data by trusted third party (TTP) that is the central signing authority (CSA). The proposed architecture integrates multiple authentication devices to access the central signing authority (CSA). It also integrates multiple service providers to provide a non-repudiation service with a single authenticated device. The model will provide non-repudiation services to any type of device including mobile. Although this architecture makes use of strong authentication, it is out of 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 published regularly.

A 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), *Information technology – Open systems interconnection – Security frameworks in open systems-Part4: Non-repudiation framework*

TSB Note: All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations:

5. Conventions

In this Recommendation:

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 recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance. 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 the specification.

6. Delegated non-repudiation architecture

6.1 Introduction

6.2 Entities

7. Requirements for a delegated non-repudiation service

8. Delegated non-repudiation service models

8.1 Type 1 model

8.2 Type 2 model

8.3 Type 3 model

Appendix A: Template for a new work item

Question:	7 /17	**Proposed new ITU-T Recommendation**	August/September 2012	
Reference and title:	Rec. ITU-T X.sap-9 "Delegated non-repudiation architecture based on X.813"			
Base text:	C 735		**Timing:**	April-2015
Editor(s):	Keun-ok Kim, Korea (Republic of), kko@fsa.or.kr Hee-won Shim, Korea (Republic of), hwshim@fsa.or.kr Seong-Hyeon Song, Korea (Republic of), decash@fsa.or.kr		**Approval process:**	AAP

Scope:

This Recommendation will create an enhanced non-repudiation model based on X.813 in support of application services. The user can authenticate and generate non-repudiation evidence for the transaction data by trusted third party (TTP) that is the central signing authority (CSA). The proposed architecture integrates multiple authentication devices to access the central signing authority (CSA). It also integrates multiple service providers to provide a non-repudiation service with a single authenticated device. The model will provide non-repudiation services to any type of device including mobile. Although this architecture makes use of strong authentication, it is out of scope of this Recommendation.

This Recommendation describes the delegated non-repudiation service models and operations for each of the service models. This architecture also defines the security requirements of the delegated non-repudiation service.

Summary:

The non-repudiation is to prevent entities from denying that they have sent or received electronic transaction data in the telecommunication network. This proposed Recommendation will create an enhanced non-repudiation model based on X.813 in support of application services. The proposed architecture can generate and verify the non-repudiation evidence for the transaction data by trusted third parity (TTP) that is the central sign authority (CSA).

The proposed architecture integrates multiple authentication devices to access the trusted third party that is the central signing authority (CSA). It also integrates multiple service providers to provide a non-repudiation service with a single authenticated device. The delegated non-repudiation architecture provides the ability to manage user authentication centrally. The service providers can provide the service of a user authentication and non-repudiation without additional construction of authentication systems.

This Recommendation describes the delegated non-repudiation service models and operations for each of the service models. This architecture also defines the security requirements of the delegated non-repudiation service.

The delegated non-repudiation architecture reduced the computation and operations of client aspects for user authentication and non-repudiation service. Thus this delegated non-repudiation architecture is more suitable for mobile devices.

Relations to ITU-T Recommendations or to other standards (approved or under development)**:**

- X.813, Information technology – Open systems interconnection – Security frameworks in open systems – Part 4: Non-repudiation framework
- X.sap-6, Non-repudiation framework based on a one time password

Liaisons with other study groups or with other standards bodies: ISO/IEC SC 27/WG 2, GSMA, 3GPP SA3, IETF
Supporting members that are committing to contributing actively to this project: Korea, ETRI, KISA, KT, China, Uganda, MBNA Canada