

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1155

(10/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Security protocols

Guidelines on local linkable anonymous authentication for electronic services

Recommendation ITU-T X.1155



International
Telecommunication
Union

Documents
Document Sharing Hub

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
PKI related Recommendations	X.1340–X.1349
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.1155

Guidelines on local linkable anonymous authentication for electronic services

Summary

In electronic services or e-services, there are various occasions where privacy violations are of concern. Service providers may gather users' personal information in the processes of subscription, purchase or delivery. They may be able to access and exploit users' personal data that is collected during the service processes. The consequences these threats pose to user privacy, such as personal data leakage and tracking, are very serious emerging social issues. Therefore, technological solutions for preserving privacy in e-services are necessary. Anonymous authentication that allows users to be able to authenticate themselves without revealing their identity is the most fundamental means of addressing the privacy threats associated with e-services.

Recommendation ITU-T X.1155 provides guidelines on local linkable anonymous authentication for e-services. This includes the privacy threats of e-services, the requirements of local linkable anonymous authentication, the functions that satisfy these requirements and a general model of local linkable anonymous authentication for e-services.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1155	2015-10-29	17	11.1002/1000/12599

* 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/>.

© ITU 2016

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

Table of Contents

	Page
1 Scope.....	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	3
5 Conventions	3
6 Overview.....	4
6.1 Privacy threats in e-services	5
6.2 Complete anonymity and its side effects	5
6.3 Anonymous authentication	6
7 Issues in anonymous authentication	7
7.1 Traceability issues	7
7.2 Linkability issues.....	7
7.3 Local linkability issues of anonymous authentication mechanisms.....	11
7.4 Anonymous authentication mechanisms and their properties	11
8 Requirements of anonymous authentication for subscription-based e-services	12
8.1 Requirements for secure authentication	12
8.2 Requirements for anonymity in subscription-based services	13
8.3 Relationship between the requirements and privacy-related issues	14
9 Framework of local linkable anonymous authentication for e-services	15
9.1 Entities.....	15
9.2 Processes among the entities	16
9.3 Local linkable anonymous authentication mechanisms	18
Appendix I – Use cases.....	19
I.1 E-commerce use case	19
I.2 E-voting use case	20
Bibliography.....	23

Copyright © 2015 ITU-T. All rights reserved.

Downloaded from <https://www.itu.int/ITU-T/standards/itu-t-standards.aspx>

Recommendation ITU-T X.1155

Guidelines on local linkable anonymous authentication for electronic services

1 Scope

This Recommendation provides guidelines on local linkable anonymous authentication for electronic services. This Recommendation includes the following items:

- privacy threats of electronic services;
- requirements for local linkable anonymous authentication;
- functions that satisfy the requirements;
- models of local linkable anonymous authentication for electronic services.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 anonymity [b-ITU-T X.1252]: A situation where an entity cannot be identified within a set of entities.

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

3.1.3 claimant [b-ITU-T X.1252]: An entity that is or represents a principal for the purposes of authentication.

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

3.1.5 key [b-ISO/IEC 9798-1]: Sequence of symbols that controls the operation of a cryptographic transformation.

3.1.6 linking base [b-ISO/IEC 20008-1]: Public data element, optionally specific to a group signature linker, which is involved in the group signature process if using this data element to link multiple signatures created by the same signer is required.

3.1.7 personally identifiable information (PII) [b-ITU-T X.1252]: Any information (a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, (b) from which identification or contact information of an individual person can be derived, or (c) that is or can be linked to a natural person directly or indirectly.

3.1.8 privacy [b-ITU-T X.1252]: The right of individuals to control or influence what personal information related to them may be collected, managed, retained, accessed, and used or distributed.

3.1.9 pseudonym [b-ITU-T X.1252]: An identifier whose binding to an entity is not known or is known to only a limited extent, within the context in which it is used.

3.1.10 revocation [b-ITU-T X.1252]: The annulment by someone having the authority, of something previously done.

3.1.11 verification [b-ITU-T X.1252]: The process or instance of establishing the authenticity of something.

3.1.12 verifier [b-ITU-T X.1252]: An entity that verifies and validates identity information.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 anonymous authentication: An authentication in which the personally identifiable information of a claimant is not known to the verifier.

NOTE – In cryptographic terms, the level or strength of anonymity should be computed by a theoretical mechanism and an anonymous authentication should satisfy a certain level or strength of anonymity. However, this concern is not considered in this Recommendation.

3.2.2 anonymous claimant (or anonymous user): An entity (or service user) who uses anonymous authentication for preserving privacy.

3.2.3 anonymous identifier: An identifier which is not related to and is not used to infer the personally identifiable information of a claimant. Pseudonym is one example of anonymous identifier and is seen by a verifier, while random value is used in anonymous authentication based on group signature. This random value should be treated securely as a cryptographic key and is not given to a verifier through the authentication process.

3.2.4 authentication token: A message consisting of data fields which contain information that is used to generate an authentication transaction for (entity) authentication. In (entity) authentication, an authentication token consists of an identifier and its corresponding key or secret credential such as password. Likewise, an authentication token used in anonymous authentication consists of an anonymous identifier and its corresponding key or secret credential.

3.2.5 authentication transaction: A message set exchanged in a particular communication for anonymous authentication between a claimant and a verifier.

3.2.6 complete anonymity: A situation where an entity is never identified nor authenticated both in the present and in the future.

3.2.7 conditional traceability: A property where an entity can be traced with a specific condition.

3.2.8 controllable linkability: A property where linking is possible by an entity that possesses a special linking key.

3.2.9 full linkability: A property of anonymous authentication in which linking is always possible by any verifier.

3.2.10 issuer: An authorized entity that issues an (anonymous) authentication token to a claimant, confirming that the personally identifiable information of the claimant is presented and verified.

3.2.11 linkability: A property where linking is possible in anonymous authentication.

3.2.12 linking: Process used to determine whether two or more anonymous authentication transactions were performed by the same claimant, even if it is impossible to identify the specific claimant of these transactions.

3.2.13 local linkability: A property where linking is possible only for multiple anonymous authentication transactions presented to the same verifier.

3.2.14 non-anonymous authentication: An authentication which is not anonymous authentication. In this authentication process, personally identifiable information of a claimant is known to the verifier.

3.2.15 opener: An authorized entity that has a capability to find out an anonymous identifier from an anonymous authentication transaction using a special key called an opening key.

3.2.16 opening: Process by an authorized entity called an opener to find out an anonymous identifier from an anonymous authentication transaction.

3.2.17 signer-centric linkability: A property where linking multiple anonymous authentication transactions depends on the information that the signer owns or generates.

3.2.18 traceability: A property where it is possible to find out the personally identifiable information of a claimant in anonymous authentication.

3.2.19 traceable anonymous service: The service in which it is sometimes necessary to trace the anonymous user.

3.2.20 tracer: An authorized entity that has a capability to find out the personally identifiable information from an anonymous identifier.

3.2.21 tracing: Process by an authorized entity called a tracer to find out the personally identifiable information of the claimant from an anonymous identifier.

3.2.22 tracking: Process to collect the previous authentication transactions or other data of a claimant in order to infer the claimant's privacy-related information.

3.2.23 unlinkability: A property where linking is always impossible by a verifier in anonymous authentication.

3.2.24 untraceability: A property where tracing is always impossible in anonymous authentication.

3.2.25 untraceable anonymous service: A service in which it is impossible to trace the anonymous user.

3.2.26 verifier-centric linkability: A property where linking multiple anonymous authentication transactions depends on the information that the verifier owns or generates.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Anonymity Issuer
BI	Blind Issuer
CA	Certification Authority
CL-GS	Group Signature with Controllable Linkability
DAA	Direct Anonymous Attestation
IdP	Identity Provider
PC	Personal Computer
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SNS	Social Network Service
TAC	Traceable Anonymous Certificate
TV- STB	Television Set-Top Box

5 Conventions

None.

6 Overview

With the prevalence of various high-end terminals, such as personal computers (PCs), television set-top boxes (TV-STBs), cell phones and high speed broadband wired or wireless network access, various services through electronics technology have become commonplace throughout the world. The electronic services or e-services include e-commerce, information searching, e-mail and social network service (SNS). For example, customers can buy products not only without using cash but also in an e-commerce environment where cards are not present.

Some of these services, including web search engines, do not require subscription for them. In most services, users generally register their personally identifiable information (PII) for the subscription. Then, users log in to the services by an authentication process. After successful authentication, they are authorized to access the services. In this scenario, the service providers often provide the personalized services for their registered customers such as mileage offer, personalized web page, personalized advertisement, etc.

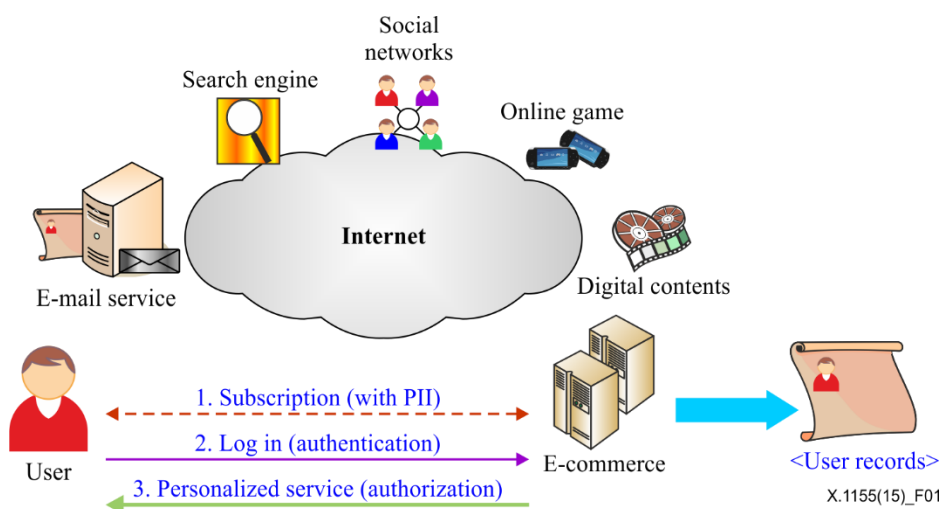


Figure 1 – Typical electronic services

However, if the customers are privacy-savvy, this service scenario is not desirable to them. Their PII is provided to the service providers in a subscription process. Moreover, service use patterns can be accumulated in order to classify them or provide user-customized services. If users increasingly use these various services, the possibility of privacy invasion is augmented because users are easily identified by PII in many services. To avoid these privacy threats, anonymity becomes a considerable concept. For anonymity, PII should not be registered with the service providers because the providers should not be able to identify their customers with PII. However, in the latter case, it will become more difficult to find out a customer who has committed a cybercrime. Therefore, in order to make the conventional subscription-based services privacy-enhanced and crime-resistant simultaneously, it is sufficient for these services to use a privacy-enhanced technology which has a traceable property. In this Recommendation, these conventional services are referred to as traceable anonymous services. Examples of these services can include e-commerce, e-mail, e-auction, etc.

Meanwhile, new services which traditionally require privacy can emerge, such as e-voting, public opinion surveys, anonymous teaching evaluations, etc. In these types of services, the confirmation of PII is necessary before accessing the service. However, it should be impossible to identify who used the service or to trace an unknown customer. In other words, privacy is essential and core for those services. These types of services are referred to as untraceable anonymous services in this Recommendation.