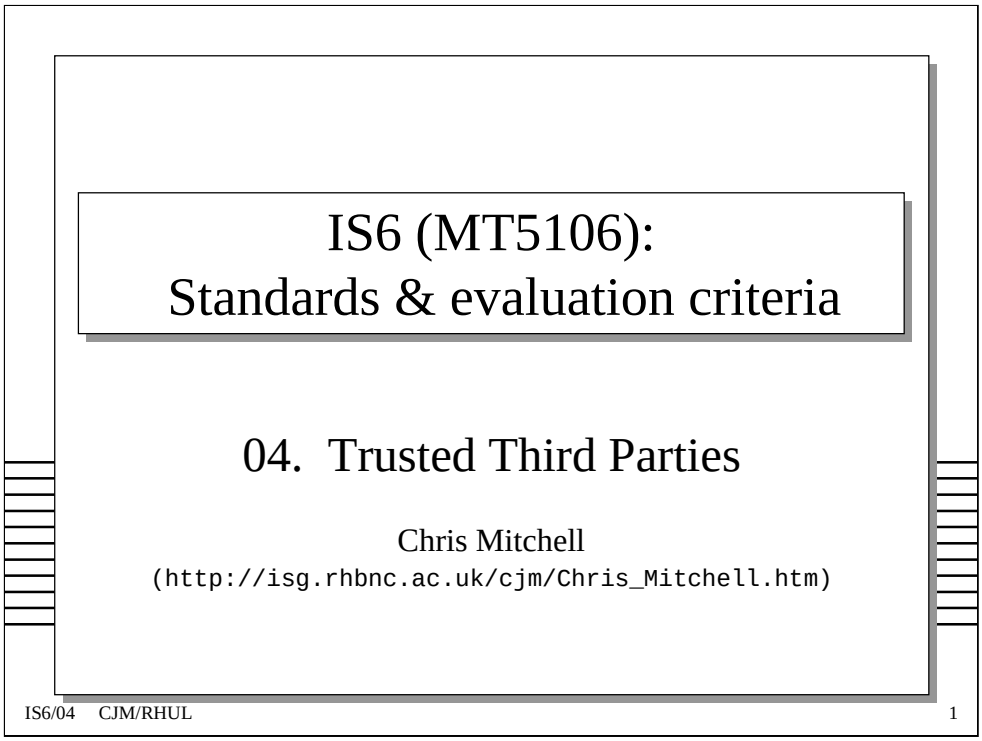
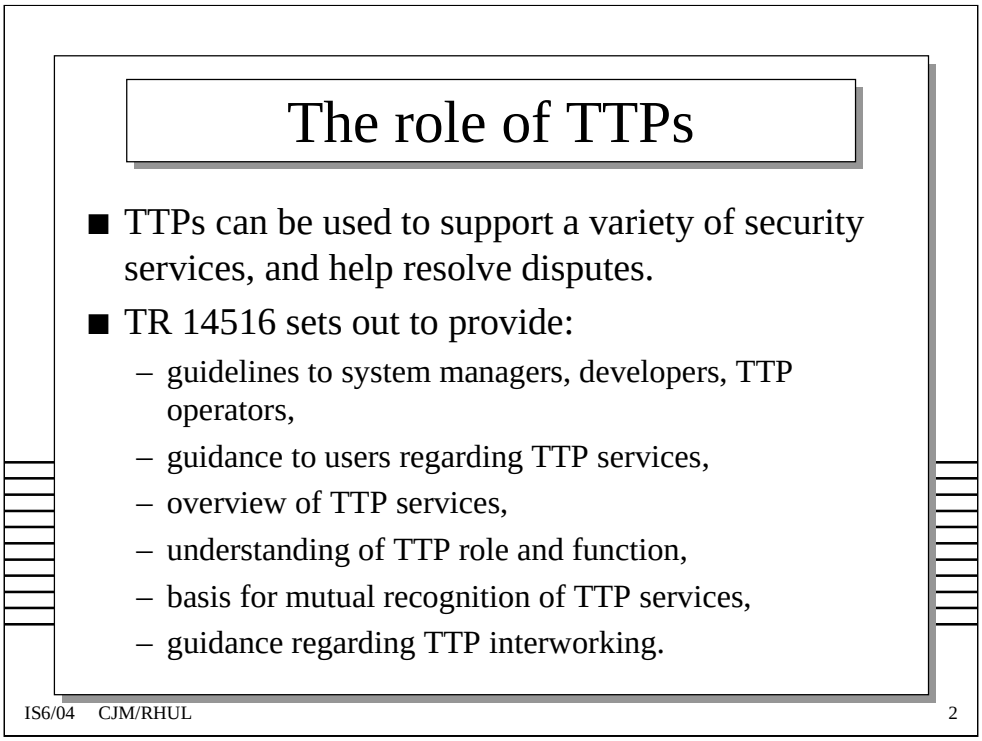


We now consider the ISO/IEC technical report concerned with the use and management of *Trusted Third Parties*, or *TTPs*, namely ISO/IEC TR 14516. This material is not covered in any of the recommended texts, although Section 8.4 (pages 212-213) of Warwick Ford's *Computer Communications Security* discusses the use of TTPs in providing non-repudiation services.

The recommended background reading associated with this part of IS6 is as follows:

• ISO/IEC JTC1/SC27 N2138, *PDTR 14516: Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party Services*. November 1998.



Before considering the draft ISO/IEC Technical Report, we briefly consider the role which may be played by TTPs in secure systems.

TTPs can be used to support a wide variety of different security services. Moreover TTPs can be used to provide evidence to resolve disputes.

TR 14516 sets out to:

• provide guidelines to system managers, developers and TTP operators, on the use and management of TTPs,

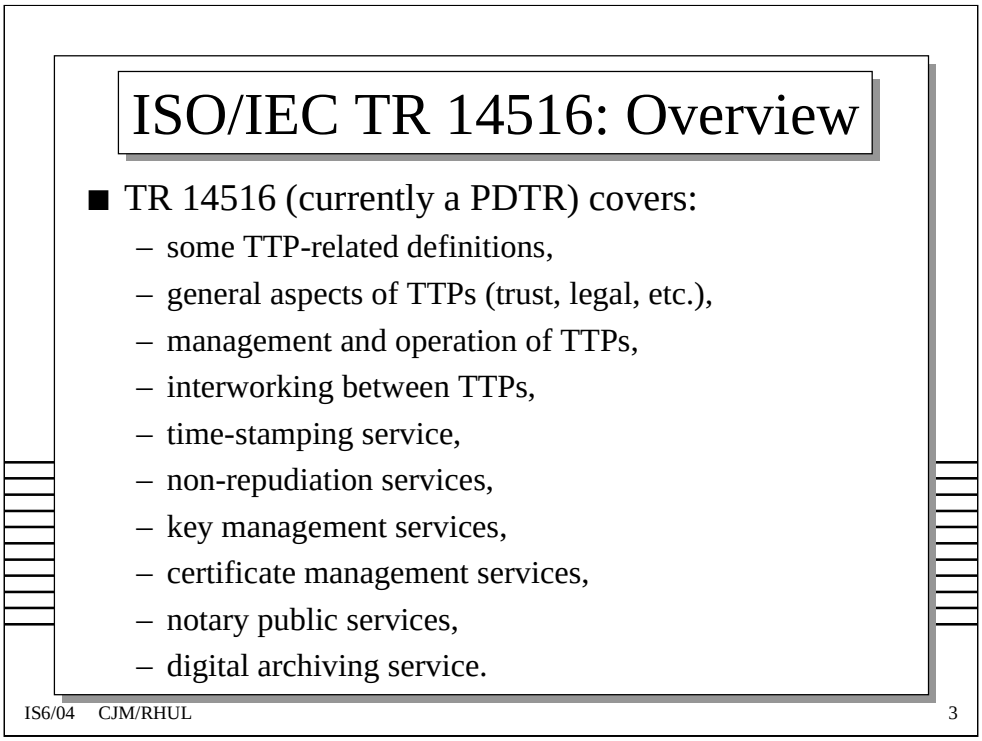
• provide guidance to users regarding the services provided by TTPs, and the respective roles and responsibilities of TTPs and users,

• provide an overview of the services provided by a TTP,

• provide an understanding of the role and function of TTPs,

• provide a basis for the mutual recognition of services provided by different TTPs, and

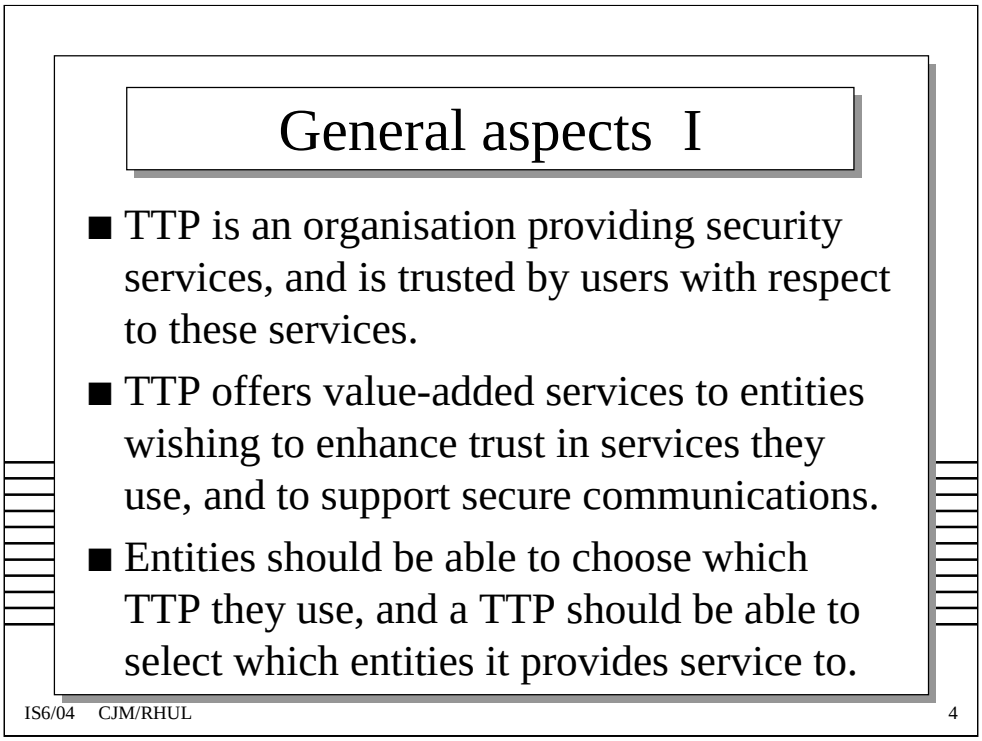
• provide guidance regarding interworking between TTPs.



The current version of ISO/IEC TR 14516 (a PDTR) covers the following main topics.

- Some definitions relevant to the use of Trusted Third Parties in secure systems.
- The general aspects of TTPs (the need for trust, legal and contractual obligations, etc.).
- The management and operational aspects of a TTP.
- Interworking between TTPs.
- Time stamping service.
- Non-repudiation service.
- Key management services.
- Certificate management services.
- Notary public services.
- Digital archiving service.
- Other services.

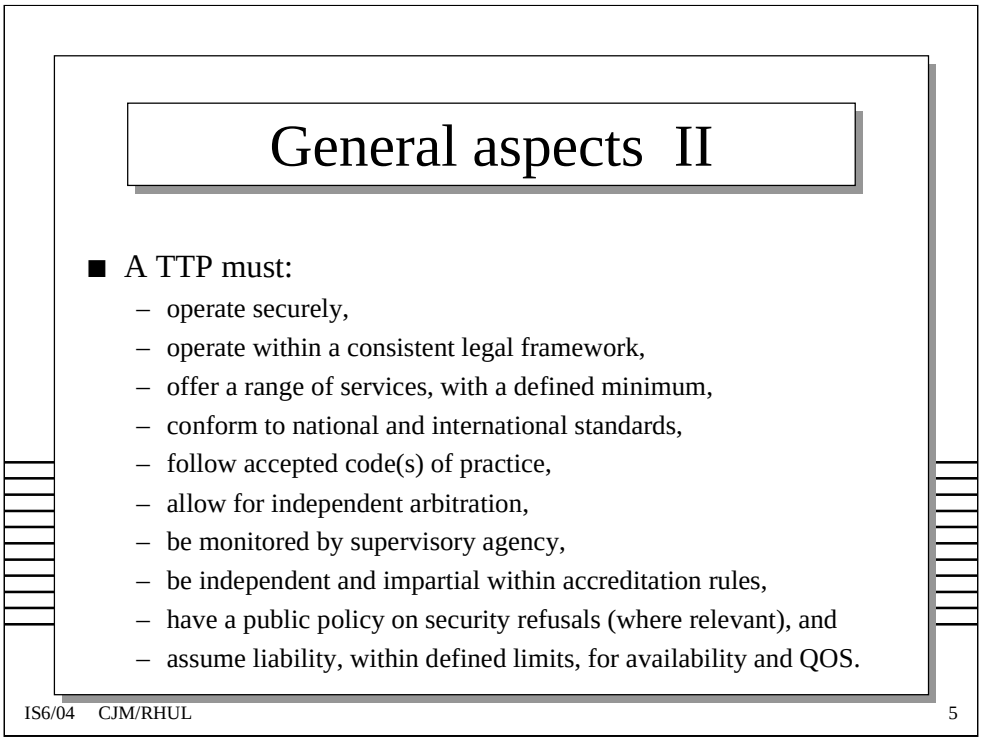
TR 14516 also contains some appendices, including one on CA management.



A Trusted Third Party (TTP) is an organisation providing security services, and that is trusted by users with respect to its TTP security activities.

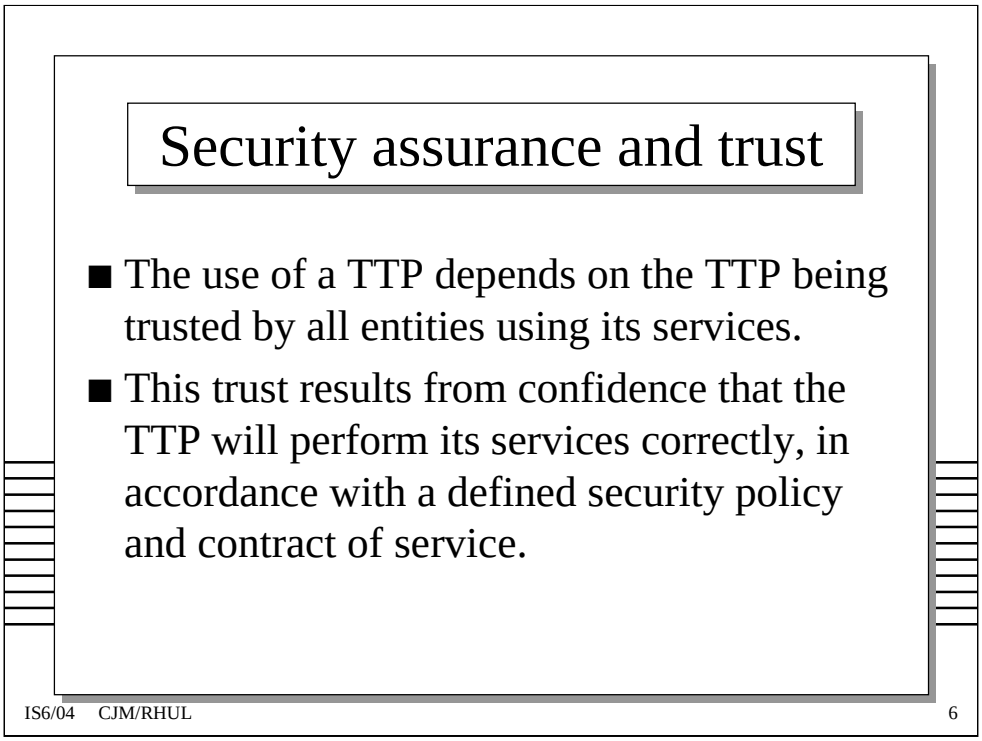
A TTP may be used to offer value added-services to entities wishing to enhance the trust and business confidence in services they use, and to help support secure communications between partners. TTPs need to offer secure and available services.

Entities should be able to choose which TTP they use, and a TTP provider should be able to select which entities it provides service to.

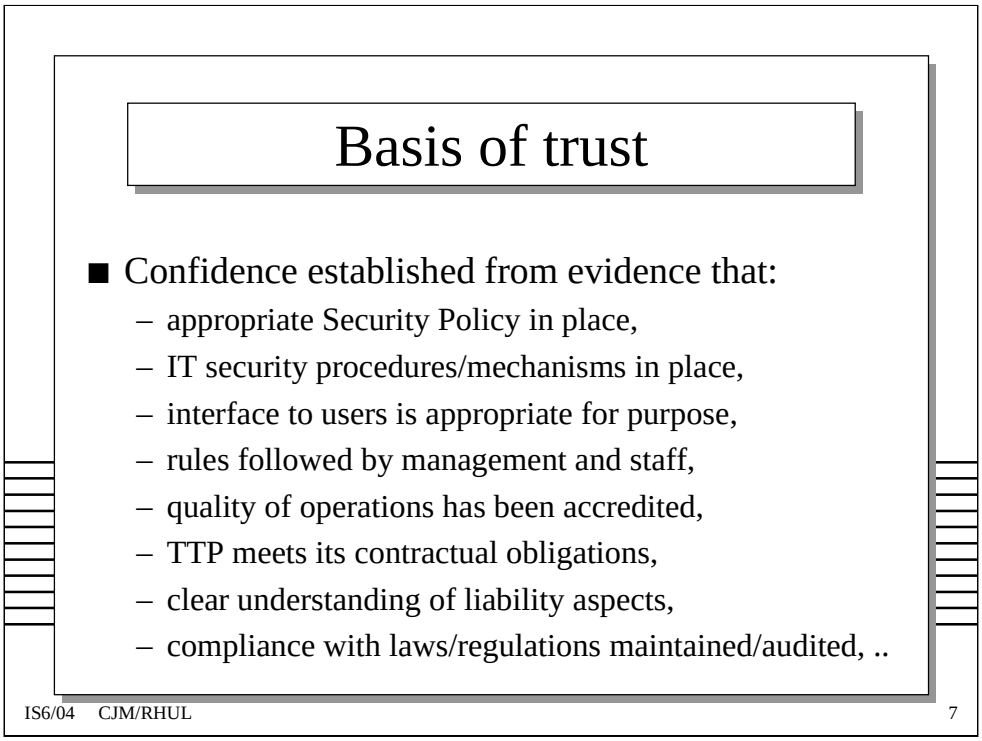


To be effective, a TTP must:

- operate securely,
- operate within a legal framework which is consistent among the participating entities,
- offer a range of services, with a defined minimum,
- conform to national and international standards, where applicable,
- follow an accepted best code of practice,
- allow for independent arbitration, without compromising security,
- be monitored by a supervisory agency,
- be independent and impartial in its operation, within accreditation rules,
- have a public policy on security refusals (where relevant), and
- assume liability, within defined limits, for availability and quality of service (QOS).

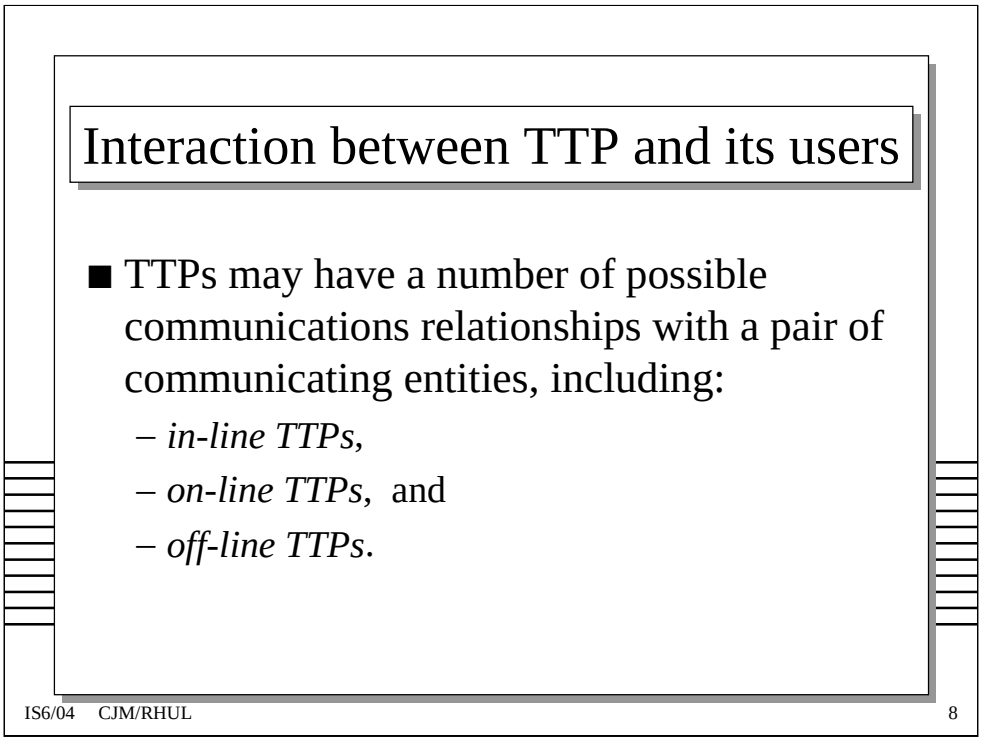


The use of a TTP depends on the TTP being trusted by all entities using its services. This trust results from confidence that the TTP will perform its services correctly, in accordance with a defined security policy and contract of service.



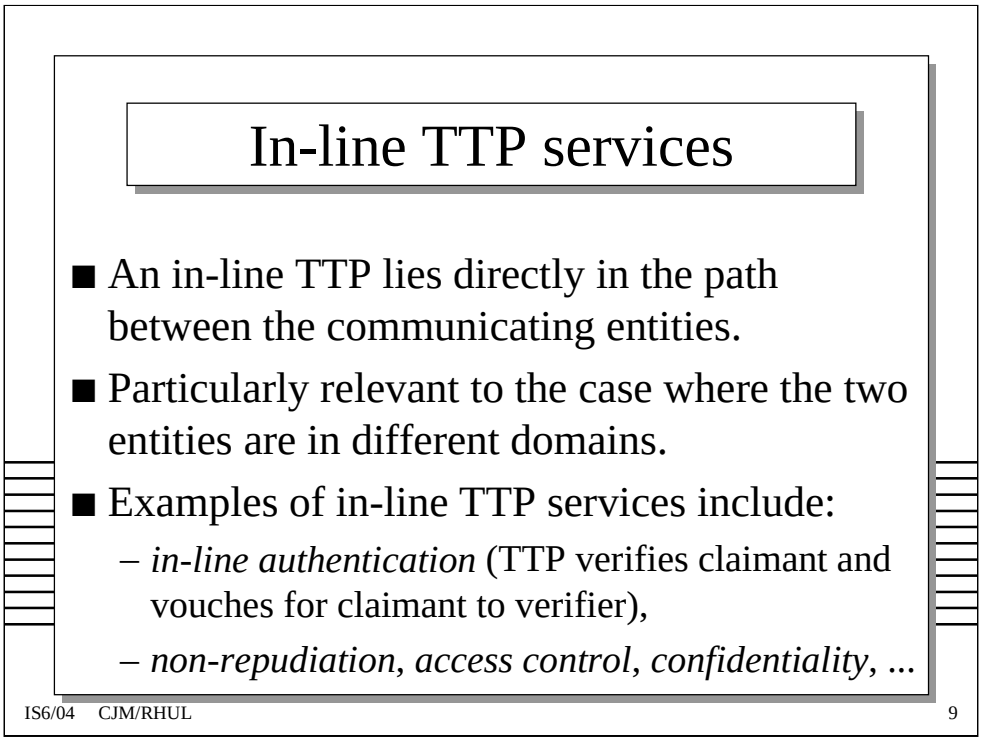
Such confidence can be established through evidence that:

- there is an appropriate Security Policy in place,
- correctly implemented IT security procedures and mechanisms have been put in place to address potential security threats,
- the TTP security operations are being carried out correctly and with clearly defined roles and responsibilities,
- the interfaces and procedures for communicating with users are appropriate for the functions to be performed,
- the rules and regulations are followed by management and staff,
- the quality of the processes, operations and working practices has been accredited,
- the TTP meets its contractual obligations according to a formal contract with its users,
- there is a clear understanding and acceptance of the liability aspects,
- compliance with laws and regulations is maintained and audited,
- known threats and safeguards are clearly identified,
- a threat and risk assessment is done initially and reviewed on a regular basis.



From the viewpoint of communications between a pair of entities, there are a number of possible locations for a TTP, notably:

- *in-line TTPs*,
- *on-line TTPs*, and
- *off-line TTPs*.

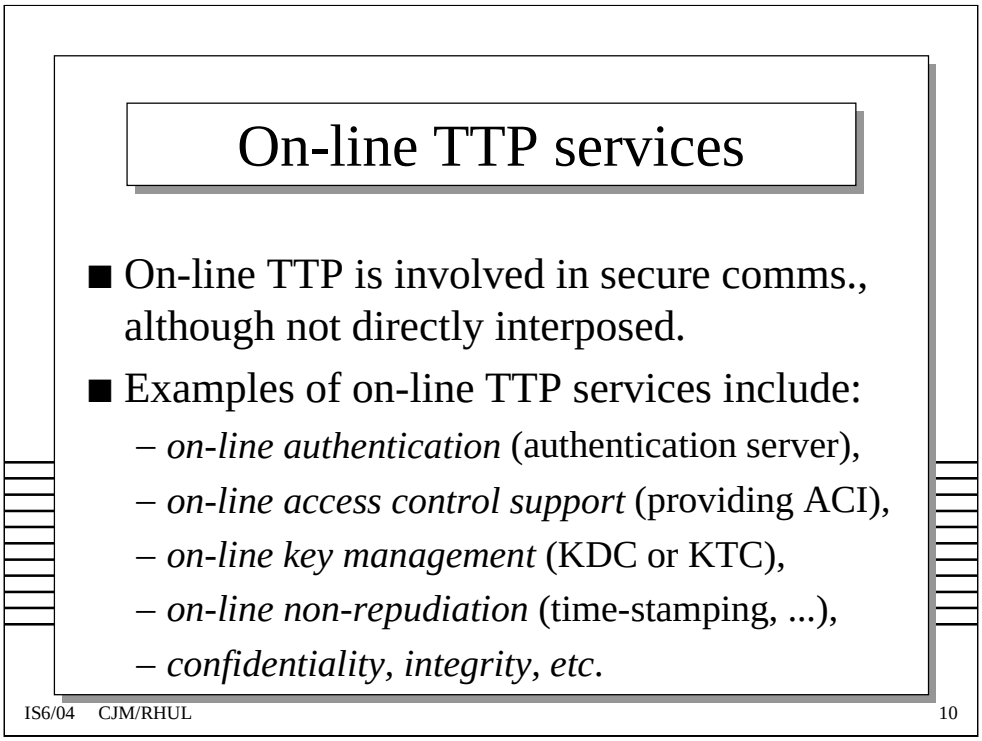


An in-line TTP lies directly in the communications path between the two entities. It is of particular importance when the two entities are in different security domains and use different security mechanisms (and are thus unable to take part in direct security exchanges).

Examples of in-line TTP services are:

• *in-line authentication* - the TTP authenticates the claimant and vouches for the identity of the claimant to the verifier (the verifier authenticates the TTP).

• *other in-line security services* - an in-line TTP may play a role in the provision of other services such as: non-repudiation, access control, confidentiality, and data integrity.



An on-line TTP is involved in instances of secure communication between the two entities; however it does not lie in the communications path between the entities. Instead it will be requested by one or both of the entities to provide or register security-related information.

Example of on-line TTP services include:

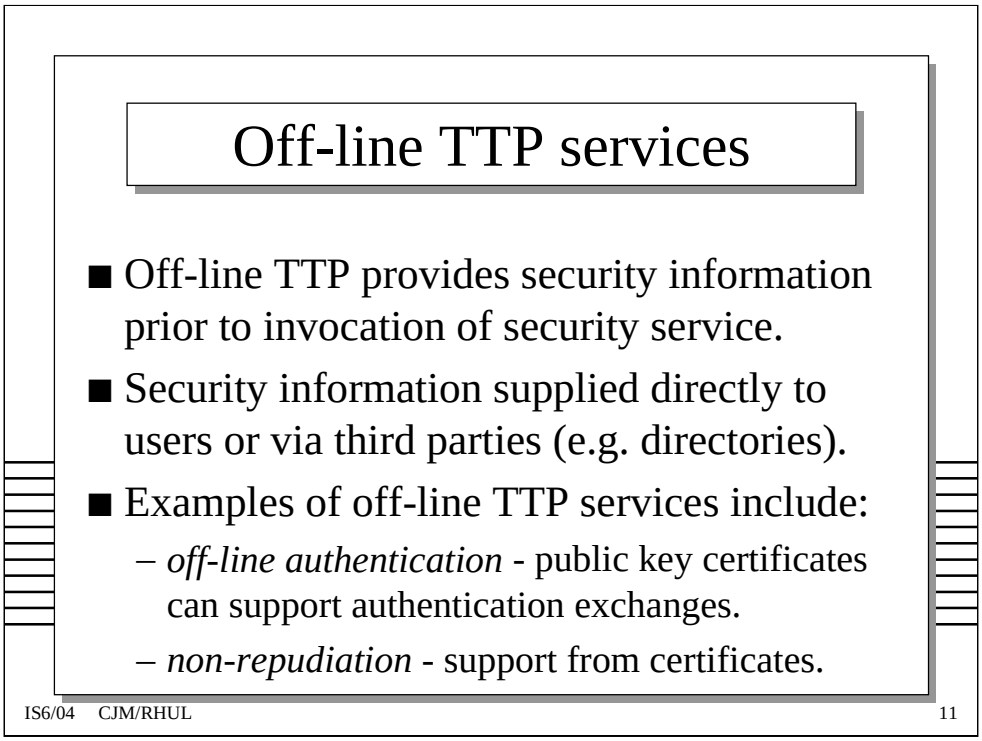
• *on-line authentication* - an entity authentication service may use an on-line TTP as part of an authentication exchange mechanism.

• *on-line access control support* - an on-line TTP may provide access control information on request.

• *on-line key management* - an on-line TTP can act as a Key Distribution Centre or Key Translation Centre to support symmetric key management mechanisms.

• *on-line non-repudiation* - an on-line TTP may support non-repudiation services in a variety of ways, including: generating signatures, time-stamping and/or notarising messages.

• *other on-line security services* - an on-line TTP may also support other security services, such as confidentiality and data integrity services.

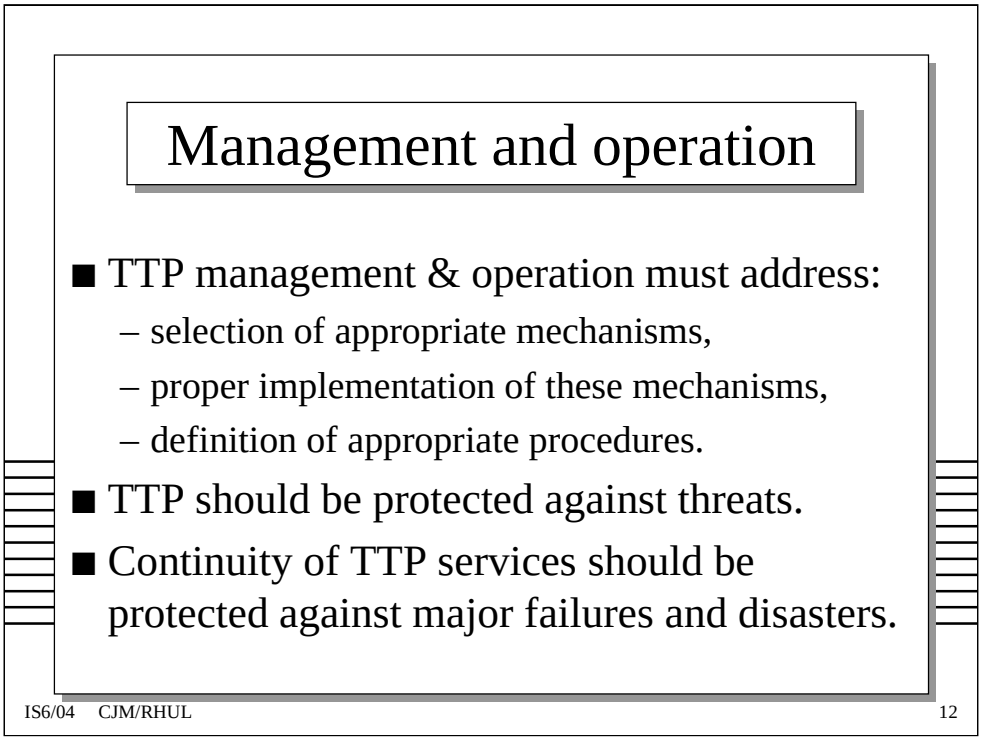


An off-line TTP will support the provision of certain security services. However it will not be involved in any on-line transactions; instead it will provide security-related information at some prior time, either directly to the entities involved or to some other, not necessarily trusted, third party which will be available on-line to the communicating entities.

Example of off-line TTP services include:

• *off-line authentication* - an off-line TTP may generate public key certificates in advance, which can then be used as part of an authentication exchange mechanism. These certificates may be lodged directly with the authenticating entities, or made available via an on-line directory service.

• *off-line non-repudiation* - an off-line TTP may generate public key certificates to support the provision of non-repudiation services.

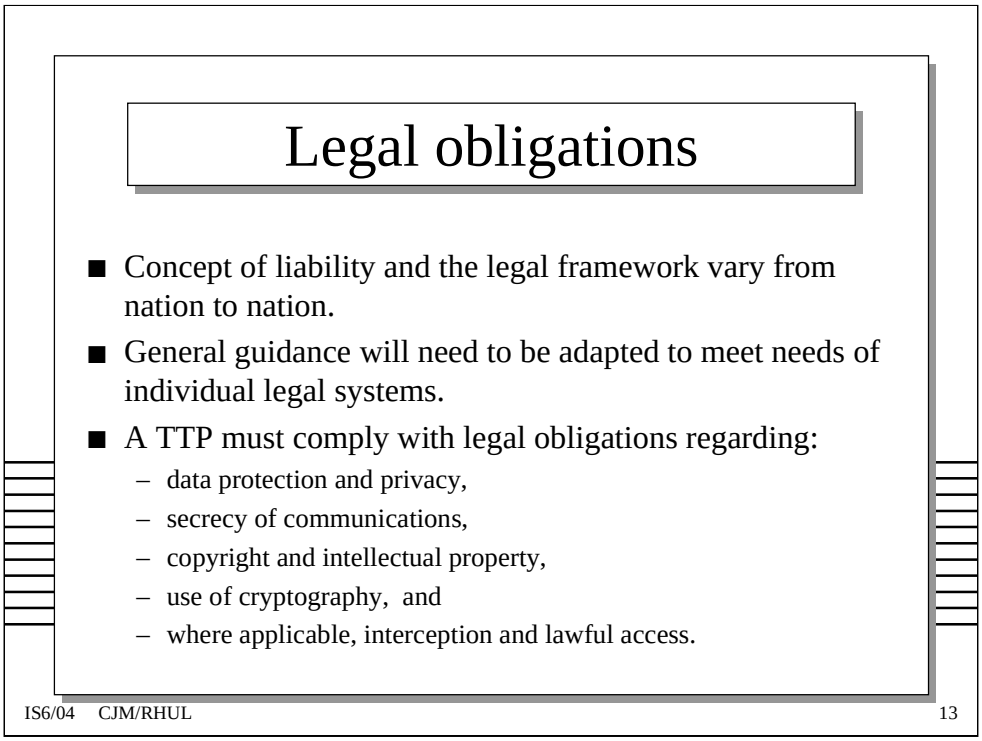


The TTP management and operation must address the following issues:

- the selection of appropriate mechanisms, with regard to the services provided and the Security Policy,
- the proper implementation of these mechanisms, particularly with regard to physical security, business continuity, etc., and
- the definition of appropriate procedures, e.g. for personnel management, information classification, authorisation, incident handling, etc.

The TTP should be adequately protected against threats.

The continuity of TTP services should be protected against major failures and disasters.

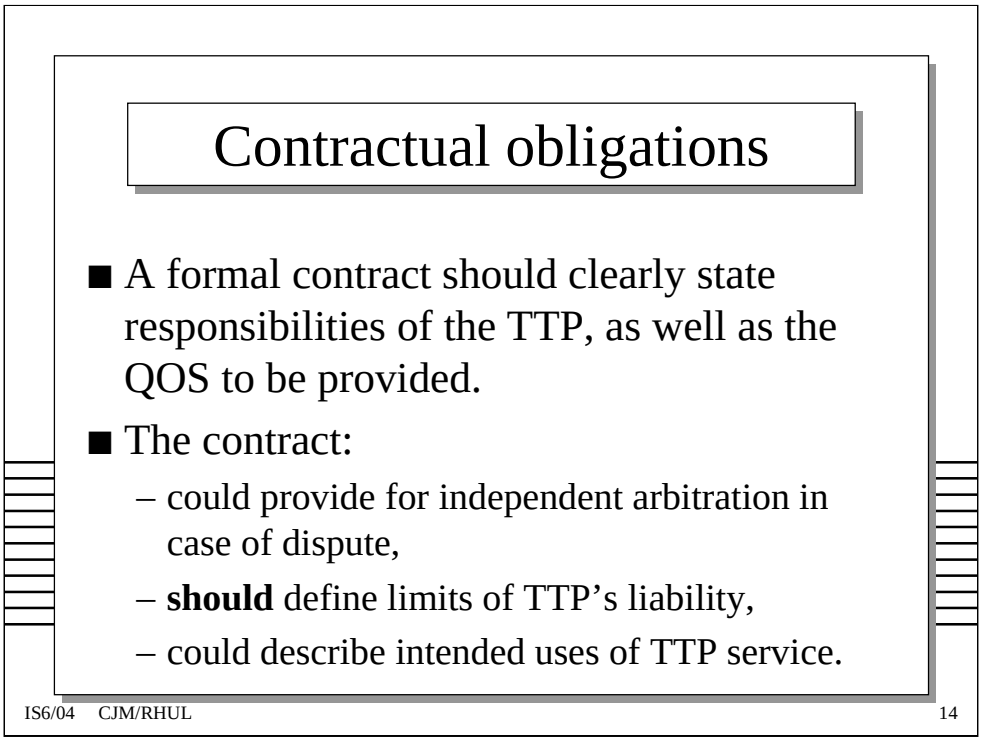


The concept of liability, and the legal framework, will vary from nation to nation. Thus general guidance will need to be adapted to meet the needs of individual legal systems.

A TTP must comply with all national and international legal obligations, particularly those regarding:

- data protection and privacy,
- secrecy of communications,
- copyright and intellectual property,
- use of cryptography, and
- where applicable, interception and lawful access.

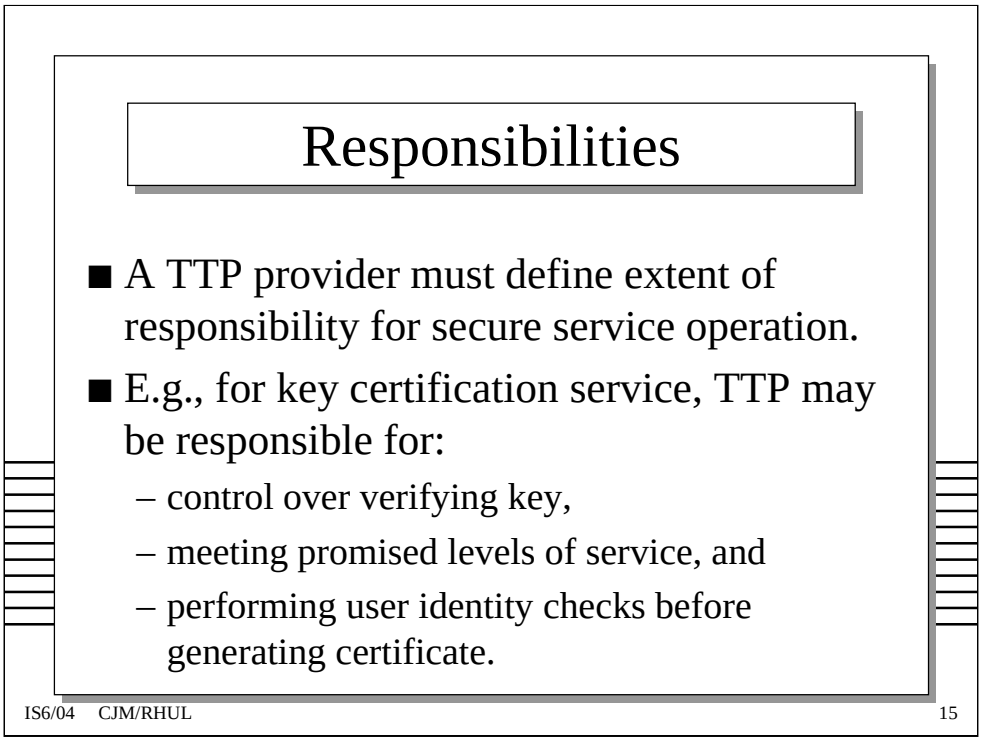
The TTP should assess and manage its liabilities and, where necessary, ensure it has sufficient insurance cover to meet its liabilities.



A formal contract between a TTP and a user of the TTP's services should clearly state the responsibilities of the TTP, as well as the quality of service (QOS) to be provided.

The contract:

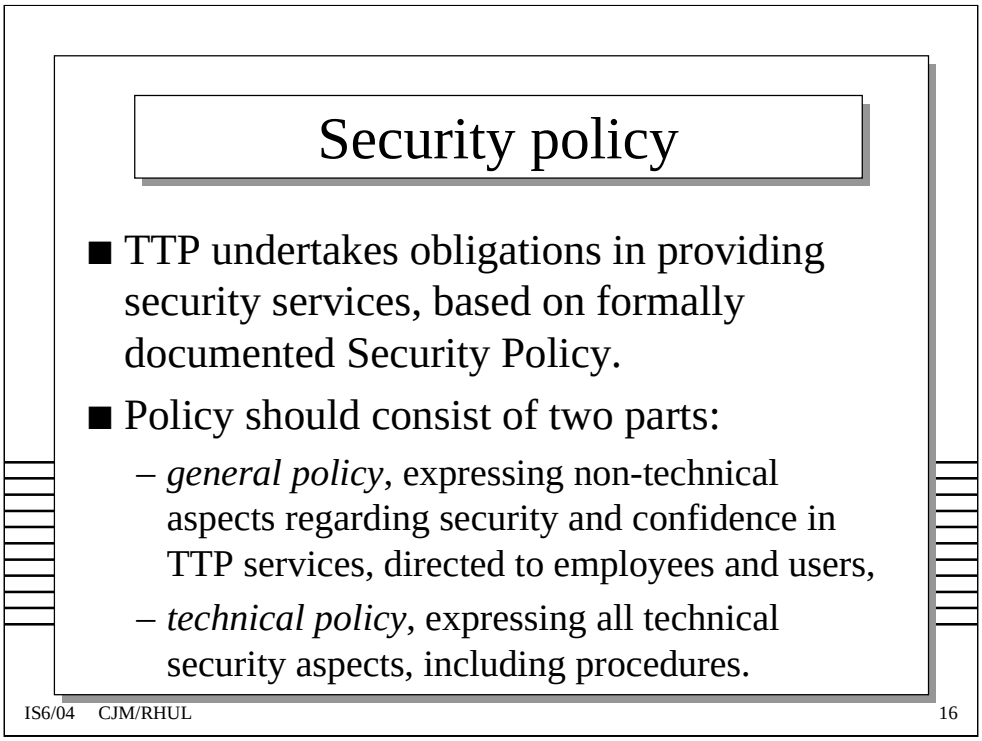
- could provide for independent arbitration in case of dispute,
- should define the limits of the TTP's liability, and
- could describe the intended uses of the TTP service.



A TTP provider must define the extent of its responsibility for secure service operation, as well as the extent of liabilities which will be accepted in the event of security breaches.

E.g., for a key certification service, the TTP may be responsible for:

- control of the verifying key,
- meeting promised levels of service, and
- performing user identity checks before generating a certificate.

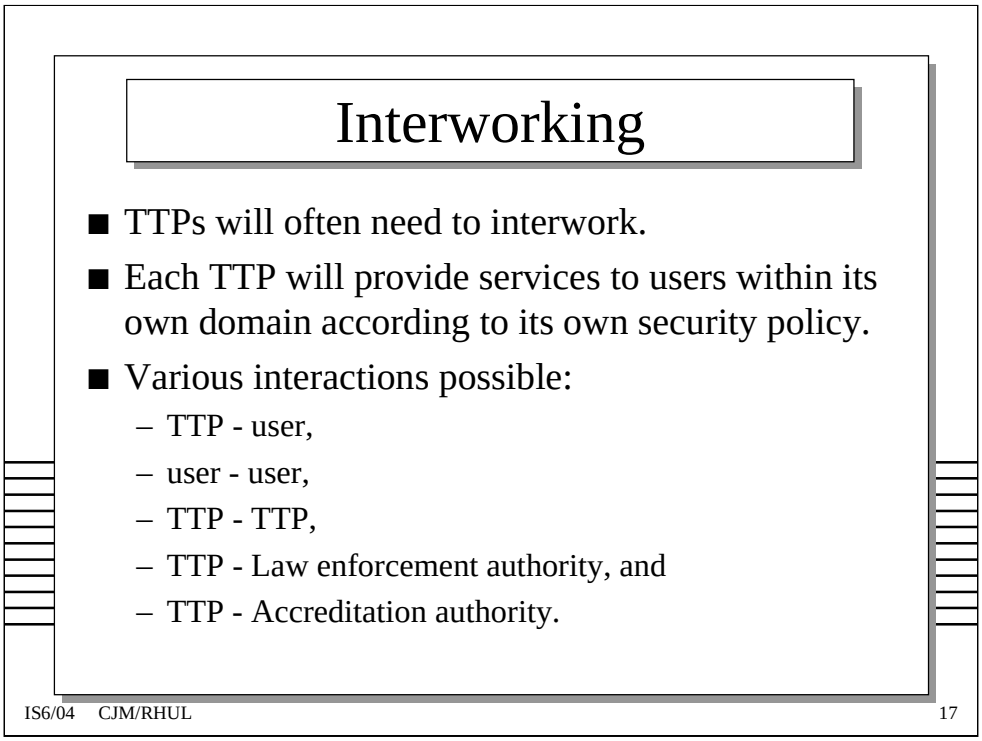


The TTP undertakes certain obligations in offering and operating security services, based on a formally documented Security Policy for the TTP organisation.

This Security Policy should consist of two parts:

• a *general policy*, expressing non-technical aspects regarding security and confidence in TTP services, directed to employees and users, and

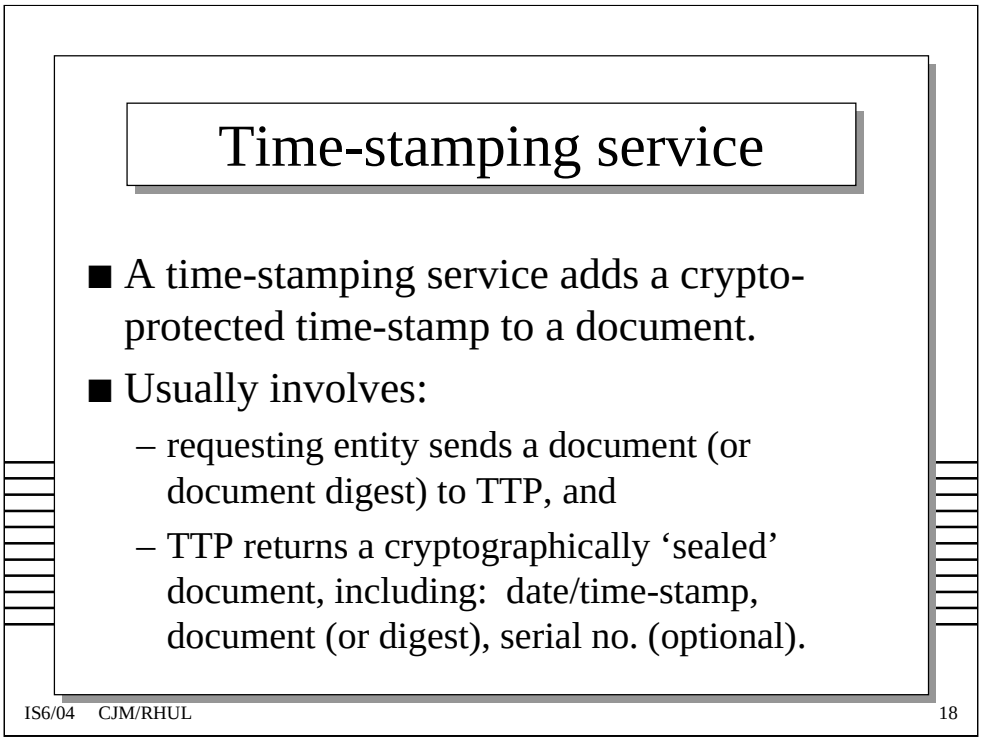
• a *technical policy*, expressing all technical security aspects, including routines and procedures which must be followed in connection with technical aspects of security provision.



TTPs will often need to interwork. Each TTP will provide services to users within its own domain according to its own security policy.

Various interactions between types of entity are possible:

- TTP - user,
- user - user,
- TTP - TTP,
- TTP - law enforcement authority,
- TTP - Accreditation authorities (i.e. organisations set up to accredit TTPs).

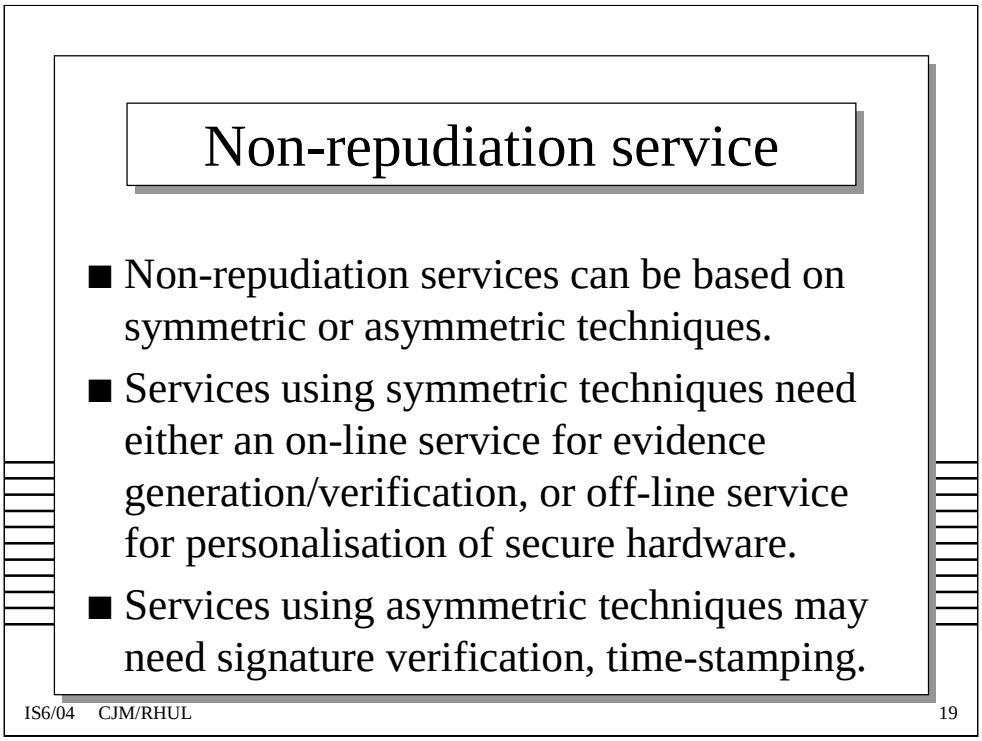


A *time-stamping service* adds a time-stamp to a document, as well as a cryptographic seal on the document and time-stamp, enabling any subsequent modifications to be detected.

Time-stamping usually involves the following steps:

- the entity requesting the service submits a document (or a document digest), and
- the TTP returns a 'sealed' document, containing:
  - time/date stamp of sealing,
  - the document itself (or the digest), and
  - an (optional) serial number.

Use of a message digest potentially saves bandwidth (reducing communication costs), and conceals the document content from both the TTP and any interceptors of the exchange. The digest could be computed using a one-way hash-function.

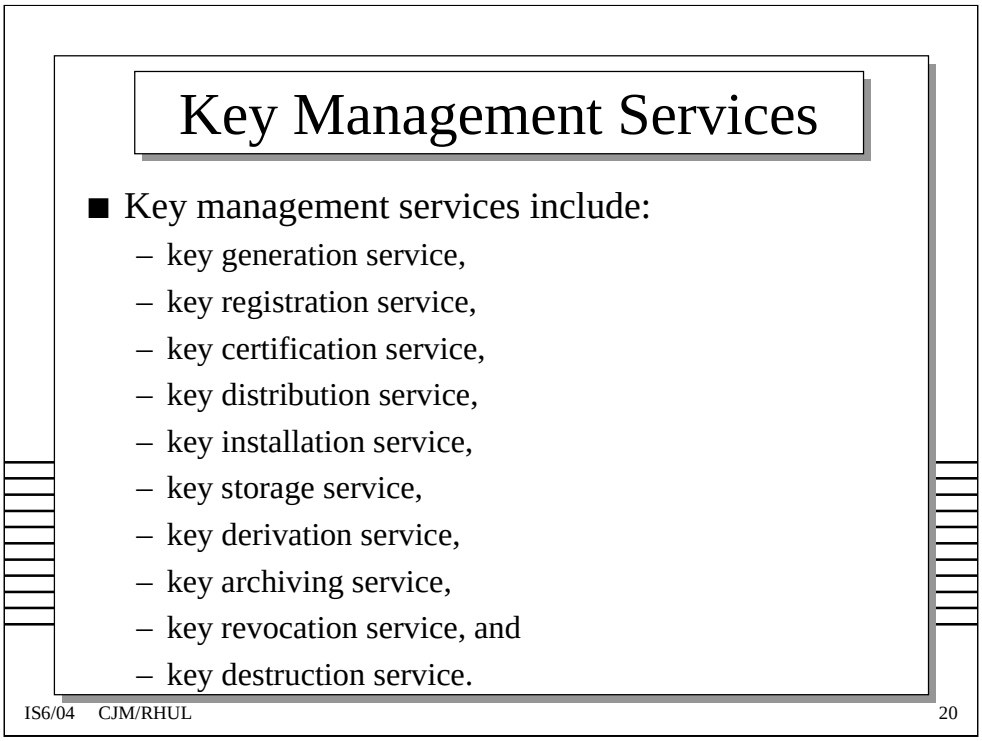


Non-repudiation services can be based on the use of either symmetric or asymmetric cryptographic techniques. This is described in more detail in ISO/IEC 13888 Parts 1-3.

A non-repudiation service using symmetric techniques can be based on one (or more) of:

- an in-line TTP service,
- an on-line TTP service for generating and verifying evidence, and generating 'secure envelopes', or
- an off-line TTP service for personalising (adding keys to) trusted cryptographic hardware, e.g. a smart card or security module.

A non-repudiation service using asymmetric techniques does not necessarily need a TTP to generate evidence, although TTPs will typically be needed both for certificate management services, and to resolve disputes.



Key management services include:

• *key generation service*, i.e. the generation of secret and unpredictable numbers for use as keys with cryptographic algorithms,

• *key registration service*, i.e. registration of keys for entities,

• *key certification service*, i.e. providing public key certificates,

• *key distribution service*, i.e. the distribution of keys to entities,

• *key installation service*, i.e. making a key available for use,

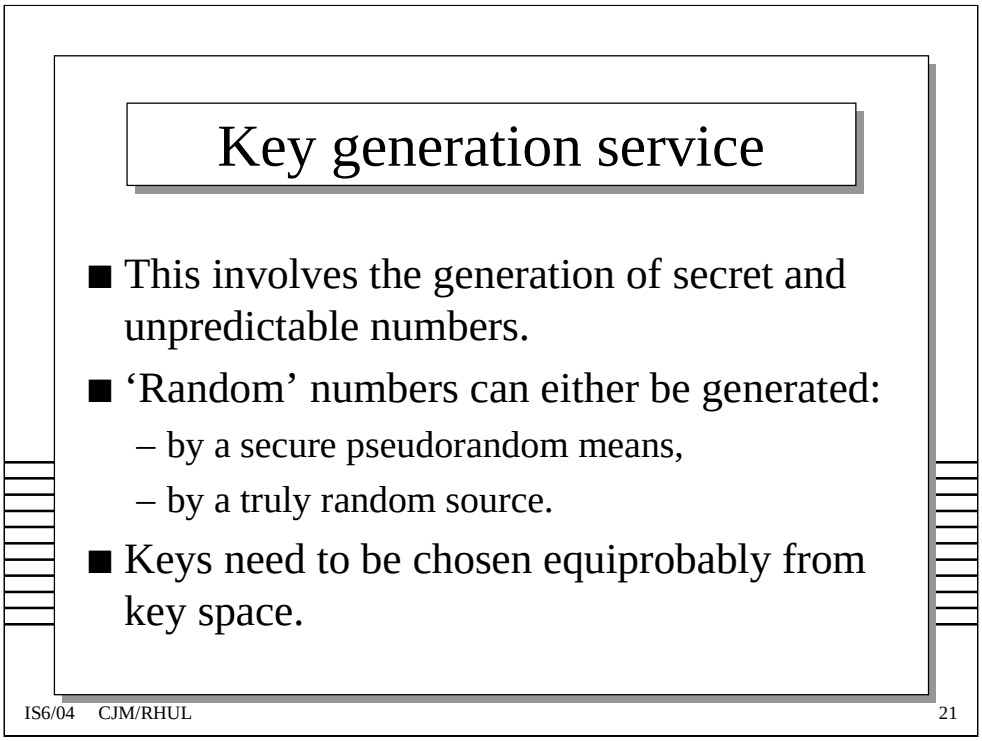
• *key storage service*, i.e. the secure storage of keys (current/short term),

• *key derivation service*, i.e. the generation of keys from an 'original' key,

• *key archiving service*, i.e. the long-term storage of keys,

• *key revocation service*, i.e. the secure deactivation of a key when a key is known or suspected to be compromised, and

• *key destruction service*.



Key generation relies on the generation of secret and unpredictable numbers. 'Random' numbers can either be generated:

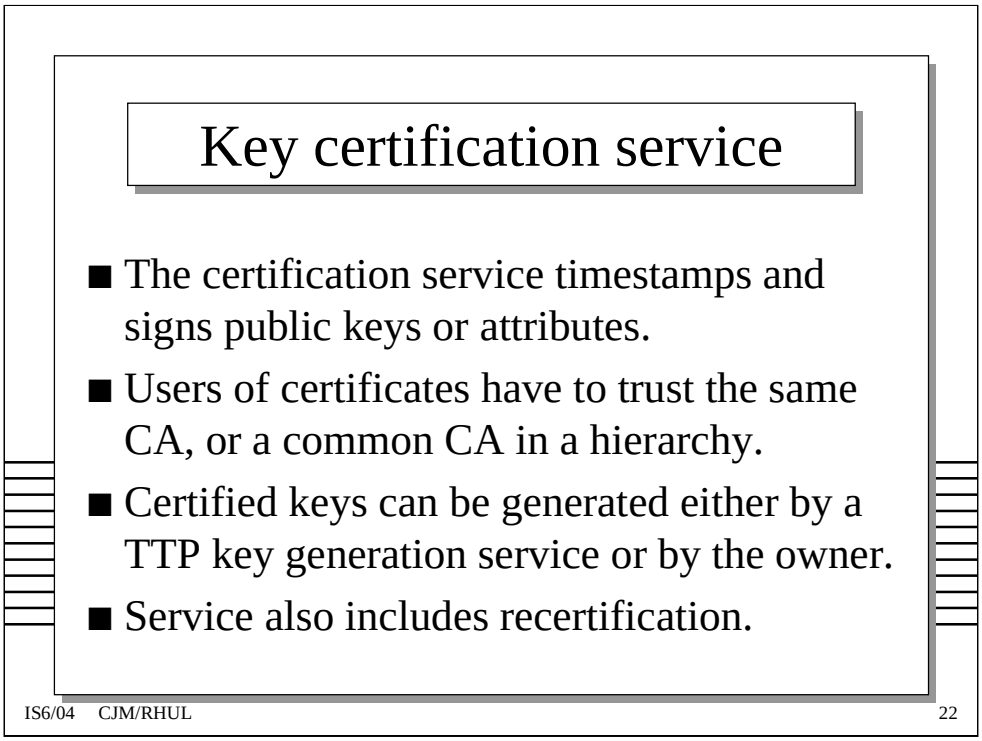
– by a cryptographically secure pseudorandom means,

– by a truly random source.

For a symmetric algorithm, keys should be chosen equiprobably from the entire key space.

For an asymmetric algorithm, keys should again be chosen approximately equiprobably from (at least) a large subset of the key space.

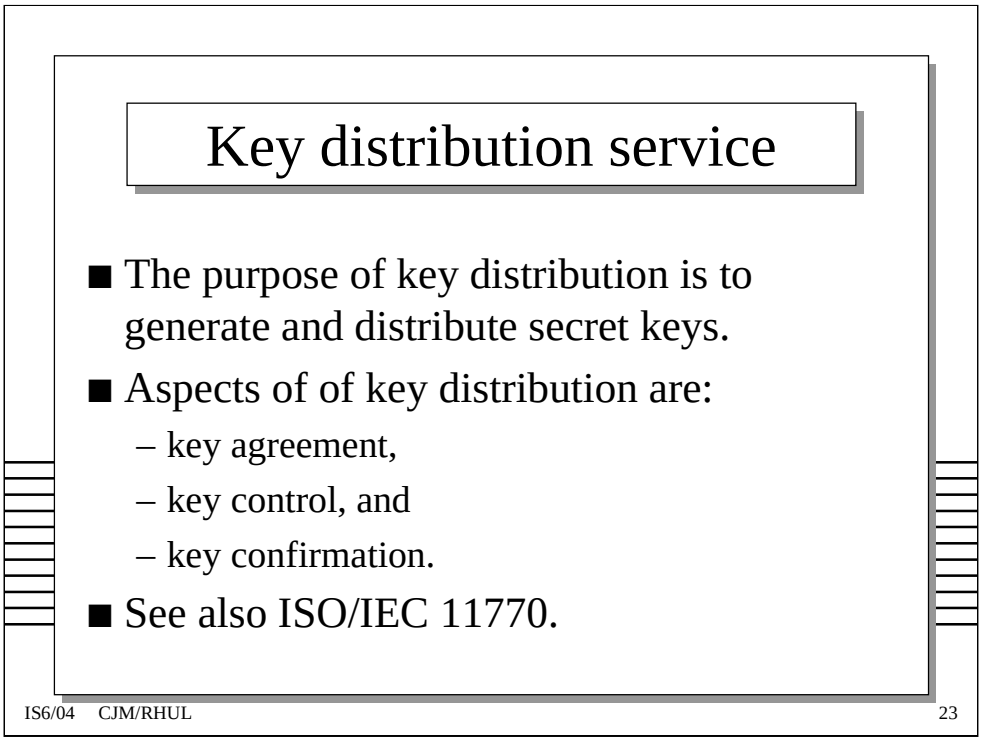
See also Internet RFC 1750.



The certification service timestamps and signs public keys or attributes.

Users of certificates have to trust the same CA, or a common CA in a hierarchy.

Certified keys can be generated either by a TTP key generation service or by the owner. This service also includes recertification



The purpose of key distribution is to generate and distribute secret keys. (The term ‘key establishment’ is more general - see definitions from ISO/IEC 11770).

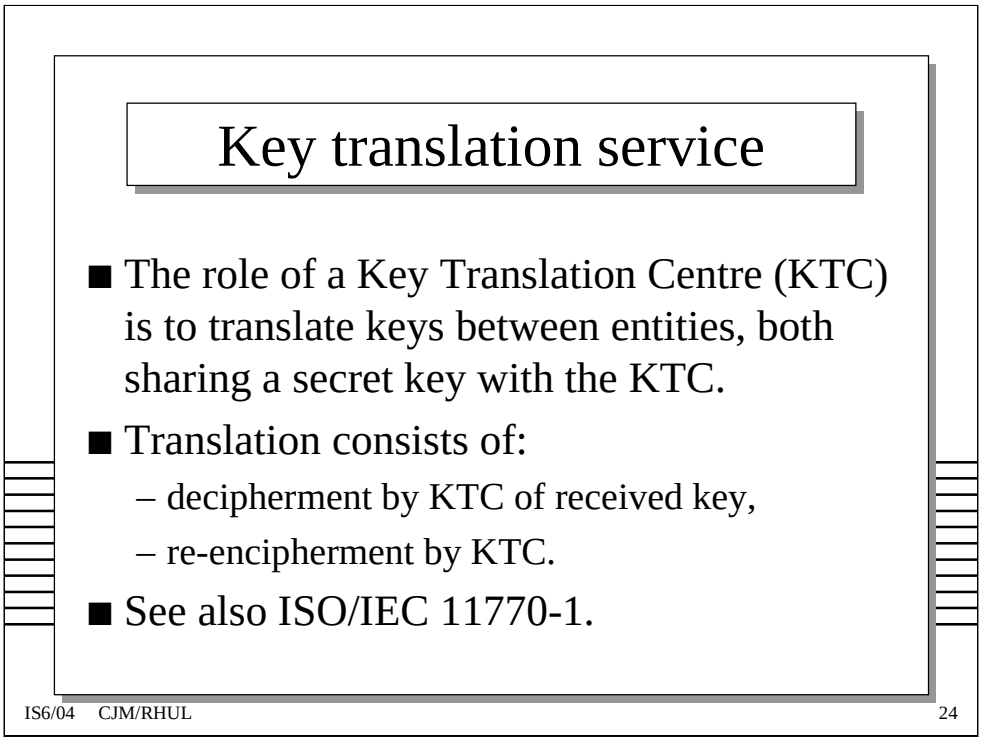
Key distribution mechanisms may provide some or all of:

– *key agreement*, i.e. the establishment of a key between two entities,

– *key control*, i.e. where one entity can choose the key established between two entities, and

– *key confirmation*, i.e. where one entity is provided with evidence that the other entity is in possession of the shared key.

See also ISO/IEC 11770.



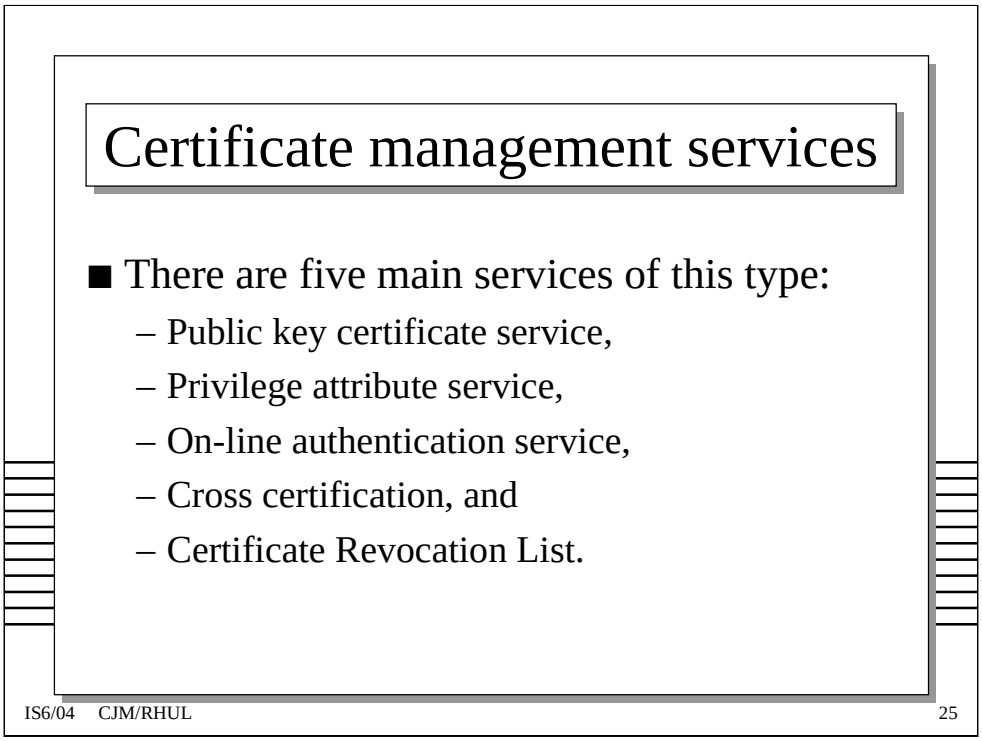
The role of a Key Translation Centre (KTC), providing a *Key Translation Service*, is to translate and distribute keys between entities, both sharing a secret key with the KTC.

The translation process itself consists of:

• decipherment by the KTC of a received enciphered key,

• re-encipherment by the KTC of the key, and forwarding it to the appropriate entity.

See also ISO/IEC 11770-1.



There are five main services of this type:

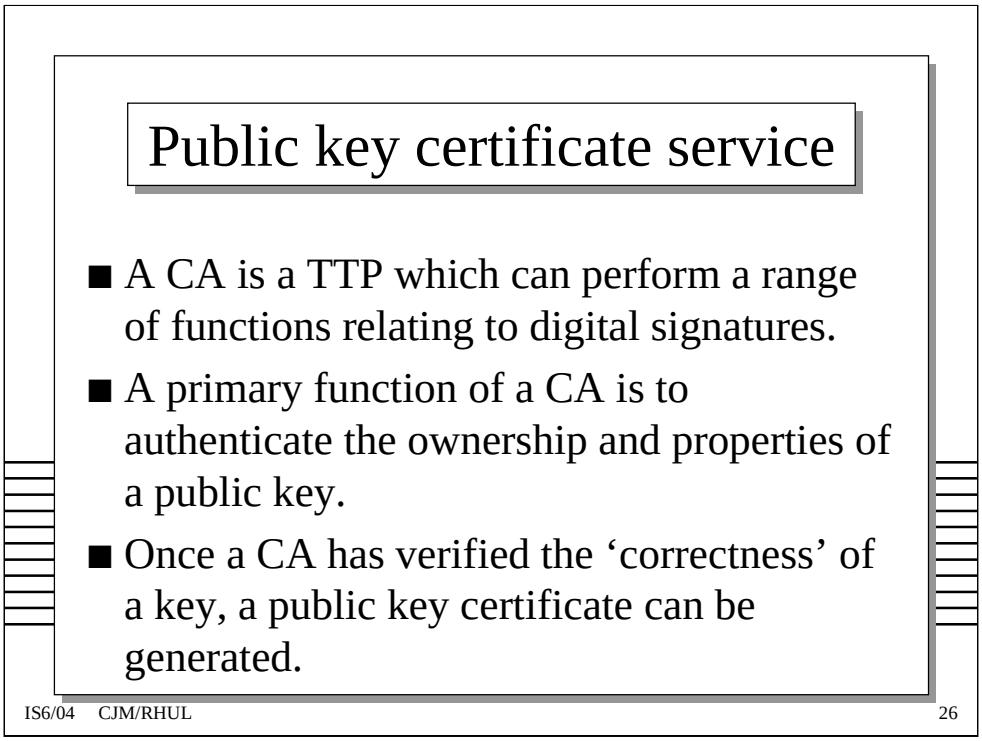
• *Public key certificate service*, i.e. generating public key certificates,

• *Privilege attribute service*, i.e. generating certificates for other information about an entity (e.g. access control rights),

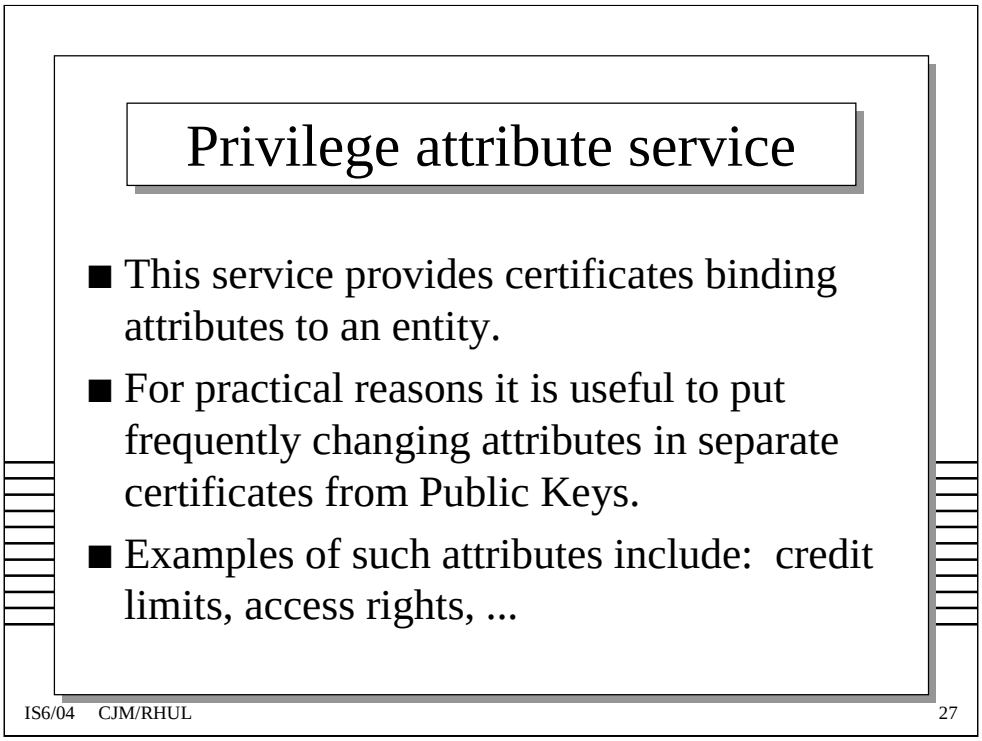
• *On-line authentication service*, i.e. acting as an authentication server,

• *Cross certification*, i.e. generating public key certificates for other CA's public keys,

• *Certificate Revocation List*, i.e. maintaining a signed list of revoked certificates.

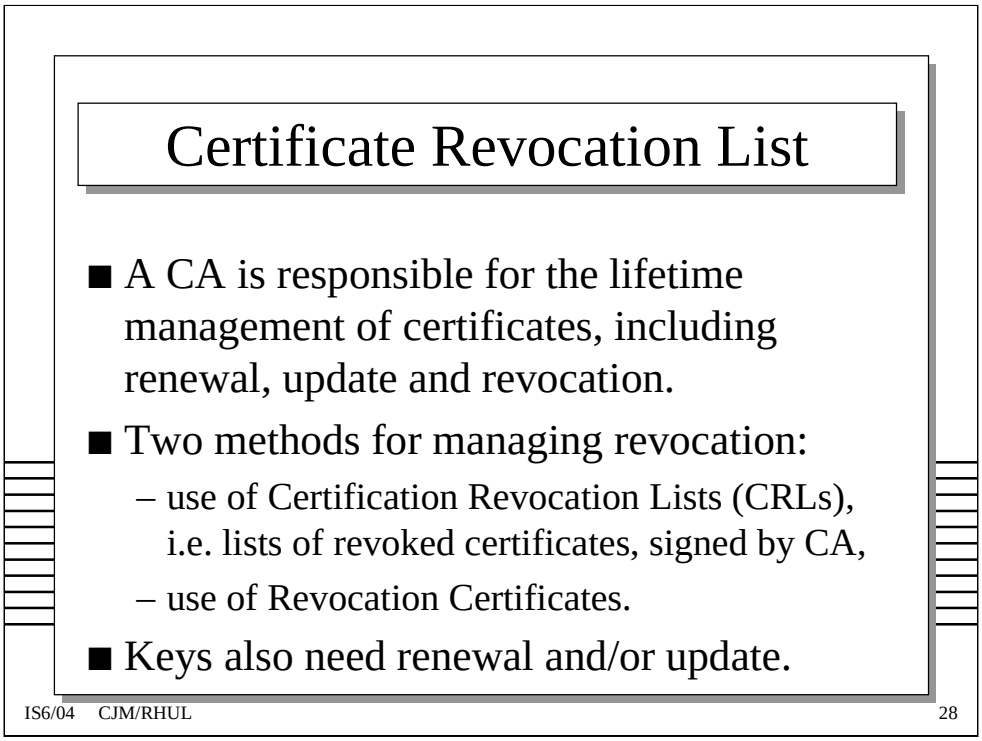


A Certification Authority (CA) is a TTP which can perform a range of functions relating to digital signatures. A primary function of a CA is to authenticate the ownership and properties of a public key. Once a CA has verified the 'correctness' of a key, a public key certificate can be generated.



The *Privilege Attribute Assignment Service* provides certificates binding 'attributes' to an entity, separately to an entity's Public Key Certificate. For practical reasons it is useful to put frequently changing attributes in such separate certificates. Examples of appropriate attributes include: credit limits, access rights, ...

The attribute certificates will all be linked back to a Public Key certificate.



A CA is responsible for the lifetime management of certificates, including recertification, update and revocation.

The revocation of a certificate means that it is deemed to be invalid before its expiry date. There may be many reasons for this, e.g. compromise of the Private Key, name change, organisation change, etc. There are two commonly discussed methods for managing revocation:

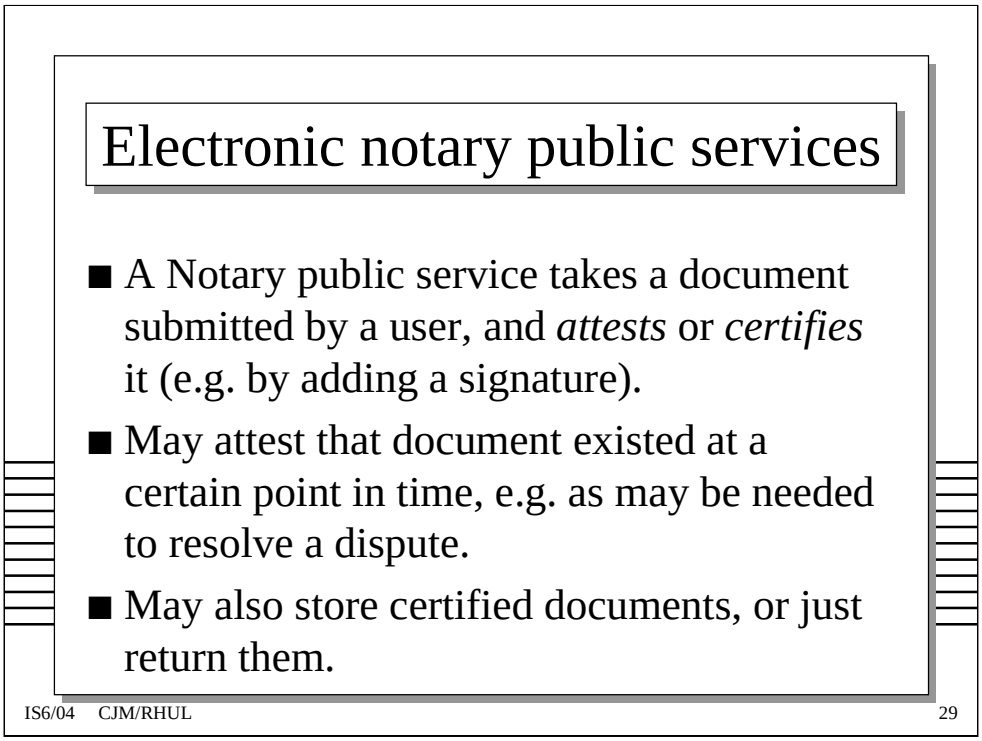
• the use of Certification Revocation Lists (CRLs), i.e. lists of revoked certificates, signed by the CA,

• the use of Revocation Certificates, i.e. a signed statement that an individual certificate has been revoked.

CRLs need to be routinely updated, even when no new certificate revocations have occurred, in order that the CRL user can verify it has the ‘latest’ CRL.

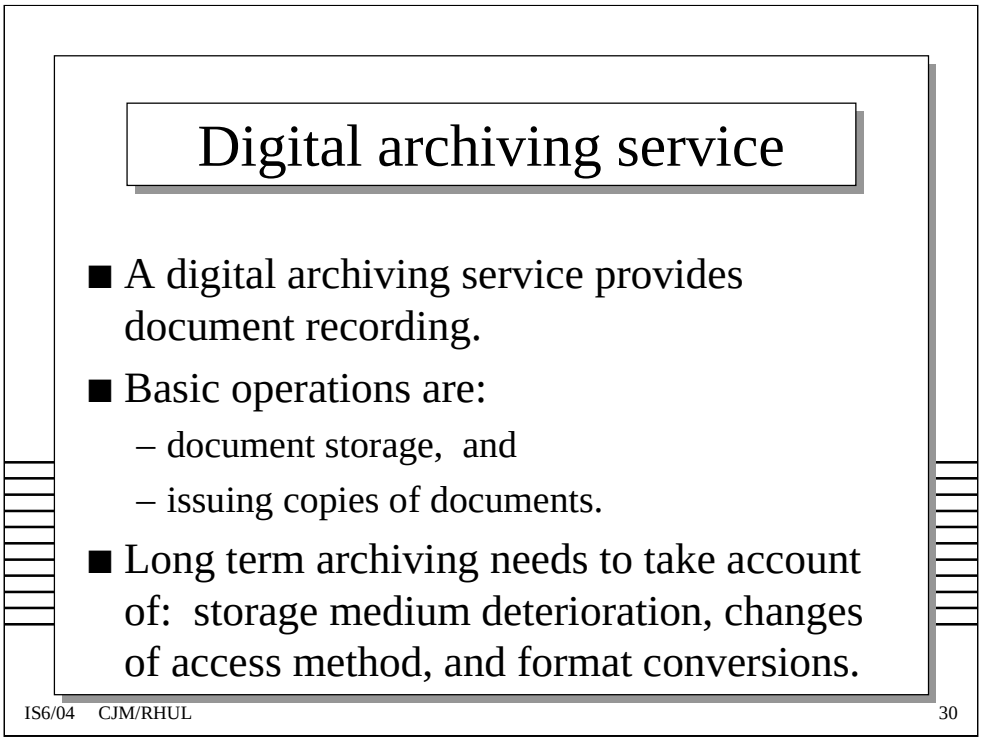
The *renewal* of a certificate means a new certificate is generated containing the same Private Key as a previous certificate but with different associated information (in which case the ‘old’ certificate must be revoked - if it has not already expired). This might, for example, be used where the Private Key has not been compromised, but an entity has changed his/her name.

Key *update* refers to where a new Key Pair is generated and certified.



A Notary public service takes a document submitted by a user, and *attests* or *certifies* it (e.g. by adding a signature).

The service may, for example, attest that document existed at a certain point in time, e.g. as may be needed to resolve a dispute. The service may also store certified documents, or just return them to the service user.



A *digital archiving service* provides document recording services. Its basic operations are:

• document storage - the TTP may need to keep a dated copy of the document in secure storage for long periods, and

• issuing copies of documents - the TTP will, on request, issue a signed copy of a document (including initial date of registration with the service).

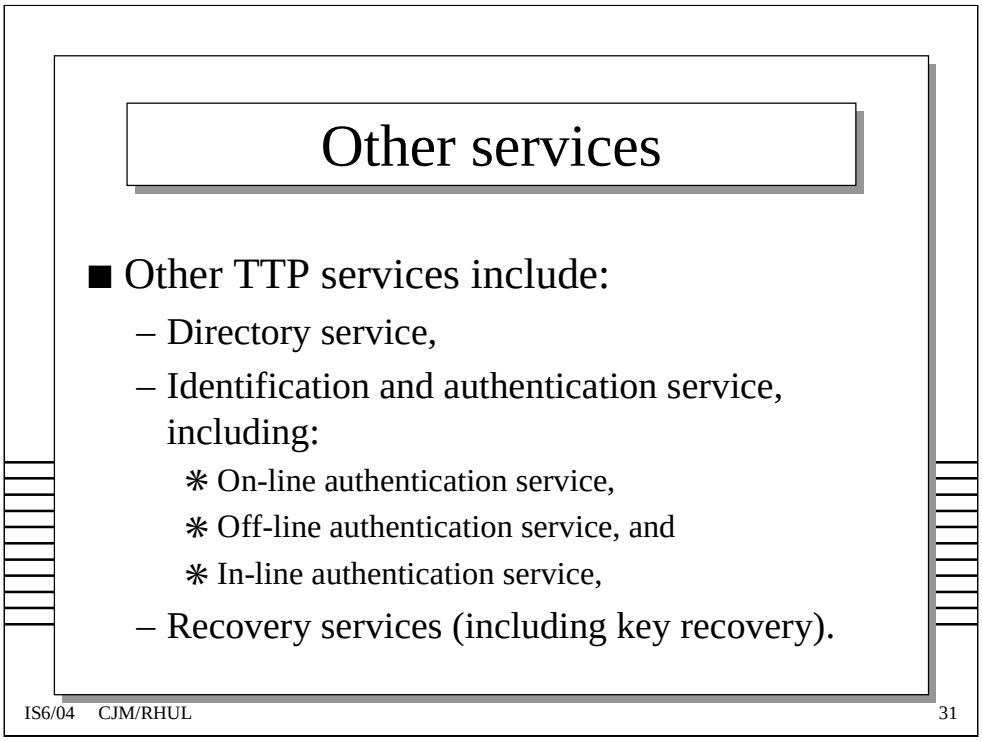
Integrity of stored documents is TTPs own affair (not primarily cryptography-dependent).

For long-term storage (e.g. storage for 30 years or more), some issues are:

• certain storage media (e.g. magnetic media) deteriorate and need regular 'refreshing' to prevent data loss,

• methods for accessing archived data will change, which will mean that stored data will need to be transferred from one medium to another, and

• information on the document format (e.g. ASCII, Postscript, HTML, RTF) will need to be stored with the document, and software will need to be provided to enable users to access data stored in 'old' formats.



Other TTP services include:

Directory service, i.e. the provision of trustworthy information regarding entities,

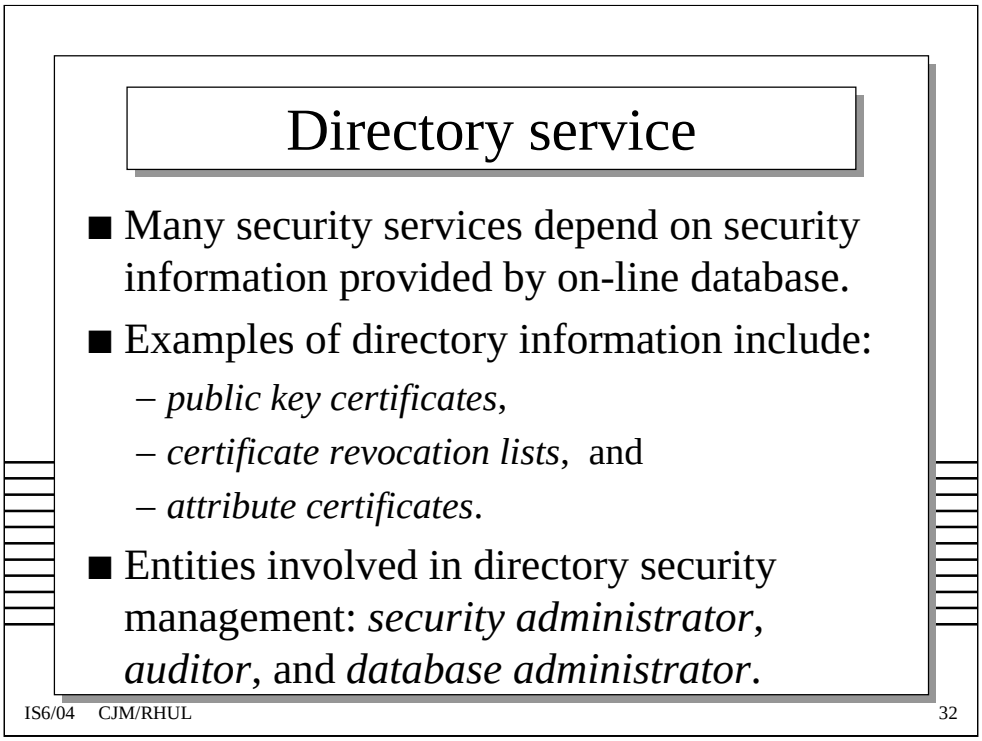
Identification and authentication service, including:

• On-line authentication service,

• Off-line authentication service, and

• In-line authentication service, and

Recovery services (including key recovery).

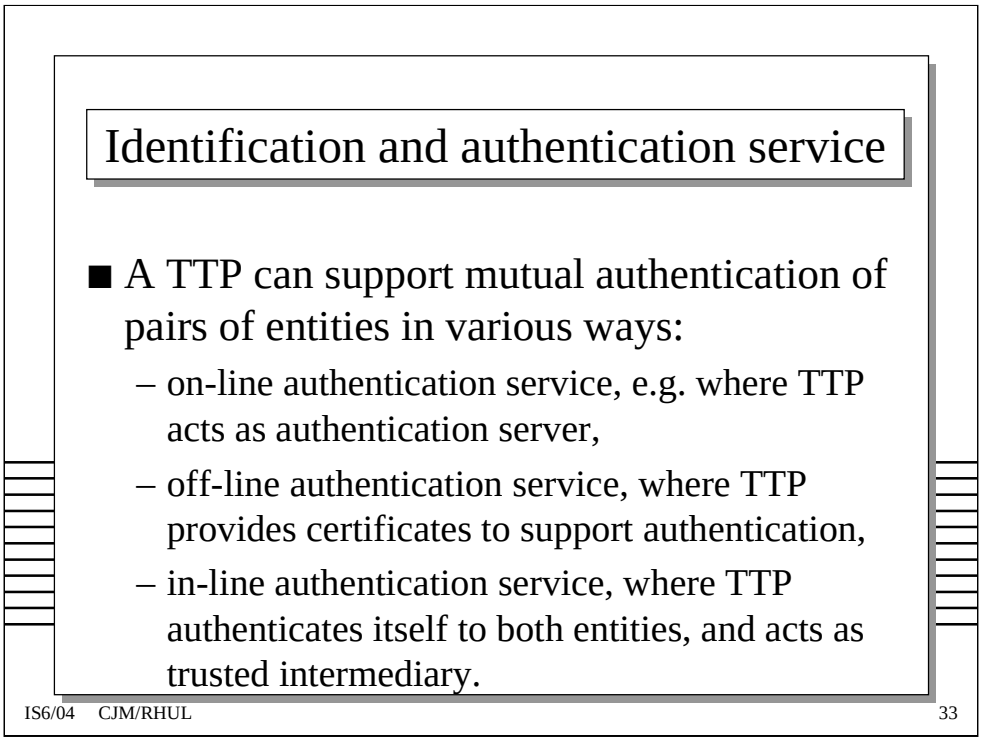


There are many examples of security services which rely on security-relevant information (which typically must be trustworthy) provided by a directory, i.e. an on-line database. Examples of security-relevant information which may be provided by a directory include:

- public key certificates,
- certificate revocation lists, and
- attribute certificates.

The following entities (roles) are involved in the security management of a directory service:

- *Security administrator* - responsible for the definition of access rules (e.g. the directory service is publicly available or restricted to a closed user group),
- *Auditor* - who reviews the audit trail periodically, to detect security violations,
- *Database administrator* - responsible for maintaining the security-relevant part of the directory.



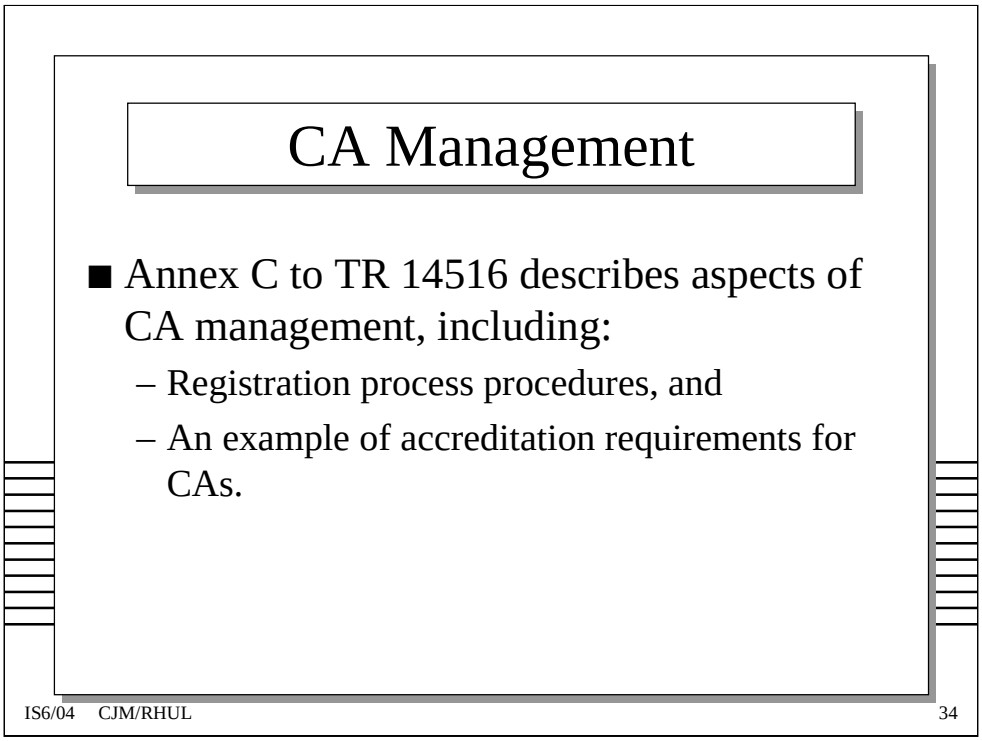
A TTP can support mutual authentication of pairs of entities in various ways.

• It can provide an *on-line authentication service*, e.g. where the TTP shares a secret key with each entity, and acts as an authentication server.

• It can provide an *off-line authentication service*, where the TTP provides certificates to support authentication.

• It can provide an *in-line authentication service*, where the TTP authenticates itself to both entities, and acts as a trusted intermediary.

These three approaches are all discussed in more detail in ISO/IEC 10181-2, the authentication framework. Specific examples of authentication mechanisms are given in ISO/IEC 9798.



Annex C to TR 14516 describes aspects of CA management, including:

- Registration process procedures, and
- An example of accreditation requirements for CAs.