International Telecommunication Union

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

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/.

Table of Contents

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 date 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.

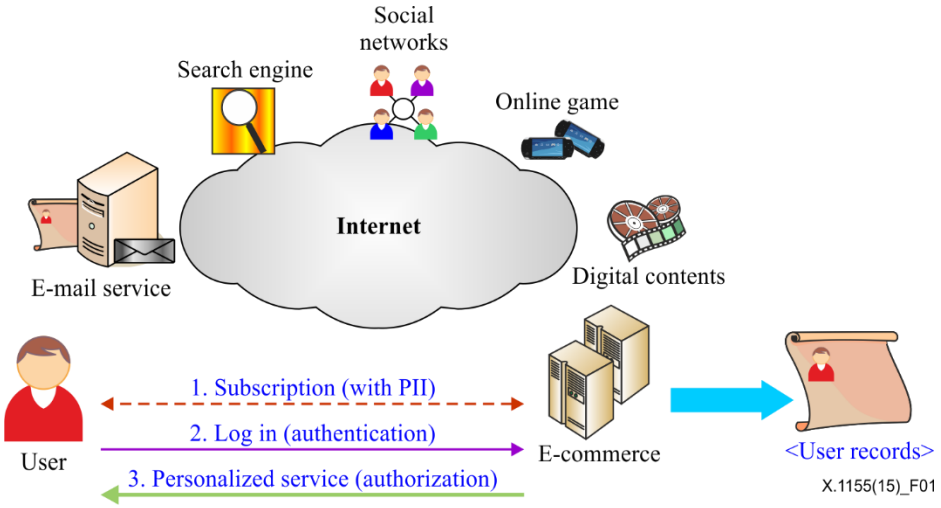

Figure 1 – Typical electronic services

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.

6.1 Privacy threats in e-services

While gaining the benefits and convenience of e-services, the possibility of user privacy invasion usually increases. Service providers usually gather users' personal information in the process of subscription, authentication, or service use. To cope with users' fraud or problems during the services, service providers request PII during the subscription or in an authentication step.

Moreover, service providers may request or gather excessive or unnecessary personal information, including age, gender, interests, visit pages, or shopping patterns. This information can be directly bound to the users' PII. Online service providers tend to consider this information necessary for their services. However, this could pose two types of privacy threat.

6.1.1 Leakage of PII and other associated information

The first privacy threat concerns the leakage of users' personal information. Users are sometimes required to provide their sensitive personal information including PII in order to use e-services. However, users have no means to manage their information and they cannot control the information flow. In some cases, PII is leaked due to careless management by service providers. Thieves may obtain the personal information by hacking the database of online shopping malls or by bribing database managers. Database encryption cannot be an effective countermeasure.

Moreover, the increasing number of entities holding personal information makes it much more difficult to keep the users' sensitive details hidden from the respective parties. PII may also be stolen when users mistakenly access phishing sites.

6.1.2 Profiling issue in inter-services

The second privacy threat is a profiling issue. Whenever a user visits a specific page or a service, the user could be profiled and his/her behaviour (as well as shopping patterns, tastes, whereabouts and activities, etc.) may be known to the service provider.

If service providers collude, the historical data will be more meaningful and the user may be tracked easily. Furthermore, this tracking information is bound to their PII if PII should be registered in the subscription process.

6.2 Complete anonymity and its side effects

Complete anonymity is a situation where an entity is not identified and authenticated. This situation can be a countermeasure against privacy threats, which were described in clause 6.1. However, if service providers neither identified nor authenticated the users to provide complete anonymity, there would be no privacy threat, but the following side effects could exist.

6.2.1 Illegal actions by abusing anonymity

In complete anonymity, users do not have to confirm their PII, which means that it is possible for an anonymous user to do illegal actions such as cybercrime, online defamation, disguise, etc. There is no means to identify who the illegal user is. For example, in e-commerce, there will be many illegal transactions or fraud. Therefore, there should be a way whereby legal users remain anonymous but the anonymity of users performing illegal actions can be cancelled.

Another example is e-voting where there can be many duplicate votes or proxy votes. In this example, however, though duplicate or proxy voting is illegal, the anonymity of the illegal user should not be cancelled. A better solution would be to make it possible to check the user's voting authority anonymously and to make it impossible for any user to do duplicate or proxy voting.

6.2.2 Impossibility of personalized services

As mentioned earlier, the service providers often provide personalized services for their registered customers in the typical services. These personalized services are possible if the providers can

identify their users. However, with complete anonymity, the users cannot check their purchase history in the e-commerce services.

In the e-voting service, it is possible that some users may want to change their vote during the voting period. In this case, the service provider should be able to find out if the previous and current votes are indeed from the same user.

6.3 Anonymous authentication

Considering the privacy threats described in clause 6.1, preserving user privacy is definitely required in e-services. What service providers really need to know is not the user's personal information but rather his/her privilege to get the service. As a result, privacy-preserving technologies are required to be applied to e-services. These technologies include anonymous authentication, anonymous payment, anonymous channel, privacy-preserving data mining, etc.

Among these privacy-preserving technologies, the most prominent candidate is to make use of anonymous authentication. In most e-services, authentication is a basic and fairly essential security function. This is because authentication is related to the service processes such as subscription and log-in. Users should be able to be authenticated anonymously and this is done by not presenting their PII to the service providers. Therefore, if an anonymous authentication mechanism is used, the service providers cannot access PII and as a result PII cannot be bound to other personal information such as personal mileage, service use records, etc.

On the other hand, unconditional and permanent anonymity is not always desirable. Some people abuse anonymity to perpetrate cybercrimes. Completely anonymous access, which is very significant for privacy, could result in other vulnerability issues, such as masquerading, falsification and repudiation. Therefore, it is necessary that anonymity can be removable and that the user's identifiable information can be accessed in exceptional conditions. In addition, to avoid the tracking problem, authentication transactions should not generally be linked.

Anonymous authentication technology may be useful in e-commerce or in other security-required environments because it fulfils security and privacy needs. Anonymous authentication mechanisms include cryptographic anonymous authentication mechanisms and pseudonym-based mechanisms.

6.3.1 Cryptographic mechanisms

Cryptographic anonymous authentication is a mechanism in which a user can be authenticated while a certain level of anonymity is still satisfied. In the mechanism, a verifier can only know if the claimant is a valid user, but the verifier does not know the claimant's identifier. There are many cryptographic anonymous authentication mechanisms, including group signature [b-Chaum] and [b-Hwang], direct anonymous attestation (DAA) [b-Brickell], traceable signature [b-Kiayias] and ring signature [b-Rivest], etc. Ring signature has the property of being unlinkable and untraceable; however, it is impractical because it uses multiple public keys and its signature size generally grows with the group size.

Group signature, DAA and traceable signature are mechanisms which can provide anonymity using a group public key. A claimant of the group has its own private key and makes his/her signature for authentication. The signature can then be verified with one group public key. The verifier just knows the correctness of the signature.

These mechanisms are similar but include small variations. Group signature is very practical for traceable anonymous services including e-commerce because group signature provides anonymity with conditional traceability. In group signature, an authorized party or parties can trace the signature, or reveal the identifier of the signer. In DAA, unlike group signature, the anonymous transaction cannot be traced. Traceable signature has more functionality in user tracing and signature claiming than group signature, which are not necessarily required in most services. Anonymous digital signature mechanisms using a group public key and anonymous authentication

based on the signature mechanisms are standardized in [b-ISO/IEC 20008-2] and [b-ISO/IEC 20009-2].

6.3.2 Pseudonym-based mechanisms

Pseudonym-based anonymous authentication mechanisms can also provide conditional traceability. In these mechanisms, the claimants use the pseudonym instead of their PII in the authentication process after receiving the pseudonym from a trusted issuer. These mechanisms include IETF TAC [b-IETF RFC 5636] and security assertion markup language (SAML) [b-ITU-T X.1141].

In IETF TAC, a pseudonym certificate named traceable anonymous certificate (TAC) is issued from the certification authority (CA). The claimants use TAC when they want to be authenticated by a service provider. In SAML, the claimants should access a trustee identity provider (IdP) in order to get an issued pseudonym when they want to log in to the services. Anonymous authentication transactions using pseudonym-based mechanisms are always linkable if the claimant uses the same pseudonym.

7 Issues in anonymous authentication

As mentioned in clause 6.2, complete anonymity is undesirable in most subscription-based services. To control the anonymity level, two kinds of properties should be considered in anonymous authentication: traceability and linkability.

7.1 Traceability issues

As mentioned in clause 6.2, complete anonymity has two side effects: illegal actions by abusing anonymity and the impossibility of using personalized services. The easiest way to cope with illegal action is to revoke the claimant's anonymity. Therefore, if it is possible to use tracing to find out the claimant's PII, then the claimant's anonymity can be revoked. However, tracing is exceptional and should be done only by an authorized trustee. In traceable anonymous services, this conditional traceability may not encounter any problems if there is no regulation issue. As a result, anonymous authentication with conditional traceability should be used in traceable anonymous services.

In untraceable anonymous services, tracing functionality should be avoided because of the service feature. Instead of tracing illegal actions, it is better to prevent the actions in the services. For example, if someone tries to duplicate voting or proxy balloting in the e-voting services, the illegal balloting should be inspected and blocked before it is applied to the voting result. This prevention is not related to traceability. Rather, if the claimant can be identified from anonymous authentication transactions, manipulation or fraud cannot be possible. Of course, it should be impossible to find out PII from this identification. In conclusion, the anonymous authentication with untraceability (and linkability) should be used in untraceable anonymous services.

DAA and ring signatures have a property of untraceability. In group signatures, traceable signatures and pseudonym-based mechanisms, an anonymous claimant can be traced by the trustee with trace authority. However, the mechanism with conditional traceability can be changed to an untraceable mechanism if provided with special hardware.

7.2 Linkability issues

Another side effect of the impossibility of anonymity in personalized services can arise within a complete anonymous environment because there is no means to detect if any two or more transactions are from the same claimant. Service providers should be able to link the transactions, but the profiling issue will occur if all transactions are linkable. Therefore, it is important to take an appropriate level of linkability to solve both the profiling and personalization issue.

7.2.1 Linking domain and local linkability

Two or more (anonymous authentication) transactions are "linked" when it can be determined whether or not these transactions have been performed by the same user, even if it is impossible to identify the specific user of these transactions. There are three levels of linkability: full linkability, local linkability and unlinkability.

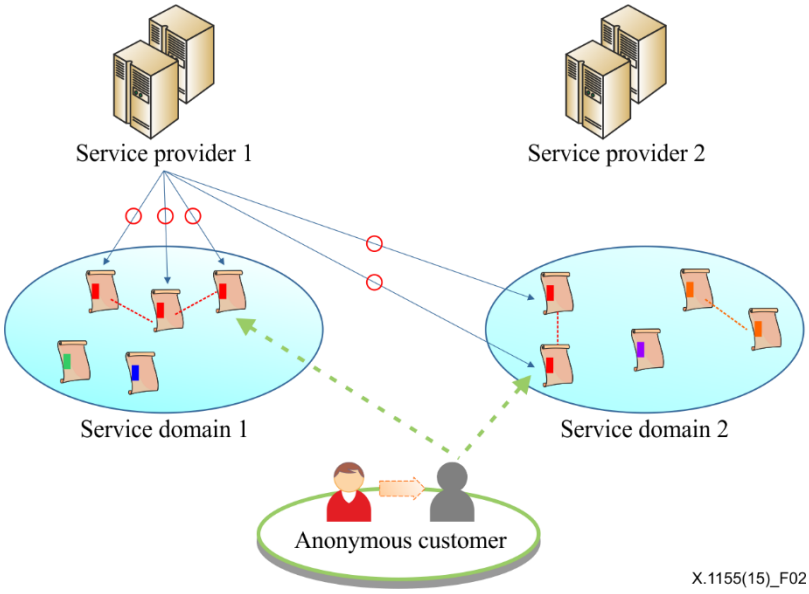

Figure 2 – Concept of full linkability

In an anonymous authentication mechanism with full linkability, all authentication transactions are linked. This means that anyone can determine if two transactions are generated from the same user or not. One example of fully linkable anonymous authentication is described in [b-IETF RFC 5636]. In the IETF TAC model, the traceable anonymous certificate (TAC) is an ITU-T X.509 certificate which contains the pseudonym in the Subject name field. If a user has one TAC and generates all anonymous authentication transactions using it, the verifier or others who can see the transactions are able to know that the transactions are from the same user because all pseudonyms in the transactions are the same. In Figure 2, service provider 1 can link all transactions from the customer.

Therefore, this property of full linkability may be dangerous for the users' privacy for the following reasons. First, as linked transactions are accumulated, anonymous users can be characterized by their transactions and the probability that their anonymity will be lost increases. Second, users could be monitored for their shopping and spending patterns, which could be regarded as an invasion to their privacy. Third, if the identifiable information of a user is disclosed from any one anonymous transaction, anonymity will be fully cancelled for all the other transactions.

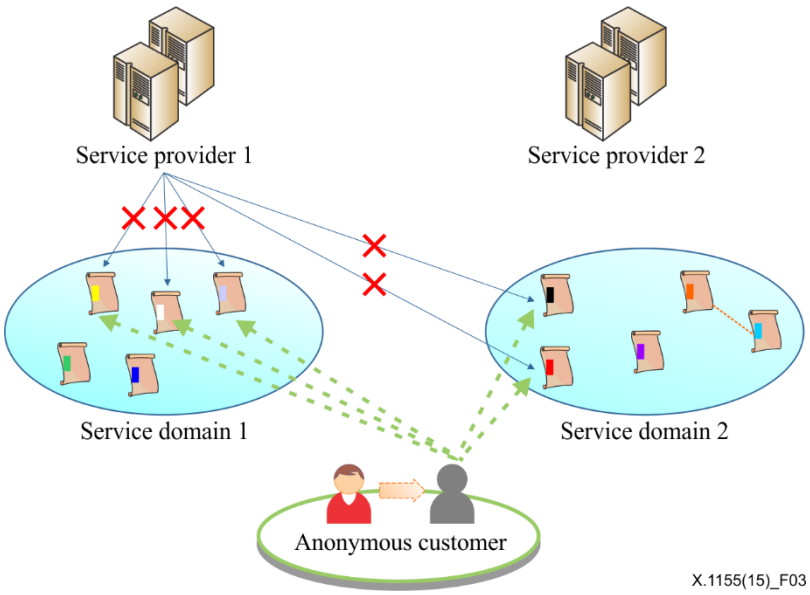

Figure 3 – Concept of unlinkability

In contrast to full linkability, in the case of unlinkability it cannot be determined if authentication transactions with unlinkability are from the same user. Suppose that the user generates an anonymous authentication transaction (Tr_A) in order to be authenticated to a service provider, and the user generates another transaction (Tr_B) to the provider later on. If the used mechanism is unlinkable, then there is no means for the service provider to determine if Tr_A and Tr_B are from the same user. This concept of unlinkability can be seen in Figure 3.

Anonymous authentication mechanisms with unlinkability can provide more robust privacy than those with full linkability because tracking is impossible, but this feature is not suitable for the subscription-based e-services. In order to have subscribers and analyse their service use pattern, the service providers generally provide personalized services, such as a mileage service. In the mechanisms with full linkability such as non-anonymous authentication mechanisms or pseudonym-based mechanisms, the personalized services can be provided easily as all authentication transactions and service use histories are linked with PII or a pseudonym. However, the service providers using unlinkable anonymous authentication mechanisms have no method to make personalized services for their customers.

Therefore, fully linkable anonymous authentication has a privacy problem and unlinkable anonymous authentication also has a problem in that the impossibility of tracking makes it unsuitable for a subscription-based service. Local linkability is induced to solve this contradictory situation. Local linkability is a feature where two or more authentication transactions from the same anonymous user are linked only by a specific service provider to whom the transactions are given, but other service providers or entities cannot link to these transactions. In Figure 4, service provider 1 can link the user's transactions which are given to it, but it cannot link the other transactions given to service provider 2. Equally, service provider 2 can link the transactions which are given to it, but it cannot link the transactions given to other service providers including service provider 1.

With this type of anonymous authentication mechanism, the service provider is able to track an anonymous user's history in the service domain while the user cannot be tracked over multiple domains. In other words, a service provider can identify anonymous users in the service domain with its local identifier, but there is no means to find out whether $User_A$ in $Service_1$ and $User_B$ in $Service_2$ are the same user.

For example, service providers generally want to manage the log-in history and purchase records of their customers. Service providers may be willing to find out their customers' preferences and

provide a personalized service for each customer in order to raise their revenues. With a local linkable anonymous authentication mechanism, they can provide this type of service.

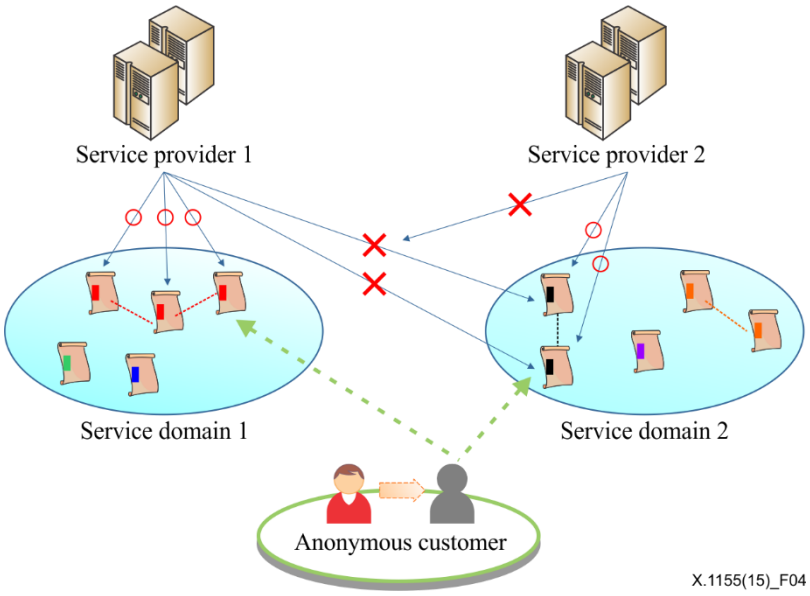

Figure 4 – Concept of local linkability

7.2.2 Signer/verifier-centric linkability

Generally, group signature-based anonymous authentication mechanisms do not have linking capability except by an opener. However, DAA and traceable signatures allow signer-centric linkability. Signer-centric linkability is a property where linking multiple anonymous authentication transactions depends on the information that the signer owns or generates. On the other hand, verifier-centric linkability is a property where linking depends on the information that the verifier owns or generates.

In DAA, a claimant can generate a public data called as linking base which is used for linking authentication transactions. If transactions are generated with the same linking base from the same claimant, the verifier will easily detect this phenomenon. In traceable signatures, the manner to provide linkability is somewhat different from that of DAA. Traceable signature has the property of "signature claiming" where the signer of a signature claims a given signature that he/she has signed. By modifying this function, the signer can prove that he/she is the originator of these two signatures. This is also signer-centric linkability, but the difference is when and how the verifier can link the signatures. The linking base is inserted into the authentication transaction by the signer so that the verifier can link the multiple transactions in the authentication process in DAA, while the linking information is generated and can be linked when the claimant wants to be linked even after the authentication process in traceable signatures.

Though signer-centric linkability supports customer privacy, service providers prefer the verifier-centric linkability, which means that the service provider decides to link the anonymous authentication transactions depending on the verifier's information. In anonymous authentication with signer-centric linkability, the verifier cannot link if the signer does not want to. Therefore, with signer-centric linkability, the service provider cannot always generate and manage the customer's personalized information.

As mentioned in clause 7.2.1, local linkability is a feature where multiple authentication transactions from the same anonymous user are linked only by a specific service provider to whom the transactions are given; however, other service providers or entities cannot link these transactions. If the signer-centric linkable mechanism is used, other service providers might be able

to link to the signer's intention. Therefore, if a mechanism has a local linkability property, it should have verifier-centric linkability as well.

7.3 Local linkability issues of anonymous authentication mechanisms

7.3.1 Local linkable mechanisms

In anonymous authentication mechanisms based on the traditional group signature, all transactions are not linked. However, [b-Hwang] proposed another group signature called group signature with controllable linkability (CL-GS), which has a new function of controllable linkability. This controllable linkability enables a special verifier which has a linking key to check if two signatures are from the same signer. By controlling the linking key, it is possible to provide local linkability.

In CL-GS, by handling a linking key, it is also possible to make it have signer or verifier-centric linkability. To make it have verifier-centric linkability and local linkability, different linking keys have to be distributed to each verifier. Clause 10.3 of [b-ISO/IEC 20009-2] describes how to achieve local linkability in CL-GS.

7.3.2 Emulating local linkability

In pseudonym-based anonymous authentication mechanisms, all transactions using the same pseudonym are linked. In order to make all transactions not fully linked for local linkability, multiple pseudonyms can be issued to the user. In this case, an individual pseudonym should be used for each service provider. However, multiple pseudonyms would be inconvenient for users where they should manage their pseudonyms directly, as in for example [b-IETF RFC 5636].

This case is analogous to that of anonymous authentication mechanisms with signer-centric linkability. In signer-centric linkable schemes such as DAA or traceable signatures, the user should control linking information whenever he/she accesses the service provider for local linkability. For example, he/she uses the same linking base for the same service provider while he/she uses a different linking base for a different service provider necessarily in DAA. The difference is that multiple pseudonyms are issued by a trustee while signer-centric linking information is generated by the signer.

In an environment where an IdP or a trusted server can manage the multiple pseudonyms for a specific user with SAML, emulating local linkability might be implemented easily without the user's inconvenience. However, the IdP or the trusted server is able to know all the services that the user logs in to automatically. This property may cause a profiling issue, as mentioned in clause 6.1.2.

The mechanisms mentioned in this clause do not provide local linkability but can only emulate it. In emulating, security or privacy may be sacrificed partially. For example, if the customer presents the same pseudonym or linking information to the various service providers by mistake, all transactions will be linked by them. Service providers can generate the global tracking information of the customer by colluding together, which may again cause a profiling issue.

7.4 Anonymous authentication mechanisms and their properties

Table 1 summarizes theoretical bases and properties of the anonymous authentication mechanisms described in clause 6.3.

Table 1 – Anonymous authentication mechanisms and their properties

	Theoretical base	Linkability	Traceability	Remarks
CL-GS	Cryptography (Group public key)	Generally unlinkable (local linkable by controlling linking key)	Traceable by trustee (untraceable with modification)	Standardized in ISO
DAA	Cryptography (Group public key)	Generally unlinkable (local linkable by emulation, signer-centric linkable with linking base)	Untraceable	Standardized in ISO
Traceable signature	Cryptography (Group public key)	Generally unlinkable (local linkable by emulation, signer-centric linkable with signer claiming)	Traceable by trustee (untraceable with modification)	
Ring signature	Cryptography (Ring of multiple public keys)	Generally unlinkable	Untraceable	No trustee, not practical
IETF TAC	Pseudonym	Linkable (local linkable by emulation)	Traceable by trustee	Standardized in IETF
ITU-T SAML	Pseudonym	Linkable (local linkable by emulation)	Traceable by trustee	Online trustee needed for authentication Standardized in ITU-T

8 Requirements of anonymous authentication for subscription-based e-services

This clause deals with two types of requirements of anonymous authentication for e-services. The first type of requirements is for secure authentication, which means that no authorized user should be able to cheat the authentication server. If the authentication mechanism is secure, impersonation or unauthorized access would be impossible. These requirements do not concern privacy threats, but they are necessary for the service provider to be able to authenticate its customers correctly.

The second type of requirements is to prevent privacy threats. In order to overcome the privacy threats, anonymous authentication technology may replace non-anonymous authentication technologies that are based on PII. The core idea is to cut off PII from the other information using anonymous authentication mechanisms. However, the side effects of anonymity should be considered when an anonymous authentication mechanism is applied. The requirements to treat all issues which are described in clauses 6.1 and 6.2 are addressed in clause 8.2.

8.1 Requirements for secure authentication

As an authentication technology, the following requirements should be considered:

- **Authenticity**: The authentication mechanisms should provide a process where the service provider can verify if the authentication transaction is generated from the valid authentication token of the user.
- **Revocation**: There should be a revocation method in the authentication systems to disable an invalid authentication token (e.g., the compromised key or authentication token of an

entity who withdraws the subscription) from further access to the system. In the same way, the anonymous authentication mechanism should include revocation functions.

- **Unforgeability**: Any entity (including the trusted party, if possible) should not be able to forge other's authentication token or transaction.

Authentication schemes which are proven or known as secured by academic or standards organizations generally satisfy the above requirements. For example, anonymous authentication schemes in [b-ISO/IEC 20009-2], [b-IETF RFC 5636], and [b-ITU-T X.1141], etc. also meet these requirements.

8.2 Requirements for anonymity in subscription-based services

8.2.1 Common requirements

Four privacy-related issues are introduced in clause 6. Two of these privacy-related issues are leakage of PII and the profiling issue; both are included in the privacy threats in general e-services. The easy way to solve these issues is to use an anonymous authentication mechanism in the services. This means that the first requirement is "anonymity" to cope with the privacy threats.

However, anonymity has its side effects, as mentioned in clause 6.2. The first side effect is illegal actions by abuse. To deal with or prevent illegal actions, only the authorized user should be able to get the services. This means that confirmation of PII is required before the customer has an anonymous authentication token issued. When issuing the token, the issuer can bind the user's PII and anonymous identifier because the token includes an anonymous identifier. In traceable anonymous services, where an anonymous user who performed an illegal action should be opened, the anonymous identifier and the corresponding PII are extracted from the anonymous transaction using traceable mechanisms.

In untraceable anonymous services, PII should not be extracted using untraceable mechanisms. In this case, illegal actions such as duplicate votes shall be detected and eliminated by the service provider. Duplicate votes are possible in two cases. The first case is when the service provider can issue to the user multiple anonymous authentication tokens. The second case is when the user with one token can generate multiple anonymous authentication transactions which are not linked. In this case, the service provider cannot know if the multiple votes are from the same anonymous identifier or not. To prevent the first case, the verification of the user's PII is required so that two or more anonymous tokens cannot be issued per user. In order to make the second case impossible, with the linkable property, the service provider is required to know which transactions are from the same user.

Therefore, the common requirement against abusing anonymity in traceable and untraceable anonymous services is the "confirmation of PII" in the issuing process of anonymous tokens.

The second side effect of anonymity is that the service provider cannot provide the personalized service. This means that unlinkable anonymous authentication is not suitable for the service. However, fully linkable anonymous authentication is not desirable in the privacy aspect because it leads to profiling. Clause 7.2.1 introduces local linkability which can make the personalized service possible without a profiling issue.

- **Confirmation of PII**: When a user receives an anonymous authentication token, he/she should be confirmed with his PII to prove that he/she has the right to get the token.
- **Anonymity**: In online transactions, the identifiable information of users should be anonymous and should not be exposed to the service providers or unauthorized entities. While user authentication is processed and services are provided normally, it should not be possible to identify the user.
- **Local linkability**: Online service providers need to have linkability to analyse the users' service use patterns, not exceeding their own service domains. Multiple transactions from

different service domains should not be linkable even when the service providers collude. In some services such as e-voting, this property is used to prevent illegal actions such as duplicate voting, etc.

8.2.2 Requirement for traceable anonymous services

In traceable anonymous services, it would be helpful to find out the PII of an illegal user. The issuer knows the user's PII and the corresponding anonymous identifier if the common requirements are implemented. Then another necessary process is to find out the anonymous identifier from the anonymous authentication transaction. Therefore, (conditional) traceability can also be a requirement for traceable anonymous services.

- **Traceability**: In some services, with the anonymity of the users' authentication, there should also be a countermeasure that allows for the identification of persons performing illegal actions. Traces should be performed by one or more trusted parties. When a user is traced, the parties should be able to provide the proof that the traced information is valid.

8.2.3 Requirement for untraceable anonymous services

As mentioned in clause 6.2.1, anonymity should not be cancelled in untraceable anonymous services such as e-voting. Therefore, the anonymous authentication mechanisms should be untraceable and PII of any customer should not be revealed.

- **Untraceability**: In untraceable anonymous services such as e-voting, there should be no means to trace anonymous users from anonymous authentication transactions. This means that the anonymous authentication mechanisms for the services should have the property of untraceability.

8.3 Relationship between the requirements and privacy-related issues

Clause 8.2 describes the requirements that are necessary for privacy. The relationship between the requirements and privacy-related issues is shown in Table 2.

Table 2 – Relationship between the requirements and privacy-related issues

	Privacy threats		**Side effects of anonymity**	
	Leakage of PII	**Profiling issue**	**Illegal actions**	**Impossibility of personalized service**
Confirmation of PII			X (Note 1)	
Anonymity	X	X		
Traceability			X (Notes 1 and 2)	
Untraceability	X (Note 3)			
Local linkability		X	X (Note 1)	X
NOTE 1 – Confirmation of PII should be combined with traceability or local linkability to prevent illegal actions. As a countermeasure against illegal actions, traceable anonymous services require traceability while untraceable anonymous services need local linkability instead of traceability. In the former, an example of which can be e-commerce, the anonymity of illegal users should be cancelled by regulation or law. In the latter, an example of which can be e-voting, all users including illegal users should not be traced. Instead, local linkability can be used because the duplicate voting transactions of the same user will be linked and can be prevented.				

Table 2 – Relationship between the requirements and privacy-related issues

	Privacy threats	Side effects of anonymity
NOTE 2 – Traceability is necessary only in traceable anonymous services. NOTE 3 – Untraceability is necessary only in untraceable anonymous services. In those services, it should be always impossible to find out the customer's PII even if the customer performed illegal actions.		

9 Framework of local linkable anonymous authentication for e-services

Four entities of local linkable anonymous authentication are classified into claimant, verifier, issuer and opener. From among these four entities, the functions of each entity are derived and five processes are illustrated. The adjusting aspects are introduced when local linkable anonymous authentication mechanisms are applied.

9.1 Entities

To satisfy the requirements of anonymous authentication, users should have the valid anonymous authentication tokens. This means that there should be a trusted organization that has the role of issuing an anonymous authentication token for the right user. With the issued tokens, users want to be authenticated anonymously by the service providers. The service providers require the capability of linking the authentication transactions to provide a personalized service to their customers. When any user performs malicious or illegal actions based on anonymity, the service provider requests to open the anonymous user to a trusted organization which has opening authority. Therefore, there should be four entities for subscription-based e-services using local linkable anonymous authentication: the user, the service provider and two trusted organizations of issuing and opening.

There is a claimant and a verifier in the general authentication. A claimant is defined as an entity that is or represents a principal for the purposes of authentication and a verifier as an entity that verifies and validates identity information. The user who is willing to get service from the service providers can be a claimant because the user should prove that he/she has a right privilege for the service. The service provider can be a verifier because it should be able to verify the anonymous authentication transactions from a claimant.

In addition to the two entities of a claimant and a verifier, two more entities are still necessary for the two trusted organizations of issuing and opening. As the first trusted entity, an issuer is defined as 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. The second trusted entity is an opener and is defined as 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.

The basic role of a claimant is to authenticate itself anonymously to a verifier. For this role, there are two functions. One function is to request an anonymous authentication token from the issuer and the other function is to request an anonymous authentication using the issued token.

The role of a verifier is to check if the authentication request from a claimant is valid. A verifier should be able to verify the anonymous authentication transactions which are generated by claimants and to link the verified transactions for the purpose of local linkability. Furthermore, a verifier should be able to request the opening from the opener for dealing with illegal claimants if the authentication mechanism is traceable.

The issuer and the opener are designated entities that have principal roles such as issuing, opening and tracing, which support the claimant's and verifier's roles of anonymous authentication.

The role of the issuer, as a trusted entity, is to issue anonymous tokens to claimants. The issuer should be able to verify PII and any related information which are presented by the claimants and if this information is correctly verified, the issuer should issue an anonymous authentication token including an anonymous identifier. Therefore, the issuer would know the corresponding PII if the anonymous identifier is given to it. In other words, the issuer has the capability of tracing an anonymous identifier. If there is no way to find out the anonymous identifier in an anonymous authentication, the issuer cannot have the tracing capability. This means that the used anonymous authentication mechanism is untraceable.

The role of another trusted entity, the opener, is to open the anonymous identifier of a claimant. For this role, the opener should have the function to compute an anonymous identifier from the presented anonymous authentication transaction. If it is necessary to find out PII, the opener requests that the issuer trace the computed anonymous identifier. There shall be no opener if the used mechanism is untraceable.

A summary of each entity function is shown in Table 3.

Table 3 – Entities and their functions in anonymous authentication framework

Entity	Functions
Claimant	Request anonymous authentication token using PII (step 1-1 in Figure 5) Request authentication (step 2-1 in Figure 5)
Verifier	Verify transaction (step 2-2 in Figure 5) Link the transaction (mechanism dependent) (step 3-1 in Figure 5) Request opening (step 4-1 in Figure 5)
Issuer	Verify PII (step 1-2 in Figure 5) Issue anonymous authentication token (step 1-3 in Figure 5) Trace PII (mechanism dependent) (step 5-2 in Figure 5)
Opener	Request tracing (step 5-1 in Figure 5) Open transaction (mechanism dependent) (step 4-2 in Figure 5)

9.2 Processes among the entities

There are five processes for the local linkable anonymous authentication: anonymous authentication token issuing between the claimant and the issuer, authentication using the issued token between the claimant and the verifier, linking authentication transactions of the verifier, opening anonymous identifier by the opener and tracing the claimant's PII from the anonymous identifier by the issuer.

Figure 5 shows the processes of local linkable anonymous authentication.

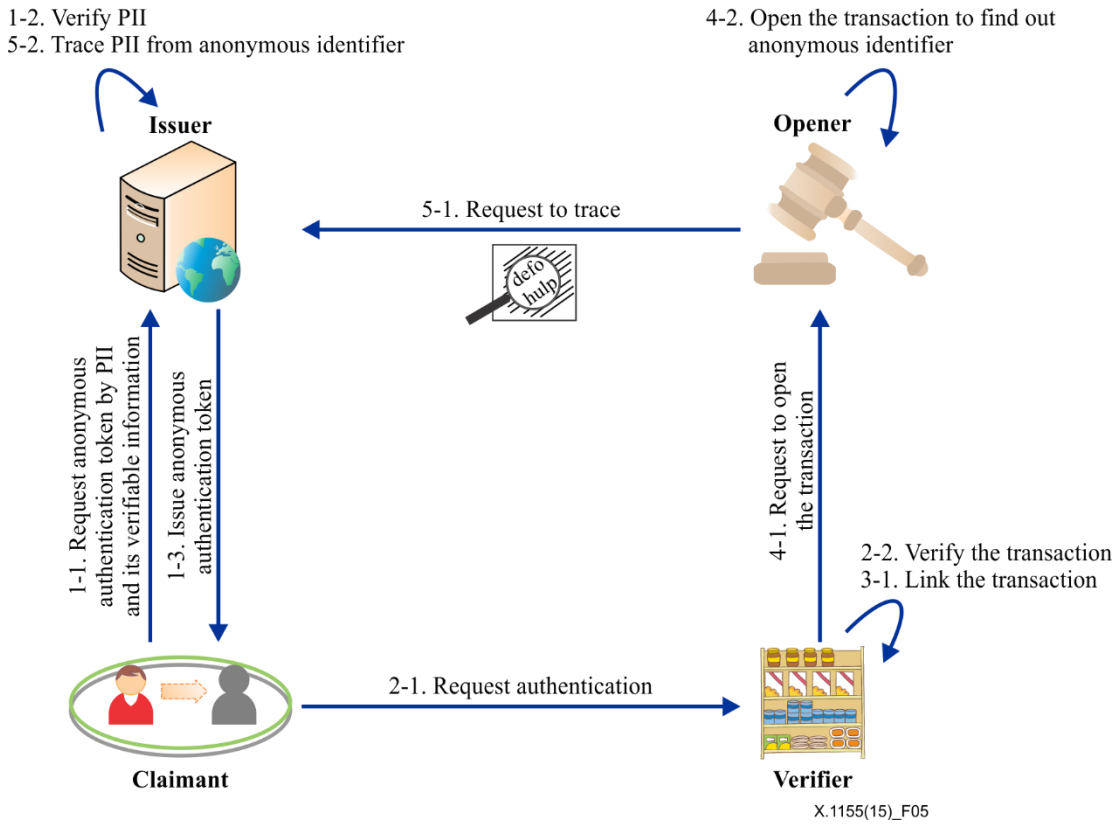

Figure 5 – Processes of local linkable anonymous authentication

The first process (step 1-1, 1-2, 1-3 in Figure 5) in the framework is the issuing of an anonymous authentication token. In the process, the claimant requests an anonymous authentication token by presenting PII and its verifiable information to the issuer for confirmation of PII. The issuer verifies the presented information and generates the anonymous authentication token. Then the issuer submits the token to the claimant. If the used anonymous authentication mechanism has a traceable property, the issuer should keep the anonymous identifier and PII pair in its database for future possible traceability.

The second process (step 2-1, 2-2 in Figure 5) is the anonymous authentication between the claimant and the verifier. The claimant requests authentication for services and generates an anonymous authentication transaction. The verifier checks if the authentication transaction is valid. In this process, the verifier should not be able to know any personally identifiable information of the claimant for anonymity.

The third process (step 3-1 in Figure 5) is linking the transactions by the verifier for local linkability. This process shows if two or more given transactions are from the same claimant or not. This is possible with a cryptographic computation using the verifier's linking key in some anonymous authentication mechanisms, while the transactions can be linked by using the same pseudonym of the same claimant in other mechanisms.

If the mechanism is traceable, the following two processes can exist. In the fourth process of opening (step 4-1, 4-2 in Figure 5), the verifier requests the opener to open the anonymous transaction. Then the opener calculates the anonymous identifier from the transaction using its opening key for traceability. For an untraceable anonymous service, this process should be impossible.

In the fifth process of tracing (step 5-1, 5-2 in Figure 5), the opener sends the identifier to the issuer. The issuer extracts PII from the database in which it kept the identifier and PII pairs.

9.3 Local linkable anonymous authentication mechanisms

9.3.1 Anonymous authentication mechanisms based on group signature

In the mechanisms based on group signature providing local linkability, the verifier should have a linking key. For traceable anonymous services, all of the processes in Figure 5 are necessary.

If these mechanisms should be untraceable for an untraceable anonymous service such as e-voting, the opening key should be removed so that the opening is impossible in the mechanisms. However the opening key is necessary to generate other related public keys and linking keys in the group signature providing local linkability. Therefore the opening key should be removed after the related keys are generated.

One way to remove the opening key is to use a tamper resistant device. First, the opening key is generated in the tamper resistant device. Then, the device calculates the related public keys and linking keys and transmits them to the corresponding entities including the issuer, claimants and verifiers. After completion of the transmission, the device is physically removed. If this process is successful, the opener and steps 4-1, 4-2, 5-1 and 5-2 in Figure 5 could be omitted for untraceable anonymous services.

9.3.2 Pseudonym-based anonymous authentication mechanisms

In pseudonym-based mechanisms such as IETF TAC [b-IETF RFC 5636] or SAML [b-ITU-T X.1141], a pseudonym is provided to a verifier during the authentication process. Consequently, there is nothing to do for opening because the pseudonym is an anonymous identifier by itself. In this case, the verifier and the opener in Figure 5 can be combined into one entity or the verifier can be regarded as having an opening capability.

If a user uses one pseudonym in all authentication transactions in pseudonym-based mechanisms, the mechanisms are "fully linkable". In order to make these mechanisms locally linkable, multiple pseudonyms should be issued for a claimant and one of the pseudonyms should be allocated for one verifier.

The IETF TAC mechanism separates the tracing function to prevent one entity from revealing PII of an anonymous claimant unilaterally. There are two issuers: the blind issuer (BI) which has a function of verifying PII of a claimant, and the anonymity issuer (AI) which issues the anonymous authentication token for the claimant. The two issuers share a special token. When BI verifies a user's PII successfully, a PII verifier issues a valid token to the user which is bound to PII. The user requests an authentication token (TAC) from AI with the special token.

When a claimant with a pseudonym should be traced, AI finds the special token bound to the pseudonym on TAC from the database and requests BI to get PII. BI should not be able to know or compute the token from a pseudonym. Afterwards, BI finds out the corresponding PII of the claimant from the token. Therefore and in the same manner as for mechanisms based on group signature, if AI and BI are physically different entities, neither of them can trace independently and they must cooperate to trace an anonymous claimant.

It is impossible to make pseudonym-based mechanisms untraceable because the opening process cannot be removed.

Appendix I

Use cases

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

I.1 E-commerce use case

With e-commerce services, the users can easily purchase goods, e-contents and services through high speed networks. They can buy books containing political issues, toys which can hint that the buyer has a child, accessories containing religious symbols or luxuries showing the economic power of the buyer. The purchase history can show many kinds of the buyer's personal information. This type of information including the purchase history is gathered and recorded automatically. Moreover, if the information is combined with a real name or a social security number, it would be possible to figure out a specific person's preferences using the databases of multiple service providers. Furthermore, personal information leakage by a malicious hacker is another important threat. If the leaked information contains the user's preferences based on the purchase history, the threat becomes more significant.

To overcome this problem, anonymous authentication is a good solution. Users or customers get their anonymous authentication tokens from a certified issuer. Then the user goes to an e-commerce service where there are some goods the user is interested in and logs in to the service using his/her token. Then the user can buy products without providing his/her personal information.

To be applied to e-commerce, it is desirable that the anonymous authentication mechanism be traceable and locally linkable. Malicious anonymous customers (example: users who use a stolen credit card) should be opened by a special entity. This opening process should be done according to the law or regulations. Moreover, the entity should have the authority to enable it to revoke the malicious customer's anonymity by legal procedure. One example of such an entity is a court of justice.

As mentioned in clause 7.2, unlinkable anonymous authentication does not have a way to identify an e-commerce service provider's customers and be fully linkable when there is a privacy problem. Therefore, local linkability is an important function for e-commerce service providers. They want to manage their customers and provide personalized services, such as mileage point services, coupon services, purchase record page or item recommendation page services. Generally, the number of customers is regarded as an important asset for the e-commerce company.

Figure I.1 shows how local linkable anonymous authentication can be applied to e-commerce services. In step 1-1, the customer should provide PII and its verifiable information to the anonymous token issuer. If the issuer confirms that PII is verified, it generates an anonymous authentication token and sends it to the customer secretly.

In step 2-1, the customer joins the e-commerce service 1 anonymously to be a member of this service. At the same time, the customer should send the anonymous authentication transaction to the service provider. In step 2-2, the service provider verifies the transaction and checks if the customer is already a member or is not using the local linking algorithm. After joining, the customer can log into the service and purchase some goods (step 2-3). In step 2-4, the provider also verifies the log-in transaction and tries to find out which member is the anonymous customer.

While the customer is purchasing the goods, the payment procedure is done simultaneously (step 2-5). PII might be inferred through some kind of payment information. For that reason, the payment information would be provided to the e-commerce service provider in an encrypted form. This situation can be repeated in the same manner in the delivery procedure (steps 2-6 and 2-7). If

the goods are not the physical things (for example, digital contents like a file with an audio recording), steps 2-6 and 2-7 can be omitted. The payment and delivery procedures are outside the scope of this Recommendation.

If the customer wants to log in again to check his/her mileage, the anonymous authentication transaction should be made, verified and linked locally in steps 2-8 and 2-9. These steps are the same as steps 2-3 and 2-4. In step 2-10, the customer will get his personalized page including his mileage, purchase history, etc.

When a malicious user abuses the anonymity to perform a fraud or make an illegal purchase (step 3-1), the service provider can request to open the anonymous authentication transaction (step 3-2). Then the court of justice opens the transaction to find out PII of the criminal by a lawful procedure (step 3-3).

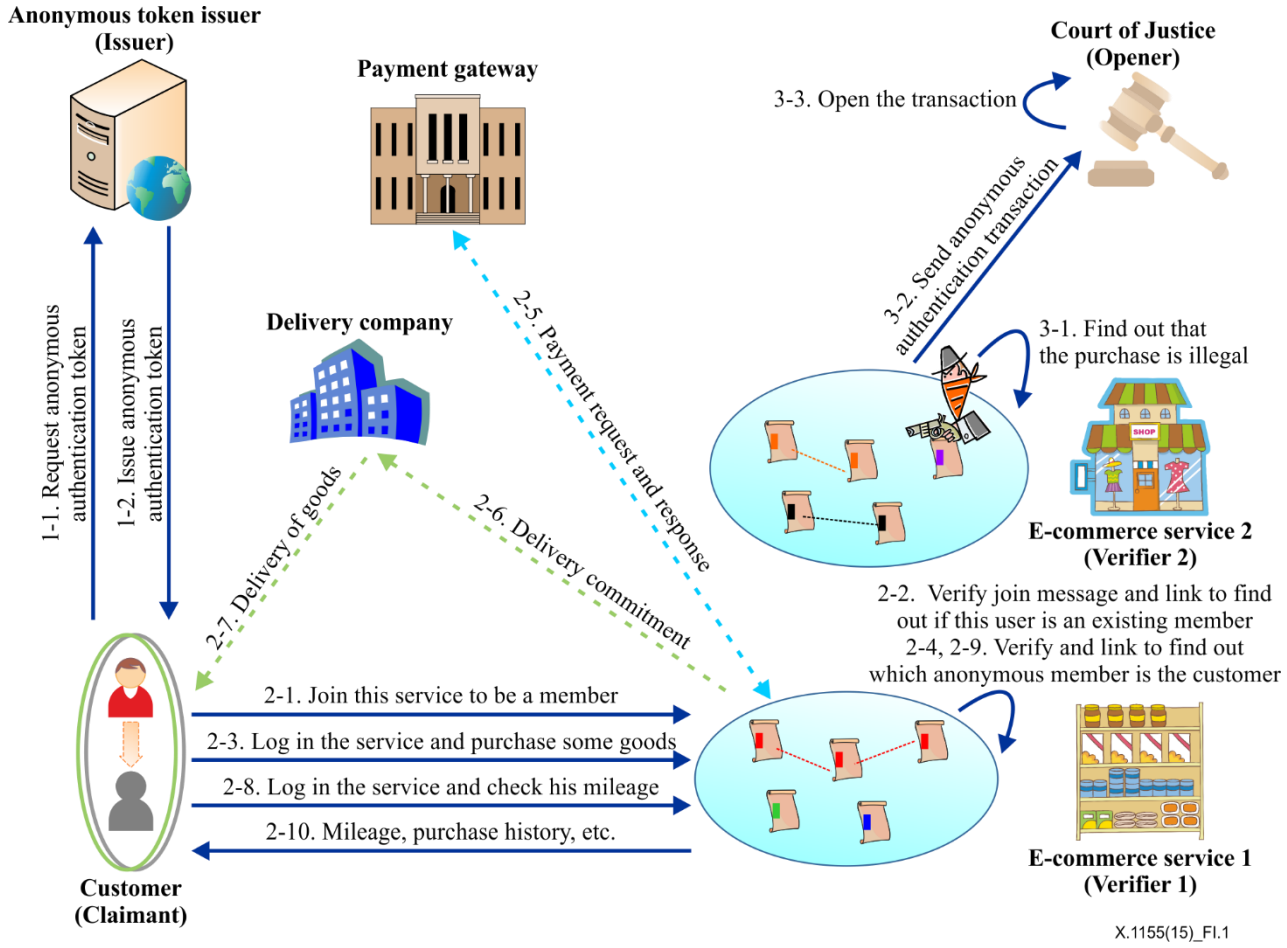

Figure I.1 – E-commerce use case

I.2 E-voting use case

A voting system is used as a means through which voters make a choice among many options. For example, in an election or policy referendum, a voting system is generally used in most countries. A similar system can be applied for a survey of public opinion or for gathering statistical information.

The basic voting principles include secret balloting and "one person, one vote". Secret balloting means that a voter's choice should be anonymous. This principle is very important to providing privacy to all voters. "One person, one vote" means that all voters have equal rights to make a political decision. To maintain this principle, each voter should be individually identified, and the voting system should provide ways to find out duplicate votes or illegal votes.

Therefore, these principles should be kept in an electronic voting system or e-voting system. For secret balloting, anonymous and untraceable authentication can be a good solution. If the voting transaction is generated using an anonymous authentication mechanism, all voting transaction data could be opened to the public. Even if all the voting records, including the transaction data, are opened, there is no means of knowing who voted which option. In this case, all votes can be recorded more easily and accurately.

However, anonymity can be a hurdle to providing the principle of "one person, one vote". More precisely, for the unlinkable anonymous authentication mechanism there is no way to detect duplicate votes. The confirmation of PII in the issuing process guarantees that one voter has only one anonymous authentication token. With linkability, the principle, "one person, one vote", could be maintained. The property of linkability means that duplicate or multiple votes by a token of one voter can be detected by the voting server using a linking algorithm.

Another benefit of linkability in the e-voting system is that any voter can check his/her choice and change it in the voting period. In this scenario, a person, who already voted to generate a voting transaction, can make a transaction to request his voting result and another transaction to change his choice. Then the voting server tries to check if the transactions are from the same voter by using a linking algorithm. After the successful linking, the server processes the transaction of the voter's change request.

For this reason and benefit, the linkable property is important for e-voting. In particular, local linkability is better for the e-voting scenario than full linkability. If the authentication is fully linkable, the voter can be linked in voting server 1 and 2. It is then known which candidates the voter selected in voting server 1 and 2, respectively, though there is no way to know or identify who the voter is. This is not deemed suitable because the political bias or propensity of a voter can be tracked easily. For example, a certain voter who selected a candidate of a political party A in voting server 1 may be known to support the revised regulation for public health service in voting server 2. This kind of example can hurt the privacy of the voter through tracking. If the voting data are accumulated over the long term, the voter is even identified to a specific person in the real world. Local linkability, not full linkability, should be applied to e-voting services, especially where privacy is very important.

Figure I.2 shows how local linkable anonymous authentication can be applied to the e-voting system. In step 1-1, the voter should provide PII and its verifiable information to the voting management system. If the system confirms that the voter's PII is verified and the voter has the right to vote, the system generates an anonymous authentication token and sends it to the voter secretly.

In steps 2-1, 2-3 and 2-6, the voter should make authentication transactions in the requests for the verifier to check if the requests are authorized and are from the same voter. In step 2-2, the voting server should verify the voting transaction and check if this vote is the initial one and not a duplicate one. In steps 2-4 and 2-7, the server should also verify the request transaction and find out which vote is from this voter using a linking algorithm. If the request is correct, then the system processes it and sends the result in steps 2-5 and 2-8. For secret balloting, there should be no trusted entity which has open and trace authority.

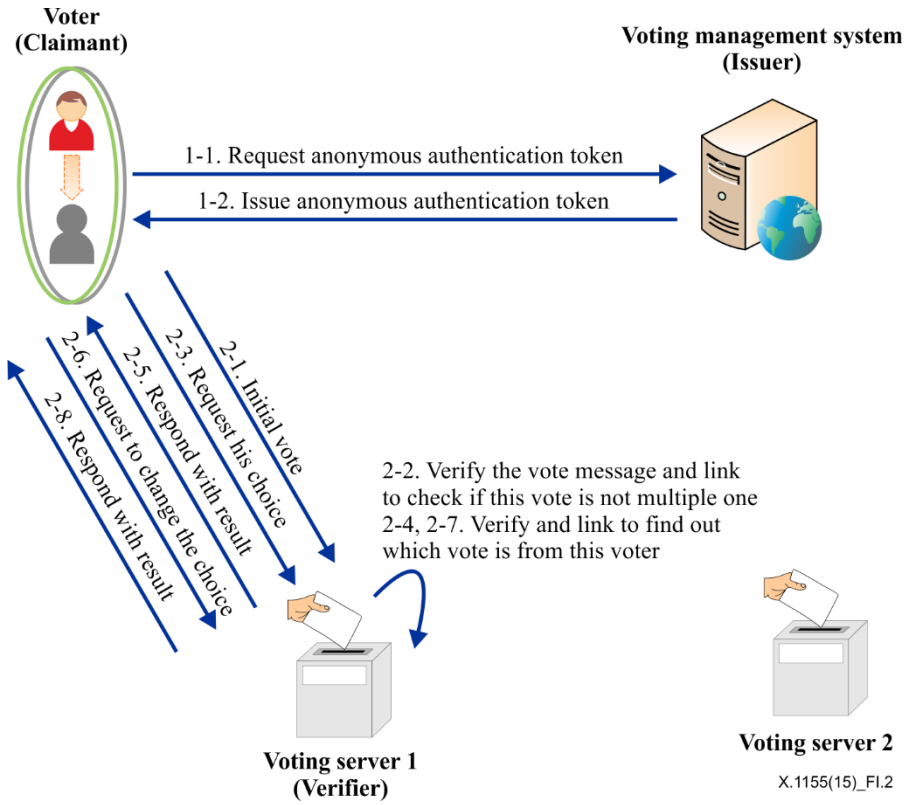

Figure I.2 – E-voting use case

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.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

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

[b-ISO/IEC 9798-1] ISO/IEC 9798-1:2010, *Information technology – Security techniques – Entity authentication – Part 1: General*.

[b-ISO/IEC 20008-2] ISO/IEC 20008-2:2013, *Information technology – Security techniques – Anonymous digital signatures – Part 2: Mechanisms using a group public key*.

[b-ISO/IEC 20009-1] ISO/IEC 20009-1:2013, *Information technology – Security techniques – Anonymous entity authentication – Part 1: General*.

[b-ISO/IEC 20009-2] ISO/IEC 20009-2:2013, *Information technology – Security techniques – Anonymous entity authentication – Part 2: Mechanisms based on signatures using a group public key*.

[b-ISO/IEC 29191] ISO/IEC 29191:2012, *Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication*.

[b-IETF RFC 5636] IETF RFC 5636 (2009), *Traceable Anonymous Certificate*.

[b-Brickell] Brickell, E., Camenisch, J., and Chen, L. (2005), *The DAA scheme in context*, Trusted Computing (Mitchell C. ed.), The Institute of Electrical Engineers.

[b-Canard] Canard, S., and Traoré, J. (2003), *On Fair E-Cash Systems Based on Group Signature Schemes*, ACISP 2003, Vol. 2727 of LNCS, pp. 237-248.

[b-Chaum] Chaum, D., and van Heyst, E. (1991), *Group signatures*, EUROCRYPT 1991, Vol. 547 of LNCS, pp. 257-265.

[b-Hwang] Hwang, J., Lee, S., Chung, B., Cho, H., and Nyang, D. (2011), *Short Group Signatures with Controllable Linkability*, LIGHTSEC 2011, pp. 44-52.

[b-Kiayias] Kiayias, A., Tsiounis, Y., and Yung, M. (2004), *Traceable signatures*, EUROCRYPT 2004, Vol. 3027 of LNCS, pp. 571-589.

[b-Rivest] Rivest, R., L., Shamir, A., and Tauman, Y. (2001), *How to leak a secret*, ASIACRYPT 2001, Vol. 2248 of LNCS, pp. 552-565.

[b-Traoré] Traoré, J. (1999), *Group Signatures and Their Relevance to Privacy-Protecting Off-Line Electronic Cash Systems*, ACISP 1999, Vol. 1587 of LNCS, pp. 228-243.

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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016