18

A comparison of schemes for certification authorities/Trusted Third Parties

A. van Rensburg
IBM Park Private Bag X9907
2146
Sandton
South Africa
Tel: +27 11 302 8619
Fax: +27 11 302 8778
E-mail: alicem@johic1.vnet.ibm.com

Prof B. von Solms
Rand Afrikaans University
Johannesburg
South Africa
Tel: +27 11 489 2843
Fax: +27 11 489 2138
E-mail: basie@rkv.rau.ac.za

Abstract

A comparison of schemes employed by certification authorities or trusted third parties to generate certificates.

Keywords

Certificate, certificate authority, cryptography, digital signature, key, security, trusted centre, trusted third party, public key

1. Introduction

1.1 Background

The application of information technology rapidly evolved from stand-alone centralised computer systems, where no or very little interaction with other computer systems was required, to distributed computing environments, establishing communication among different institutions using different computing systems, to the current trend of open systems and world wide accessibility via the internet and intranet.

As the need for interconnectability increased, information shared over these networks have become more and more exposed to misuse. Therefore it has become increasingly important for information security to address:

- Information privacy.
- Information integrity in term of:
  - origin of data.
  - destination.
  - content.
  - and ultimately non-repudiation.
- Identification and authentication between communicating parties

The requirements listed above can only be provided by applying cryptographic methods. Cryptography is the only known mechanism which can provide information confidentiality and data integrity economically within the information technology environment.

There are two general forms of key-based cryptographic algorithms known as symmetric and asymmetric. Symmetric algorithms are characterised by the ability of the enciphering key to be calculated from the deciphering key and vice versa. In most cases both encryption and decryption keys are the same. The security of a symmetric algorithm rest in the key and therefore the key needs to be kept secret. When two entities need to communicate private information, the same key has to be loaded into both systems with secrecy as well as with integrity. In most systems this application is performed by specially assigned security personnel.

Public-key algorithms are designed so that the key used for encryption is different to the key used for decryption with the additional proviso that the decryption key can not be calculated from the encryption key. The encryption key can therefore be made public. When two entities need to communicate private information between each other the public key of the receiving entity needs to be loaded into the sending entity's system. Since there is no risk in divulging the public key, this eliminates the need to load keys in secret. The loading of the public key however still needs to be done with integrity.

Public-key cryptography and symmetric cryptography work best together. The strength of public-key cryptography resides in key distribution and providing authentication. Symmetric cryptography is orders of magnitude faster and very suitable for the protection bulk information.

By applying these cryptographic algorithms in various ways, solutions for the above mentioned problems can be found in particular:

- Encryption and decryption to provide data privacy.

- Message authentication codes and digital signatures to provide integrity. Message authentication codes and digital signatures are equivalent to a cyclic redundancy check value except that the process involves a secret key during generation and verification cycles. Digital signatures have an additional advantage in that non repudiation can be achieved since only the entity which owns the private component of the public-key pair could have produced the digital signature. This is equivalent to a person hand-signing a document.
- Digital certificates to aid identification and authentication. A digital certificate is an electronic credential issued by a trustworthy organisation. The digital signature vouches for an entity's (an individual's, business's or organisation's) identity and authority to conduct any transaction over a network. The digital certificate can be seen as equivalent to an ID book, passbook or driver's license.

  More specifically: a public key certificate is a public key together with other unique identification which is digitally signed by a trustworthy authority. The objective is to certify that the information of the holder of the public key is valid and that the public key really belongs to the holder.

  Certificates are the result of an arbitrated protocol that utilises a third party to ensure authentication between communicating entities. These third parties may be referred to as certification authorities, trusted centres or electronic notaries.

1.2 Purpose

This paper examines the entities which create these certificates and the methods employed by these entities to achieve a trusted environment where these certificates can be used.

The purpose of this paper is to analyse the functionality of these certification authorities with the purpose of building a reference model.

A common minimum level of trust is required for open certification services provided by certification authorities interconnected in the network. A common framework for certification authorities can be useful with the accreditation of certification authorities, contribute to open standards for multiparty protocol and enable greater interoperability in an open environment.

2. A reference framework for certification authorities

2.1 Introduction

Certificates are used for the identification and authentication of a wide variety of entities in a wide variety of applications such as:

- Users, merchants, payment gateways, card issuers and aquirers for the purpose of performing financial transactions over a network.
- Point-of-sale devices for the purpose of establishing a secure channel for the interchange of keys.
- Users for the purpose of exchanging documents over the network.

Several certification authority applications have been developed to address the certification of public keys in each of these applications. These certification authority applications provide a specific set of functions within a specific framework of trust. This section first addresses some of the different trust models already implemented in order to meet certification requirements, followed by a breakdown of functions implemented by a certification authority and is structured as follows:

- 2.2 Trust models.
- 2.3 Functions.
- 2.4 Critical success factors.
- 2.5 Conclusion.

2.2 Trust models

Certification of public keys means that some trusted third party assures the binding of a public key and related person or entity. There are several possibilities how this trust can be realised:

- **Unstructured trust model.** Each certificate is self-certified and distributed with some personal assurance of validity. This provides bilateral end-user-to-end-user certification in that it trusts only in bilateral assurance.

  Pretty Good Privacy (PGP) (reference: Schneier) is an example. PGP uses a distributed approach to key management. There are no certification authorities. Each user generates and distributes their own public key. Users can sign one another's public keys, adding extra confidence to the key's validity. An entity which signs another's public key becomes an introducer for that entity. The user of the public key examines the list of introducers who have signed the key, if one of the introducers is trusted by this user, then the new public key can be accepted. If two introducers are marginally trusted then the key could also be trusted.
- **Single trusted arbitrator** such as Kerberos (reference: Schneier). **Kerberos** is a trusted third-party authentication protocol based on symmetric cryptography where a Kerberos server acts as a trusted arbitrator for each transaction.
- **A set of certification authorities** which are committed to certain security policies and operation modes. These certification authorities receive their trust from a broad user community due to their commitment to their certification behaviour and public control.

  Privacy-enhanced mail (PEM) (reference: Schneier) is an example. PEM adopted a very rigid hierarchical trust model. Each certification authority had to ensure that it

certified only certificates subordinate to it in the name space. The resulting tree structure had only one root - that of the Internet Society.

- **Cross-certification model.** An intermediate model which again consists of a series of certification authorities but some certification authorities can cross-certify each other. Such a model was implemented by TESTFIT (reference: TESTFIT).
- **A hierarchy of certification authorities,** where each certification authority is certified by a certification authority at a level higher to achieve a hierarchy of trust. Each certificate is validated by traversing through the signature chain, verifying each certificate up to the root. **Secure Electronic Transaction (SET)** (reference: SET 96) is an example.

The usage of public-key based security services depends on a common set of rules that determine the security behaviour of all participants. This is especially important for the relationship between users and the certification authorities where the relationship is based on trust. These security policies govern the behaviour of certification authorities and the communication rules between the certification authorities and their clients as well as the characteristics of the security services between the users. The security policies are reflected in the trusted model and are eventually implemented as a series of security protocols or functions.

2.3 Functions

Independence of hardware, software and operating system specifics is a prerequisite for any generic model. The reference framework needs to adhere to the above criteria and also specifically address independence of security policies, cryptographic algorithms, cryptographic protocols and trust models as discussed in the previous section.

In its simplest form the certification process may consist of the association of a public key with the user's unique identifying details, followed by the structuring of this information together with an expiration date, into a formal structure and finally signing this structure with the private key of the certification authority. A more complex process may include aliasing, authentication with the use of time windows and initialisation services. The reference framework specifies a super set of functions which supports any certification process, from the most simple to the most complex.

In order to understand the requirements for a certification authority, some implementations of certification authorities were studied. Two of these case studies are described in subsequent sections of this document.

By studying a number of different implementations of certification authorities, it became clear that the certification procedure may be divided into the following sub-processes. Depending on a number of factors, the certification authority may perform all or only selected of the following sub-processes:

Certification practise statement

A certification practise statement should be generally accessible to all potential participants of a networking group so that business conduct of the certification authority and the client is understood. The security policies employed, different types of certificates provided and other general information required for certification should also be accessible.

Synchronisation

This step allows the requester and the certification authority to synchronise their cryptographic working environments. Details of the security environment such as cryptographic algorithms supported, preferred cryptographic protocols for certification and key exchange can be communicated during this phase. In many certification authority applications the cryptographic methods and protocols have been pre-arranged and are not negociable.

This step may also establish a secure communication channel between requester and certification authority so that the registration request may be transmitted securely to the certification authority.

Registration

A requesting entity needs to subscribe to a specific network group it wishes to join. Every user wishing to participate in a specific networking group must register with a certification authority. The registration process is initiated when the requester sends a registration request to the certification authority. The certification authority replies by stipulating the required information for the requester to join an exclusive application group. A registration form as used in SET (reference: SET 96) is an example of such an information list.

A section of the registration form will also request some uniquely identifying information relevant to the requesting entity. This unique information will eventually be tied to the public key during the certification process. The content of the uniquely identifying information depends on the entity being certified and the purposes for which the certificate will eventually be used. The registration form can also include policies which must be signed by the requester and which will serve to bind the requester to certain conduct within the group it wishes to join.

The following describes some of the information sent by the requester for registration:

- The requesting entity's public key if the entity is capable of generating its own public secret key pair.
- Unique identifying information.
- The purposes for which the public key will be used. Usage of keys may be separated into keys exclusively used for signing and keys exclusively used for encryption.
- The current state of the certificate - if it is a new certificate or an existing certificate to be renewed.

The registration process may be conducted personally or by correspondence. Alternatively, electronic registration may be considered for convenience.

Authentication

Once an entity registered, the application form is evaluated to ensure the integrity of the requesting party.

Authentication can be defined as consisting of those procedures an mechanisms that allow a computer system to ensure that the stated identity of some external entity is correct. Authentication approaches generally involve some sort of validation approach to produce evidence or confidence that a reported identity must be valid.

Once a certification authority receives a request for certification, the credentials of the requester are inspected to evaluate the request. The authentication process can be compared

to a credit check and depends on the purposes for which the requested certificate will be used. The extent to which authentication is performed also depends on the grading, strength and value of the certificate requested. The authentication process may range from a manual to fully automated process depending on the authorisation policies agreed beforehand.

A variation of the process may pre-authenticate entities where sponsors introduce potential requesting entities to the authentication authority before the requesting entity approaches the certification authority. A white list may be compiled containing all entities which are expected to request certification and which may be positively identified. Such a variation is only useful where the number of requesting entities are low and the identity of these requesters can be determined with a high level of certainty.

Authentication of an entity is best done face to face but this is not always practical. Therefore the authentication authority may need further communication with the requesting entity to ensure the positive identification of the requester. Such communication may include some challenge to the requesting entity to prove that the requesting entity is not impersonating another. Challenges may vary and may include pre-defined operations executed on request such as the calculation of a modification detection code of the microcode contained in a device.

Time window intervals can also be used to prevent one entity from impersonating another. A time interval is agreed between the authentication authority and the requester during which the requester is expected to send a certification request containing the unique identity of the requester. If only one such request is received during the window, the authentication authority may assume that the requester is authentic, if two or more requests are received in the same interval the certification requests are denied. The time interval mechanism needs to be used in conjunction with other means to ensure that the certification request was not intercepted and an impostor's certification request accepted instead.

The authentication authority may operate a chain of authentication authorities, each of which examine an applicant's credentials, verify the applicant's identity and authorise the issuance of the certificate.

Key generation

The process of generating a public key pair is a resource intensive process. Not all entities may be capable of performing such a task. Especially some POS devices may have limited public key capability. For these cases the certification authority may generate a public key pair and send the key pair to the requesting node over a secure channel. Some cryptographic protocols rely on the generation of the keys by the certification authority.

Naming and aliasing

Each participant in the network needs to be identified by a unique name. If the number of participants is high, the use of a name may not be sufficient. A service is required which will guarantee unambiguous names or aliases which can be used to uniquely identify a participant in the network.

The unique user information also depends on the entity to be identified. For a user an identity number could be considered and for POS devices an internal unit number could be used. In some cases a pseudonym needs to be generated since the original user identification

number may lead to misuse of the user's information as is the case in credit card transactions as explained in SET (reference: SET 96).

Key personalisation

The process of associating a particular public key with specific user information, is key personalisation. One and only one registered entity must be identified with a particular public key pair. This is especially important in the case where the requesting entity has to rely on another entity to generate the public key pair.

Certificate structures

X.509 is a standard for the structuring of certificate data which includes both the public key, unique identifying information and authentication for the key. Imbedded in the certificate are the validity dates as well as the identifying information of the authorising authority which enables signature chaining.

Extensions to the structure allow other information such as certificate policies, key usage restrictions and other application specific information to be imbedded in the certificate.

Certificate generation

Digital certificates are created by applying the private key of the certification authority to the personalised key. Key separation should be implemented, differentiating between keys used for signing and keys used the encryption of other keys.

Certificate revocation lists

A compromised certificate is revoked and listed in a certificate revocation list (CRL). This list has to be readily available within the environment where the certificate was active.

It is therefore very important that the integrity of the CRLs are maintained throughout the network. Certification identifiers can be employed as a mechanism to check the integrity of a CRL. This identifier is used in communications and ensures end users screen certificates against the latest revocation information.

Certificate directory management

On-line directories may be provided which contain the public keys and associated certificates for public access. X.500, a global directory service standard is an example of such a mechanism. These on-line directories may act as an electronic telephone directory and can be of great use in a large network where it is impossible for everybody to have all potential partner's addressing details and also serves to shield the users from complicated addressing details. These directories may however also be distributed for use in an off-line environment.

Although certificate directories are not an essential component in the certification process, the certification authorities would be the ideal hosts for such facilities due the trusted nature of the certification authority.

Distribution of certified material

This step allows two entities to exchange any other information required for the requester to actively participate in the network group once the requester has been certified. Some of the data required, excluding the certificate, may even be distributed before or during the registration process. This process would require an additional step after certification to complete the data required for an entity to actively participate in a network group. Alternatively the distribution of certified material may be performed once certification has been successfully completed. In an off-line environment, the distribution of this operational material may be more economical when distributed together with the certificate. Off-line distribution may employ the use of a PIN protected smart card for the distribution of this material.

In an on-line environment the initialisation process may be started when an entity sends an initialisation request to a certification authority. This request includes information reflecting the current operational state of the requester and may include:

- Identification check values or thumbprints of the certificates of other entities which may be required such as the certificate of the root certification authority. The list of certificates required for a particular user could be defined as a subset of the public key directory.
- Identifiers of certification revocation lists. These identifiers provide an economical way for the certification authority to validate that the requester operates on the current revocation lists.

The certification authority inspects the operational state of the requester and responds to the initialisation step with certificates, revocation lists and identifiers which where either stale or absent from the request.

The purpose of this step is to ensure that the requesting entity establishes a relatively trusted working environment. In addition, this step allows the requesting entity and the certification authority to synchronise their working environments with regards to the objects required by the particular application.

Integrity of the root public key.

Special attention needs to be given to assure the integrity of the public key of the certification authority at the top of the trust hierarchy since the integrity and the trust of the whole certification process hinges on this public key. One of the popular schemes is to publish the public key in publications. However, when the root public key needs to be renewed, some additional mechanisms need to be employed to ensure all entities will use the new root public key. In addition, methods need to be employed to ensure that the replacement of the root public key is indeed authentic and not an attempt to impersonate the certification authority.

SET (reference: SET 96) implements a mechanism which generates a renewal key at the same time the root public key is generated. The hash of the renewal key is already present in the self-signed root certificate when shared with subordinates. When the root key is to be renewed, users can validate that the new root key is indeed a relation of the old root key.

Miscellaneous functions

The certified authorities are trusted entities and therefore may provide additional services which require a high level of integrity. These services may include initialisation functions, date and time stamping services and key repository services. In cases where sensitive information needs to shared with entities not capable of communicating over a network or where a secure protocol can not be established, the certification authority may provide facilities to provide keys and certificates directly to the entity for example by injecting this information into POS devices. Such services may be offered by an initialisation service.

Date and time stamping services may be supplied where an authentic time and date is required.

A service for archiving keys can be useful where specific keys need to be shared among members of a selected group, especially when some participants are not capable of using public key functions. Such a service would be responsible to validate users requesting specific keys, ensure that the keys are communicated to the requesting users in a secure manner and ensure that users only access keys they are entitled to. The convenience offered by such a service must be weighed carefully against the potential risks involved in keeping secret keys in a central repository.

Critical success factors

- Certification authorities need to adhere to some common set of rules that will establish trust of the users in the certification authority. Accreditation of certification authorities would reassure users of a proper trusted environment.
- User software needs to be verified to ensure that cryptographic protocols are adhered to.
- End user applications must check for expired certificates. This would require that the end user systems would have to date and time synchronise with some entity in the network trusted to keep the proper date and time.
- Ensure all users use the current revocation lists to prevent unauthorised access.
- Certification authority root key revocation and renewal. The trusted chain hinges on the integrity of the root public key. Special care needs to be taken that the root key can be distributed with integrity.

Conclusion

The certification processes may be performed by one single entity or processing may be distributed among several entities, each specialised to perform a subfuntion or a group of subfunctions.

The following list includes some suggestions for some possible arrangements with variations on distribution within the SET (reference: SET 96) environment.

- One entity performs all subfunctions for its clients.
- One entity receives, processes and approves certificate requests and forwards the information to the appropriate entity to issue the certificate.
- Certificate requests are received by an independent registration authority which processes the certificate application and forwards the requests for approval to an authentication authority which in turn forwards all approved requests to a certification authority for

certification.

The following two chapters describe the certification process for SET and for TESTFIT. Each certification authority is described in detail to provide information for the last chapter where a reference model and both case studies are compared. In addition two well known certification schemes, Pretty Good Privacy (PGP), described in paragraph 2.2 on page 4, and VeriSign are also compared with the reference model.

3. Certification authority of the Secure Electronic Transaction (SET).

3.1 Overview

Secure Electronic Transaction (SET) (reference: SET 96) protocol was designed by Visa and MasterCard as a method to secure bankcard transactions over open networks. Transactions are performed on-line or store-and-forwarded such as electronic mail. Various certificates are used in SET including:

- Cardholder certificate which is an electronic representation of the bankcard and the customer signature for the transaction. The certificate binds the public key to an account number which is effectively protected using a blinding technique so that only the certification authority, the issuer and the cardholder know the account number and the name of the cardholder
- Merchant certificate which functions as an electronic substitute for the payment brand decal which appears in the store window.
- Payment gateway certificates which authenticate the payment gateways to users and merchants.
- Issuer certificates.

3.2 Hierarchy

Since a bogus certification authority could be set up to create certificates that would contain the same information as that contained in a valid certificate, it is essential that the signature of the certification authority itself be certified as authentic by a higher level certification authority. The highest level certificate is called the root and will is self-signed, distributed and verified by a number of independent methods.

Certificates are verified through a hierarchy of trust. each certificate is linked to the signature certificate of the entity that digitally signed it. The public signature key of the root is known to all SET software and may be used to verify each of the certificates in turn. The path through which the certificates are validated is called the signature chain.

3.3 Functions of the certification authority

Registration authority

Registration is performed on-line with the use of electronic registration forms. This process is initiated by the user requesting a registration form. As part of this request the user also includes a thumbprint for every certificate and certificate revocation list in the user's secure cache.

The certification authority identifies the financial institution from the request and sends the relevant registration form together with any certificates and revocation lists either absent or identified as out of date.

The user's trusted cache is updated to contain the latest certificates and revocation lists in preparation for when the user receives its own certificate. The details requested in the

registration form differ depending on the entity requesting certification. In the case of a cardholder, the account number which would be used to uniquely identify the cardholder, is protected with a blinding technique to prevent the account number from being misused. The user submits the registration form and receives a receipt from the certification authority against which the user may query progress of certification.

Authentication authority

The processes and mechanisms involved in authorising certification is not part of SET and these are governed by policies as determined by the issuers.

Certification authority

Each entity must generate its own public key pair. Separate key sets are used for digital signatures and encryption purposes as well as for on-line and off-line processing. Catalogues are an example where a separate set of keys need to be used for off-line processing since the expiry date of the keys need to reflect the expiry of the catalogue offering.

The certification process associates the unique identification with the public key as provided during the registration process. This information such as with expiry dates, identity of the certification authority creating the certificate and other extensions is formatted into a X.509 structure which is signed by the certification authority.

Each certificate is linked to the signature certificate of the certificate issuing entity. The signatures are validated by following the trust hierarchy to the root. This path is referred to as the signature chain. The following list is also checked when a certificate is validated.

- Certificate association.
- Current date is within validity period.
- Intended key usage is valid.
- Key usage restriction is valid.
- The certificate is an end entity.
- Certificate type corresponds with the context in which the certificate is being used.

Special provision has been made for the generation and renewal of the root key. A replacement key is generated at the time when the root key is generated. The replacement key is stored securely until needed and the hash of this replacement root key is contained within the current self-signed root certificate. When a user receives a root key renewal, the user is obliged to verify the new root certificate by comparing the hash of the new root key with the hash contained in the current root key to ensure that the new root key is indeed the replacement of the current root key. This implies that the replacement root key is always pregenerated.

Revocation lists

Revoked certificates are added to a certificate revocation list. For each revocation list a check value is calculated which may be used to ensure that a user always uses the current revocation list. Different lists are maintained for different user groups for example, separate lists are maintained for the different card brands.

Certified material distribution

Material such as the certificates of other entities and revocation lists are distributed during the registration process. Special provision has been made to ensure the integrity of the root key.

- Root key distribution. The root key is initially distributed with the SET software. This distribution channel must be trusted. Some validation of the root occurs as a result of its initial use during contact with the certification authority.

  An alternative mechanism for initial distribution is provided by open distribution of the root key by some other channel and distribution of the hash of the root via another channel. The hash would be entered by the user to verify the root.

  The root key is distributed in a self-signed certificate. The root key certificate is available to software vendors to include with their software.
- Root key validation. Software can validate the root key by requesting the hash of the root key from the certification authority. If the software does not have the root key or the root key is found to be invalid, the root key may be requested from the certification authority. In this case the user will have to enter a string which corresponds with the hash of the root certificate. This string needs to be obtained from another reliable source. The replacement root key is validated by comparing the hash of the replacement key with the hash of the of the replacement key previously distributed.

4. Certification authority of TESTFIT - TTP and Electronic Signature Trail For Inter-modal Transport

4.1 Introduction

This project established a pan-European network of interworking Trusted Third Parties (TTPs), to provide services to support the electronic signing of documents which are used for the transport of freight across Europe. The TTPs specifically provide services to allow users to exchange electronically signed documents in a secure manner. As far as security is concerned, the participants in this pilot to a large extent rely on the inherent features of the communication media used, such as voice recognition, written signatures and stamps on paper documents.

The primary objective of the TESTFIT (reference: TESTFIT) project was to demonstrate the feasibility of establishing a pan-European network of interconnecting TTPs.

4.2 Hierarchy

The Trusted Third Party (TTP) environment consists of a number of TTPs connected together in a non-hierarchical network. Each TTP provides services to subscribers within its own domain. Interworking between users served by different TTPs is facilitated by interconnected service providers.

4.3 Functions of the TTPs

The services offered are the basic services required to support electronic signing of documents by users, such as :

User registration

Users register for the TTP service by filling out a registration form. A section of the form requests the name with which the user's key is to be personalised, addresses for billing purposes and other application related data.

Naming and aliasing

The naming format needs to provide for the unambiguity of names. This may be achieved by using information such as passport numbers, addresses and other information.

Key generation

The TTPs are responsible for the generation of all secure key pairs. The keys are issued to the users on PIN protected smart cards.

Key personalisation

This procedure is responsible for assigning a public key pair to the registered name of one user.

Key certification

Each TTP signs the public keys of the users within its own domain. TTPs also cross-certify keys between each other to allow users from different domains to communicate with each other.

Certificate revocation

When a certificate is revoked an immediate black-list stamp is associated with the relevant certificate. This information is also published on the public key directory.

Public key directory services

The TTPs provide a continuous updated directory of all certified keys issued by the TTP. The history of the lifetime of each key is also recorded. The directory service also includes revoked certificates as well as cross-certified public keys for users from different domains to be able to communicate.

Key distribution

Keys and certificates are distributed using smart cards. The smart card contains the user's secret key, certified public key, and the TTP's public certification key. The user's public key, certificate as well as the TTP's public key can be read from the smart card but can not be altered. The user's secret key can not be read from the smart card.

Revocation lists and the public key directories are distributed on-line via data modems and are also available on the request from the user.

5. Comparison of case studies

The following table compares both study cases with the list of functions as described in the reference model. This table of comparison is implemented primarily to test the reference framework against established implementations of certified authorities.

The following describes the table layout:

- Where the case study complies, the details are added into the table in **bold** text.
- Processes which are not implemented are left blank.
- Processes not implemented by the certification authority but supplied by other means are written in *italics* and details are added to the table.

Reference framework	**SET**	**TESTFIT**
Information	*Prearranged*	*Prearranged*
Synchronisation	*Prearranged - cryptographic protocols based on RSA and DES*	*Prearranged - cryptographic protocols based on RSA and DES*
Registration	**Electronic registration**	**Registration by mail**
Authentication	*Not prescribed and performed by issuer*	**Performed by certification authority**
Key generation	*End user generate own keys*	**All keys generated by certification authority**
Naming and aliasing	*Determined by end user*	*Determined by end user*
Key personalisation	**Performed by certification authority**	**Performed by certification authority**
Certificate structures	**X.509 standard supported**	**Proprietary structure**
Certification	**Certificate chaining implemented**	**Single hierarchy with cross-certification**
Revocation lists	**Seperation of CRLs implemented**	**Implemented**
Public key directory		**Public key directory implemented**
Certified key distribution	**On-line**	**Off-line on smart cards and on-line**
Certification authority public key integrity	**Pre-generated replacement**	**Certification authority public key distributed via PIN protected smart cards**

Reference framework	**PGP**	**VeriSign**
Information	**Informtion published on the internet**	**Information published on the internet**
Synchronisation	*Prearranged - cryptographic protocol based on* RSA *and IDEA*	*Prearranged - cryptographic protocol based on RSA*
Registration		**Electronic registration**
Authentication	**Self authentication**	**Authentiation depends on grade of certificate requested**
Key generation	**End user generate own keys by executing specific PGP command**	*End user generate own keys with own software/hardware*
Naming and aliasing	**Self determined**	**Performed by crtification authority**
Key personalisation	**Self determined**	**Performed by certification authority**
Certificate structures	**Proprietary**	**X.509 standard supported**
Certification	**Self certification**	**Certificate chaining implemented**
Revocation lists		**Revoked certificates are published in the VeriSign repository**
Public key directory		**Repository provided**
Certified key distribution	*Communicating parties exchange relevant information as required*	**Certificates are collected via the internet by providing a PIN**
Certification authority public key integrity	**Pass phrase protected**	**Integrity ensured**

References

Abad Peiro, J Asokan, N Waidner, M (1996) Payment Manager - Overview. SEMPER Activity Paper 212ZR054 <http://semper:zurich.ibm.com/info/212ZR054.ps.gz>

Amorosso, E (19XX) Fundamentals of computer security technology

Burton, S Kaliski, Jr (1993) An Overview of the PKCS Standards. RSA Laboratories < http://www.rsa.com/pub/pkcs/doc or http://www.rsa.com/pub/pkcs/ps/ >

European Commission DG-XIII.B.6 Infosec 94 - Phase II (1995) TESTFIT - TTP & Electronic Signature Trial For Inter-modal Transport

Europay International (1994) IC Card Specifications for Payment Systems - Part 3

IBM (1996) Internet Security Policy and Directives

IBM (1992) Transaction Security System Concepts and Programming Guide: Volume I, Access Controls and DES Cryptography GC31-3937

IBM (1992) Transaction Security System Concept and Programming Guide: Volume II, Public-Key Cryptography GC31-2889

Janson, P Waidner, M (1996) Electronic Payment Systems. SEMPER Activity Paper 211ZR018 <http://semper.zurich.ibm.com/info/211ZR018.ps.gz>

MasterCard Visa (1996) Secure Electronic Transaction (SET) Specification Book 1: Business Description

MasterCard Visa (1996) Secure Electronic Transaction (SET) Specification Book 2: Programmer's Guide

Schneier, B (1994) Applied cryptography. John Wiley & Sons, Inc

Tsudik, G (1996) Zurich iKP Prototype (ZiP): Protocol Specification Document. IBM Zurich Research. <http://www.zurich.ibm.com/Technology/Security>

VeriSign (1996) Certification Practice Statement. VeriSign < http://www.verisign.com/repository/CPS/intro.html >

Zimmermann, P (1993) Pretty Good Privacy Public Key Encryption for the Masses: PGP User's Guide