Draft EG 201 057 V1.1.1 (1997-05)

ETSI Guide

Telecommunications Security; Trusted Third Parties (TTP); Requirements for TTP services

Reference
DEG/SEC-003000 (9sc00icq.PDF)

Keywords
ISDN, multimedia, security

ETSI Secretariat

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights

ETSI has not been informed of the existence of any Intellectual Property Right (IPR) which could be, or could become essential to the present document. However, pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out. No guarantee can be given as to the existence of any IPRs which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Security (SEC), and is now submitted for the ETSI Membership Approval Procedure (MAP).

An ETSI Guide (EG) is an ETSI deliverable, containing informative elements, adopted for publication by the ETSI membership.

Introduction

Achieving the appropriate level of user confidence in the application of IT systems for processing and communicating information is closely related to the need for practical and appropriate technical and legal controls to protect this information. Users across a wide range of industrial sectors and user communities need to have confidence that such systems can be relied upon to support their business obligations and commitments, and to provide a level of trust in the protection of their information.

There is a need to facilitate the growing importance and development of electronic commerce, the European Information Infrastructure (EII) and the Global Information Infrastructure (GII) by the introduction of suitable measures to safeguard the integrity and confidentiality of electronic information. The provision of Trusted Third Party (TTP) services to satisfy this user need, and the requirement to be compliant with national legislation, is of major importance to establish the appropriate level of user assurance.

TTP services can be considered as value-added communication services available to users that need to enhance the trust in the services used. By signing up to a licensed or accredited TTP, the user will be able to communicate securely with every user of every TTP with whom his TTP has an agreement (or shares a common root in the case of a hierarchical infrastructure of TTPs). Therefore, TTPs could be able to offer value with regard to integrity and confidentiality of the electronic information being carried by these communications. A TTP has been defined by ISO/IEC as a security authority or its agent, trusted by users with respect to security-related activities, e.g. to support the use of digital signatures and confidentiality services. The role of TTPs may include providing assurance that:

- messages and transactions are being transferred to the right recipient at the right location;
- messages are received in a timely, secure and accurate manner from the claimed originator/sender;
- for any business dispute that arises, there are appropriate mechanisms for establishing and presenting evidence of what happened.

This document has been prepared by the ETSI Technical Committee SEC, to define the requirements for TTPs.

Annex A provides an executive summary of the requirements for TTP services. Annex B provides some examples of the use of TTP services and annex C presents information on international and national policies in this field.

1 Scope

This ETSI Guide (EG) describes the requirements for TTP services, as might be needed to support the growing demand for measures to safeguard the integrity and confidentiality of electronic information. In particular, these requirements include provision for TTP based key management, key certification and key escrow/recovery, authentication, access control and non-repudiation services.

The general aim of this standardization work is towards:

- a Europe-wide solution to aid the development of a TTP network, whilst recognizing the broader need for international solutions and interoperability;
- the provision of a range of TTP services to be offered to a variety of industrial sectors and other user communities; and
- providing compatibility with a range of communications systems, interfaces and protocols (e.g. internet/intranet, mobile networks, public networks, private networks).

This EG covers a set of general requirements for a TTP scheme, more specific technical requirements related to TTP services and functions, and interfaces. These take in account some of the requirements relevant to the commercial and legal environment.

Annex A of this EG provides a summary of the requirements for a TTP scheme, both general and specific. Annex B provides some examples of the use of TTP services and annex C provides some information on international policies.

The requirements given in this EG (see annex A for a summary) will be translated into a number of technical specifications for TTP functions and interfaces and these will be the subject of a set of standards.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] Jefferies N, Mitchell C and Walker M: "A Proposed Architecture for Trusted Third Party Services" In Dawson E and Golic J (Eds.), Lecture Notes in Computer Science 1029, Cryptography; Policy and Algorithms Conference pp 98-104, Springer Verlag, 1996.

[2] Howard P and Mitchell C: "Requirements for Trusted Third Parties", ASPeCT Project, ACTS Programme, 29 May 1996.

[3] Howard P and Mitchell C: "Trusted Third Party Services", ASPeCT Project, ACTS Programme, 21 June 1996.

[4] Denning, D.E and Branstad, D.K.: "A Taxonomy for key escrow encryption systems", Comms. of the ACM 39, No. 30, pp 33-40, March 1996.

[5] ISO/IEC JTC1/SC27 N1358 (Working Draft 14516-1): "Guidelines for the use and management of Trusted Third Party Services - Part 1: General Overview", May 1996.

[6] ISO/IEC JTC1/SC27 N1360 (Working Draft 14516-2): "Guidelines for the use and management of Trusted Third Party Services - Part 2: Technical Aspects", May 1996.

[7] ISO/IEC 7498-2: 1988, Information technology - Open systems interconnection - Basic reference model - Part 2: Security Architecture.

[8] ISO/IEC 9594-8: "Information technology - Open systems interconnection - The directory authentication framework", November 1993.

[9] ISO/IEC 9798: "Information technology - Security techniques - Entity Authentication - Part 1: General Model", 1996.

[10] ISO/IEC 10181: "Information technology - Security frameworks in open systems":

Part 1: Security Framework.

Part 2: Authentication Framework.

Part 3: Access Control Framework.

Part 4: Non-repudiation Framework.

[11] ISO/IEC 11770: "Information technology - Security techniques - Key Management":

Part 1: Framework.

Part 2: Mechanisms using symmetric techniques.

Part 3: Mechanisms using asymmetric techniques.

[12] ISO/IEC CD 13888: "Information technology - Security techniques - Non-repudiation":

Part 1: General Model.

Part 2: Using Symmetric Techniques.

Part 3: Using Asymmetric Techniques.

[13] Draft amendments DAM 4 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions (X.509 v3), July 1995.

[14] ECMA-219: "Authentication and Privilege Attribute Security Application with related key distribution functions", 2nd edition, March 1996:

Part 1: Overview and Functional Model.

Part 2: Security Information Objects.

Part 3: Service Definitions.

[15] ECMA-235: "The ECMA GSS-API Mechanism", March 1996.

[16] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data.

[17] Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the Integrated Services Digital Network (ISDN), and in the digital mobile networks.

[18] Council Decision of 19 December 1994 on the joint action adopted by the council on the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods, 94/942/GBVB (Pb Nr. L 367), 31 December 1995.

[19] Council Regulation (EC) Nr. 3381/94 of 10 April 1995 setting up a Community regime for the control of exports of dual-use goods (Pb. Nr. L 90), 21 April 1995.

[20] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

[21] Draft Model EDI Agreement K.U. Leuven and ICRI in association with the Belgium National Chambers of Commerce Federation (B).

[22] German Digital Signature Law (Gesetz zur digitalen Signatur, December 1996).

[23] Excerpt from IDA, Legal Aspects of the interchange of data between administrations, Final report, February 1996.

[24] Bangemann Report, "Europe and the Global Information Society, Recommendations to the European Council", Brussels, 26 May 1994.

[25] Sixth Strategic Review Committee, "Final Report on European Information Infrastructure", May 1995.

[26] Eurobit, ITI and JEIDA, "Global Information Infrastructure (GII)", January 1995.

[27] Proceeding from EDITT, TEDIS EDI Trusted Third Party Workshop, 2nd Edition, Barcelona, Spain 8-10, February 1995.

[28] Housley R., Ford W. and Solo D.: "Internet Public Key Infrastructure: Part I - X.509 Certificate and CRL Profile", Internet Draft, 3 November 1996.

[29] Farrell S., Adams D. and Ford W.: "Internet Public Key Infrastructure: Part III - Certificate Management Protocols", Internet Draft, June 1996.

[30] "Federal Public Key Infrastructure (PKI) Technical Working Group Specifications":

Part A: Requirements for the Federal PKI, TWG96- (January 1996).

Part B: Technical Security Policy, TWG96-001 (January 1996).

Part C: Concepts of Operation, TWG95-108 (November 1995).

Part D: Interoperability Profiles.

Part E: X.509 Certificate and CRL Extensions Profile.

[31] IEEE P1363: "Standard for Public Key Cryptography".

[32] National Institute of Standards and Technology, FIPS Publication 185: Escrowed Encryption Standard, February 1994.

[33] Baum M.: "Federal Certification Authority Liability and Policy", NIST-GCR-94-654, June 1994.

[34] INFOSEC Reports, 1992-95, European Commission/DGXIII.

[35] ETSI ETR 331 (DTR/NA-002310): "Definition of User Requirements for Lawful Interception of Interception of Telecommunications Requirements of the Law Enforcement Agencies", September 1996.

[36] Architecture for Public-Key Infrastructure, The Open Group, August 1996.

[37] Final Text of ITU-T X.509 | ISO/IEC 9594-8 DAM 2 1996 The Directory - Authentication Framework - Amendment 2 on Enhancement of Directory Operational Security; ISO/IEC JTC 1/SC 21 and ITU-T Q15/7 Collaborative Editing Meeting on the Directory, Phoenix, October 1996.

[38] Blakley B. and the APKI Working Group: "Architecture for Public-Key Infrastructure", Internet Draft, November 1996.

[39] Koops Bert-Jaap: "A Survey of Cryptography Laws and Regulations", The Computer Law and Security Report, November-December 1996.

[40] Resolution of the Council of the European Union: "International Requirements on the Lawful Interception of telecommunications", 17 January 1995.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document, the following definitions apply:

access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. (ISO 7498-2 [7])

asymmetric cryptographic technique: A cryptographic technique that uses two related transformations, a public transformation (defined by a public key) and a private transformation (defined by a private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. (ISO 11770-1 [11]).

NOTE 1: A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key management system. With asymmetric cryptosystems there are four elementary transformations: sign and verify for signature schemes, encipher and decipher for encipherment systems. The signature and decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published.

NOTE 2: If the same cryptosystem is used for different services, then keys used for confidentiality services should not be used for integrity services.

attribute certificate: A set of attributes of a user together with some other information, rendered unforgeable by the digital signature created using the private key of the certification authority which issued it. (ITU-T X.509 | ISO/IEC 9594-8 DAM 2 [8])

authentication: The provision of assurance of the claimed identity of an entity. (ISO/IEC 10181-2 [10])

certificate: An attribute certificate, public key certificate or privilege attribute certificate.

Certification Authority (CA): An authority (e.g. a TTP) trusted by one or more users to create and assign certificates. Optionally the certification authority may create the user's keys. (ISO/IEC JTC1/SC27 N1358 [5] and N1360 [6])

Certificate Revocation List (CRL): A list of certificates which are no longer valid. A CRL is generated and distributed by a TTP. (ISO/IEC JTC1/SC27 N1358 [5] and N1360 [6])

digital signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient. (ISO 7498-2 [7])

evidence: Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. (ISO/IEC 13888 [12])

key distribution: This is a set of procedures to provide key management information objects securely to authorized entities. (ISO/IEC 11770-1 [11])

key escrow/recovery system: A key escrow/recovery system is an encryption system with a backup decryption capability that allows authorized persons (users, officers of an organization or law enforcement authorities) under certain prescribed conditions, to decrypt ciphertext with the help of key escrow/recovery information supplied by one or more trusted parties who hold special data recovery keys. (reference [4])

key management: The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy. (ISO/IEC 11770-1 [11])

Law Enforcement Agency (LEA): An organization authorized by a lawful authorization, based on a national law, to receive the results of telecommunication interceptions. (ETR 331 [35])

lawful authorization: Permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation for a network operator or service provider. Typically this refers to a warrant or order issued by a lawfully authorized body. (ETR 331 [35])

lawful interception: The action (based on the law), performed by a network operator or service provider, of making available certain information and providing that information to a Law Enforcement Monitoring Facility. (ETR 331 [35])

non-repudiation service: A security service which counters the threat of repudiation.

Privilege Attribute Certificate (PAC): A set of privilege attributes issued by a security authority or TTP, that is protected by integrity and data origin authentication, and includes an indication of a time period of validity. (ECMA-219 [14])

private key: That key of an entity's asymmetric key pair which should only be used by that entity. (ISO/IEC 9798-1 [9], ISO/IEC 11770-1 and 3 [11])

privilege attributes: Attributes associated with a security subject that, when matched against control attributes of a security object, are used to grant or deny access to that security object. (ECMA-219 [14])

public key: That key of an entity's asymmetric key pair which can be made public. (ISO/IEC 9798-1 [9], ISO/IEC 11770-1 and 3 [11])

public key certificate: Public key information of an entity signed by the certification authority and thereby rendered unforgeable. (ISO/IEC 9798-1 [9], ISO/IEC 11770-1 and 3 [11])

repudiation: Denial by one of the parties involved in a communication of having participated in all or part of the communication (ISO 7498-2 [7])

secret key: A key used with symmetric cryptographic techniques and usable only by a set of specified entities. (ISO/IEC 11770-1 and 3 [11])

security token: A set of security relevant data that is protected by integrity and data origin authentication from a source which is not considered a security authority. (ISO/IEC 10181-1 [10])

symmetric cryptographic technique: A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation. (ISO/IEC 9798-1 [9], ISO/IEC 11770-1 [11])

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

A-I	Application Interface
CA	Certification Authority
CRL	Certificate Revocation List
DTS	Digital Time-stamping Service
EDI	Electronic Data Interchange
EII	European Information Infrastructure
GII	Global Information Infrastructure
I&A	Identification and Authentication
IT	Information Technology
KER-I	Key Escrow/Recovery Interface
LEA	Law Enforcement Agency
PAC	Privilege Attribute Certificate
PAC	Privilege Attribute Certificate
T-I	Inter-TTP Interface
TTP	Trusted Third Party
U-I	User Interface

4 General aspects

4.1 Use of a TTP

A trusted third party (TTP) can be described as an entity trusted by other entities with respect to security-related services and activities. A TTP would be used to offer value added services to users wishing to enhance the trust and business confidence in the services they receive and to facilitate secure communications between business trading partners. TTPs need to offer value with regard to integrity, confidentiality and assurance of the services and information involved in the communications between business applications. In addition, users will require TTP services to be available when they need them within the terms of the agreed service contract.

Typically, a TTP will be an organization, licensed or accredited by a regulatory authority, which will provide security services, on a commercial basis, to a wide range of bodies, including those within the telecommunications, finance and retail sectors.

The initiatives such as the European Information Infrastructure (EII) and the Global Information Infrastructure (GII), which aim to facilitate the development of electronic commerce, are good examples where there is a need for security services and TTPs. This is an important part of the motivation to use TTPs to support secure communications in commercial systems and a variety of industry sectors. For example, a TTP could be used to support the provision of digital signatures to secure the integrity of documents. In addition, they could provide end-to-end encryption services to users, and incorporate e.g. key escrow/recovery functionality to support a recovery or backup function for a key to enable recovery if the key is lost (typically for documents and files that have been encrypted by employees) or to support the demand for lawful interception.

The use of TTPs is dependent on the fundamental requirement that the TTP is trusted by the entities it serves to perform certain functions. However, the TTP can also assure the user of the trustworthiness of another of its clients to the extent that it is who it claims to be and providing that the other TTP client also trusts the TTP to perform the required functions. This has the advantage that trust between any two entities in a TTP domain can be established without having to set up individual bilateral agreements.

In practice, TTPs could exist in both public and corporate domains, at the local, national and international level. TTPs should have trust agreements arranged with other TTPs to form a network, thus allowing a user to communicate securely with every user of every TTP with whom his TTP has an agreement. However, users might not have to communicate with other TTPs other than their own to enable such secure communications to take place. Any TTP scheme should also allow for both national and international operation, allowing users in any country, where an appropriate TTP resides, to communicate securely. Online communications between TTPs should not be required. However, in some circumstances response times may necessitate on-line communications between TTPs.

A TTP scheme should ensure that any attempted abuse by a user can be detected, and in addition those with lawful authorization to have access to information cannot fabricate false evidence.

A TTP service can be composed of a number of services, each provided by independent organizations on a commercial basis. For example, a notary service provider can sub-contract the CA and directory services to other organizations. A TTP architecture might have a modular design and interfaces to allow for flexible configuration of the system according to the needs of different roles and organizations.

Any TTP standards should not restrict the form of electronic communication that can be supported..

4.2 Delimitation of security services for confidentiality and digital signatures

In order for an international network of TTPs to be fully effective it will be necessary for governments of participating TTPs to resolve a number of policy issues relating to the regulation and certification of key holders or key management systems, mutual recognition of digital signatures, permissible cryptographic algorithms and conditions for authorized access by another nation. Whilst it is not within the competence of this document to advise on these issues, it is appropriate to recommend that there should be no key escrow/recovery used solely for authentication purposes except at the request of the user.

4.3 Establishing trust in a TTP scheme

A TTP will be an organization, which may be licensed or accredited by a national authority or regulatory body, which will provide security services to a range of users, including those within the telecommunication, financial, retail and manufacturing sectors. These security services will be provided to users on a commercial basis. The user should have the possibility to choose a TTP from those available. Depending on the TTP functions to be supported, accreditation of the service and trust by the users should be based on evidence regarding:

- trust in the organization and its regulation: that the integrity of the organization carrying out the TTP role can be relied upon and it can be checked and verified;
- the accredited quality of the operations, processes and working practices involved: that they are well defined, implemented and carried out correctly both in the administrative and in the technical sense;
- compliance with widely adopted standards and certification of the TTP against agreed codes of practice in the area of operations;
- compliance with laws and regulations;
- the existence of a legally binding contract between the user and the third party and between co-operating TTPs;
- liability of fraud and misuse and insurance to cover it;
- timeliness, the TTP performs its functions according to agreed time parameters, for example response times or frequency of delivery or update;
- statement and correct implementation of a security policy, covering technical, administrative and organizational requirements for security with special emphasis on the following requirements:
    - system integrity, that is assurance that the TTP performs its function in such a way that it cannot be impaired or harmed;
    - integrity of user data, that it is complete, unmodified and that its source and origin can be verified;
    - availability, that is that authorized users are ensured access to services and information they are entitled to;
    - confidentiality, when the TTP is entrusted with information that is sensitive and private to an entity;
    - procedures established to audit the TTP's system security.

The aim of the security policy is:

- to form the basis of trustworthiness with regard to security as seen by co-operating TTPs and users;
- to form the basis of detailed security specifications for the procurement of technical systems and for the implementation of procedures;
- to ensure consistency among administrative, organizational and technical security requirements.

In general, high-level security requirements for TTPs are concerned with the:

- traceability of operations and transactions;
- availability of services and information; and
- integrity of users and co-operating actors.

Security requirements at a more detailed level are summarized in clause A.2.

It is foreseen that different business areas and applications will require different levels of trust, which may demand different strength for the applied protection mechanisms and procedures.

Security services and mechanisms will be specified as integral parts of the profiles to be defined for different TTP services.

4.4 TTP management

The commitment of a TTP to provide a security related service should take the form of a documented security policy. The policy shall identify all relevant targets, objects and threats related to the services provided. It should provide the rules, directives and procedures regarding how the specific security services and the associated security level are assured (see references [5] and [6]).

A TTP shall take responsibility of liability within defined limits as stated in a formal contract. The liability of a TTP needs to be managed against the specific functions it supports. The contract shall also cover legal aspects regarding the operation of a TTP (e.g. such as its use in providing a key escrow/recovery service). Clause 7 of this document covers the legal and commercial aspects of TTPs.

These requirements are subject to national laws and international treaties and should be interpreted in accordance with applicable national policies.

4.5 User interactions with TTPs

4.5.1 Communication relationship between TTP and user

TTPs can be categorized according to their communication relationships with the users they serve (see references [5] and [6]. The type of relationship adopted will influence the services that it will be capable of fulfilling. A TTP may provide its services through a combination of the different modes for different parts of its service.

4.5.1.1 Off-line TTPs

An off-line TTP (see figure 1) does not interact with the user entities during the process of the given security service. Instead the interaction to provide, or register, security-related information is carried out off-line as a separate interaction.

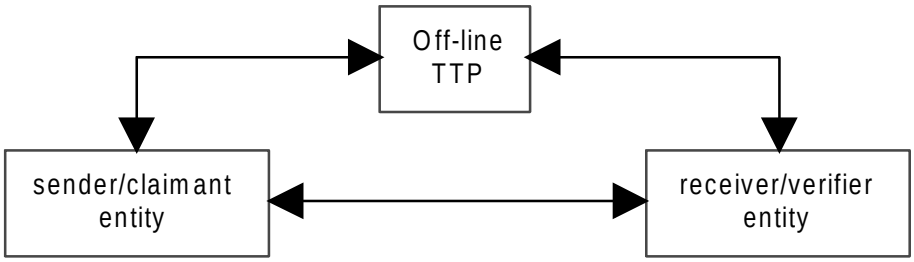

Figure 1: Off-line TTPs

4.5.1.2 On-line TTPs

An on-line TTP (see figure 2) is requested by one or both entities in real-time to provide, or register, security-related information. Such a TTP is not in the communications path between the two entities.

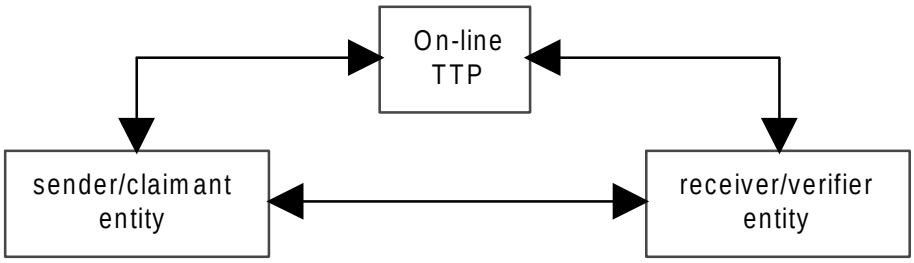

Figure 2: On-line TTPs

4.5.1.3 In-line TTPs

An in-line TTP (see figure 3) is positioned in the communication path between the entities. Such an arrangement allows the TTP to offer a wide range of security services directly to users. Since the TTP interrupts the communication path, different security domains can exist on either side of it.

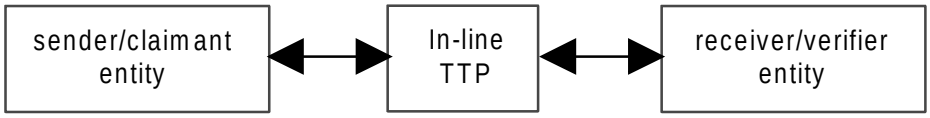

Figure 3: In-line TTPs

4.5.2 Initial user registration with TTPs

A user may need to initially register with a TTP before being able to receive its services and this requirement will be dependent on the TTP functions supported. This may involve a binding contract between the user and the TTP. On the initial registration, the TTP would be responsible for correctly identifying users, issuing the user with registration information including the provision of certificates and keys and, where appropriate, carrying out credit checks on whether the user can pay for the services to be provided.

4.5.3 TTP authentication and access control

The requirement for authentication and access control depends on the TTP service. When a user requests services from his TTP, the TTP and user should authenticate each other to guard against masquerade attacks. When the TTP and user have authenticated each other, the TTP should protect against unauthorized access to the TTP's resources. This will be provided through an appropriate access control mechanism, where only authorized users are allowed to access or invoke certain services. The access control mechanism may be provided by physical means for off-line TTPs. However, where users communicate with on-line TTPs there is likely to be a requirement for an automatic means of control, e.g. through the use of a secure computer operating system.

4.5.4 TTP service interface

Typically the user will send requests for a particular service to a TTP. The TTP will then respond appropriately by providing the user with the specified service. Whatever their individual roles, capabilities or operating environment, TTPs may need to be able to interoperate via a set of common interfaces. These interfaces will be described in the ETS on TTPs.

4.6 TTP services, functions and applications

TTP services can be categorized using a functional scheme which categorizes TTP services according to the user's perspective. The functional classification used in this document is restricted to TTP security services, which includes the use of TTPs to support cryptographic technologies.

4.6.1 Services

TTP services are split into six general categories as listed below:

- key management services for symmetric cryptosystems;
- key management services for asymmetric cryptosystems;
- key escrow/recovery services;
- identification and authentication support services;
- access control support services;
- non-repudiation services.

The services are composed of a common set of core TTP functions which will be implemented as a set of internal components providing services through external interfaces. Alternatively, these functions can be implemented by different TTPs depending on the nature of the application environment. These six categories are discussed in detail in clause 5.

4.6.2 Applications

The six general categories attempt to classify all possible security services that may be offered by TTPs. These services may be used in specific applications of a TTP. The TTP applications may provide services from any one or more of the six general categories in order to fulfil a particular role or requirement. For example, an application of a TTP may be to support a digital signature infrastructure by acting as a certification authority for public keys, or to act as a trusted key distribution centre. Annex B describes some of the potential applications of TTPs.

5 TTP services and functions

5.1 Key management services for symmetric cryptosystems

TTPs that support the management of secret keys for use in symmetric cryptosystems may offer a wide range of security services including authentication, integrity protection, confidentiality, non-repudiation and access control.

A TTP could offer separate generation and distribution services depending on the requirements. For example, the user may request a TTP to distribute a key generated by some other entity. A TTP may be asked to generate a key but not distribute it.

5.1.1 Secret key generation

A TTP may be required to generate secret keys for secret key cryptosystems. Secret key generation will involve randomly selecting a key value from all possible values for a given cryptosystem. In this scheme, the user would request the TTP to generate a secret key for a given symmetric cryptosystem. The key may then be used by the TTP itself, distributed to the user or distributed to another entity on the user's behalf.

5.1.2 Secret key distribution

Secret keys generated by a TTP, or provided by a user, may have to be distributed to other entities. This needs to be carried out in a secure way using suitable techniques. In addition, a user may request a TTP to distribute a secret key to another entity on its behalf.

5.1.3 Secret key revocation

A TTP may be needed to revoke a secret key, which has been previously distributed. Key revocation may be required for a number of reasons including suspicion that a particular key has been compromised, or changes in the purpose for which the key was being used.

5.1.4 Secret key storage and retrieval

A TTP may be required, for various reasons, to provide for the storage of keys. This needs to be done in a secure way. For example, such storage should safeguard the confidentiality and integrity for any keys stored. Safeguards to secure the storage of keys include physical, technical, procedural and legal measures, including the use of encipherment.

The retrieval of keys needs to be safeguarded against the unauthorized access to such keys. Again these safeguards can include a combination of physical, technical, procedural and legal measures.

5.1.5 Secret key archival

Once a key has come to the end of its operational life, it may have to be archived. In this scheme, a user would request a TTP to archive a secret key. Before storing the key in a storage facility, the TTP should add a time-stamp, integrity protect and/or encrypt the key. Clearly, the TTP should implement suitable access control mechanisms in order to prevent unauthorized parties from retrieving the key.

5.2 Key management services for asymmetric cryptosystems

TTPs that support the management of public/private key pairs for public key cryptosystems may offer a wide range of security services including authentication, integrity protection, confidentiality, non-repudiation and access control. If the same cryptosystem is used for different services, then keys used for confidentiality services should not be used for integrity services.

A TTP could offer separate generation and distribution services depending on the requirements. For example, the user may request a TTP to distribute a key generated by some other entity. A TTP may be asked to generate a key but not distribute it.

The key management for public key cryptosystems is inherently different to that for symmetric cryptosystems. In particular, the distribution of public keys does not require confidentiality protection but does require integrity protection in order to guarantee the key's authenticity.

5.2.1 Public/private key pair generation

A TTP may be required to generate key pairs for public key cryptosystems. Key pair generation will involve randomly selecting a key pair value from all possible values for a given public key cryptosystem. In this scheme, the user would request the TTP to generate a key pair for a given public key cryptosystem. The key pair may then be used by the TTP itself, distributed to the user or distributed to another entity on the user's behalf.

5.2.2 Public key certification

To guarantee the authenticity of the public key, it needs to be certified by a certification authority trusted by users of the public key. In this role, the certification authority is acting as a TTP. The certification process will produce a public key certificate containing essential information about the key including, validity dates for the certificate, the key itself, and a digital signature for the certificate calculated using the certification authority's private key. The digital signature can then be verified by potential users using the certification authority's public key.

5.2.3 Public/private key pair distribution

In asymmetric cryptosystems, the sender may use the public key of the recipient to encrypt data and the recipient may use its corresponding private key for decryption. The sender must be sure that the recipient's public key is genuine, otherwise an attacker may have substituted the key for its own public key, thereby allowing the attacker to retrieve the data. Similarly, if the sender uses the private key to sign data, the recipient should be sure that the public key used to verify the signature is genuine.

In this scheme, a user may request the TTP to distribute the key pair, which the TTP has previously generated for the user. This will involve distributing the private key to the user in confidence, and distributing the corresponding public key to the user in the form of a certificate. Alternatively, a user may request a TTP to distribute a key pair to another entity on its behalf. A user may also want a TTP to distribute a public key certificate to a public directory server, where it can be accessed by a large number of potential users. However, it may be convenient for the TTP that generates public key certificates to act as a directory server for them.

5.2.4 Public/private key pair revocation

A TTP may be required to revoke a public or private key, which has previously been distributed. Key revocation may be required for a number of reasons including suspicion that a particular key has been compromised, or changes in the purpose for which the key was being used. When operating as a certification authority, a TTP will be responsible for regularly generating and distributing Certificate Revocation Lists (CRLs), containing a list of certificates which, although not expired, are no longer valid. Where certificates are retrieved in real time from an on line service, the revocation of a certificate may also be indicated by replacing the valid certificate by one which is marked as being revoked.

Since time may be an important factor when keys have been compromised, a TTP should be able to react quickly to a request for key revocation while still ensuring that only authorized entities may initiate revocation of a key.

5.2.5 Public/private key pair storage and retrieval

A TTP may be required, for various reasons, to provide for the storage of keys. This needs to be done in a secure way. For example, such storage should safeguard the confidentiality and integrity of any private keys stored and the integrity of any public keys stored. Safeguards to secure the storage of keys include physical, technical, procedural and legal measures, including the use of encipherment.

The retrieval of keys needs to be safeguarded against unauthorized access to such keys. Again these safeguards can include a combination of physical, technical, procedural and legal measures.

5.2.6 Public/private key pair archival

Once a key pair has come to the end of its operational life, it may have to be archived, in which case a user may request a TTP to archive a key pair. Before storing the key pair in a storage facility, the TTP should add a time-stamp, integrity protect and/or encrypt the key pair. Clearly, the TTP should implement suitable access control mechanisms in order to prevent unauthorized parties from retrieving the key pair.

5.3 Key escrow/recovery services

Key escrow/recovery services relate to the safeguarding of keys to enable data to be decrypted whether it is data being communicated or in storage (see references [2] and [4]. Typical areas of application include those of lawful interception (see subclause 7.5), lawful access (see subclause 7.6) and user/business access. The main difference between these areas of application are the prescribed conditions under which decryption of ciphertext can take place.

For example an organization may choose to operate a data recovery service to recover business files and company information that have been encrypted by employees. It might simply be that the owner of the file needs to have access to escrowed keys to employ emergency decryption to recover data encrypted by keys that have been lost or damaged.

Another example might be that a law enforcement agency has the lawful authorization to receive escrowed keys from a TTP to lawfully access a user's incoming and outgoing communications. This requirement is subject to national law and international treaties and should be interpreted in accordance with applicable national policies.

In a key escrow/recovery system a TTP might combine the roles of a key generation and/or distribution agent for its users, as well being a supplier of user keys. A TTP operating such a system will also need to deal with issues such as key revocation, storage, retrieval and reconstruction. Keys need to be safeguarded against compromise, loss or abuse. This includes reliability and resiliency for protecting keys from compromise and for enabling data recovery. These safeguards can include a combination of physical, technical, procedural and legal measures. For example, this includes safeguards such as the use of encryption, authorization procedures, auditing, separation of duties, split knowledge, two person control, trusted systems.

5.4 Identification and authentication support services

Authentication with respect to the use of TTP's (e.g. for user registration, see subclauses 4.5.2 and 4.5.3) and for the support of TTP services and applications is a fundamental requirement. The TTP will typically be responsible for generating and checking information by which other entities identify a user, and hence will need to take some care in properly identifying a user before issuing that user with newly generated keys, key certificates. and other security related items. A TTP can be used as an authentication server in authentication schemes that involve third parties. The services can be categorized according to whether the authentication server is on-line, off-line or in-line.

5.4.1 On-line authentication services

In symmetric authentication schemes, there is a requirement for every verifier to maintain a secret symmetric key with every claimant (see ISO/IEC 10181 [10]). This may not be practical for end-to-end user authentication. Instead, a trusted on-line authentication server could be introduced. This would share a secret key with every claimant and verifier. Two general approaches to this scheme are outlined below:

- in the first approach, the claimant encrypts or seals a message with its secret key and sends it to the verifier. Since the verifier does not share the claimant's key, it must obtain it through a separate exchange with the server. This exchange should be secured using a shared key between the server and the verifier;

- in the second approach, the claimant first obtains a ticket from the server which contains a secret key to be used by the claimant to authenticate itself. The communication with the server is protected using a secret key shared between the server and the claimant. After the exchange, the claimant authenticates itself by encrypting or sealing a message with the secret key it received from the server and sending it to the verifier for checking.

5.4.2 Off-line authentication services

With asymmetric authentication the need for the authentication server to be on-line is removed (see ISO/IEC 10181 [10]). Instead, verifiers can obtain certified public keys for claimants and certificate revocation lists from an off-line server, prior to or during authentication. This information can be cached and reused to avoid having to communicate with the server each time authentication is initiated. However, if a user wants to be absolutely certain that a certified public key has not been revoked it should verify the status of the certificate or the certificate revocation list with the server.

An off-line authentication server may act simply as a directory server for certificates generated by another TTP acting as a Certification Authority (CA).

5.4.3 In-line authentication services

In-line authentication involves an authentication server positioned in the communication path between claimant and verifier. The authentication is, in effect, split into two sets of interactions. Firstly, the claimant attempts to authenticate itself to the server, which vouches for the identity of the verifier. Secondly, the verifier attempts to authenticate the server, which vouches for the identity of the claimant. This scheme has the advantage that the claimant and verifier may belong to different security policy domains. The server may apply different mechanisms to each domain to realize the different security policies of each domain.

5.5 Access control support services

A TTP can be used to certify privileges for access control (see ISO/IEC 10181 [10]). Certified privileges may be obtained from a TTP either in the form of a Privilege Attribute Certificate (PAC) (see ECMA-219 [14]), an attribute certificate or as additional attributes within a public key certificate (reference [13]. In addition, a TTP may be responsible for access control to information it uses in providing the TTP functions.

NOTE: This is one of the two most common approaches to providing access control services. The other approach is where the resource checks the identity of the user against a privilege list held at the resource. The best approach depends on particular circumstances. However, the use of a TTP only seems applicable to the privilege attribute approach.

The PAC will contain a list of resources that the user may wish to access and the associated privilege level that the user has been assigned. A user will send a request for a given privilege attribute to a TTP, which will then identify and authenticate the user. If the current security policy states that the user is authorized to make the requested access, then the TTP will generate and certify the privilege attribute. The privilege attribute certificate is then distributed by the TTP by publishing it in a directory.

The veracity of privilege information can be checked on demand by anyone who obtains the TTP's public certification key. The PAC may need to be revoked if changes in access control privileges are required, or if a compromise of sensitive information is suspected.

5.5.1 Generation of certificates for access control

A TTP may be required to generate a certificate for access control for a particular user. The first stage of this process would be to authorize the certificate depending on the current security policy within the operating domain. The second step would be to collect the relevant information about the user, the possible addition of a current time-stamp, and the actual generation of the access control information. The final step would be to certify the information by adding a digital signature generated using the TTP's private key.

5.5.2 Distribution of certificates for access control

Once the certificate for access control has been generated for a particular user, the TTP may be required to distribute it to a separate directory server. Note also that the TTP may act as a directory server for certificates it generates

5.5.3 Revocation of certificates for access control

A TTP may be required to revoke a certificate for access control, which has previously been distributed. Certificates for access control revocation may be required for a number of reasons, including changes in security policy. When acting as a server for certificates for access control, a TTP will be responsible for regularly generating and distributing revocation lists, containing a list of certificates for access control which, although not expired, are no longer valid.

5.5.4 Archival of certificates for access control

Once a certificate for access control has come to the end of its active life, it may have to be archived. Typically, a user would request a TTP to archive a certificate for access control. Before storing the certificate for access control in a storage facility, the TTP should add a time-stamp, integrity protect and/or encrypt the key pair. Clearly, the TTP should implement suitable access control mechanisms in order to prevent unauthorized parties from retrieving the certificate for access control.

5.6 Non-repudiation services

Non-repudiation services involve many different aspects including commercial, legal and technical. This document concentrates primarily on the technical aspects. In this respect TTPs have an important role to play in the provision of non-repudiation services. ISO/IEC 10181 [10] describes the application of non-repudiation services in open systems. It identifies non-repudiation mechanisms which involve TTPs. These are listed below:

- non-repudiation involving a TTP security token;
- non-repudiation using a digital signature (the TTP supports digital signatures);
- non-repudiation using time-stamping (the TTP carries out time-stamping);
- non-repudiation using an in-line TTP;
- non-repudiation using a notary.

In general, a non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. Its purpose is to provide evidence about a particular event or action. There are four distinct phases to non-repudiation services:

- evidence generation;
- evidence recording;
- evidence verification; and
- dispute resolution.

TTPs may be involved in all of these phases as described in ISO/IEC 13888 [12] which specifies a number of security techniques for non-repudiation services. However, their involvement depends on the mechanism used. For example, the use of asymmetric cryptographic techniques to generate and verify evidence may or may not require the involvement of a TTP, whereas the use of symmetric cryptographic techniques in evidence generation and verification requires a TTP.

NOTE: This standard uses the term ‘evidence’ to address the technical instrument to provide proof. This use of the word evidence should not be confused with the more formal legal use of the word.

5.6.1 Evidence generation

Evidence generation follows an invocation of the service by a non-repudiation service requester. Relevant evidence may include the identities of the entities involved, the communicated data, and the date and time. Additional information that may be required could comprise mode of transfer, location of entities or creator of data. The evidence may be generated by the evidence subject, perhaps in conjunction with a TTP, or by a TTP alone.

5.6.2 Evidence recording

A TTP may also have to record evidence in a non-repudiation role so that it can be retrieved by an evidence user or adjudicator. The evidence to be recorded will typically be received via an interface with the network over which the communication entities are sending messages. The recording process may involve the addition of a time-stamp and certain user-related information.

5.6.3 Evidence verification

The purpose of evidence verification is to provide the evidence user with the confidence that the supplied evidence will be adequate in the event of a dispute arising. The evidence verifier may be the evidence user, or a TTP trusted by the evidence user.

5.6.4 Dispute resolution

In dispute resolution, an adjudicator is responsible for collecting evidence from the disputing parties and possibly a TTP in order to make a decision which will resolve the dispute.

5.7 Auxiliary support services

The following services, which are not part of the four distinct phases described in subclause 5.6, are identified below. These are also important non-repudiation services which may be offered by a TTP:

- time-stamping;
- audit;
- delivery authority.

5.7.1 Time-stamping

A TTP may be required to certify that it has affixed a signature to a data item at a particular time. This is an important function, e.g. in certification, and non-repudiation evidence recording services. The time-stamping function will involve the receipt of information to be time-stamped, the addition of a time-stamp and a signature, and the transmission of the signed, time-stamped information back to the requester.

5.7.2 Audit

A TTP may act as an on-line authority which would carry out audit functions (e.g. logging, analysis, and reporting). In this role, the TTP would monitor the transfer of data and provide evidence about what was monitored. This is an important function, e.g. in non-repudiation evidence recording services.

The audit function will involve the reception of audit information, the storage of audit information, and the supply of audit information when required.

5.7.3 Delivery authority

A TTP may act as an on-line authority that interacts with the intended recipient of data and releases the data if, and only if, correct proof of delivery is provided by the recipient. The delivery authority function will involve the receipt of information to release once appropriate evidence is received, the receipt and verification of evidence, and the release of information.

5.8 Functions against services

Table 1 provides an example of the TTP functions that may be used in combination to provide the various TTP services as detailed in subclauses 5.1 to 5.7:

Table 1

	TTP services					
TTP Functions	**Symmetric key management**	**Asymmetric key management**	**Key escrow/ recovery**	**I&A**	**Access Control**	**Non-Repudiation**
Key generation	✓	✓	✓	✓		
Key distribution	✓	✓	✓	✓		
Key revocation	✓	✓	✓	✓		
Key archival	✓	✓	✓	✓		✓
Key storage/retrieval	✓	✓	✓ (see note 2)	✓	✓	✓
Key reconstruction			✓			
Public key certification		✓		✓	✓	✓
Certification for access control				✓	✓	
Claimant/verifier exchanges				✓		✓
Evidence generation						✓
Evidence recording						✓
Evidence verification						✓
Dispute resolution						✓
Time-stamping	✓	✓	✓	✓	✓	✓
Audit	✓	✓	✓	✓	✓	✓
Delivery authority						✓

NOTE 1: For each TTP service indicated not all of the TTP functions that are marked by "ticks" are necessary. The specific implementation of the TTP service will dictate which of these functions are optional and which are necessary.
NOTE 2: Not all schemes will need to provide key storage.

The TTP services and functions described in this subclause may be combined in a variety of ways according to the security requirements to be satisfied, for example, to meet the need for confidentiality or integrity. It should be noted that this is not a definitive table but that it does relate the major services and functions a TTP might support.

The standards and specifications referenced in [1] to [15], and [28] to [36], inclusive, provide more background information and details on many of the functions given in this subclause. They also provide most of the definitions and terminology used here.

6 TTP interfaces

6.1 Types of interface

A number of interfaces are needed to support the working and interoperability of a TTP, and the users and applications it serves. The following types of interfaces may be required to support the list of functions identified in clause 5:

- User Interface (U-I);
- Key Escrow/Recovery Interface (KER-I);
- inter-TTP Interface (T-I);
- Application Interface (A-I).

The four interfaces can be logically split into two **service** interfaces (user and key escrow/recovery) over which the TTP offers its services, and two **non-service** interfaces (inter-TTP and application) which are used to support the services offered by the TTP.

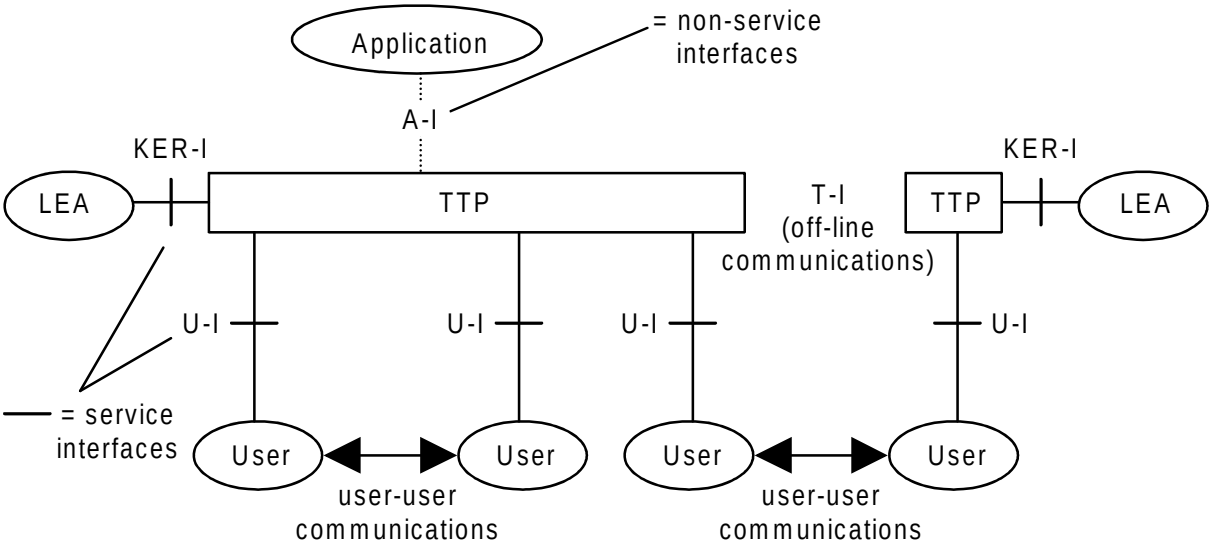

Figure 4: General interface configuration

Figure 4 shows a general configuration containing all four interfaces. The selection of services and functions to be supported by a TTP will determine the extent to which all these interfaces need to be supported and the specific configuration to be implemented. In the case of the interface, KER-I, an Law Enforcement Agency (LEA) is given in this example as the entity interacting with the TTP. This entity may however be any authorized user in accordance with the definition of key escrow/recovery (see subclause 3.1).

Secure administration and operation of the TTP also involve the operator interface which is not covered in detail in this specification. The operator interface must be implemented in a way which supports secure operation of the TTP. The operator interface might be a human or administrator interface.

6.2 Interface requirements

6.2.1 User interface

The User Interface (U-I) is the means by which a user interacts with a TTP in order to request and receive a TTP service. The user interacts with the TTP in different ways depending on what type of service is being offered. The TTP services involving the user interface are listed below together with a description of the role of the user interface in providing that service:

a) key management services:

for key management the user can request the generation, distribution, archival or escrow/recovery of various cryptographic keys via the user interface. In addition, the TTP can act as a certification authority for public keys which it generates and distributes. Certification is done using the TTP's secret key. The management of public key certificates involves the TTP providing certificate revocation lists to users via the user interface;

NOTE: The TTP may be lawfully obliged to provide this service whether or not the user has requested it according to national laws.

the user can request all or just some of the above actions to be carried out. Each action can be qualified with certain parameters, e.g. to indicate which key to distribute and where to distribute it to. Users should be able to update their keys, where possible, according to the requirements of their own security policies;

in case the TTP generates a private/public key pair for the user, the private key must not be distributed across the user interface. The authenticity and security of the private key are assured through the inherent security provided by the physical means of communication such as registered mail;

users can verify public key certificates distributed by the TTP using the TTP's public key. It is assumed that this public key is not distributed across the user interface since there will be no means to verify its authenticity cryptographically. Instead, the authenticity of the public key is assured through the inherent security provided by physical means of communication such as registered mail;

b) identification and authentication services:

in on-line or off-line identification and authentication the user can request the generation, distribution or archival of cryptographic keys or authentication tokens via the user interface. Again, these actions can be qualified with parameters;

the user can use the cryptographic keys or authentication tokens when he wants to authenticate himself to another user. The other user can also interact with a TTP in a similar manner in order to be able to verify the identity of the claimant. Although the above scheme deals with unilateral authentication, it could be easily extended to cope with mutual authentication;

in the case of in-line authentication the TTP is positioned between two users who wish to authenticate each other. In the scheme the verifier sends a request to authenticate the claimant to the TTP, via the user interface. The TTP responds by authenticating the claimant on behalf of the verifier via the user interface. Conversely, the verifier authenticates the TTP via the user interface where the TTP is vouching for the identity of the claimant;

c) access control services:

in access control the user can request the generation, distribution or archival of privilege attribute certificates via the user interface. The TTP acts as a certification authority for privilege attributes that it issues. Such privilege attributes are certified using the TTP's secret key. The management of privilege attribute certificates can involve the TTP providing certificate revocation lists to users via the user interface. Each action can be qualified with certain parameters to indicate what is to be accessed and what privileges are required;

users can verify privilege attribute certificates distributed by the TTP using the TTP's public key. Again, it is assumed that this public key is distributed in an authentic manner using physical means of communication;

d) non-repudiation services:

non-repudiation services can make use of a TTP indirectly in order to generate, distribute or archive various cryptographic keys which are used to support the non-repudiation service. Such requests are made via the user interface. Again, actions can be qualified with parameters;

non repudiation services can involve the TTP directly. The user can request that the TTP generate, transfer, store, retrieve or verify evidence. The TTP responds by sending or gathering appropriate information via the user interface. Here, the requests can be qualified with information to indicate what information should be collected;

the user can request that the TTP time-stamps certain information as part of a non-repudiation service. In addition, a TTP can be requested to act as a delivery authority for a particular user. Again for both these interactions, the user interface will be important;

the user can request that the TTP resolve a dispute which has arisen between himself and another user. The TTP responds with a decision and supporting evidence. This can involve interaction with other TTPs and/or an adjudicator.

6.2.2 Key escrow/recovery interface

The KER-I is the means by which a law enforcement agency can request and receive from a TTP escrowed information for confidentiality purposes, to enable encrypted communications lawfully intercepted to be decrypted. It can also be used as part of an organization's data recovery service or for lawful access (see subclause 5.3).

This interface can be used in TTP services which involve the generation and distribution of cryptographic keys intended to be used for encryption. As such, this interface is only used in providing TTP supported key management services. Moreover, the presence and usage of this interface depends on the particular legal requirements which exist in the TTP's operating environment.

When acting as a key management server the TTP can generate and distribute an encryption key to a particular user. The TTP may be legally obliged to escrow information which will enable a law enforcement agency to decrypt data which has been encrypted. This can include releasing a secret key to be used in a symmetric algorithm, or releasing a private key to be used in an asymmetric algorithm.

Any TTP scheme will need to provide escrowed confidentiality information to enable access to a user's incoming and outgoing communications. In the general case (see reference [2]), where the communicating users have two separate TTPs (T_A and T_B) and the communication is two-way, four scenarios might exist (where the first two correspond to what seem to be the most likely scenarios):

- the TTP T_A is required by a lawful authorization to provide access to keys relating to outgoing communications from a user for which it acts;
- the TTP T_B is required by a lawful authorization to provide access to keys relating to incoming communications to a user for which it acts;
- the TTP T_A is required by a lawful authorization to provide access to keys relating to incoming communications (from a user for which it acts) to a user for which it does not act;
- the TTP T_B is required by a lawful authorization to provide access to keys relating to outgoing communications (to a user for which it acts) from a user for which it does not act.

In each scenario the TTP provides the LEA with the relevant escrowed information. This will involve use of the interface KER-I and may involve interaction with another TTP via the inter-TTP interface (T-I).

6.2.3 Inter-TTP interface (T-I)

The T-I is the means by which a TTP can interact with other TTPs. This interface can be used to ensure the inter-working of TTPs in providing services over different user domains.

In general, TTPs should not be required to interact on-line during the process of a given TTP service. Rather the TTPs would usually interact off-line in order to carry out actions which are required to support services which are offered to users. In some cases the response times may be critical. Reliance upon on-line TTP interaction is likely to impose serious performance degradation on some TTP services.

TTPs can interact in different ways depending on what type of service is being offered. The TTP services involving the T-I are listed below together with a description of the role of the T-I in providing that service:

a) key management services:

in acting as a certification authority a TTP generates and distributes public key certificates which can be verified using the TTP's own public key. A TTP's public key may in turn be certified by another TTP. The T-I could be used by TTPs in process to exchange and verify each others' certificates. The T-I is also used to send revocation lists and alert messages between TTPs;

certain TTP services such as key escrow/recovery require two TTPs to interact in other ways, e.g. to generate a shared secret. Some other schemes involving a group of TTPs can require the generation of a shared conference key. In this case inter-TTP communication may not be required. Instead, the application interface could be used by the TTP to interact with a public database containing information that could be used to calculate the conference key;

b) identification and authentication services:

on-line and off-line user authentication can involve inter-TTP communications if a public key is to be verified through a certification path. This is similar to the use of the T-I as identified above for key management services;

in-line authentication may involve a sequence of more than one in-line TTPs, where one TTP will act as the claimant for the next TTP which acts as the verifier. In this case the T-I is used to carry out authentication between TTPs;

c) access control services:

again, access control services can involve the verification and management of public key information requiring interaction between TTPs via the T-I;

d) non-repudiation services:

again, non repudiation services can involve the verification and management of public key information requiring interaction between TTPs via the T-I. In addition, evidence generated as part of a non repudiation service may need to be shared between TTPs via the T-I.

6.2.4 Application interface

The Application Interface (A-I) is the means by which a TTP can interact with other (non-TTP) applications. These applications can be used to support the TTP in carrying out its role.

The application interface can be used to support access and availability of services and information needed by the TTP. For example, this could be an interface to some directory service to some management facility or some network operator/service provider application.

a) key management services:

in offering a key management service a TTP can interact with a public database in order to obtain information about another entities public key. In this case the application interface will be used to allow the TTP to communicate with the directory;

the application interface also allows management entities to interact with the TTP to provide information on how it should operate in its current environment This can include policy directives on key management services. The application interface can also be used to alert the TTP of security related events which may affect the operation of the TTP, (e.g. the TTP may have to revoke a certificate it has issued);

b) identification and authentication services:

the TTP can interact with applications to support its functional and operational role. Such interaction may involve the use of one or more authentication services;

c) access control services:

the TTP can interact with applications which are specific to the user's domain in order to obtain information on the local access control security policy;

d) non-repudiation services:

TTPs can interact with management elements in a network via the application interface in order to obtain evidence which may be used in a non-repudiation service. In addition, a TTP can pass evidence to an external adjudicator via the application interface. The adjudicator can then make a decision which would settle the dispute.

7 Legal aspects

The use and application of TTPs should comply with the relevant national laws and regulations. For example, concerning, the protection of personal data, issues related to the use and export of cryptographic functions, lawful interception and lawful access.

7.1 Liability

Liability between a TTP and a user shall need to be defined by an initial legally binding contract. Beside the mutual agreement about the future use of digital signatures, the contract shall also cover legal aspects regarding the services offered.

In case of transactions between users, liability shall be guaranteed by the use of a digital signature scheme provided by a TTP. In case of any dispute between users a TTP could provide evidence. Non repudiation services could provide the evidence required.

7.2 Legal basis for digital signatures

Transactions in general, require an agreement between the parties involved. Such an agreement is often confirmed by the use of a signature. Current national laws provide the legal base for (the use of) these signatures. Accordingly, electronic transactions require (electronically) signed agreements. As agreements are mostly presented in electronic form the integrity needs to be guaranteed. Moreover, it is of importance that the agreement can not be repudiated by any party involved. The use of a digital signature scheme supports both demands.

The Swedish Customs Act (1987) legally approves the exchange of electronic information, including the use of digital signatures, within customs administration. In Belgium a framework for EDI (Electronic Data Interchange) agreements is in gestation. Forthcoming German regulations on multimedia will take account of the use of digital signatures. Controls on the use of digital signatures exist in no other European country, but export control regulations do apply. It can also be remarked that South Korea and many American states, such as Utah and Oregon, already have legislative recognition of digital signatures. In conclusion, a European wide legal base for (the use of) digital signatures is lacking.

7.3 Protection of privacy and personal data

Application of encryption to guarantee confidentiality achieves the protection of privacy. As privacy protection is essential for users of these services, a TTP is trusted also to respect the privacy domain of its users.

With service provision in general, different kinds of individual user information is being stored. By this information a user profile can be created, which can also be used for internal market analysis. The fear of individual user information being passed on to, for example, direct marketing organizations is justified. The probability that a TTP will pass on individual user information is low. The existence of a TTP implicitly depends on the trust of its customers. However, there is always a possibility individual user information could be misused. The passing on of such information should be severely restricted or forbidden, and should be addressed in TTP contracts, and licences as appropriate, according to national and European legislation.

The European Commission has made two proposals, Directives [16] and [17], to establish a common framework for data protection within the European Union. The first proposal has resulted in a general privacy directive (Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data [16]).

The second proposal relates to a specific telecommunications privacy directive (Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the Integrated Services Digital Network (ISDN), and in the digital mobile networks). At this moment an agreement concerning this directive has been accomplished at political level. Since this directive concerns new functions in telecommunications networks, and a TTP provides new functions, a TTP has to operate in correspondence with both privacy directives.

7.4 Export control

Export of cryptographic functionality is subject to different types of policies and regulations. On 1 March 1995 a European Union regulation was established concerning the export control of so called "dual-use goods" (Council Decision of 19 December 1994 on the joint action adopted by the council on the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods, 94/942/GBVB [18] and Council Regulation (EC) No. 3381/94 [19] of 10 April 1995 setting up a Community regime for the control of exports of dual-use goods (Pub. No. L 90), 21 April 95). These are products which are being applied in the public sector as well as in the military sector.

This regulation can be seen as the European contribution to the Wassenaar Arrangement. The Wassenaar Arrangement is an international agreement to be able to control the export of strategic goods and of products which are on the dual-use goods list. This agreement is the follow up of the former worldwide COCOM.

Cryptographic functions related to confidentiality services, such as algorithms or key management functions, which are intended for export have to be specified in conformity with export control regulations. The ability to act accordingly depends on the transparency of export control criteria.

7.5 Lawful interception

TTP key management systems provide a means to balance the respective interests of users and LEAs in relation to key escrow/recovery for confidentiality purposes; ideally such a key management infrastructure should facilitate national and international interoperability. Lawful access across national boundaries may be achieved through the use of multilateral agreements between nations.

Lawful interception of telecommunications traffic is commonly recognized as an important instrument to fight crime and to assure national security. LEAs have the need to intercept incoming and outgoing telecommunications traffic, which is transported via telecommunications networks, without knowledge of e.g. the interception subjects and the foreign country or countries involved. There are strict conditions and demands with regard to the use of this instrument. Accordingly, a lawful authorization is required corresponding to the national laws and regulations of the individual countries.

Naturally, the intercepted telecommunications traffic needs to be interpretable for the LEAs. The European resolution on lawful interception says that if network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, LEAs require the network operators/service providers to provide intercepted communications *"en clair"* (i.e. the encryption applied by these parties has to be removed) (European Union Council Resolution on International Requirements for the Lawful Interception of Telecommunications, January 1995 [40]).

This resolution refers to the situation in which encryption is included in the basic telecommunications service (e.g. the digital mobile system GSM). In this case the network/service provider controls the use of the encryption, which is provided by them, in the public telecommunications network.

An on-line and off-line TTP does not control the use of encryption on a telecommunications network. It provides the means for encryption as a value added service to be applied by the user. Hence, an on-line and off-line TTP can not provide intercepted telecommunications traffic *en clair*. However, an in-line TTP is positioned between the end-users in the telecommunications network and therefore controls the use of encryption, applied by the in-line TTP, in this network. Accordingly, the intercepted telecommunications traffic can be provided *en clair*.

The telecommunications traffic has to be made interpretable by the LEA. The on-line and off-line TTP architectures may support lawful interception by providing the appropriate key(s). An in-line TTP architecture will have to support lawful interception by providing the intercepted communications *en clair*. Moreover, TTPs may support also the providing of keys in case of stored information.

The provisioning of keys and the *en clair* telecommunications traffic can be supported by the key escrow/recovery service. Beside fulfilling the specific governmental requirements regarding interception, this service can also be used to support disaster recovery of data. For example, in case of lost or corrupted cryptographic keys, copies of these keys can be provided. The key escrow/recovery service therefore strikes a balance between both the governmental and market demands.

The handover of *en clair* telecommunications traffic requires a lawful interception handover interface.

7.6 Lawful access

Lawful access allows those entities that have some lawful authority under the law (e.g. criminal, public, civil, private or business law), to have access to certain information in order discharge their legal duties.

A law enforcement agency might have the need to decrypt data stored in an encrypted form. In case the stored data has been encrypted by the user, a TTP may support lawful access by the provisioning of the appropriate key(s). When the encryption is applied by the TTP itself, the TTP may have to provide the encrypted data *en clair*. Lawful access across national boundaries may be achieved through the use of multilateral agreements between nations.

It may be the case that there is a requirement for lawful access to data stored in an encrypted form, not related to criminal or public law, but related to civil, private or business law, where those that have been lawfully authorized to deal with the case in question need access to such data to discharge their legal duties e.g. dealing with a bankruptcy or a civil liability suit. Businesses need to observe statutory or civil obligations and to comply with legal requirements, e.g. the keeping of accounting records. It may be that lawyers, auditors or accountants need access to carry out their activities, e.g. checking company accounts and records, or even, in the case of solicitors and executors dealing with the administration of a deceased person's estate may need access to relevant stored data which may have been securely retained using encryption.

Beside fulfilling the specific governmental requirements regarding lawful interception and the requirements regarding lawful access, the key escrow/recovery service can also be used to support disaster recovery of data. For example, in case of lost or corrupted cryptographic keys, copies of these keys can be provided. The key escrow/recovery service therefore strikes a balance between both the specific governmental and market demands.

8 Commercial issues

The design and operation of a TTP scheme may be such that it is capable of offering services to users on a commercial basis. The use of such a TTP scheme should provide visible benefits for the user. It is important however, that the standards to be developed do not unnecessarily restrict such commercial TTP operations. The following subclauses highlight commercial requirements that should be taken into account in the formulation of the standards.

8.1 Competition and openness

It is expected that an open market will develop for the provision of TTP services, with competition between TTP service providers and possible co-operative inter-working between TTPs where necessary. Any TTP scheme should therefore permit national and international operation thus allowing users in any country, where an appropriate TTP resides, to communicate securely.

The interfaces required to enable this inter-working between users subscribing to different TTPs should be implemented using open standards and publicly available specifications. This will allow all forms of electronic communication to be supported by the scheme.

Any standardized TTP scheme should also be based on well known techniques and details of the scheme should be publicly available. In addition, the standardized scheme should not be dependent on a single encryption algorithm,

The standard to be developed, from the requirements given in this document, should aim as far as possible to avoid creating barriers for clients of the TTP and for these clients to be able to communicate securely to one another.

8.2 Scope and flexibility

It is envisaged that TTPs will vary greatly in the nature and scope of their operations. For example, in terms of the:

- TTP services they provide and the internal functions they implement;
- number of users and clients they can support;
- application areas and interfaces they serve;
- nature of their users and clients.

The services which a TTP may provide to its clients will be a commercial decision. Any TTP standard should not unnecessarily restrict the variety of TTPs that can be implemented. In particular, the standard should, as far as possible, avoid mandating aspects that would prohibit or penalize the providers of small-scale TTPs, or limit large scale TTPs being implemented.

8.3 Licensing and accreditation

The services provided by a TTP will have to be trusted by their clients. In a global environment supporting, e.g. electronic commerce, there will have to be trust of, and between, the various bodies fulfilling this function.

TTPs supplying services to the general public will need to create such trust and provide some form of assurance of this fact. In such cases an organization wanting to operate a TTP may be required to be licensed or accredited to ensure that they can fulfil certain "fit for purpose" criteria. For example, do they have appropriate liability cover, what is the competence of those employees operating the TTP, do they adhere to quality management standards, and do they have the necessary security measures in place to manage the TTP process. As with the other commercial aspects of operating a TTP, the ETS to be developed should avoid mandating anything that would have an adverse effect on their competitiveness, on how they are implemented or present barriers with regard to their use, as a result of any such licensing.

8.4 Billing of TTP services

In the case where the TTP services are offered on a revenue generating basis, the TTP may need to be able to bill its clients for the use of TTP services. The charging should be based on the value of the services received by the user. Any charging should be visible to the customer.

As part of the inter-connection between TTPs, there may need to be some form of exchange of billing information to support cross-charging. The storage and exchange of billing information needs to be protected against unauthorized access and modification (see subclause 7.3). This storage and exchange of billing information is not planned to be standardized in the TTP specification.

Annex A:
Basis for a standardized TTP scheme

This annex provides a summary of the requirements that have been presented in the various clauses of this document.

These requirements form the basis for a set of TTP standards. They are grouped according to whether they relate to general matters of TTP implementation and operation, specific security matters related to the management of TTPs or if they relate to the specification of internal functions and operations, and external interfaces.

A.1 General standardization requirements

1) Any TTP standards should facilitate the design and operation of TTPs services to be offered to users on a commercial basis. By signing up to a licensed TTP, the user should be able to communicate securely with every user of every TTP with whom their TTP has an agreement.

2) In addition, to supporting secure communications between users, the TTP standards should also support the protection of data in storage:

   - the distribution of cryptographic keys that can be used to protect data in storage;

   - the ability for lawful access to cryptographic keys to be used for protecting data in storage.

NOTE: Lawful access should not apply to keys used for authentication and data integrity.

3) A TTP scheme based on these standards should allow national and international operation thus enabling users in any country, where an appropriate TTP resides, to communicate securely.

4) Any TTP standards should not restrict the form of electronic communications that can be supported.

5) TTP standards should be based on well known and publicly available security techniques and specifications. In addition, these standards should support a variety of encryption algorithms, in both hardware and software.

6) Any TTP standards should enable TTP schemes to be implemented which are compatible with the different laws and regulations of participating countries concerning data protection, lawful interception, as well as on the use, export and sale of cryptographic mechanisms.

7) Any TTP standards should enable practical solutions to be implemented such that:

   - users can update their keys, where possible, according to the requirements of their own security policies;

   - a user should not need to communicate with TTPs other than their own;

   - they should not require on-line communication between TTPs;

   - access can be provided to the user's incoming and outgoing communications, where lawful authorization is given;

   - any attempted abuse of the TTP scheme can be detected;

   - those with lawful authorization to have access to information cannot fabricate false evidence.

8) Interfaces and protocols specified by TTP standards should include the required security functions to protect the interactions among entities of the TTP scheme and to support secure interoperation.

A.2 Security requirements for a TTP scheme

In practice an assessment should be carried out to identify the level of risk associated with the TTP scheme to be implemented. The type and strength of security requirements to be selected will depend on the specific services provided by the TTP as well as on the risks involved in case the TTP would become compromised. The security requirements associated with these identified risks should be specified in a security policy for the TTP implementation. This assessment and policy development should take into consideration the following:

1) actors, such as users, administrators and operating personal of the TTP should only have access to information and resources they are entitled to;

2) the administrative procedures shall ensure the unique and secure identification, and registration of users and operators of the TTP services;

3) highly sensitive information, which is fundamental for the trust in the TTP scheme, such as the private key of a CA or the top-level key of a Key Distribution centre, shall be generated, installed and managed by well-documented and trustworthy procedures;

4) in order to ensure the traceability of operations and transactions and the accountability of subjects related to the scheme the following measures shall be taken with the required strength:

   - authentication of subjects;

   - electronic signature of all security sensitive requests, transactions and operations;

   - non-erasable audit log records of all security sensitive events, but which are not open/releasable to other than proper authorities (i.e. not available to users or auditors);

5) in order to protect the privacy and business interests of all the involved actors, information at interfaces, carried by protocols and on storage media, shall have the required level of integrity and confidentiality protection;

6) system security, such as operating system security, of all components governed by the security policy of the TTP shall provide the necessary protection in the actual operating environment (e.g. terminal equipment in places);

7) adequate security management shall cover the initiation, monitoring and control of the security services protecting the TTP scheme;

8) procedures shall be available to recover the secure state of the scheme in case of a security breach. This implies the recovery or replacement of top-level secret key(s) of the TTP;

9) mechanisms may need to be in place to safeguard against any single point of vulnerability that might exist in systems where a TTP is able to recover the encrypted data by using key escrow/recovery;

10) if required by the security policy of the parties involved the TTP shall provide the means to ensure that only keys needed by an authorized entity can be recovered by the TTP.

A.3 TTP functional and interface requirements to be standardized

A set of TTP standards is required to cover the functional requirements described in clause 5 of this document. This includes specification of the external interfaces described in clause 6 to enable external entities to interact with the TTP.

Also required is a specification of the internal operations and interfaces to support the various internal TTP functions and the provision of TTP services.

The following requirements need to be considered and implemented in accordance with the general requirements listed in clause A.1:

1) these standards should enable TTP schemes to offer a range of services including some or all of the following:
   - key management services;
   - key escrow/recovery services;
   - identification and authentication services;
   - access control services;
   - non-repudiation services;
2) to provide the TTP services identified in clause A.3, item 1) some or all of the following functions need to be specified in the standard (see table in subclause 5.7 to determine which functions are needed by which service):
   - key generation;
   - key distribution;
   - key revocation;
   - key archival;
   - key storage/retrieval;
   - key reconstruction;
   - public-key certification;
   - certification for access control;
   - claimant/verifier exchanges;
   - evidence generation;
   - evidence recording;
   - evidence verification;
   - dispute resolution;
   - time-stamping;
   - audit;
   - delivery authority;

3) these standards should enable TTP schemes to implement some or all of the following interfaces, as described in clause 6:

   - User Interface (U-I);
   - Key Escrow/Recovery Interface (KER-I);
   - inter-TTP Interface (T-I);
   - Application Interface (A-I).

   The exact specification of these interfaces will depend on the specific services the TTP offers and the internal functions it needs to implement to provide these services. Some of these interfaces may be mandatory, e.g. KER-I, in the case of encrypted communications and lawful authorization, and some will be standard, such as U-I.

Annex B:
Examples of the use of TTP services

B.1 TTP based security services

There are a number of applications and security services that could be based on TTP services. For example, the application of digital signatures for integrity purposes to support inter-business use of electronic commerce, or end-to-end confidentiality with support for lawful interception using TTP key management services.

Both digital signatures and end-to-end confidentiality are seen as increasingly important services as users are becoming more likely to transfer commercially sensitive and critical information via telecommunications networks. However, in the case of end-to-end encryption, there is also a need to be able to provide legal interception where necessary and appropriate which demands the use of a key escrow/recovery mechanism. In this case a TTP could be used to act as a key escrow/recovery centre.

Other examples might be secure billing, authentication servers, certification services, directory services and notary services.

B.2 Certification Authority

In order to support the use of digital signatures, a TTP can act as a CA by carrying out public key certificate generation. There may be different infrastructures, hierarchical and non-hierarchical, to support CAs, as defined in various international standards (see references [10], [13]. [28], [29], [30] and [36]). A widely accepted format for such certificates is specified in the 1993 version of ITU-T Recommendation X.509 [37] (known as X.509 version 2). This standard is also published as an International Standard called ISO 9594-5 [8]. A revised version of this specification (known as X.509 version 3) is currently under development. This CA will need to have its own digital signature key pair.

The generation of a user public key certificate by a certification authority (TTP) requires the following main steps:

- the user identity needs to be verified;
- the CA needs to be supplied with a public signature verification key for the user. This may be part of a key pair generated in advance by the user, in which case the user will pass the CA its public key, or it may be part of a key pair generated by the CA for the user, in which case the CA also needs to pass both parts of the key pair to the user;
- the CA will need to pass its public signature verification key to the user;
- the CA can then generate the user certificate, which will be a string containing the user name, user verification key, certificate expiry date, and other information, all signed using the CA's private signature key;
- the user certificate will then be passed to the user, as well as possibly being distributed by other means (e.g. via an X.500 directory).

In acting as a certification authority a TTP generates and distributes public key certificates which can be verified using the TTP's own public key. A TTP's public key may in turn be certified by another TTP leading to a situation where a certification path is formed. Thus in order to verify a given public key, the user may have to verify an ordered sequence of certificates until he reaches a public key which he believes to be authentic. The T-I could be used by TTPs to exchange and verify each others certificates. There are two general methods in which a user can obtain an authentic public key. Either the user himself can verify all the certificates in the certificate path, or his TTP can verify the certificates in the path and generate a cross certificate for the public key. The user can then verify the cross certificate using his own TTP's public key. The T-I is also used to send revocation lists and alert messages between TTPs.

CRLs can be generated and distributed by a TTP or any other TTP at a higher level in a hierarchy of TTPs.

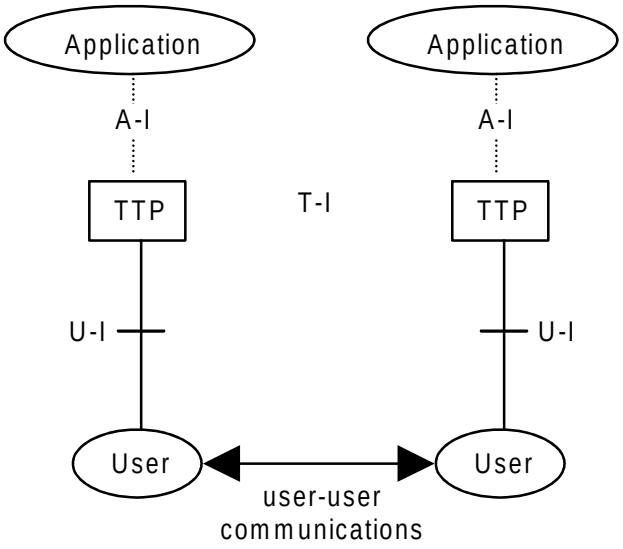

Figure B.1: General configuration for supporting digital signatures

Figure B.1 shows a general interface configuration to support those services that would use digital signatures. This configuration needs to be considered with respect to the above comments on CAs and the generation and distribution of certificates.

B.3 Key escrow/recovery centre

The obvious approach to supporting end-to-end encryption is to make use of precisely the same certification structure as is commonly proposed to support digital signatures (see above). Instead of requiring the TTP to sign the user public verification key, the TTP is asked to sign the user's public encryption key (for some asymmetric encryption scheme), acting as a type of CA.

However, in the case of end-to-end encryption, there is a potential need to support key escrow/recovery. That is, in many countries, government agencies, or other legally supported bodies, may need the means to decrypt some users' traffic (both incoming and outgoing). Typically, a TTP will be required to supply the keys to decrypt a particular user's messages to an LEA, given that the interception agency has the appropriate legal authority (lawful authorization).

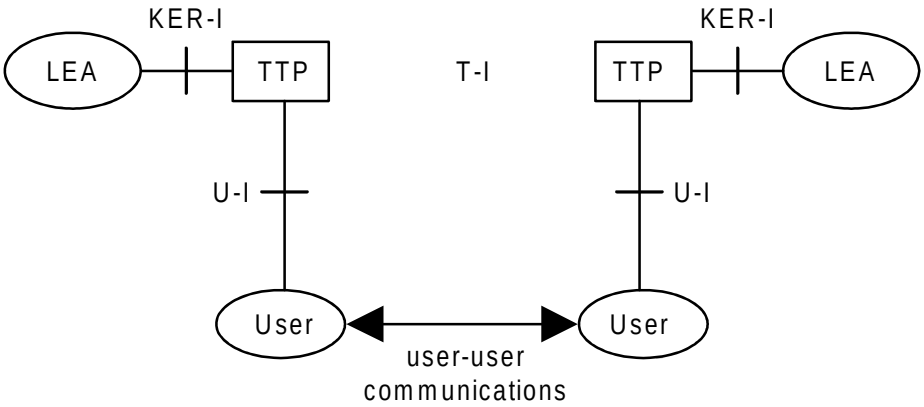

Figure B.2: General end-to-end encryption configuration with key escrow/recovery

There are a number of schemes to support lawful interception that have been devised, many of them making use of some kind of TTP. Typically such a TTP combines the roles of a key distribution agent for its users, and as a supplier of user keys (under lawful authorization) to an interception agency.

It is important to note that, unlike the CA used to support digital signatures, TTPs used to support end-to-end encryption may need to be on-line in certain cases.

A TTP could also offer a disaster recovery service based on key escrow/recovery. A user could retrieve lost or corrupted keys from a TTP using a similar mechanism to that used to uncover keys for lawful interception.

B.4 Trusted key distribution centre

In this role, a TTP could securely generate and load secret key information onto a physically secure device. Such a device may be used as an identity module for identification and authentication purposes, for example. The user trusts the key distribution centre to destroy, or securely archive, the secret key after it is loaded onto the physically secure device.

B.5 Fraud detection centre

A TTP could act as an entity which can alert various parties to possible fraudulent behaviour based on real-time event sequence monitoring and audit. The advantage of using an external TTP for this purpose, is that the TTP can independently monitor all entities in a particular system to identify fraud scenarios that occur between different entity domains. The user trusts the fraud detection centre not to fabricate evidence regarding the user's involvement in fraudulent activity.

B.6 Legal services

Legal TTP services are offered essentially to prevent disputes, or resolve them in a structured, efficient, accepted by all parties involve and non-controversial way.

Prevention of disputes arises essentially from the very ability of legal services to assign responsibility and fault, should one occur. Thus, legal services must essentially be able to verify the application or non-application of rules and the evidence pertaining to them.

Legal services may or may not generate the evidence itself. In other words the question is whether a third party offering a trusted service also arbitrates litigation's pertaining to its principal service.

Example of these services are the notary services: Notary services derived from the traditional Notaries functions. The notary is asked to assess the identity of the party/parties using identification documents the party provides. The notary is requested to take the acknowledgement of the party. In taking an acknowledgement, notaries need not read or vouch for the accuracy or legal effect of terms that are incorporated by reference. In fact, in some jurisdictions notaries are not permitted to read the content of the document being notarized, including incorporated terms. The notaries form of acknowledgement does not represent that the notary has either reviewed or approved any portion of the agreement/form, including the incorporated terms and conditions.

B.7 Guaranteed date and time stamping

Digital Time-stamping Service (DTS) issues time-stamps which associate a date and time with a digital document in a cryptographically strong way. The digital time-stamp can be used at a later date to prove that an electronic document existed at the time stated on its time-stamp. For example, a physicist who has a brilliant idea can write about it with a word processor and have the document time-stamped. The time-stamp and document together can later prove that the scientist deserves the Nobel Prize, even though an arch-rival may have been the first to publish. To be reliable, the time-stamps must not be forgeable. The use of a DTS would appear to be extremely important, if not essential, for maintaining the validity of documents over many years.

Suppose a landlord and tenant sign a twenty-year lease. The public keys used to sign the lease will expire after, say, two years; solutions such as re-certification of the keys or resigning every two years with new keys require the co-operation of both parties several years after the original signing. If one party becomes dissatisfied with the lease, that party may refuse to co-operate.

The solution is to register the lease with the DTS at the time of the original signing; both parties would then receive a copy of the time-stamp, which can be used years later to enforce the integrity of the original lease.

B.8 Negotiable document transaction

Some conventional physical documents, such as, e.g. the bill of lading and the bill of exchange, must be negotiable. The possession of the document must allow to give title to anybody who can present it. The electronic equivalent is also needed.

Negotiable documents entail that their physical uniqueness must be protected against duplication; it must be easy to distinguish a copy from its original. This is the case with hand signed paper documents; the hand-written signature cannot be copied such that the copy could not be distinguished from the original. True, a digital signature does protect the integrity of the signed electronic document; however, it can be easily copied so that the physical original cannot be discerned from its copies.

This impedes the usage of electronic communication, e.g. in maritime trade. The sender of a cargo produces a unique document, the bill of lading, hands a copy to the shipper and sends the protected original to the receiver. The receiver may trade the original and its title or keep it. Whoever presents the original to the shipper will be handed over the cargo. The shortcoming of the paper bill of lading is the fact that it takes time to transport it, particularly as it is a piece of value and must be well protected. Therefore, an electronic substitute should be found that protects its originality and can be transacted in telecommunication systems.

B.9 Storage of electronic information

The TTP saves users' files in safe locations and maintains a personal directory for the user. The user can access that directory at any time to see what files have been saved and when they were saved. Alternatively, the records may be kept off-line. Retention needs and duration will vary according to applicable laws and records retention and other management policies.

Such a facility could also be used to provide a means for users to protect software using escrow/recovery techniques to counter the impact of commercial and operational failures.

Annex C:
National and international policies

The following provides some information on national and international policies related to TTPs. Additional information can be found in references [16] to [23] and [39], or via the Internet Web page given at the end of each clause.

C.1 European Union

Following the first INFOSEC programme (1992 - 1995) [34], the European Commission, together with SOGIS, is preparing a specific Council Decision concerning Trusted Third Party/ European Trust Services (TTP/ETS). It is a special program with a considerable policy impact. Within this framework all national policies within the European Union have to be realized in order to establish a pan-European TTP infrastructure. A TTP will typically be licensed and can provide security services such as:

- authenticity and integrity functions: key verification, digital signatures, time stamping;
- confidentiality functions: protection of the confidentiality of messages by, for example, key distribution and encryption;
- so-called key retrieval/recovery/escrow services: the re-distribution of keys in case of loss, sickness of employee or delivery of keys to support lawful interception.

The point of departure is that the market will form these developments by itself in correspondence with the specific needs of the government concerning public safety and national security.

In addition, the European Union and European industry have a number of activities related to EII - see reference [25], the Information Society - see reference [24] and the GII - see references [24] and [26]. Applications for TTPs and the need for standardization in this area are featured in many of these activities.

Further information and updates can be found on the Internet Web page:

http://www.cordis.lu/infosec

C.2 France

The French cryptography policy is accommodated by telecommunications legislation and is now subject to change. The use of cryptography related to confidentiality will be liberalized. However, confidentiality services need to be obtained from a TTP licensed by the French government. Other cryptographic applications to protect integrity and authenticity will more or less be free to be used in the new situation.

Further information and updates can be found on the Internet Web page:

http://www.telecom.gouv.fr/francais/activ/techno/tecncom.htm

C.3 Germany

At this moment the German government is working on a draft Multimedia Act (Informations - und Kommunikationsdienste - Gesetz - IuKDG). This will include telecommunications services, digital signatures as well as requirements to adjust other types of legislation. It is expected that the legislative part on digital signatures ("Digital Signature Act": Signaturgesetz - SigG [22]) will be approved in the beginning of 1997. According to this law, and the underlying ordinance, the Regulation Authority, after checking their concepts and technical/organizational aspects, grants licences and key certificates to "trust centres" and the trust centres generate and give key-pair certificates (public and private/secret key) to their customers.

Key management and time stamping services are the trust centres main responsibilities. If persons using different signature schemes (algorithms) want to communicate, the trust centres involved may provide the possibility to do so. The strength of the algorithms has to be evaluated by the Regulation Authority.

It is noted, that although in the given procedure it is allowed to use any digital signature method, only the one which complies with the law is accepted as the legally binding alternative to a handwritten signature.

Further information and updates can be found on the Internet Web page:

http://www.iid.de/rahmen/iukdg

C.4 Netherlands

As a result of international developments and the request by market parties, interdepartemental debates have taken place concerning cryptography policy and regulation. This discussion continues.

In accordance with the obligation to co-operate in case of lawful interception, public network operators and service providers have to deliver the original signal i.e. the encryption applied by these parties has to be removed. The encryption used in the (individual) application domain (end-to-end encryption) has to be dealt with otherwise.

The TTP concept will also be introduced in the Netherlands. The Dutch government now has the task of creating prior conditions concerning the boundaries within which a TTP structure can be established by the market sector. This also includes quality aspects. If this approach does not lead to any results, cryptography legislation could be reconsidered.

C.5 United Kingdom

The United Kingdom government recently published a policy paper on regulatory intent concerning the use of encryption on public networks. This policy proposes the licensing and regulation of TTPs to provide a range of information security services to users, whether they are corporate users or individual citizens. The services which a TTP may provide for its customers will be a commercial decision. Typically, provision of authentication services may include the verification of a client's public key, time stamping of documents and digital signatures. TTPs may also offer a service of key retrieval (for documents and files that have been encrypted by employees) in addition to facilitating the real time encryption of a client's communications. The government intends to bring forward legislation on TTPs following consultation on detailed policy proposals.

Further information and updates can be found on the Internet Web page:

http://www.dti.gov.uk

C.6 OECD

At the beginning of 1996 the OECD established, via the ICCP, a high level expert group to work on a set of guidelines for the development of an international cryptography policy, and also for the elaboration of the G7-GII program. The final draft of these guidelines is expected early in 1997.

C.7 United States of America

On 1 October 1996 vice-president Al Gore announced that the American government wants to have a more liberal export control policy for advanced commercial encryption technology during a period of two years. Firstly the maximum key length will be stretched to 56 bits, providing a key recovery system is built into the product concerned A longer key length is maintained for cryptographic products that are applied in the financial sector. Secondly, a TTP is to make the key available to the authorities with a lawful authorization, so the information enciphered by this product can be deciphered. If a Key Recovery Centre (read TTP) is located abroad, the required key(s) must be made available through regular extradition treaties and bilateral agreements. The use of key recovery products in the United States is not bound to restrictions, though. If after two years it becomes clear that a cryptographic product does not support a key recovery system, the export of this product will be prohibited. In addition the export license will have to be renewed every six months during this period. It is not clear yet what the material and judicial consequences of such bilateral agreements will be. Also the National Institute of Standards and Technology (NIST) are developing specifications for a Federal Public Key Infrastructure [30] (see also references [32] and [33]).

Further information and updates can be found on the Internet Web page:

http://csrc.nist.gov/

History

Document history		
Edition 1	June 1995	Publication as ETR 189
V1.1.1	May 1997	Membership Approval Procedure MV 9728: 1997-05-13 to 1997-07-11