International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1152

(05/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Secure end-to-end data communication techniques using trusted third party services

Recommendation ITU-T X.1152

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1152

Secure end-to-end data communication techniques using trusted third party services

Summary

Recommendation ITU-T X.1152 defines basic interfaces, interactions and security considerations for secure end-to-end data communication using on-line trusted third party (TTP) services.

This Recommendation also identifies online TTP services which can be used to support secure end-to-end data communication between two entities.

Source

Recommendation ITU-T X.1152 was approved on 29 May 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

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/.

CONTENTS

Page

Recommendation ITU-T X.1152

Secure end-to-end data communication techniques using trusted third party services

1 Scope

This Recommendation defines basic interfaces, interactions and security considerations of online trusted third party (TTP) services for secure end-to-end data communication.

This Recommendation also identifies online TTP services which can be used to support secure end-to-end data communication which is a connection-oriented communication between two entities with no eavesdropping, injection and modification of data, unauthorized access and repudiation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is published regularly. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

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

[ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 audit trail [ITU-T X.800]: Data collected and potentially used to facilitate a security audit.

3.1.3 authentication [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.

3.1.4 authorization [ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.5 availability [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.6 certification service [b-ITU-T X.843]: The service of creating and assigning certificates performed by a CA.

3.1.7 confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

3.1.8 credentials [ITU-T X.800]: Data that is transferred to establish the claimed identity of an entity.

3.1.9 directory service [b-ITU-T X.843]: A service to search and retrieve information from a catalogue of well defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses, etc. An example is provided by a directory service conforming to Rec. ITU-T X.500.

3.1.10 eavesdropping [ITU-T X.1121]: Anonymous attackers can actively intercept transmitted data, causing a leakage of data.

3.1.11 electronic digital archiving service [ITU-T X.842]: The electronic digital archiving service is a service provided by a document recorder, at which electronic documents are registered for safekeeping and for retention as a permanent record. The archiving of electronic documents in encrypted form may be required in some instances, especially where the data is highly sensitive and requires extra protection.

3.1.12 electronic notary public service [ITU-T X.842]: Notary public services are high level services that make use of a number of basic services such as time stamping, certification, directory service, digital archiving and non-repudiation. In principle a document will be given to the TTP, and the TTP attests or certifies this document by use of digital signatures or some other means. Part of this service may be a directory service, where the information, such as formerly certified documents, may be retrieved from a database or directory.

3.1.13 injection and modification of data [ITU-T X.1121]: This occurs when an unauthorized entity inserts, changes or deletes information transmitted between a mobile terminal and an application server. The unauthorized entity could be a person, a program, or a computer.

3.1.14 integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.15 key distribution service [ITU-T X.842]: The purpose of a key distribution service is to distribute keys securely to authorized entities. Depending on the TTP's security policy, keys may have to be forwarded to other TTP services, e.g. a directory service. These services could be provided by the same or another TTP.

3.1.16 key generation service [ITU-T X.842]: This service is invoked to generate keys in a secure way for a particular cryptographic algorithm.

3.1.17 key management [ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.18 on-line TTP service [ITU-T X.842]: The TTP is involved in all first time secure exchanges between the entities. However, the TTP is not required for follow-up exchanges and is not positioned in the communication path between the entities.

3.1.19 repudiation [ITU-T X.1121]: This attack occurs when a sender or receiver denies the fact of having transmitted or received a message, respectively.

3.1.20 security association [b-ITU-T X.803]: A relationship between two or more entities for which there exist attributes (state information and rules) to govern the provision of security services involving those entities.

3.1.21 security domain [b-ITU-T X.803]: A set of elements, a security policy, a security authority and a set of security relevant activities in which the set of elements are subject to the security policy, administered by the security authority, for the specified activities.

3.1.22 security policy [ITU-T X.800]: The set of criteria for the provision of security services (see also identity-based and rule-based security policy).

3.1.23 time stamping service [ITU-T X.842]: The time stamping service seals a digital document by cryptographically binding a trusted time to it (typically to a hash representation of it called "message digest" or "message imprint"), thus providing a means to detect any modification, such as backdating and avoid replay attacks or other forgeries.

3.1.24 trusted third party [b-ITU-T X.810]: The trusted third party is an organisation or its agent that provides one or more security services, and is trusted by other entities with respect to activities related to these security services.

3.1.25 unauthorized access [ITU-T X.1121]: This threat occurs when an illegal entity gains access to an application server by masquerading as a real mobile user.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 certified credential: Certified credential is the credential that is authorized by TTP.

3.2.2 control path: Control path is the route between one entity and TTP to control the secure data communication path.

3.2.3 credential mapping service: Credential mapping service is a TTP service that translates an entity's credential for one security domain to the entity's credential for another security domain.

3.2.4 location service: Location service is a TTP service that provides information with regard to the current location of an entity on the network.

3.2.5 peer entity: The peer entity is the entity with which an entity performs secure end-to-end data communication.

3.2.6 policy determination service: The policy determination service is a TTP service that determines security protocols and/or algorithms that are used for data confidentiality and/or data integrity in data transmission phase.

3.2.7 presence service: Presence service is a TTP service that provides availability information of an entity.

3.2.8 secure data communication path: Secure data communication path is the route between two entities to exchange application data between two entities with no eavesdropping, injection and modification of data, unauthorized access and repudiation.

3.2.9 translated credential: Translated credential is a kind of certified credential that belongs to a security domain and is translated from another credential, which belongs to another security domain, by credential mapping service.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

App	Application
CA	Certification Authority
IP	Internet Protocol
MAC	Message Authentication Code
SA	Security Association
SCS	Secure Communication Service

TLS	Transport Layer Security
TTP	Trusted Third Party
URI	Uniform Resource Identifier
VPN	Virtual Private Network

5 Convention

None.

6 TTP services for secure end-to-end data communication

There are various security requirements for data communication as described in [ITU-T X.800], [ITU-T X.805], [ITU-T X.1121] and other security related ITU-T Recommendations. In addition, there are many kinds of security mechanisms/protocols to satisfy these security requirements.

Nowadays, security is an essential and important function for data communication. Basically, each communication layer shall implement necessary security functions. Many designers have designed many secure communication protocols. However, it is inefficient and difficult for all applications to implement all security functions.

Therefore, it is very useful that the network or a trusted third entity on the network (hereafter referred to as "TTP") perform essential (or minimal) security functions on behalf of applications. Although [ITU-T X.842] defines major security services provided by TTP, there is no concrete description as to which TTP services should be used or how to be used when applications perform secure communication.

The purpose of this Recommendation is to define basic interfaces and interactions with online TTP services used for secure end-to-end data communication which is a connection-oriented communication between two entities with no eavesdropping, injection and modification of data, unauthorized access and repudiation. Moreover, this Recommendation also aims to define online TTP services to support the secure end-to-end data communication between two entities.

7 System model

Figure 1 is the system model defined in this Recommendation.

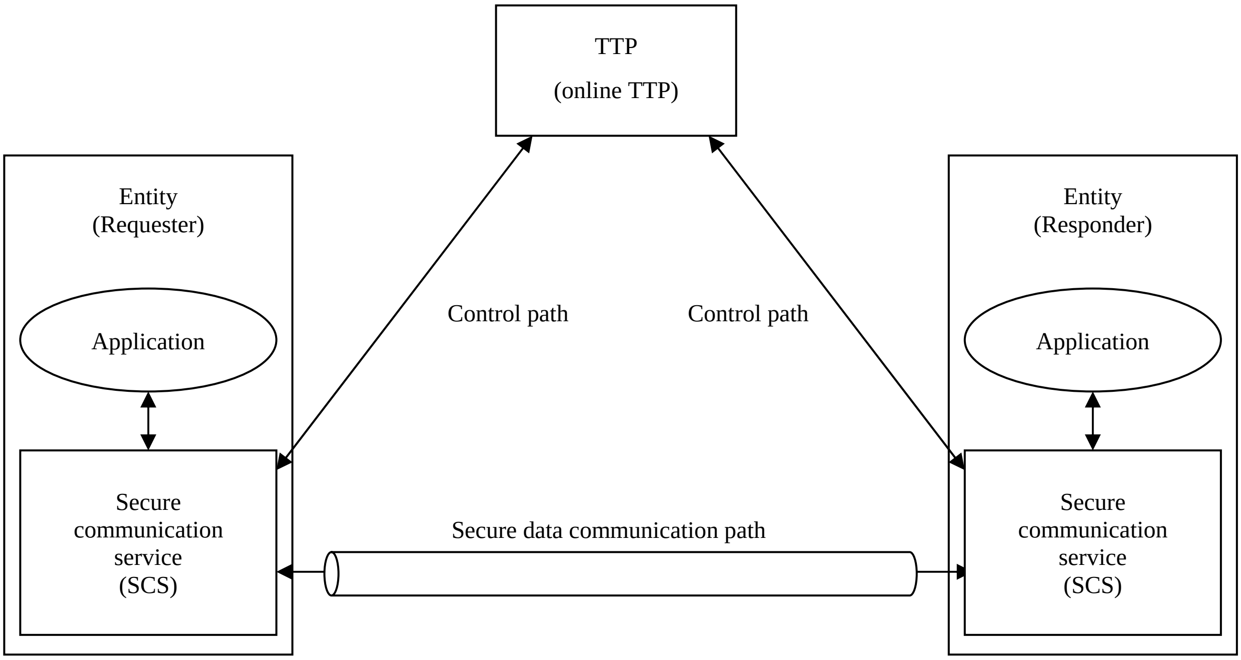

Figure 1 – Secure end-to-end data communication based on online TTP services

Figure 1 shows a TTP (online TTP), which provides some security services, and two entities. Each entity has an application and a secure communication service (SCS), which holds a control path with the TTP and a secure data communication path with the peer entity's SCS to provide secure end-to-end data communication to the application.

It is noted that these two entities play different roles in this connection-oriented communication: one entity is the requester of secure end-to-end data communication, and another entity is the responder to secure end-to-end data communication. Hereafter, the requester entity is described as "Requester" and the responder entity is described as "Responder".

8 Processes of a secure end-to-end data communication

It is important to identify what security functions are performed during secure end-to-end data communication to define what and how TTP services are used for secure end-to-end data communication.

This clause breaks the secure end-to-end data communication between two entities down into three phases: establishment, data transmission and termination, and describes which security functions are performed during each phase.

NOTE – Certain secure communication might not perform all of processes described below.

8.1 Establishment phase

Establishment phase of secure end-to-end data communication is the phase to set up a secure data communication path to transmit application data between two entities.

Establishment phase (almost sequentially) consists of the following processes:

- Identification process
- Authentication process
- Authorization and access control process
- Policy determination and distribution process

8.1.1 Identification process

The identification process is a process to identify the peer communication entity for later processes (authentication, authorization, etc.). In this process, the entities exchange their credentials. In some cases, the entities exchange their "certified" credentials, which are credentials authorized by the TTP, to identify the peer entity. Public key certificate is one example of certified credentials.

This process may also contain a process retrieving current location of the peer entity or a process checking the availability of the peer entity.

8.1.2 Authentication process

The authentication process is a process to verify whether or not the peer entity is the legal owner of the credential retrieved in the identification process. In this process, the entities exchange authentication information, such as digital signature or password.

For example, when public key certificate is used as credential, one entity verifies the digital signature made by a private key corresponding to a public key contained in the communication peer entity's public key certificate. Also, the entity discovers the certification path from its trust anchor to the peer entity, and checks the validity of all certificates containing the constructed certification path.

8.1.3 Authorization and access control process

The authorization and access control process is a process to examine that both entities have enough privilege to communicate with each other and to control the secure data communication path establishment. In this process, the entities may exchange authorization information.

In some cases, the entities exchange their attribute certificates and check whether the communication peer entity's attribute meets access conditions (for example, the user of the peer entity must be over 13 years old to receive PG13 contents delivered).

8.1.4 Policy determination and distribution process

The policy determination and distribution process is a process for two entities to determine and share security associations for data transmission phase. To prevent eavesdropping, injection and modification of data, unauthorized access and repudiation, the security association might contain security protocol and security settings of the protocol, which could be encryption algorithm, message authentication algorithm, and session keys for these algorithms, etc., for example.

8.2 Data transmission phase

Data transmission phase of secure end-to-end data communication is the phase to transmit application data in which the security associations shared during establishment phase are enforced.

To prevent eavesdropping, injection and modification of data, unauthorized access and repudiation, the following security functions are performed concurrently during data transmission phase:

- Data confidentiality process
- Data integrity process
- Audit trail process

8.2.1 Data confidentiality process

Data confidentiality process is a process to transmit application data with confidentiality.

In many cases, the sender encrypts application data with a session key that is a shared secret during the policy determination and distribution process, and the receiver decrypts application data with the same shared secret.

The data encryption with shared secret prohibits not only eavesdropping but also unauthorized access because the peer entity who does not have the shared secret cannot communicate with the entity.

8.2.2 Data integrity process

Data integrity process is a process to transmit application data with integrity.

In many cases, message authentication code (MAC) or digital signature is used for this purpose.

For example, when MAC is used, the sender generates a MAC from application data and a session key that is a shared secret during the policy determination and distribution process, and sends the application data with the generated MAC. The receiver verifies the received MAC (i.e., the receiver generates a MAC from the received application data and compares it with the received MAC).

Data integrity process prohibits the injection and modification of data.

8.2.3 Audit trail process

Audit trail process is a process to generate a collection of data for secure audit to prohibit repudiation.

8.3 Termination phase

Termination phase of secure end-to-end data communication is the phase to delete the secure data communication path set-up during the establishment phase.

9 Online TTP services to support secure end-to-end data communication

This clause describes which TTP functions are used for each of the processes described above.

9.1 TTP services for establishment phase

9.1.1 TTP services for identification process

In the identification process, one entity should interpret the credential retrieved from the peer entity. In the case that two entities belong to different security domains, the peer entity's credential has to be translated to the form which can be interpreted via the credential mapping service.

There are two types of credential mapping services: for the entity or for the peer entity.

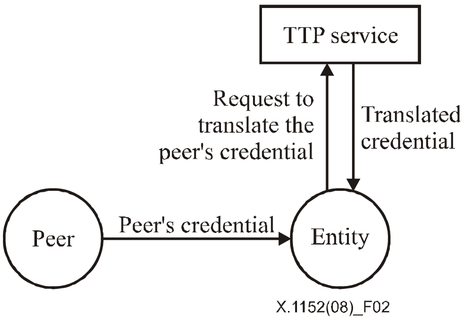

Figure 2 – Online credential mapping service for the entity

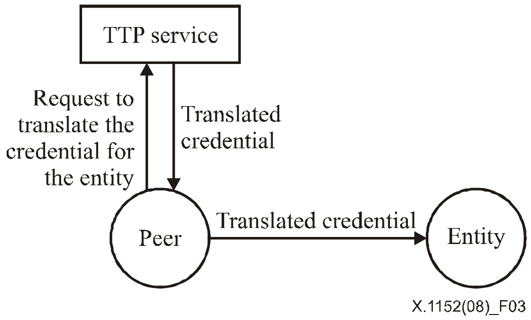

Figure 3 – Online credential mapping service for the peer entity

In Figure 3 above, "translated credential" is a kind of certified credentials. Therefore, other TTP services, such as certificate management service and directory service, can be used to issue and retrieve certified credentials which contain certificates.

In addition, the entity, who tries to have a secure communication with the peer entity, may use the TTP service that manages current location of the peer entity (location service) to retrieve the current location of the peer entity or the TTP service that manages presence of the peer entity (presence service) to check the availability of the peer entity.

9.1.2 TTP services for authentication process

In the authentication process, the authentication service can be used to verify the peer entity's credential on behalf of the entity. This service can also be used to verify the validity of the peer entity's credential if the credential is a certified credential.

The authentication service can be achieved as online TTP service.

9.1.3 TTP services for process of authorization and access control

In the authorization and access control process, directory service can be used to manage and provide one entity's access conditions and/or the communication peer entity's privileges. The entity retrieves this information from the directory service and makes access decision.

Access control service can be used for access decision on behalf of the entity.

9.1.4 TTP services for process of policy determination and distribution

In the policy determination and distribution process, key management service, especially key generation service and key distribution service, can be used to share the session key.

Other TTP services, such as policy determination service, can be used to determine the security association (security protocols and algorithms for data confidentiality and/or data integrity) in the data transmission phase.

9.2 TTP services for data transmission phase

9.2.1 TTP services for data confidentiality process

There are no online TTP services for the data confidentiality process.

9.2.2 TTP services for data integrity process

There are no online TTP services for the data integrity process.

9.2.3 TTP services for audit trail process

For the audit trail process, time stamping service, non-repudiation service and/or electronic notary public service (especially, evidence generation service and/or evidence storage service) can be used.

9.3 TTP services for termination phase

To avoid reply attack or unexpected information leakage, reuse of the same security associations should not be allowed. Therefore, key management services might be used to destroy the security associations used in the communication and to ensure no reuse of the same security associations.

To make audit trails, electronic notary public service (especially, evidence generation service and/or evidence storage service) may be used.

9.4 Possibilities of online TTP services to support secure end-to-end data communication

Table 1 shows a summary of the TTP services that can be used in each process of secure end-to-end data communication.

Table 1 – Possibilities of using online TTP services in secure end-to-end data communication

Processes of secure communication		Possible online TTP services
Establishment	Identification	Certificate management service, Directory service, Credential mapping service, Location service, Presence service
	Authentication	Authentication service
	Authorization and access control	Directory service, Access control service
	Policy determination and distribution	Key management service (Key generation service, Key distribution service), Policy determination service
Data transmission	Data confidentiality	None
	Data integrity	None
	Audit trail	Time stamping service, Non-repudiation service, Electronic notary public service, Electronic digital archiving service
Termination		Key management service, Electronic notary public service

9.5 Integration of TTP services

As mentioned above, there are many possible TTP services for secure end-to-end data communication. In order to use many TTP services, the entities have to access each TTP service, interact with each TTP service to establish a secure communication session, and manage the state of the secure communication session one by one.

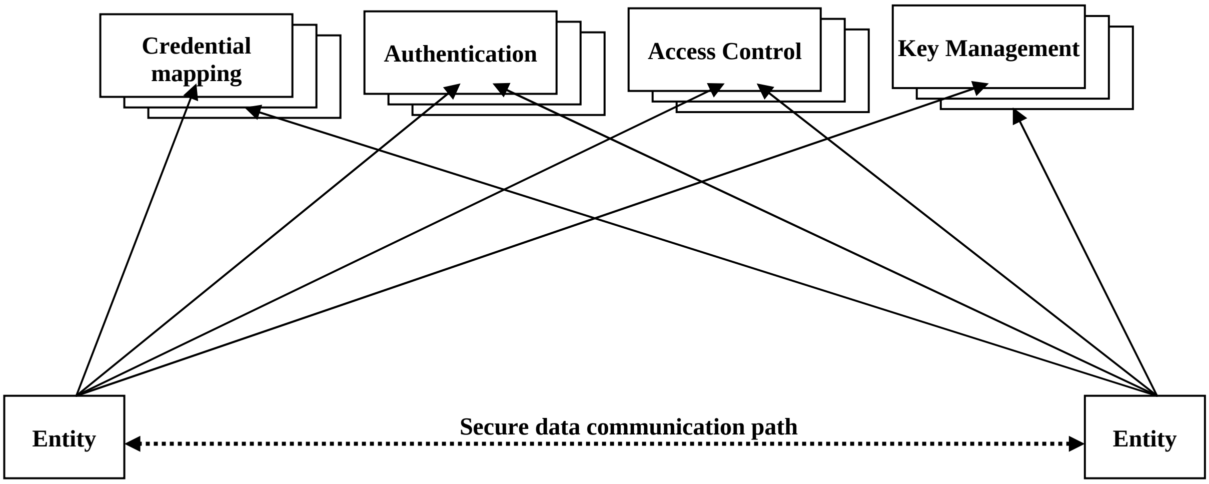

Figure 4 – Example of accessing each TTP service one by one

To reduce cost, it is useful to introduce a service that integrates multiple TTP services and manages the states of these secure end-to-end data communications called "secure session control service".

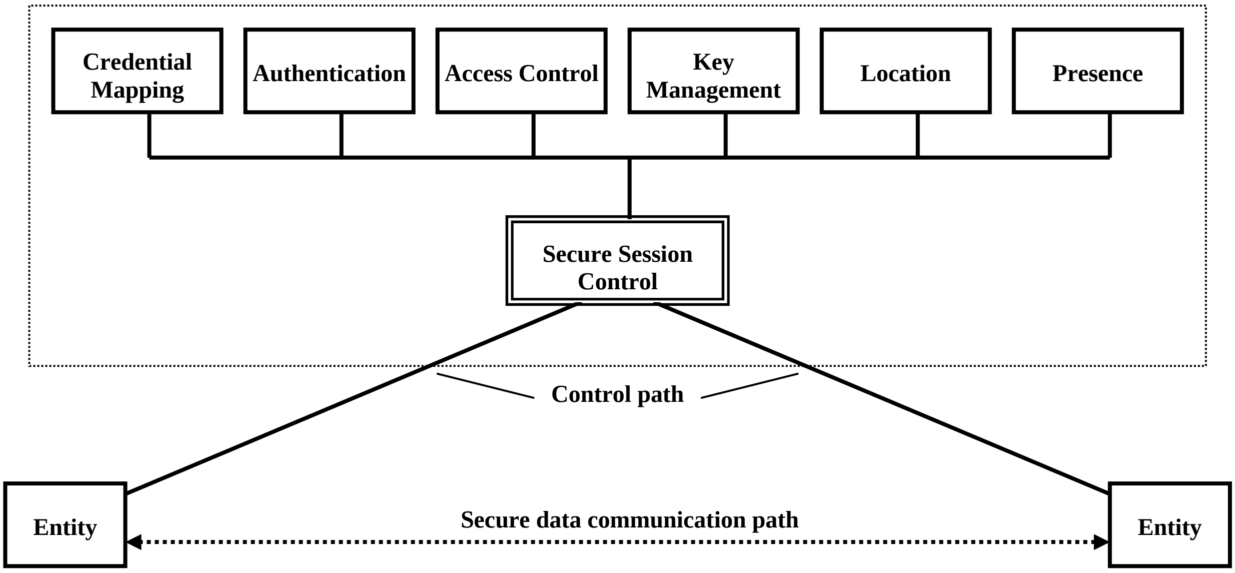

Figure 5 – Example of secure session control service

For example, the secure session control service may integrate TTP services related to the establishment phase (e.g., credential mapping service, authentication service, access control service, key management service, location service and presence service), unifies all accesses from entities, transforms request/response messages from one TTP service to another, and manages the states of these secure end-to-end data communications between entities.

10 Basic interfaces for secure end-to-end data communication based on online TTP

This clause describes the basic interfaces for the secure end-to-end data communication in Figure 1. There are three types of interfaces between components: Requester-TTP interface, Responder-TTP interface and Requester-Responder interface. In addition, there are three types of internal interfaces within component: TTP internal interface, Requester internal interface and Responder internal interface.

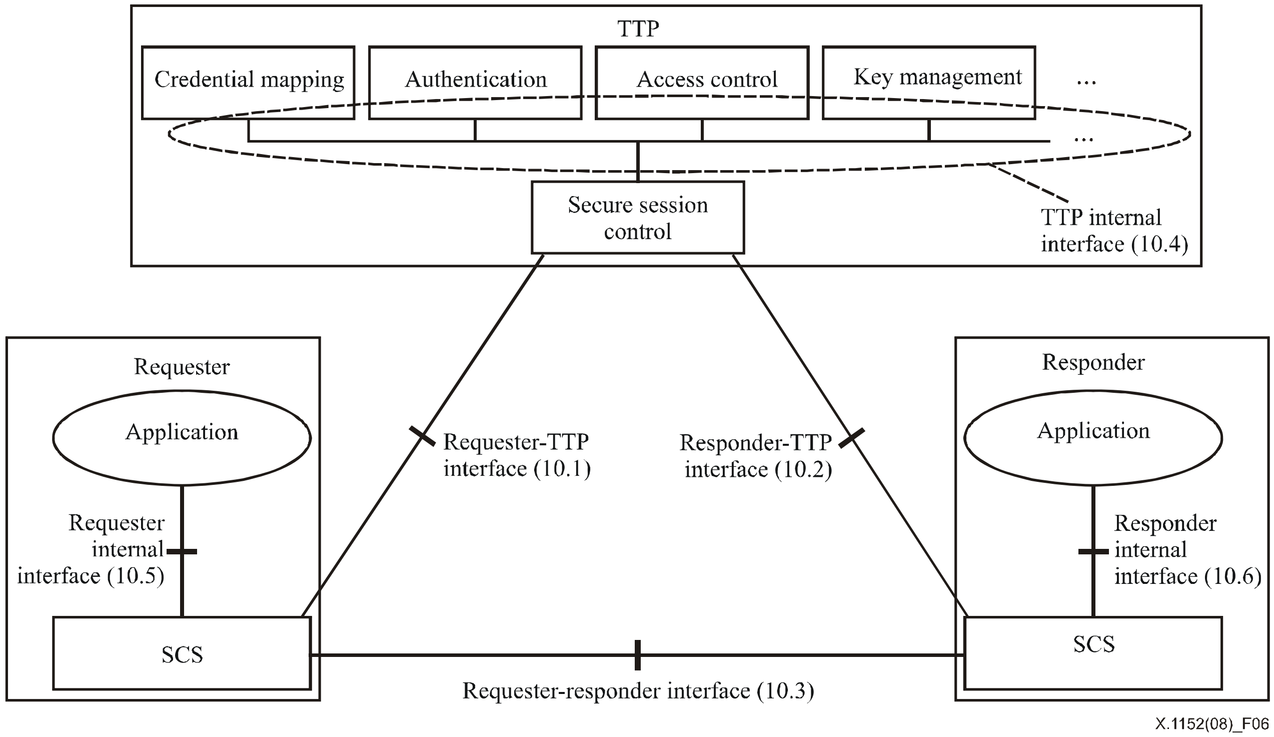
TTP
Credential mapping
Authentication
Access control
Key management
...
...
Secure session control
TTP internal interface (10.4)
Requester
Application
Requester internal interface (10.5)
SCS
Requester-TTP interface (10.1)
Responder-TTP interface (10.2)
Responder
Application
Responder internal interface (10.6)
SCS
Requester-responder interface (10.3)
X.1152(08)_F06

Figure 6 – Basic interfaces for the secure end-to-end data communication based on online TTP

10.1 Requester-TTP interface

Requester-TTP interface is the interface between the Requester and TTP where TTP authenticates the Requester and the Requester requests for TTP to control the secure data communication path between the Requester and the Responder, and to make audit trails of data transmission.

10.2 Responder-TTP interface

Responder-TTP interface is the interface between the Responder and TTP where TTP authenticates the Responder and sends the Responder the Requester's request to control the secure data communication path, and the Responder requests for TTP to make audit trails of data transmission.

10.3 Requester-Responder interface

Requester-Responder interface is the interface between the Requester and the Responder, where the Requester and the Responder exchange protected application data through the secure data communication path that was set up by TTP.

10.4 TTP internal interface

TTP internal interface is the interface within TTP where one TTP service communicates with other TTP services to handle messages from the Requester or the Responder.

Example:

– the interface for authentication service to resolve credential of one entity to handle authentication request message;

– the interface for access control service to retrieve an entity's attribute from presence service to handle establishment request message.

10.5 Requester internal interface

Requester internal interface is the interface between the application and the secure communication service in the Requester, where the application sends/receives application data to/from the application on the Responder.

In addition, some applications might request secure communication service to control the secure end-to-end data communication path with the Responder and to make audit trails of data transmission.

10.6 Responder internal interface

Responder internal interface is the interface between the application and the secure communication service in the Responder, where the application sends/receives application data to/from the application on the Requester.

11 Basic interactions for secure end-to-end data communication based on online TTP

This clause describes basic interactions for secure end-to-end data communication in Figure 1 along the following scenario:

i) *Establishment of control path*

At the beginning, the Requester and the Responder each establishes a control path with TTP respectively.

During the establishment of control path, TTP performs the identification process and the authentication process on behalf of both entities.

ii) *Establishment of secure data communication path*

After establishment of the control path, the Requester starts to establish a secure data communication path with the Responder.

During the establishment of secure data communication path, TTP performs the authorization and access control process and the policy determination and distribution process on behalf of both entities.

iii) *Secure data transmission*

Once the secure data communication path between the Requester and the Responder is established, data (application data) is transmitted (exchanged) via the secure data communication path between the Requester and the Responder.

During the secure data transmission, the Requester and the Responder perform the data confidentiality process and the data integrity process.

iv) *Audit trail creation*

During the secure data transmission, the Requester or the Responder may request TTP to create audit trails of data transmission.

During the audit trail creation, TTP performs the audit trail process on behalf of both entities.

v) *Termination of secure data communication path*

After data transmission is finished, the Requester (or the Responder) starts to terminate the secure data communication path between the Requester and the Responder.

During the termination of secure data communication path, the Requester and the Responder perform the termination phase.

vi) *Termination of control path*

After all data transmission is finished, the Requester and the Responder each terminates its control path with TTP respectively.

Because i) and vi) are entity level granularity processes, i) and vi) are performed only once. However, because ii), and v) are communication level granularity processes, ii) and v) may be performed several times if the Requester communicates with the Responder several times in the scenario above.

11.1 Preconditions

Before describing basic interactions, the preconditions for secure end-to-end data communication based on online TTP are described in this clause.

11.1.1 Preconditions for identification

In the case that various applications with different credential structures run on a SCS, credential mapping is required for the identification process. Therefore, TTP will maintain relations between one credential in one security domain and another credential in another security domain.

11.1.2 Preconditions for authentication

For the authentication process, both entities are certified by TTP or an external certification service. In the case that both entities are certified by TTP, each entity retrieves and stores its own TTP certificate.

In the case that external certification service is used, both entities and TTP trust the external certification service that certifies the entities. For example, in the case of using PKI in the external certification service, a certain CA may certify each entity (or user of entity) and TTP, and will issue a certificate for them. In addition, each entity retrieves and stores its own CA certificate, and TTP retrieves and stores its own CA certificate as well.

11.1.3 Preconditions for authorization

For authorization, access control service may maintain a set of attributes and access policies of each entity.

11.1.4 Preconditions for policy determination

For policy determination, key management service may maintain a set of policies for secure end-to-end data communication, according to available protocols and/or algorithms of each entity.

11.2 Establishment of control path

To establish the control path between one entity and TTP, the following interactions are performed.

1) SCS of one entity sends *authentication request* to TTP.

2) TTP identifies the credential of the entity from an *authentication request*.

3) If TTP can identify the entity, TTP authenticates the entity. Otherwise, TTP returns error as an *authentication response*.

4) If TTP can authenticate the entity, TTP registers security policies that are included in the *authentication request*. Otherwise, TTP returns error as an *authentication response*.

5) TTP returns an *authentication response* message to the SCS of the entity.

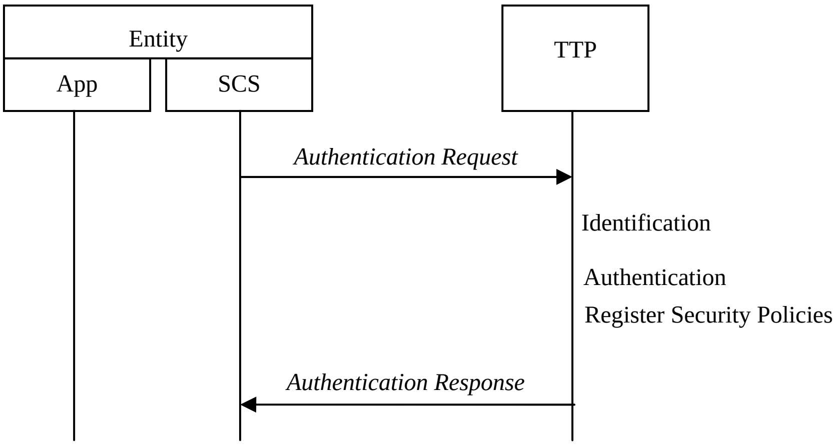

Figure 7 – Establishment of control path between entity and TTP

11.3 Establishment of secure data communication path

After the establishment of the control path between the Requester and TTP and the control path between the Responder and TTP, the Requester can request to establish secure data communication path between the Requester and the Responder as follows.

1) SCS of the Requester sends a *discovery request* to TTP to resolve the location of the application of the Responder.

   NOTE – The location of the application could be URI, IP address, etc.

2) TTP resolves the location and returns it as a *discovery response*.
3) If SCS of the Requester can retrieve the location, SCS creates an *open request* and sends it to TTP.
4) TTP performs authorization decision based on the credentials that are included in the *open request*.
5) If authorization decision is successful, TTP determines the security associations for data transmission phase. Otherwise, TTP returns error as an *open response*.
6) TTP sends the *open request* and *security association* for data transmission phase to SCS of the Responder.
7) SCS of the Responder checks if the *open request* and *security association* for data transmission phase are acceptable.
8) If they are acceptable, SCS of the Responder stores *security association* and returns an *open response*. Otherwise, SCS of the Responder returns error as *open response*.
9) TTP checks if the *open response* is an error message or not.
10) If it is not an error message, TTP sends the *open response* and *security association* for data transmission phase to SCS of the Requester. Otherwise, TTP sends the *open response* to SCS of the Requester.
11) SCS of the Requester checks if the *open response* is an error message or not.
12) If it is not an error message, SCS of the Requester stores *security association* for data transmission phase.

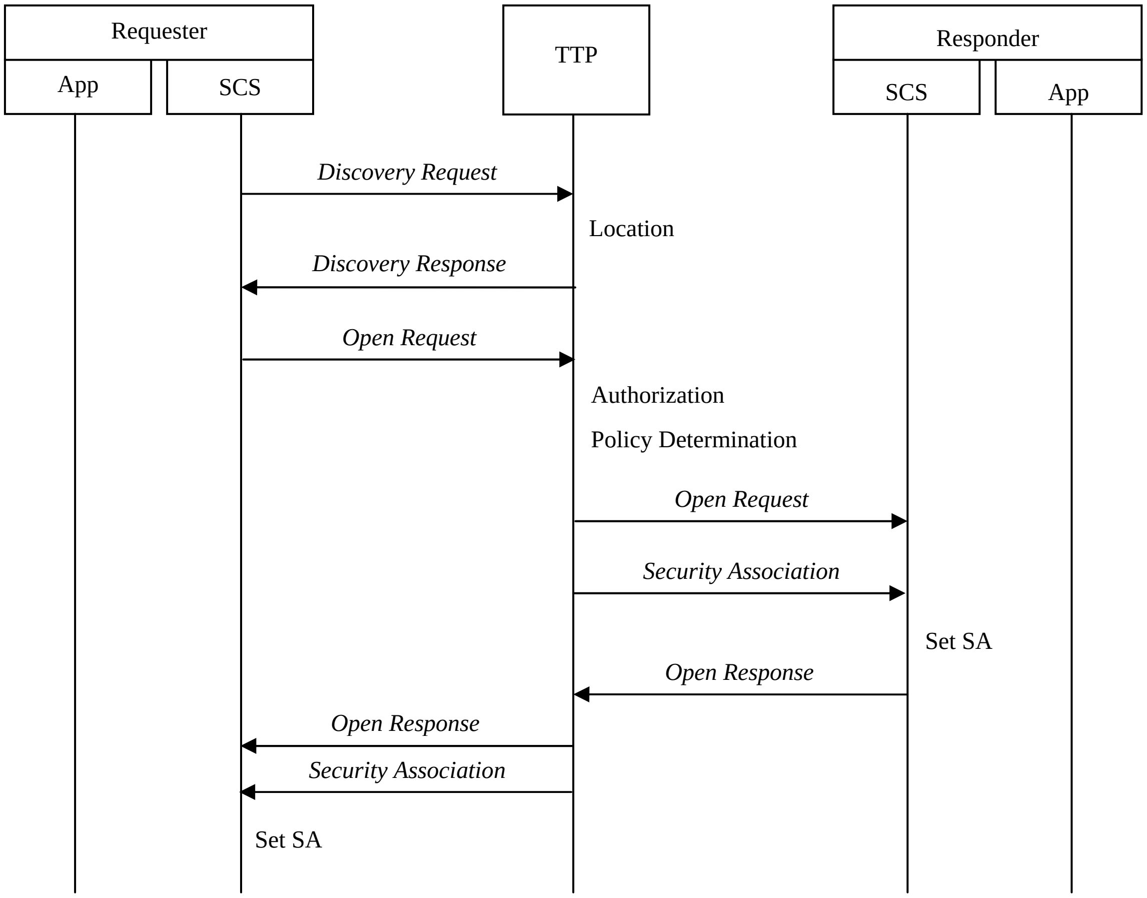

Figure 8 – Establishment of secure data communication path between Responder and Requester

11.4 Secure data transmission

After the establishment of the secure data communication path between entities, one entity can send application data to the peer entity as follows.

1) Application asks that SCS sends *application data* to the peer entity.

2) SCS enforces the security associations to *application data* and retrieves the *protected application data*.

3) SCS sends the *protected application data* to the peer entity via the secure data communication path.

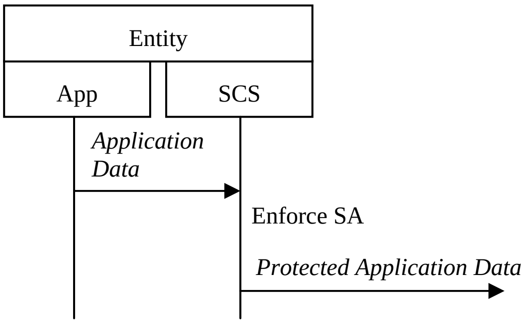

Figure 9 – Secure data transmission between entities (sending data)

In addition, one entity can receive *protected application data* from the peer entity as follows.

1) SCS receives the *protected application data* from the peer entity via the secure data communication path.

2) SCS checks if there are available security associations to enforce to the *protected application data*.

3) If security association exists, SCS enforces the security association to the *protected application data* and retrieves the *application data*. Otherwise, SCS drops the *protected application data* off.

4) If SCS can retrieve the *application data* successfully, SCS sends the *application data* to the application. Otherwise, SCS drops the *protected application data* off.

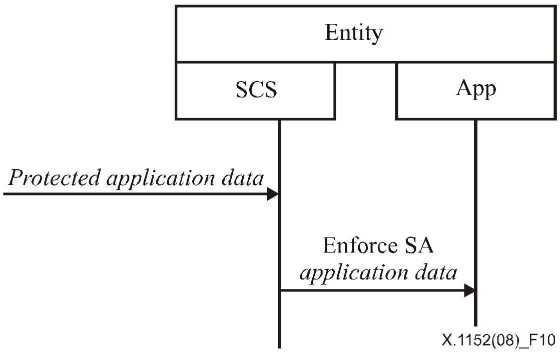

Figure 10 – Secure data transmission between entities (receiving data)

11.5 Audit trail creation

During the secure data transmission, SCS can request TTP to make audit trails as follows.

1) When SCS receives *application data* from application (or receives *protected application data* from the peer entity), SCS sends an *audit request* to TTP.

2) When TTP receives the *audit request* from an entity, TTP creates or updates audit trails according to the *audit request*.

3) After sending the *audit request* to TTP, SCS sends *application data* (*protected application data*) to the peer entity (the application).

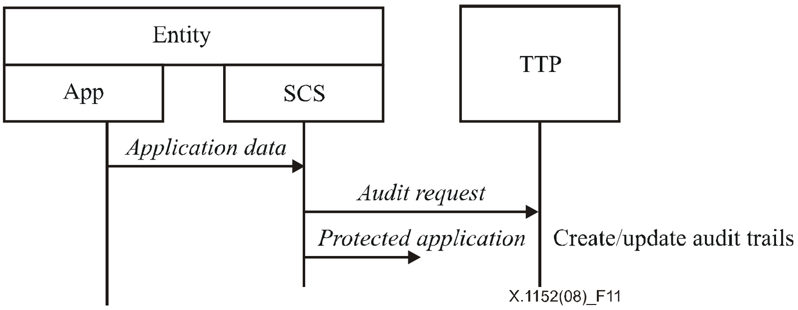

Figure 11 – Creation of audit trails (sending data)

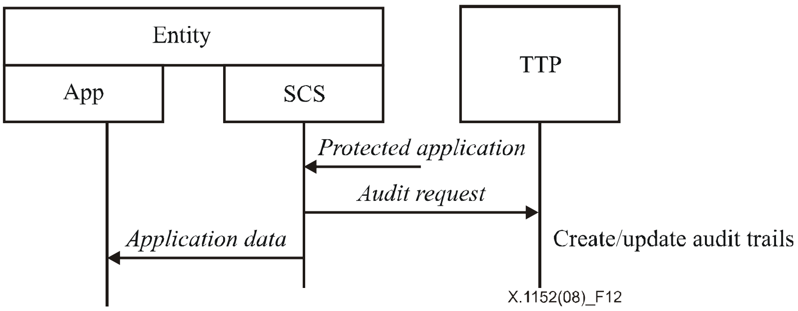

Figure 12 – Creation of audit trails (received data)

NOTE – Some applications might request SCS to send *audit request* to TTP when the application sends/receives application data to/from the peer entity.

11.6 Termination of secure data communication path

After the data transmission is finished, the secure data communication path is terminated as follows:

1) SCS of the Requester sends a *close request* to TTP.

2) When TTP receives the *close request* from the Requester, TTP sends a *close request* to the Responder.

3) When SCS of the Responder receives the *close request* from TTP, it deletes the security associations and returns a *close response* to TTP.

4) When TTP receives the *close response* from the Responder, TTP performs the termination process of the secure data communication path and sends a *close response* to the Requester.

5) When SCS of the Requester receives the *close response*, it deletes the security associations.

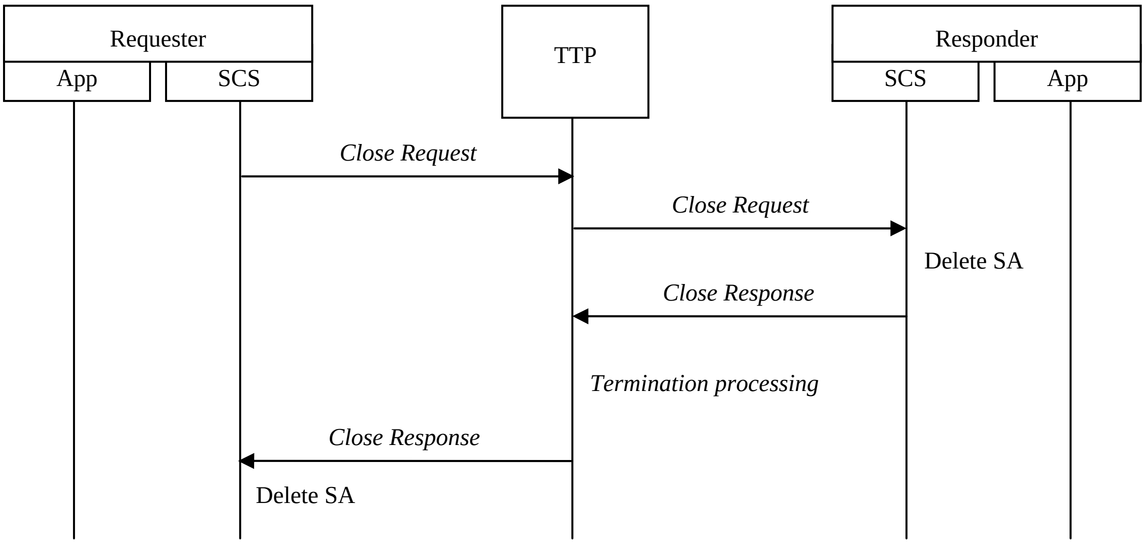

Figure 13 – Termination of the secure data communication path between Responder and Responder

11.7 Termination of control path

To terminate the control path, the following interactions are performed.

1) SCS of an entity sends a *termination request* to TTP.

2) When TTP receives the *termination request* from an entity, TTP deletes security policies of the entity, which are stored in the establishment of control path process, and returns a *termination response* to the entity.

3) When SCS of the entity receives the *termination response* from TTP, SCS of the entity terminates the control path with TTP.

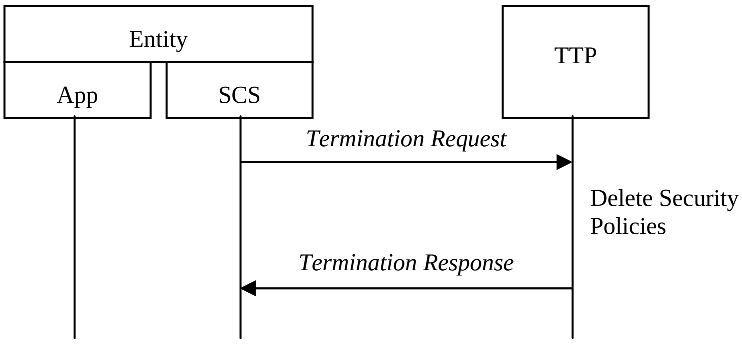

Figure 14 – Termination of control path between entity and TTP

12 Security considerations

To make secure end-to-end data communication between entities using TTP services, TTP is requested to be managed and operated as specified in [ITU-T X.842].

In addition, there are the following security considerations.

12.1 Requester-TTP interface

The communication between the Requester and TTP should be free from eavesdropping, injection and modification of data.

And the Requester should authenticate TTP to prevent from masquerading TTP.

12.2 Responder-TTP interface

The communication between the Responder and TTP should be free from eavesdropping, injection and modification of data.

And the Responder should authenticate TTP to prevent from masquerading TTP.

12.3 Establishment of the secure data communication path between entities

The security level of authentication performed by TTP should satisfy the security level of the secure data communication path between the Requester and the Responder. For example, when TTP authenticates the Requester by password authentication and the Responder requires certificate-based authentication, TTP should refuse the communication request from the Requester to the Responder.

12.4 Stored data in the entity

Entities have to store secret information for authentication (e.g., private key of the entity) and information to authenticate TTP (e.g., X.509 certificate of TTP, CA certificate of TTP or CA certificate of the entity as trust anchor). Because their leakage allows vipers to masquerade as an entity or TTP, entities should store them in the entity to protect them from unauthorized access.

12.5 Stored data in the TTP

TTP also has to store secret information for authentication (e.g., private key of TTP) and information to authenticate the user (e.g., CA certificate of TTP or CA certificate of an entity as trust anchor). Because their leakage allows vipers to masquerade as an entity or TTP, TTP should store them in TTP to protect them from unauthorized access.

In addition, TTP may hold privacy sensitive information as a part of entities' attributes. To avoid invasion of privacy, TTP should protect this information from unauthorized access and should verify the correctness of their information whenever TTP registers and updates this information.

Annex A

Re-establishment

(This annex forms an integral part of this Recommendation)

A.1 Re-establishment process of a secure end-to-end data communication

There is another process of secure end-to-end data communication, "Re-establishment". Re-establishment is a process to avoid compromising key information of existing secure data communication path. The re-establishment phase consists of re-authentication of the peer entity and renew of the key information.

A.2 TTP services for re-establishment process

In many cases, whole or part of the establishment process is performed in the re-establishment process. Therefore, TTP services that can be used for establishment processes can also be used.

Table A.1 – Possibilities of using online TTP services for re-establishment process

Processes of secure communication		Possible online TTP services
Re-establishment	Identification	Certificate management service, Directory service, Credential mapping service, Location service, Presence service
	Authentication	Authentication service
	Authorization and access control	Directory service, Access control service
	Policy determination and distribution	Key management service (Key generation service, Key distribution service), Policy determination service

Annex B

Entity level granularity and communication level granularity

(This annex forms an integral part of this Recommendation)

The granularity of each process in the establishment phase is classified into two types: entity level granularity process and communication level granularity process.

The entity level granularity process means that the result of the process depends on the entity. In other words, the process will make the same result, even if a certain entity tries to establish multiple secure end-to-end data communications. For example, the identification process and the authentication process are entity level granularity processes.

The communication level granularity process means that the result of the process depends on application or the secure data communication path. In other words, the result of the process might be different every time. For example, the authorization and access control process and the policy determination and distribution process are communication level granularity processes.

The difference of granularity causes different points in time to perform those processes. The entity level granularity processes can be performed by TTP only once, even if those processes are for different peer entities. On the other hand, the communication level granularity processes should be performed by TTP whenever a new secure data communication path is established.

Appendix I

Service scenario

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

This appendix gives a typical service scenario of secure end-to-end data communication using TTP services.

Managed dynamic end-to-end VPN is a typical example of use case for a number of terminals that connect through an open network and communicate with each other.

In this scenario, as shown in Figure I.1, TTP controls secure communications between terminals, but application data are directly exchanged between two terminals.

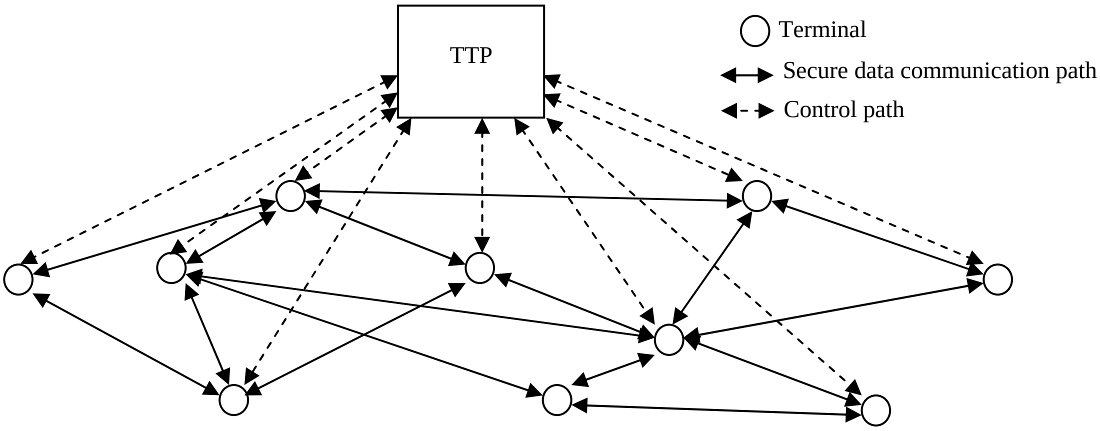

Figure I.1 – Managed dynamic end-to-end VPN

Most of the current secure communication technologies, such as transport layer security (TLS), require that two terminals authenticate each other, perform access decision, negotiate security algorithms and share secret values for secure communication directly. However, because the authentication process and/or the secret sharing process often use public key cryptography, they require quite high processing power.

In the managed dynamic end-to-end VPN scenario, it requires lower processing power for terminals to establish secure data communication between them than the current secure communication technologies, because TTP authenticates terminals in advance of communication between terminals, and TTP performs access decision and key distribution to terminals during the secure communication establishment.

On the other hand, in this scenario, TTP controls the secure communication between terminals, but does not relay any application data exchanged between terminals. Therefore, it also avoids information overload to TTP. (Current VPN technologies based on cryptography use VPN gateways to encrypt/decrypt application data. Therefore, it causes information overload to VPN gateways in the case that numerous numbers of terminals connect to VPN gateways.)

Appendix II

Relationship among this Recommendation, ITU-T X.842 and the Liberty Alliance Project

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

This appendix analyses the relationship among TTP services described in this Recommendation, TTP services defined in [ITU-T X.842] and services defined by the Liberty Alliance Project.

In Table II.1, the letter "O" denotes that there is a particular TTP service in the specification(s) and the letter "X" denotes that there is no TTP service in the specification(s).

Table II.1 – Relationship among this Recommendation, X.842 and the specifications of Liberty Alliance Project

	This Recommendation	ITU-T X.842	Specifications of the Liberty Alliance Project
Certificate management service	O	O	X
Credential mapping service	O	X	O (ID-WSF Identity Mapping Service [b-Liberty Authn])
Location service	O	X	O (ID-WSF Discovery Service [b-Liberty Disco])
Presence service	O	X	O (ID-SIS Presence Service [b-Liberty Presence])
Authentication service	O	O	O (ID-WSF Authentication Service [b-Liberty Authn])
Authorization service	O	O (Directory service, Access control service)	O (ID-WSF People Service [b-Liberty People])
Key management service	O	O	X
Policy determination service	O	X	X
Time stamping service	O	O	X
Electronic notary public service	O	O	X
Electronic digital archiving service	O	O	X

Bibliography

[b-ITU-T X.500] Recommendation ITU-T X.500 (2005) | ISO/IEC 9594-1:2005, *Information technology Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

[b-ITU-T X.803] Recommendation ITU-T X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

[b-ITU-T X.843] Recommendation ITU-T X.843 (2000) | ISO/IEC 15945:2002, *Information technology – Security techniques – Specification of TTP services to support the application of digital signatures*.

[b-Liberty Authn] Hodges, Jeff, Aarts, Robert, Madsen, Paul, and Cantor, Scott, *Liberty ID-WSF Authentication, Single Sign-on, and Identity Mapping Services Specification Version 2.0*, Liberty Alliance Project. <http://www.projectliberty.org/liberty/specifications_1>

[b-Liberty Disco] Hodges, Jeff, and Cahill, Conor, *Liberty ID-WSF Discovery Service Specification Version 2.0*, Liberty Alliance Project. <http://www.projectliberty.org/liberty/specifications_1>

[b-Liberty People] Koga, Yuzo, and Madsen, Paul, *Liberty ID-WSF People Service Specification Version 1.0*, Liberty Alliance Project. <http://www.projectliberty.org/liberty/specifications_1>

[b-Liberty Presence] Saint-Andre, Peter, *(draft)*, *Liberty ID-SIS Presence Service Specification Version 1.0-10*, Liberty Alliance Project. <http://www.projectliberty.org/liberty/specifications_1>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009