

FINAL REPORT

**Standardisation Issues for the European
Trusted Services - ETS**

by

Andrew Colleran

Quercus Information Ltd.

.....

This work has been funded by the European Commission. The opinions and views expressed may not represent official opinions and policies of the E.C.

MAY 1997

1. SUMMARY OF REPORT	1
1.1 PURPOSE.....	1
1.2 STATUS.....	1
1.3 PRIORITIES FOR ACTION.....	1
1.3.1 <i>Content of standards</i>	1
1.3.2 <i>Standards making processes</i>	2
2. SCOPE OF STUDY	3
3. REQUIREMENTS FOR STANDARDS.....	4
3.1 WHO NEEDS STANDARDS AND WHY	4
3.1.1 <i>Users of the Information Infrastructure</i>	4
3.1.2 <i>Providers of Trusted Services</i>	4
3.1.3 <i>Solution vendors</i>	5
3.2 INTEROPERABILITY, PORTABILITY AND MOBILITY	5
3.3 TYPES OF STANDARDS REQUIRED	5
3.4 REQUIREMENTS ON THE PROCESS.....	5
3.5 CONSTRAINTS ON STANDARDS.....	6
4. THE STANDARDS PROCESSES.....	7
4.1 FORMAL STANDARDISATION	7
4.2 INDUSTRY GROUPS AND SPECIFICATIONS	7
4.3 INTERNET STANDARDS.....	8
4.4 EUROPEAN STANDARDISATION	9
4.4.1 <i>High Level Strategy Group</i>	9
4.4.2 <i>Information and Communications Technology Standards Board (ICT SB)</i>	10
4.4.3 <i>CEN</i>	11
4.4.4 <i>ETSI</i>	11
5. ROADMAP FOR THE FUTURE — THE WAY FORWARD FOR STANDARDS.....	13
5.1 CRITERIA FOR RELEVANCE OF SPECIFICATIONS AND STANDARDS.....	13
5.1.1 <i>Widely adopted for current services</i>	13
5.1.2 <i>Developed by an open, industry wide body</i>	13
5.1.3 <i>Developed by an industry wide consortium</i>	13
5.1.4 <i>Supporting open public network services</i>	13
5.1.5 <i>Of general applicability</i>	13
5.1.6 <i>International or European</i>	13
5.2 VARIETIES OF TRUSTED SERVICES	14
5.3 SUPPORT SERVICES.....	14
5.3.1 <i>Public key technology</i>	14
5.3.2 <i>Non-repudiation</i>	16
5.3.3 <i>Symmetric key management services</i>	16
5.3.4 <i>Key escrow and recovery services</i>	16
5.3.5 <i>Directory Related Services</i>	17
5.3.6 <i>Time-stamping</i>	17
5.4 MANAGEMENT STANDARDS.....	17
5.4.1 <i>Mutual recognition, accreditation of services and liability</i>	17
5.4.2 <i>Evaluation</i>	18
5.5 END SERVICES	18
5.5.1 <i>Ad hoc groups</i>	19
5.5.2 <i>Project exploitation</i>	19
5.6 STANDARDS MAKING ISSUES.....	20
5.6.1 <i>Improving the processes</i>	20
5.6.2 <i>The role of European standardisation activities in relation to global activities</i>	20
5.6.3 <i>Standards making bodies</i>	21

5.6.4	<i>The representation of public interest</i>	22
5.6.5	<i>The role of SMEs in standards making</i>	22
5.6.6	<i>Incorporation of patented material in standards</i>	23
5.6.7	<i>Research and development projects and standards</i>	23
6.	SPECIFICATIONS AND STANDARDS — CURRENT AND IN DEVELOPMENT	24
6.1	ISO/IEC JTC1/SC21 OPEN SYSTEMS INTERCONNECTION, DATA MANAGEMENT AND OPEN DISTRIBUTED PROCESSING.....	24
6.1.1	<i>Framework for Authentication Services</i>	24
6.1.2	<i>The X.509 Certificate and Certificate Revocation Lists (CRL)</i>	25
6.2	ISO/IEC JTC1/SC27 IT SECURITY TECHNIQUES	25
6.2.1	<i>Mechanisms and techniques</i>	26
6.2.2	<i>Management support documents and security guidelines</i>	29
6.3	ISO TC68 BANKING, SECURITIES AND OTHER FINANCIAL SERVICES.....	32
6.3.1	<i>Guidelines for Trusted Third Party services</i>	32
6.3.2	<i>Certificate profile</i>	34
6.4	EDIFACT — SYNTAX DEVELOPMENT GROUP OF THE UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE (UN/ECE)	34
6.5	CEN	35
6.5.1	<i>TC224 — Machine readable cards, related device interfaces and operations</i>	35
6.5.2	<i>TC251 — Medical Informatics</i>	36
6.6	EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE — ETSI.....	36
6.6.1	<i>Requirements</i>	36
6.6.2	<i>Proposed first standard</i>	36
6.7	INTERNET ENGINEERING TASK FORCE (IETF).....	36
6.7.1	<i>Internet Public Key Infrastructure</i>	37
6.7.2	<i>Generic Security Services API</i>	43
6.7.3	<i>Lightweight Directory Access Protocol (LDAP)</i>	43
6.7.4	<i>S/MIME (Secure/Multipurpose Internet Mail Extensions)</i>	44
6.7.5	<i>PGP/MIME (MIME Security with Pretty Good Privacy)</i>	44
6.7.6	<i>Secure Sockets Layer</i>	45
6.7.7	<i>Simple Public Key Infrastructure (SPKI)</i>	45
6.7.8	<i>Domain Name System Security Extensions</i>	46
6.7.9	<i>Security Architecture for the Internet Protocol</i>	46
6.8	OBJECT MANAGEMENT GROUP	47
6.9	MICROSOFT CRYPTOAPI.....	48
6.10	THE OPEN GROUP.....	48
6.11	PUBLIC KEY CRYPTOGRAPHY STANDARDS (PKCS)	49
6.11.1	<i>PKCS #1: RSA Encryption Standard</i>	50
6.11.2	<i>PKCS #3: Diffie-Hellman Key Agreement Standard</i>	50
6.11.3	<i>PKCS #6: Extended-Certificate Syntax Standard</i>	50
6.11.4	<i>PKCS #7: Cryptographic Message Syntax Standard</i>	50
6.11.5	<i>PKCS #9: Selected Attribute Types</i>	51
6.11.6	<i>PKCS #10: Certification Request Syntax Standard</i>	51
6.12	SECURE ELECTRONIC TRANSACTION	51
6.12.1	<i>The participants</i>	52
6.12.2	<i>The processes</i>	52
6.12.3	<i>Issues, status and standards</i>	54
7.	PROJECTS AND STANDARDS	55
7.1	GENERAL PROJECTS	55
7.1.1	<i>ICE-TEL</i>	55
7.2	ELECTRONIC COMMERCE	57
7.2.1	<i>Secure Electronic Marketplace for Europe (SEMPER)</i>	57
7.2.2	<i>End-to-End Security over the Internet — E2S</i>	61
7.2.3	<i>OSM, an Open Service Model for Global Information Brokerage and Distribution</i>	61
7.3	. THE WORLD WIDE WEB.....	62

7.3.1 PICS (<i>Platform for Internet Content Selection</i>).....	62
7.3.2 <i>Digital Signature Initiative</i>	62
7.4 HEALTHCARE — TRUSTHEALTH	63
7.5 TELECOMMUNICATIONS.....	66
7.5.1 <i>Advanced Security for PErsonal Communications Technologies — ASPeCT</i>	66
7.6 ELECTRONIC MAIL	67
7.7 ELECTRONIC PUBLISHING, INFORMATION BROKING, COPYRIGHT MANAGEMENT	67
7.7.1 <i>Architecture for information Brokerage Service — ABS</i>	67
7.8 CHIP - SECURE ELECTRONIC TRANSACTION — C-SET	68
7.8.1 <i>Differences between C-SET and SET</i>	68
7.8.2 <i>Interoperability with SET</i>	68
7.8.3 <i>Future plans</i>	69

1. SUMMARY OF REPORT

1.1 Purpose

There are two main purposes of this report: the first is to review the current standards and specifications which exist or are being developed, which are relevant for the establishment of Europe-wide trusted services; the second is to put forward a roadmap for future standards development work.

1.2 Status

The area of standards development is always changing: existing standards are improved; new standards are introduced. This report refers to the state of standards and specifications activities at the beginning of April 1997. The report has been produced following review of work in a number of standards related organisations:

- International Standards Organisation (ISO)
- Internet Engineering Task Force (IETF)
- European Telecommunications Standards Institute (ETSI)
- European Committee for Standardisation (CEN).

The environment in which standards are produced and the motivations for standards have been considered.

The work of a number of industry groups has also been reviewed.

A number of projects funded by the European Commission have also been reviewed, in order to identify possible action to bring their results into the standards area.

1.3 Priorities for action

The main conclusions of the report and recommendations for action fall under two headings: content of standards and processes for their production. A more detailed roadmap is within the report. The underlying conclusion is that the technical standards, while not completely and formally ratified, are well advanced; what is required is a focus on implementation of applications using trusted services.

1.3.1 *Content of standards*

- Public key infrastructure to support digital signatures and other public key based operations such as non-repudiation:
 - adopt X.509 v3, for certificate format
 - promote use of Lightweight Directory Access Protocol (LDAP) for access to directories
 - adopt the work of the IETF Public Key Infrastructure Group (PKIX), either as it is or as a source for other developments of trusted service infrastructures

- certificates profiles — initiate action to minimise proliferation of certificate profiles and enable interoperability of certificates
- Smart cards — in order to provide confidence in the use of services, develop standards that support smart cards, particularly for the Secure Electronic Transaction specification
- Management standards (c.f. ISO 9000) — develop codes of practice and management guidelines to support mutual recognition of services by providers and to build confidence in services among users.

1.3.2 Standards making processes

Effective standards are made by consensus of the different players in the market place: vendors, service providers, users, representatives of the public interest. The processes should correspond to this by being open and visible.

- The IETF, as a global forum for network standards development, should be the preferred place for the development of specifications and standards to support the growth of trusted service applications. The work being done on the Public Key Infrastructure is an example of such activity.
- ISO work should focus on ratification of standards produced elsewhere, either in the IETF or in national bodies, if such ratification is needed by players in the market place.
- Groups of market players should be established to increase involvement by users and operators in the development of guidelines for the operation of trusted services.
- Standards work should be made more visible and efficient by the wider use of electronic media. This includes use of email discussion lists, document stores and directories of on-going work.

2. SCOPE OF STUDY

The objectives of this report are:

- to review the standards and specifications which exist or are being developed which enable the establishment and operation of European Trusted Services
- to identify what standards, specifications and other documents should be produced and
- to propose how that work should be done.

It should be noted that the development of standards and specifications is an on-going process and a view at a particular time may need to be revised as further standards and specifications are produced.

This report considers not only the content of the standards and specifications but also the processes which enable their production. A key attribute of a standard is that it is agreed by the community whom it concerns; it is therefore important to ensure that the processes which result in the production of standards involve, in the appropriate way, the parties concerned. The word *standard* is used formally to describe a specification which is going through or has gone through a process defined by national or international agreements according to which it is developed and agreed by a certain community, represented by a formally constituted body; these are known *as jure standards*. The word *specification*, on the other hand, is used formally of documents which may become standards or, by their demonstrated use within a community, are widely accepted in practice; this category may be called, informally, *de facto standards*. In formal language, *a specification* only becomes *ade jure standard* when it is agreed by a formal standards body. This report:

- identifies reasons for standards and specifications and their relevance to the establishment of European trusted services
- considers the processes for producing standards and specifications
- proposes a roadmap for future standards and specification related work
- reviews current standards and specifications
- examines the work of some projects relevant to standards and specifications for Trusted Services.

A Trusted Service is defined as being a service which is used by one or more entities to achieve, through cryptographic technology, confidence in the use of electronic media for the communication and storage of data. This confidence relates to the integrity of the data, who is accountable for it, who can access it and how available it is.

This report is about how standards and specifications can contribute to the establishment of Trusted Services and confidence in the electronic media the Trusted Services support.

3. REQUIREMENTS FOR STANDARDS

3.1 Who needs standards and why

3.1.1 Users of the Information Infrastructure

The Guidelines for Cryptography Policy recently published by the Organisation for Economic Co-operation and Development (OECD) emphasised the important impact on economic development and world trade of secure information and communications infrastructures. Trusted services are a major part of that infrastructure. There is thus a specific economic stimulus to the establishment of trusted services. The OECD Guidelines also highlight the need for international trade over open networks, with global interoperability, portability and mobility. For a user, interoperability means being able to work with a number of trusted services, without the need for special procedures such as data format conversion; portability means being able to move application solutions from one software and hardware environment to another and so the ability to combine an application with a choice of trusted services; mobility means being able to access the same trusted services, with the same functionality, when away from the usual place of work, particularly when in other countries.

Users will also need to have confidence in the solutions and services they use. This confidence may be based on already existing bases, such as the market presence of a service provider or vendor; it may be based on the trust already placed in an organisation for other reasons, for example, the trust relationship between a bank and its customers; it may be based on a market accepted evaluation or licensing scheme for services. Management standards such as ISO 9000, which express at any particular time the current "standard practice" or "best current practice" in an area, have a role among users in developing and establishing confidence in trusted services which comply with them.

3.1.2 Providers of Trusted Services

Service providers need standards for a number of functional reasons:

- They wish to provide services to as wide a market as possible; interoperability with their potential clients is required; their clients will not all have the same application, software and hardware systems.
- Service providers will need to establish relationships with other service providers, both in their own country and globally in order to support global transactions and the mobility of their customers, when away from their usual place of business; therefore technical interoperability among service providers is required.
- For service providers, portability of solutions means the ability to move their application systems from one software and hardware environment to another, and the ability to combine an application with a choice of trusted services, thus protecting their investment in that application.

There may also be a need for management standards, an example of which is the ISO 9000 Quality Management standard. Service providers will need to establish bases on which they can trust other service providers; standards

against which the operation of providers can be measured may assist the establishment of mutual co-operation agreements.

3.1.3 Solution vendors

Solution vendors need to produce solutions which meet the needs of users and service providers. Their solutions need to interoperate with solutions from other vendors. An incentive to developing portable solutions is the availability of a larger market for their products.

3.2 Interoperability, portability and mobility

Interoperability, portability and mobility are required in solutions and services; they are very largely achieved by agreed standards covering protocols, data formats and program interfaces. By using agreed protocols and data formats, applications and systems can interoperate without the need to develop gateway services and conversion programs changing one format to another.

Portability of solutions means they can be moved from one system environment to another and can be combined with a choice of trusted services; for users and service providers this means a protection of their investment in the deployment of the solution; for vendors it means a larger market for their solutions.

Mobility means that users can move from place to place, country to country with no loss of service provided by their trusted service. For service providers, mobility means being able to provide what the user needs wherever he is.

3.3 Types of standards required

In order to meet the market requirements, technical standards are required to support interoperability, portability and mobility. Management standards, (cf. ISO 9000) may be needed to assist service providers to establish global relationships and for users to have confidence in their service providers. Standards for evaluation of systems and services may also be required, in order to build confidence in the services provided.

3.4 Requirements on the process

Because this area of trusted services is about building confidence and trust in the information systems society, it is important that the process of standards production meets certain requirements. These requirements can be described as:

- openness — that is, the methods by which a standard is produced should be open to participation by all those concerned by the resulting standard; the phases of standard production should also be visible, preferably with versions of standards being published electronically.
- market driven — the standard should correspond to the developments of the market and its evolution, as reflected by the introduction of new products and services. This is especially relevant to the area of trusted services, which is a market still in an immature and introductory phase. Promotion of particular solutions, whether on a technical or regulatory

basis, which do not correspond to the market trends, is likely to lead to an ineffective standard.

- consensus — standards, by definition, represent an agreement; the strongest and most effective standards are those with the widest agreement, developed by consensus of the parties concerned by their production.

Standards developed in an open, market aware manner can support effective regulation, licensing and evaluation.

3.5 Constraints on standards

The area of cryptography in general is constrained by export regulations and controls on the use of cryptography for confidentiality; in some countries, these controls may include rules concerning access to encrypted data and the strength of cryptographic algorithms. These controls currently hinder global interoperability and mobility. For a current survey of law relating to cryptography, see *Crypto Law Survey* by Bert-Jaap Koops.

Any future standards in these areas, where necessary, will have to take account of regulations and controls, established by governments following the recent publication of the OECD Guidelines for Cryptography Policy. These Guidelines have established agreed international principles which will foster the development of a global secure information infrastructure, especially by stating that governments should avoid developing cryptography policies and practices which create unjustified obstacles to global electronic commerce and creating unjustified obstacles to international availability of cryptographic methods.

4. THE STANDARDS PROCESSES

4.1 Formal standardisation

Standards can be produced within any community after a process of development and agreement. However, standards in the formal sense of the word are those produced according to the so-called formal standardisation process, typified by organisations such as the International Standards Organisation (ISO). The development of formal international Information Technology (IT) standards has been done by specialist technical committees, consisting of experts from related committees in national standards bodies. The need to achieve consensus, both among the developers and between the national bodies who approve the results as international standards, has led to relatively long and sometimes unacceptable lead times from project initiation to availability of the standard. While the development of technology, especially in the area of networks and distributed systems, has been gathering speed, ISO has been trying to keep pace with it. In an attempt to improve the effectiveness of the IT standardisation process, the Joint Technical Committee of ISO and the International Electrotechnical Commission (IEC), known as JTC1, has proposed a way for Publicly Available Specifications (PAS) to be given a status as international standards in a relatively short time. Although it was always possible for established industry-specific or proprietary specifications *de facto* standards to be a starting point for development of formal standards, that formal process was seen by the main actors to be too expensive in time and resources.

The committees whose work is particularly relevant to Trusted Services are:

- JTC1/SC21 Open systems interconnection, data management and open distributed processing
- JTC1/SC27 IT Security techniques
- TC 68 Banking, securities and other financial services.

Issues

Problems in the formal standardisation process are:

- slowness of the process; a major factor is the extensive review process by national standards bodies.
- conflict of interests; academics and researchers want ideal and perfect solutions, vendors and users want solutions which work now.
- the process is a voluntary activity; those who represent the Information Technology market and can develop and review standards are not available when the pace of development speeds up.

It has yet to be seen if the proposal for the more rapid adoption as International Standards of PASs will have the desired effect of reducing the time taken to produce International Standards.

4.2 Industry groups and specifications

As the proposal from JTC1 recognises, "agreement" for specifications can be obtained by market presence. There are also many industry groups and consortia developing and promoting specifications such as:

- the Open Group, formerly X/Open
- Object Management Group
- World Wide Web Consortium (W3C)
- European Computer Manufacturers Association (ECMA)

One fundamental difference between these groups and the traditional standards bodies is that the former are not organisations open to and easily joined by any player in the IT market. Membership has a price. A consequence of a more business oriented approach is that such groups are able to progress their work more effectively than bodies which rely primarily on voluntary support. However, for their specifications to gain the acceptance of standards, these groups need to submit their specifications to a more open and public body.

4.3 Internet standards

The rapid development of the Internet over the last few years, especially its evolution from being primarily a global academic and research network to being widely used by global commerce, has brought to the fore the Internet Engineering Task Force (IETF) as a standards development body. The process of standards making within the IETF is open in that any individual can take part in a working group which is developing a standard. He merely has to persuade the other members of the group and work towards a consensus in order to achieve a result. An essential part of the standards process is the demonstration that proposed specifications work and that different implementations of the specification interwork where that is appropriate.

The process in the Internet community for the development and progression of standards is described in the document Internet Standards Process -- Revision 3 (RFC2026). The document lists the goals of the process as:

- technical excellence;
- prior implementation and testing;
- clear, concise, and easily understood documentation;
- openness and fairness; and
- timeliness.

The publishing medium for Internet standards and related documents is the series of documents called Requests for Comments (RFC). There are two main categories of RFCs:

- standards track
- non-standards track.

Standards track RFCs progress through the phases of proposed to draft to being agreed as a full Internet Standard. Non-standards track RFCs include the categories:

- Experimental
- Informational
- Historic.

Non-standards track RFCs do not have the agreement and consensus of the Internet community behind them. They may be new standards which may become standards track, they may be old standards or they may be standards

used within a particular community but which have not been subjected to the full Internet Standards process.

There are also RFCs with the classification Best Current Practice, which describe at a particular time the Internet community's best current thinking on a statement of principle or on the best way to perform some operations.

The groups which develop the Internet Standards are working groups organised in subject areas in the Internet Engineering Task Force (IETF). The standards are then considered by the Internet Engineering Steering Group (IESG), made up of the area directors of the IETF. It is possible to appeal against decisions of the IESG to the Internet Architecture Board, which is a body of the Internet Society.

Each standard has an Editor who is responsible for preparing and organising the standards in their final form. The IETF members who take part in the working groups' activities are network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Any interested individual can be a member.

Before standards enter the Internet Standards process, they are developed by a working group established with a charter or terms of reference, Development versions of the standard are published as Internet Drafts and discussed, usually on-line using electronic mail until a high degree of consensus is reached so that a draft standard can be published as a Request for Comments (RFC) document.

Not all standards development is done within the strict Internet structure; the World Wide Web Consortium (W3C) has the leading role in developing World Wide Web standards.

Other organisations use the Internet processes for publishing their specifications. For example, The Open Group has published as a draft document an Architecture for a Public Key Infrastructure. It is also possible that the Public Key Cryptography Standards, which come from RSA DSI, will be published as RFCs.

4.4 European standardisation

In recognising the need to make the standards process more effective and responsive to the needs of both vendors and users, two bodies have been set up in Europe:

- the High Level Strategy Group
- the Information and Communications Technology Standards Board (ICT SB).

4.4.1 High Level Strategy Group

The High Level Strategy Group (HLSG) is made up of representatives of four representative bodies from European industry. The bodies are:

- EACEM — the European Consumer Electronics Manufacturers
- ECTEL — the European Telecommunications Manufacturers
- ETNO — the European Telecommunications Network Operators
- Eurobit — the European Information Technology Industry.

The main task of this group has been to identify what needs to be done in the area of Information and Communications Technology, including standards, in order to establish a fully working Information Infrastructure in Europe. The group is developing requirements in a number of areas. Requirements statements have been produced on:

- electronic commerce in support of SMEs
- broadband networks
- home information services.

Among the recommendations in their report on barriers to electronic commerce were the following which relate to Trusted Services:

- the ICT SB should be actively involved in the definition of SET 2 (smartcard version of SET, including the standards for terminal equipment) (recommendation 1)
- a co-ordination process should be set up with SEMPER (ACTS project) which focuses on experimentation and trials (recommendation 2)
- roles and activity domains of security trusted third parties in the field of electronic commerce to be rapidly clarified (recommendation 7)
- business directories for electronic commerce to be developed (recommendation 8)
- pan-European legal and regulatory environment for electronic commerce to be agreed (recommendation 9)
- industry to develop conformity assessment procedures applied to electronic commerce security models and their corresponding implementations (recommendation 10).

Recommendation 1 was directed to the ICT SB. Recommendations 2 and 10 were to be followed up by the HLSG. Recommendations 7 and 8 were directed to the European Commission. Recommendation 9 was directed to the European Commission and the Council of Ministers.

4.4.2 Information and Communications Technology Standards Board (ICT SB)

The membership of the ICT SB is the "formal" standards bodies:

CEN
CENELEC
ETSI

augmented by developers of what is known as Publicly Available Specifications (PAS):

ATM Forum
Digital Audio Visual Council (DAVIC)
Digital Video Broadcasting (DVB) Project
European Association of Consumer Electronics Manufacturers (EACEM)
European Board for EDI Standardisation (EBES)
European Broadcasting Union (EBU)
European Committee for Banking Standards (ECBS)

ECMA
ERTICO
European Workshop on Open Systems (EWOS)
Network Management Forum (NMF)
The Open Group.

Observer status is held by:

European Committee for IT Testing and Certification (ECITC)
EFTA Secretariat
European Commission.

A relationship is also maintained with the following organisations, primarily in order to obtain requirements for standardisation:

European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC)
High Level Strategy Group (HLSG)
European Telecommunications Informatics Services (ETIS).

The ICT SB has three objectives:

- to analyse and co-ordinate requirements for standards and specifications, based on real market needs
- to translate requirements into plans for the creation of standards and specifications
- to allocate standards and specification development to the most appropriate body.

The ICT SB has reporting to it a **Security Group**, which shares the objectives of the ICT SB, but only with respect to security related matters. The Security Group is the place where decisions and recommendations to the ICT SB can be made on what security standardisation work should be undertaken and by whom.

4.4.3 CEN

The European Committee for Standardisation (CEN) comprises the national standards bodies of Europe. CEN has a number of Technical Committees relevant to European Trusted Services. They are:

the European Board for EDI Standardisation (EBES)
Medical Informatics (TC 251)
Smart cards (TC 224).

Standards developed by CEN committees are approved as European Standards by the national standards bodies who comprise CEN's membership.

4.4.4 ETSI

The European Telecommunications Standards Institute (ETSI) is a membership organisation consisting of companies throughout Europe who are active in the telecommunications industry, mainly as service providers or vendors. Following a recent restructuring, a Security Technical Committee, formerly known as STAG, has been constituted with responsibility for security throughout ETSI. This committee has set up an ad hoc group, open to all

bodies of the ICT SB membership, to work on a standard for Trusted Third Parties.

Standards developed by ETSI committees are submitted as drafts for ETSI approval following a public enquiry carried out by the national standards bodies. ETSI approval is given using a voting procedure giving a weight to a particular country's vote.

5. ROADMAP FOR THE FUTURE — THE WAY FORWARD FOR STANDARDS

5.1 Criteria for relevance of specifications and standards

A number of criteria have been used to select which specifications and standards are particularly relevant to the establishment of trusted services in Europe; individual standards may qualify under more than one heading. This report does not cover standards or specifications of particular cryptographic algorithms.

5.1.1 *Widely adopted for current services*

Industry, by its widespread adoption of a particular standard, is a strong indicator of the importance of a formal standard or a specification, which has the status of *ade facto* standard. Examples of such standards in the area of trusted third parties are the X.509 standard, the PKCS series (e.g. for key management, digital signatures, and certificate management), and the Microsoft Cryptography API.

5.1.2 *Developed by an open, industry wide body*

Development and promulgation of a standard, based on implementation experience, in an open manner, in a standards body which is open in its membership, is an important factor towards the general acceptance of its work. The PKI specifications being developed by the Internet Engineering Task Force (IETF) are examples of standards relevant under this heading. Work done in ISO/IEC JTC1 also qualifies under this heading.

5.1.3 *Developed by an industry wide consortium*

A number of industry consortia have been established with the objective of developing and publishing specifications. Because of their position in the market, the work of these consortia is significant. Among the specifications under this heading is the CORBA Security Specification, developed by the Object Management Group.

5.1.4 *Supporting open public network services*

Specifications and standards are only considered if they support or enable the provision of secure services over open public networks.

5.1.5 *Of general applicability*

Specifications and standards whose applicability is limited to one particular area of administration or commerce are not considered.

5.1.6 *International or European*

Standards and specifications are only considered if they are international or European.

5.2 Varieties of Trusted Services

The term "Trusted Service" describes a wide variety of services which provide different types of service to different users, whether they are application programs or human beings. One useful distinction is that between support services and end services. The classification is not rigid: some end services may be also regarded as support services. Making the distinction however is useful because of the greater urgency which is associated with standards for support services.

An example of an end service might be a confidential notarised messaging service. This end service is visible to the user and may be a basis for payment. In order to support this service, other services are required, such as key certification services, confidentiality services, and time-stamping services.

5.3 Support services

Support services can be classified under the headings:

- **Authentication:** an authentication service verifies the identity of a user or service. It is used to provide the access rights associated with the user or service and to enable accountability in the use of the system, for example, through audit trails.
- **Authenticity and integrity of electronic documents and data:** services which declare where documents come from and who is responsible for them.
- **Accountability:** services which apply to user to user transactions and relationships, such as non-repudiation services.
- **Confidentiality:** services which may include symmetric key management services (key generation and distribution) and key escrow/recovery.
- **Directories:** services to provide information about users and services.
- **Timestamping:** services to provide a time when events happen.

5.3.1 Public key technology

Public key technology for support of digital signatures is used in services for authentication, authenticity and accountability, including non-repudiation, in open networks. Public key technology can also be used for confidentiality services, such as generation and communication of symmetric keys.

A Public Key Infrastructure (PKI) comprises a number of services, which may or may not be provided by a single organisation:

- registration and certificate issuing services, which establish a relationship between a person or legal entity and a public key and produce a certificate recording that relationship and possibly more information about the person or entity, such as their professional or academic qualifications, their national identity number, their residence and so forth.
- key generation, that is the generation of a public/private key pair, which may include the storing and distribution of key material using a smart card

- certification revocation, in response to a users' request when the key is no longer valid or has been compromised
- certificate repositories, this includes filing of certificates, so making them available to users wishing to check the validity of certificates, and revocation of certificates
- key archive services, that is the storage of a public key no longer in use with a timestamped record of when it was in use so that old electronic documents can be verified even after the time the associated public key was valid
- time-stamping authorities, which provide a reliable time with a signature recording when a message digest is submitted to them.

The format of certificates which is most widely accepted is that defined by ISO/IEC JTC1 SC21, known as X.509 v3. It provides support for a wide number of applications such as electronic commerce and information provision; it supports a flexible trust model corresponding to user requirements.

STATUS AND RECOMMENDATIONS

PKI

The work of the IETF PKIX group should be monitored and endorsed subject to the final version meeting European requirements.

Certificate format

X.509 v3 should be adopted as the general purpose public key certificate format. There is a development in progress of a so-called simple public key certificate. However, this appears to respond to other requirements and at this time its definition is not stable.

It is not possible to predict the way that certificate usage will grow. A number of factors: user acceptability, public policy, vendor support will all be significant. It also seems likely that there will be a proliferation of certificate types conforming to the X.509 v3 standard. It is desirable to initiate action, such as the registration of certificate variants (e.g. use of extensions), to minimise the varieties of certificates and make interoperability easier.

Digital signature format

A format for digital signatures has been specified in the PKCS (standards #7 and #9). The World Wide Web Consortium has a project which is investigating this area in depth and can be expected to produce a comprehensive specification to support interoperability of digital signatures. This work should be followed and monitored to see if its results meet the market requirements.

Smart cards

Standards are needed for trusted components such as smart cards. The joint working group established by CEN TC224 and ISO TC68 may be a source for these standards. In addition, standard protocols for communication between a smartcard, executing security functions, and applications, including certificate management, are needed. Industry fora, such as the Java Card Forum are developing APIs for this. These activities need to be monitored. The CEN TC224/ISO TC68 will be the focal point for this area.

Application programming interfaces (APIs)

APIs need to be available for a number of PKI services

- public key delivery and verification interface
- Certification Authority agent
- local registration authority
- publication of certificates and CRLs.

A suitable body, such as the IETF PKIX working group could be a suitable place to undertake this work.

The Microsoft Cryptographic API and the Generic Cryptographic Services API from the Open Group are available to provide cryptographic service interfaces.

5.3.2 Non-repudiation

STATUS

The Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API) specification which is being produced by the Common Authentication Technology (CAT) working group of the IETF specifies a non-repudiation service. CORBA Security Services also specify a non-repudiation service.

These services include both evidence generation and evidence verification.

5.3.3 Symmetric key management services

These services may generate the secret keys used by parties to communicate with confidentiality or may facilitate the transfer of secret keys between parties wishing to communicate with confidentiality.

STATUS AND RECOMMENDATION

The ETSI work on developing a TTP standard including key management, key escrow/recovery may be expected to provide solutions in this area. The standard being produced should be widely reviewed, under the aegis of the ICT Standards Board.

5.3.4 Key escrow and recovery services.

There may be a number of different requirements for these services with respect to keys used to encrypt information. These requirements will be different depending on whether the data is being stored, as encrypted files, or communicated over telecommunications links. Within an organisation, there may be a difference between the *owner* of the data and the *user* of the data. An employer will be the owner of the data; an employee the user. If the data is being stored, then those who use or own the data may need to be able to gain access to keys used to encrypt the data and to recover it in a decrypted form. This may, for example, be required:

- if the user has lost the key
- if the user is no longer able to provide the key, because of illness, absence etc. and the owner needs access to the information
- when an employee, as a user, has left a company and there is a need by the data owner, the employer, to access files he has encrypted.

Legal authorities may also need to recover stored data from its encrypted form in the pursuance of their investigations.

When data is being communicated in an encrypted form, law enforcement authorities, in some countries, may need to be able, subject to specified legal safeguards, to access it in decrypted form. To enable this, use of a key escrow or key recovery service may be legally required. In general, users and owners of data do not require access to data being transmitted in encrypted form; their requirement is to access data stored in encrypted form.

These services only apply to keys used for the encryption of data. It should be noted that private keys used to sign documents or authenticate an entity must not be communicated to any party other than those whom they represent ("the owner"); this is to avoid any possibility of others masquerading as the owner of a key.

STATUS AND RECOMMENDATION

The recommendation of the previous section applies here too.

5.3.5 Directory Related Services

Directory access

The specifications being developed by the IETF Public Key Infrastructure (PKIX) group identify the Lightweight Directory Access Protocol (LDAP) as an important access method for retrieving information such as certificates. LDAP, developed by the IETF working group for Access, Searching and Indexing of Directories (ASID) has a wide applicability in networked applications and its use should be promoted. It is particularly suited to accessing X.500 directories but can also be used for access to directories implemented using other database technologies.

STATUS AND RECOMMENDATION

LDAP should be identified as a preferred access method for directories, in the open network environment, for use by SMEs and private citizens. Within corporate and closed environments other access methods, such as full X.500 directory access protocol, may be most appropriate.

5.3.6 Time-stamping

STATUS AND RECOMMENDATION

There is no standard for a timestamping service. The PKIX working group of the IETF has recently indicated that it will develop a protocol for a time-stamping service. This work should be monitored.

5.4 Management standards

5.4.1 Mutual recognition, accreditation of services and liability

In order to support a network of Trusted Services, individual services will have to make mutual recognition agreements with each other about, for example, cross certification of each other's certificates and mutual liability with respect

both to the services offered and the holding of or access to related keys. These mutual agreements will be much easier and more effective if there are generally agreed codes of practice and management guidelines for the operation of trusted services.

Accreditation of trusted services, which will promote development and acceptance of the services, also depends on the existence of these management standards.

Agreements will have to be made between service providers and users about their mutual responsibilities and liabilities concerning the services offered and the cryptographic keys associated with them.

STATUS AND RECOMMENDATIONS

SC27 is working on the development of guidelines for the use and management of Trusted Third Parties.

It is proposed that, since such standards are best produced by the operators of the trusted services themselves, a Europe-wide group be established to progress this subject.

5.4.2 Evaluation

A further element in developing accredited and assured services is the development of evaluation criteria.

STATUS AND RECOMMENDATIONS

The CCIB is undertaking work in this area with SC27 (ISO/IEC 15408 Evaluation criteria for IT Security); this work is not near completion. If a group is established to progress work on mutual recognition and accreditation, it is proposed that it review the CCIB and SC27 work and decide what shorter term steps are appropriate in this area. The work being done by TC36 of ECMA should also be reviewed. This work is currently represented by the draft standard of March 1997 entitled "Security Functionalities of the E-COFC (Extended Commercially Oriented Functionality Class for Security Evaluation)".

5.5 End services

The following services can be described as end services:

- notary, that is attestation that something has been done
- audit, that is recording of some action
- archive, that is deposit of information, possibly in conjunction with notarisatation
- information broking, that is, being an intermediary in the relationship between the user of information and the provider
- payment and billing, taking payment from users of information and other electronically distributed goods on behalf of providers, for example a copyright use and billing service
- electronic messaging

- registration services, holding information about the attributes of a person or legal entity; this service can also be seen as a support service to a service such as access control.
- directory services, providing information about persons or legal entities so that they can be contacted; this service can also be seen as a support service.

5.5.1 Ad hoc groups

The possible end services which can be described as trusted services are relatively diverse; services include:

- notarisation of contracts
- transaction audit
- document archiving
- negotiable document trading
- information broking
- payment and billing
- copyright use and billing service
- electronic messaging
- registration services
- directory services.

RECOMMENDATIONS

In general, for each service, codes of practice and guidelines are required to enable service providers to define the service and its quality and the agreements to be made by providers of the service with other providers and by users of the service with the providers.

The best place for this work is within industry associations or similar groups. Groups carrying out such work should be urged to publicise as much as possible their work and work with other groups. A summary database for this work should be established on a dedicated web site to promote cross-group co-operation.

5.5.2 Project exploitation

Sections of this report identify a number of projects whose work is of relevance to trusted services.

RECOMMENDATION

In order to ensure that the results of these projects, where they relate to trusted services, are widely known, it is proposed that a dedicated web site be established where project results can be published, as material which can be developed into guidelines or specifications.

5.6 Standards making issues

A number of key issues can be identified concerning the standards making process in general, which have a particular importance for the establishment of European Trusted Services. These issues are:

- life cycle processes for technical and management standards — requirements to production
- the role of European standardisation activities in relation to global activities
- which bodies should make standards
- the representation of public interest
- the role of SMEs in standards making
- incorporation of patented material in standards
- the results of research and development projects.

5.6.1 *Improving the processes*

The life cycle processes for standards have not been as effective as they needed to be. In particular, the identification of requirements for standards, based on justifiable and quantifiable grounds, has been weak. One of the responses to this weakness can be seen in the greater activity of industry consortia and other groups in the formulation of specifications, meeting their business requirements, which, at the end of their development may be submitted to the formal standards bodies for ratification as standards. . These groups may be restricted in their membership and their activities not publicly visible. The parties involved in the production of technical as compared to management standards also have different roles. Vendors and suppliers of products, systems and services will take the lead in the development of technical standards, with input of requirements from users. The production of management standards (c.f. ISO 9000) is however an activity in which those who use products and systems, particularly in order to provide services, need to take an equal part with service providers.

RECOMMENDATIONS

It is important to ensure that the processes:

- properly address the market requirements
- include all the relevant parties and
- are sufficiently open.

5.6.2 *The role of European standardisation activities in relation to global activities*

So many uses of information technology are on a global scale, so many vendors and suppliers operate throughout the world, that one concludes that standards must also be agreed globally. The goal is to achieve globally agreed standards wherever possible. On the way to that goal, however, one step may be to agree standards at a European level.

RECOMMENDATIONS

The decision to produce a European standard rather than an international standard should be a pragmatic decision based on justifiable grounds and should not make more difficult the agreement of a global standard after the European standard has been produced. Grounds for European level action may be a need:

- for a standard in a shorter time than can be achieved at the global level
- for the incorporation of particular European views, possibly related to European level structures
- to strengthen a European view for presentation to the rest of the world.

Any such European standard should use, as much as possible, already agreed international standards.

5.6.3 Standards making bodies.

For Information technology, the international standards bodies are:

- International Standards organisation (ISO)
- International Electrotechnical Commission (IEC), which is a member with ISO of the Joint Technical Committee 1 (JTC1)
- International Telecommunications Union (ITU).

The other important organisation, which although not a formally recognised standards body, is important in the development of network related specifications is the Internet Engineering Task Force (IETF).

There is a difference in method of working between the formal bodies and the IETF. The two approaches have been characterised as follows:

- the formal bodies adopt a theoretical, top down approach to the development of standards, which is rigorous and bureaucratic
- the IETF adopts a bottom up approach, which is driven by the need to implement solutions and is based on actual implementations; the process is closer to the needs of the market.

Over the last few years, the methods of working as well as the technical work have been converging. Within the ISO/IEC JTC1, procedures have been developed for more effective ratification of existing specifications as standards. Within the IETF, the move of the Internet away from a research and academic orientation towards commerce has brought with it greater involvement by commercial organisations who also are involved in formal standardisation activities.

Formal standards organisations in Europe, recognised by law at European level (Directive 83/189/EEC), are CEN, CENELEC and ETSI. These three European organisations develop formal standards through agreed, open and transparent procedures, based on a consensus of all interested parties.

The ICT(Information and Communications Technology) Standards Board has been set up by the three formal European standards bodies and now includes another twelve bodies who develop specifications in the ICT area. This board provides a focal point in Europe for capturing requirements for standards and deciding how they should be developed. It has a Security Group reporting to it, which again is a potential focal point for all information security related specification and standards issues.

RECOMMENDATION

The IETF is currently the most active forum for the development of standards to support the growth of network applications. The work being done on the Public Key Infrastructure is an example of such activity. The IETF should be preferred as the body for the most effective development of standards.

The role of the JTC1 committees should be to ratify already developed standards.

The ICT Standards Board, and the Security Group, should maintain a review function to ensure that European requirements are met by standards being globally developed.

5.6.4 *The representation of public interest*

As information technology evolves and develops more rapidly, there is an urgent need to ensure that the public interest and the needs of society are taken account of in the development of standards. Within a democratic, free market society this means that a number of sectors should express their requirements:

- private citizens
- consumer groups
- SMEs
- large corporations
- special interest groups
- public administrations
- governments.

RECOMMENDATION

This is best done by their communicating their requirements to the ICT Standards Board and its Security Group.

5.6.5 *The role of SMEs in standards making*

Although SMEs are often unable, on financial grounds, to justify active participation in the standards making process, they do rely on effective and open processes in order to be able to provide their requirements for standards, develop products, deliver services and exploit developments in information technology.

RECOMMENDATION

In order to enable SMEs to participate more in standards making:

- standards bodies should use the Internet, in particular electronic mail and web sites for document distribution
- SMEs should be encouraged and assisted to use the Internet
- organisations such as Chambers of Commerce should be used as a channel to promote greater awareness of the standards processes.

5.6.6 Incorporation of patented material in standards

Standards and specifications under development may include parts which are the intellectual property of contributors to the standard or other parties; the intellectual property may be subject to patents. It is necessary to avoid the possibility of potential monopolistic abuse of a standard, arising from the need of those who wish to comply with a standard having to purchase rights at an unfair price to use patented technology. The owner of patent rights should also not be able to impose restrictions on the use of the standard. It is also necessary that there is no dispute about who has rights to patents.

In security standardisation, the issue of patents has arisen most often with respect to cryptographic algorithms. Examples are:

- the RSA algorithm, which is patented in the US; this is referenced in an informative annex to ISO 9796 (Digital signature scheme giving message recovery), and is not part of the formal standard.
- the Diffie-Hellman algorithm, whose patent number 4200770 expired 29 April 1997, can now be freely used.
- the Digital Signature Algorithm, published by NIST, is claimed to infringe other patents which have been granted internationally.

RECOMMENDATION

Patents and other controlled technology must be identified in the development of standards.

Before a standard embodying patented technology can be agreed, it is necessary for the appropriate standards body to obtain from the patent holder a statement of the conditions on which the patented technology can be used. The guidelines developed by the ITU concerning patents should be followed; these recognise two situations where a patent holder agrees to his patented technology being included in a standard:

- The patent holder waives his rights; hence, the specification is freely accessible to everybody, subject to no particular conditions, no royalties are due, etc.
- The patent holder is not prepared to waive his rights but would be willing to negotiate licenses with other parties on a non-discriminatory basis on reasonable terms and conditions. Such negotiations are left to the parties concerned and are performed outside the ITU.

5.6.7 Research and development projects and standards

Europe, through a number of Programmes funded by the European Commission, has supported research and development projects. While it is not the objective of these projects necessarily to produce standards, it is very likely that the work of some of these projects can be a positive contribution to the development of specifications and eventually standards.

RECOMMENDATION

It is important that the results of these projects are presented and published widely to assist the overall development of agreed standards and brought into the IETF forum whenever possible.

6. SPECIFICATIONS AND STANDARDS — CURRENT AND IN DEVELOPMENT

This section considers existing standards and specifications which are relevant to the setting up and operation of Trusted Services. The standards are considered according to the committee or group which has produced them.

6.1 ISO/IEC JTC1/SC21 Open systems interconnection, data management and open distributed processing

This JTC1 sub-committee has produced a number of versions of the directory standard. Part of that standard is of fundamental importance to the establishment of Trusted Services. The standard is entitled:

ISO/IEC 9594-8:1995 Information technology -- Open Systems Interconnection -- The Directory: Authentication framework

This International Standard, which is also published as ITU-T Recommendation X.509, by which name (X.509) it is most commonly known, is important for two reasons:

- it defines a framework for the provision of authentication services;
- it defines a certificate format for public keys.

6.1.1 Framework for Authentication Services

In defining a framework, the standard recommends the use of strong authentication, involving credentials formed using cryptographic techniques, as the basis for providing secure services.

The strong authentication method described in the X.509 framework is based on public key cryptosystems. The standard notes a major advantage of such systems that user certificates may be held within the Directory as attributes, and may be freely communicated within the Directory System and obtained by users of the Directory in the same manner as other Directory information. The standard assumes that user certificates are formed by “off-line” means, and placed in the Directory by their creator. The generation of user certificates is performed by some off-line Certification Authority which is completely separate from the Directory System Agents (DSAs) in the Directory.

The standard describes the process whereby one user is authenticated to another using a certificate which contains a public key and is signed by a Certification Authority which the user trusts. This process is based on a certification path which logically forms an unbroken chain of trusted points in the Directory Information Tree between two users wishing to achieve authentication.

How keys and certificates should be managed forms a part of the standard. The responsibilities of a Certification Authority and a procedure for the revocation of certificates are described. Revocation of certificates is covered extensively in an amendment to the standard.

The authentication framework described in X.509 does not depend on the use of a particular cryptographic algorithm, but RSA is described in an Informative Annex.

Other Annexes which are not part of the recommendations are useful in describing security requirements and terms, and public key cryptography.

In order to use systems following the standard, each user must possess a unique distinguished name. Two users wishing to achieve authentication must use the same public key cryptographic algorithm and hash function.

6.1.2 The X.509 Certificate and Certificate Revocation Lists (CRL)

X.509 also specifies the syntax (in ASN.1) of a public key certificate, which is necessary when using asymmetric (or public) key cryptographic technology. Use of the X.509 certificate standard is independent of the use of an X.500 Directory. This part of the standard has been updated by an amendment arising from experience in using the earlier definition. The updated standard is identified as X.509 v3. The main purpose of the amendment is to define extensions to the certificate and development of the revocation procedure. The earlier standard proved to be too restrictive when attempts were made to use it in organisations composed of departments with different security policies; it was too strictly hierarchical. The amendments are intended to allow explicit management of trust and policies corresponding to the differing needs within an organisation and certification across hierarchies.

The extensions include the following

1. additional information about the keys involved, including key identifiers for subject and issuer keys, indicators of intended or restricted key usage, and indicators of certificate policy;
2. alternative names, of various name forms, for a certificate subject, a certificate issuer, or a CRL issuer, and additional attribute information about a certificate subject;
3. allowing constraint specifications to be included in Certification Authority (CA)-certificates (certificates for CAs issued by other CAs) to facilitate the automated processing of certification paths when multiple certificate policies are involved, e.g. when policies vary for different applications in an environment or when interoperation with external environments occurs;

The revocation procedure has been revised so that a certificate revocation list (CRL) can include indications of revocation reason, provide for temporary suspension of a certificate, and include CRL-issue sequence numbers to allow certificate users to detect missing CRLs in a sequence from one CRL issuer. Other changes have been made to make the management of CRLs more effective.

6.2 ISO/IEC JTC1/SC27 IT Security techniques

SC27 is the main committee for security related standards development. Its work can be categorised as:

- mechanisms and techniques
- management support documents and security guidelines.

6.2.1 Mechanisms and techniques

In the first category are the following standards:

ISO/IEC 9796:1991 Digital signature scheme giving message recovery

ISO/IEC 9798 Entity authentication

ISO/IEC 11770 Key management

ISO/IEC 13888 Non-repudiation

ISO/IEC 14888 Digital signatures with appendix

SC27 does not currently standardise algorithms, although this may change soon if recommendations to work on algorithms are agreed. The standards therefore have a certain abstraction.

6.2.1.1 ISO/IEC 9796:1991 Digital signature scheme giving message recovery

ISO 9796 defines a scheme for verifying the originator and integrity of a block of data. The standard specifies a digital signature scheme giving message recovery for messages of limited length using a public key system (PKS). When the verification process reveals the message, the scheme is named a "signature scheme giving message recovery".

It is primarily designed for the protection of small quantities of data such as cryptographic keys and the results of hashing longer messages.

The standard does not mandate the use of a particular PKS or the size of the keys to be used. It is therefore necessary for users to agree algorithms and key sizes.

Part 1 of the standard (on mechanisms using redundancy) is an International Standard. Part 2: (Mechanisms using a hash-function) is a draft International Standard (DIS) Part 3: (Mechanisms using a check function) and Part 4 (Discrete logarithm based mechanisms) are in working drafts (WD).

6.2.1.2 ISO/IEC 9798 Entity authentication

The purpose of entity authentication is to corroborate that an entity is what it claims to be.

The standard is in 5 parts: parts 1 (general model), 2 (using symmetric encipherment algorithms), 3 (using a public key algorithm), and 4 (using a cryptographic check function) are International Standards; part 5 (using zero knowledge techniques) is in committee draft. The second edition of part 3 is also in committee draft.

Part 1 describes the general model for the entity authentication mechanisms of part 2 (using symmetric encipherment algorithms), part 3 (using a public key algorithm), part 4 (using a cryptographic check function) and part 5 (using asymmetric zero knowledge techniques).

Part 2 specifies entity authentication mechanisms using symmetric encipherment algorithms. Part 4 specifies mechanisms using cryptographic check functions. Using either type of mechanism, the entity to be authenticated corroborates its identity by demonstrating its knowledge of a secret authentication key, which is used to encipher specific data. The enciphered data can be deciphered and its contents validated by anyone sharing the entity's secret authentication key. The claimant and verifier need to

share a common secret authentication key, the establishment of which may involve a trusted third party. Some of the mechanisms can be used to establish mutual authentication, where both entities are authenticated; some can be used to authenticate one of the entities, unilateral authentication.

Part 3 of ISO/IEC 9798 specifies entity authentication mechanisms using a public key algorithm and a digital signature for the verification of the identity of an entity. The standard does not mandate a particular algorithm; any algorithm which satisfies the requirements of the specified authentication mechanism may be used.

Entity authentication mechanisms based on public key algorithms work by the entity showing that it knows its private key used in digitally signing specific data. The verifier uses the entity's public key to verify the signature. The validity and authenticity of the public key are therefore most important; how such a key is securely obtained is outside the scope of this standard. The public key could be obtained using a certificate distributed by a trusted third party or by some other means mutually agreed by the entity and the verifier. Part 3 describes mechanisms for both unilateral and mutual authentication.

The mechanisms specified in the standard can be used in key distribution.

Part 5 of the standard is being developed. This specifies two classes of entity authentication mechanisms using zero knowledge techniques. The mechanisms provide unilateral authentication. The two classes of mechanisms are:

- identity based, where a trusted accreditation authority provides secret accreditation information which is a function of the claimant's identity
- certificate based, where a claimant has a public, private key pair and the verifier a trusted copy of the claimant's public key (how this is achieved is beyond the scope of the standard, but it may be by using a certificate signed by a Trusted Third Party).

6.2.1.3 ISO/IEC 11770 Key management

The purpose of key management is to provide procedures for handling cryptographic keys used in symmetric or asymmetric cryptographic algorithms. ISO/IEC 11770 has three parts; parts 1 and 2 are International Standards, part 3 is a draft International Standard (DIS).

The first part (**Key Management Framework- ISO/IEC 11770-1**) identifies the objectives of key management and describes general principles and concepts which are common to different ways of managing keys. This part also specifies requirements and a framework for the management of the key life cycle. It also describes a key life cycle model which identifies different states and transitions and implicitly defines key management services, which might be part of a key management system or be provided by another service provider as a trusted third party.

The other parts of the standard are:

Part 2: Mechanisms using symmetric techniques ISO/IEC 11770-2

This standard is concerned with how secret keys can be established. There are three environments for the establishment of keys:

- Point to Point, when two entities already share a secret key that can be used to establish further keys;

- Key Distribution Centre (KDC) when the two entities do not share a secret key and the KDC generates and distributes the key and
- Key Translation Centre (KTC) which converts and distributes keys for entities who do not already share a secret key

A number of key establishment mechanisms are described for each environment.

Part 3: Mechanisms using asymmetric techniques ISO/IEC DIS 11770-3

ISO/IEC 11770 Part 3 addresses the use of asymmetric techniques to:

- establish a shared secret key between two entities A and B by key agreement — the secret key is the result of a data exchange between the two entities A and B. Neither of them can predetermine the value of the shared key.
- establish a shared secret key between two entities A and B by key transport — the secret key is chosen by one entity A and is transferred to another entity B, suitably protected by asymmetric techniques.
- make an entity's public key available to other entities by key transport in an authenticated way (confidentiality is not required).

6.2.1.4 ISO/IEC 13888 Non-repudiation

This is a three part standard, which is being developed:

Part 1: General model (DIS)

Part 2: Using symmetric techniques (Committee Draft (CD))

Part 3: Using asymmetric techniques (DIS).

The purpose of a non-repudiation service is to collect, maintain, make available and validate irrefutable evidence. Part 1 describes a model for non-repudiation mechanisms providing evidence generated by non-repudiation certificates based on symmetric or asymmetric cryptographic techniques. Non-repudiation certificates establish accountability of information about a particular event or action to its originating entity. Non-repudiation mechanisms are specified to establish the following:

- non-repudiation of origin
- non-repudiation of delivery
- non-repudiation of submission
- non-repudiation of transport.

A clearly defined security policy for a particular application and its legal environment is a pre-requisite for a non-repudiation service. The security policy definition is outside the scope of this standard.

The mechanisms described in Part 1 consist of non-repudiation certificates, non-repudiation tokens, and protocols. Non-repudiation certificates require a trusted third party as an evidence generating authority when symmetric cryptographic algorithms are used. When asymmetric cryptographic algorithms are used, digital signatures of the data communicated are assured by public key certificates issued by a certification authority. Non-repudiation tokens consist of one or more non-repudiation certificates and, optionally, additional data. Non-repudiation tokens may be stored as evidence that may be used later on by disputing parties or by an adjudicator to arbitrate disputes.

Non-repudiation protocols specify the exchange of non-repudiation tokens specific for each non-repudiation service.

Part 2 (Using symmetric techniques) relies on the existence of a mutually trusted third party. The standard describes two mechanisms, one of which requires that the trusted third party is on-line for the generation and verification of evidence. The other mechanism has distribution of keys before the event for which evidence is required and so the trusted third party can be off-line.

Part 3 (Mechanisms using asymmetric techniques) describes non-repudiation mechanisms using digital signatures. A trusted third party is required to support some of the mechanisms described to perform evidence generation, evidence transmission, evidence recording or evidence verification. Non-repudiation of origin and non-repudiation of delivery can be supported without the direct involvement of a trusted third party. They can also be provided with the use of a TTP as must non-repudiation of submission and non-repudiation of transport. This standard also describes mechanisms for supporting services such as obtaining public-key certificates and revocation information, as well as time stamping and evidence recording.

6.2.1.5 ISO/IEC 14888 Digital signatures with appendix

The purpose of this standard, which is at the Committee Draft phase, is to specify digital signature mechanisms with appendix for messages of arbitrary length. When the verification process needs the message as part of the input, the scheme is named "signature scheme with appendix". The use of a hash-function is involved in the calculation of the appendix.

Part 1 of the standard, which is being developed, covers general principles and requirements for digital signature with appendix. Applications like entity authentication, key management and non-repudiation are not covered in this standard.

Part 2 of the standard defines identity-based mechanisms and specifies the fundamental structure, the mathematical functions and possible data objects which constitute the signature and verification processes of such mechanisms. This signature mechanism requires the services of a trusted authority who derives a signer's signature key from the signer's identity.

Part 3 of the standard defines certificate-based mechanisms, where the public verification key of a digital signature is obtained from some source such as a certificate.

6.2.2 Management support documents and security guidelines

SC27 is responsible for the following management support documents and security guidelines:

ISO/IEC 13335 Guidelines for the management of IT Security

ISO/IEC 14516 Guidelines for the use and management of Trusted Third Parties

ISO/IEC 15408 Evaluation criteria for IT Security.

6.2.2.1 ISO/IEC 13335 Guidelines for the management of IT Security

This Technical Report contains five parts, in various stages of development:

Part 1: Concepts and models for IT Security (complete, Technical Report)

Part 2: Managing and planning IT Security (draft Technical Report)

Part 3: Techniques for the management of IT Security (pre-draft Technical Report — PDTR)

Part 4: Baseline approach (working draft)

Part 5: Application of IT security services and mechanisms (working draft).

Part 1 of the Technical Report contains an overview of the basic concepts and models that are discussed in detail in the remaining two parts of the Technical Report.

Part 2 of the Technical Report presents the different activities related to the management of the planning of IT Security, as well as the associated roles and responsibilities within an organisation.

The main IT Security management activities include:

- determining IT Security objectives, strategies and policies
- identifying and analysing security threats to IT assets
- determining organisational IT Security requirements
- managing IT Security risks
- planning the implementation of adequate IT Security safeguards
- developing a security awareness programme
- planning follow-up programmes for monitoring, reviewing, and maintenance of security services
- developing plans for incident handling.

The report also focuses on management implications arising from the security topics addressed.

Part 3 is intended to identify the minimum requirements to be addressed in managing IT security. A recommended approach to strategic risk management is given. Risk management techniques are explained in detail as well as the development and implementation of an IT security plan.

Part 4 provides guidance on the selection of safeguards. It describes how safeguards can be selected, how appropriate protection can be achieved, and how organisation-wide baseline security can be implemented to meet the organisation's requirements. In order to provide help for the safeguard selection, manuals containing baseline safeguards are briefly described in an annex.

Part 5 provides guidance in managing and maintaining the security of sites to be connected to any external networks, particular the Internet. The guidance includes the selection and use of safeguards to support the management and maintenance of the site.

6.2.2.2 ISO/IEC 14516 Guidelines for the use and management of Trusted Third Parties

This Technical Report, which is being developed, consists of two parts, Part 1, General Overview (working draft, WD) and Part 2, Technical aspects (pre-draft Technical Report, PDTR). The target audience for the report is business users, system managers, developers and operators of Trusted Third Parties. The report will contain guidance on:

- the roles, positions and relationships of Trusted Third Parties and other related entities (e.g. network service providers, end users, etc.)
- the generic security requirements of Trusted Third Parties
- the establishment of a security policy
- the provision of security solutions and mechanisms
- the operational use and management of TTP service security
- the responsibilities of TTPs
- the services which TTPs can provide
- interworking of TTPs.

Part 1 of the report describes basic TTP services, provides guidance for designing and implementing a TTP, managing and operating a TTP and ensuring the interworking of TTPs. The basic services are: generation of cryptographic material, key escrow, key distribution, key revocation, certification, directory, authentication. Under the heading of Management and Operation are listed the subjects: security policy, procedures, liability, legal aspects, accreditation, accountability, audit, availability, quality of service and confidentiality. Part 2 of the report describes further TTP services under the groupings:

- technique independent supplementary services, such as directory or public notary services
- symmetric supplementary services, such as non-repudiation, key distribution or key translation
- asymmetric supplementary services, examples are certified key assignment with or without key generation, and non-repudiation using asymmetric techniques.

6.2.2.3 ISO/IEC 15408 Evaluation criteria for IT Security

This is a three part standard, all of whose parts are at the Committee Draft phase:

- Part 1: Introduction and general model
- Part 2: Security functional requirements
- Part 3: Security assurance requirements.

The content for this standard is being produced by the Common Criteria Implementation Board, with the close liaison of the working group in SC27; this activity of the CCIB is the result of harmonisation of the European developed IT Security Evaluation Criteria (ITSEC), the Canadian CTCPEC, and the US produced Federal Criteria. The main objective of the Common Criteria is to provide a set of security evaluation criteria that can be used for all IT security products.

Part 1 introduces the criteria and defines general concepts and principles of IT security evaluation, presenting a general model of evaluation. Constructs are presented in this part for expressing security functional and assurance requirements and specifications for IT products and systems. This part defines two forms for expressing IT security functional and assurance requirements:

- the protection profile (PP) which allows creation of generalised reusable sets of security requirements.

- the security target (ST) which expresses the security requirements and specifies the security functions for a particular product or system to be evaluated, called the target of evaluation (TOE).

The PP can be used by prospective consumers for specification and identification of products with IT security features which will meet their needs. The ST is used by evaluators as the basis for evaluations conducted in accordance with this standard.

Part 2 establishes a set of functional components as a standard way of expressing the security functional requirements for products and systems. These components are provided for use in forming the security functional requirements in Protection Profiles and Security Targets.

Part 3 defines seven evaluation assurance levels labelled EAL1 to EAL7. EAL1 represents an entry point below which no useful confidence can be held in a TOE, and EAL7 represents the highest level of confidence. The EALs are used for defining the assurance requirements in a generic Protection Profile (PP) or a TOE specific Security Target (ST).

It is planned that the criteria will be full International Standards in 1999.

6.3 ISO TC68 Banking, securities and other financial services

This committee has begun work on the subject of Trusted Third Parties and has looked at the work being done in JTC1 SC27 and ETSI Security TC. Although specific to the finance and banking sector, this work is of importance to the development of generic standards for trusted services, largely because of the experience and trusted status of the sector.

6.3.1 Guidelines for Trusted Third Party services

The committee is publishing the document, "Banking and related financial services, Information Security Guidelines" (ISO TR-13569). This document focuses on the requirement within the financial services industry for TTP technology, which offers a vehicle by which an institution can deliver assurances between its subdivisions, between itself and its customers, and between itself and its correspondent institutions. An institution may choose to set up an internal TTP function or use an external provider of TTP services.

The guidelines, as well as referring to the advice which will be provided in ETSI and JTC1 documents, recommend financial institutions who intend to use TTP services to consider the following aspects of trusted services, which are particularly important for the banking community:

- assurance
- services of a TTP
- network of TTPs
- legal issues.

6.3.1.1 Assurance

A TTP function, whether internally or externally provided can only add value when the users of the services are assured of the quality of the TTP function. Before contracting with a provider or starting operation of an internal system, the institution must satisfy itself that the following issues are addressed:

- Trust. Is the TTP organised, controlled and regulated in such a way that its operation can be relied upon, checked and verified?
- Accreditation. Is the TTP accredited by recognised national, regional, or international groups?
- Compliance. Is the TTP operating in compliance with accepted industry standards and all relevant regulation?
- Contract. Is there a legally binding contract in place covering the provision of service and addressing all the relevant issues? Are there contracts with co-operating TTPs which also address these concerns?
- Liability. Is there a clear understanding as to issues of liability? Under what circumstances is the TTP liable for damages? Does the TTP have sufficient resources or insurance to meet its potential liabilities?
- Policy Statement. Does the TTP have a security policy covering technical, administrative, and organisational requirements?

6.3.1.2 Services of a TTP

The services which a TTP can provide include:

- Key Management for symmetric cryptosystems
- Key Management for asymmetric cryptosystems
- Key Recovery
- Authentication and Identification
- Access Control
- Non-repudiation

The guidelines being published by TC68 discuss these services and their usefulness for financial service institutions throughout its text, except for Key Recovery, which is separately discussed. The guidelines describe Key Recovery as the ability of the TTP to recover, either mathematically, through secure storage, or other procedures, the proper cryptographic key used for encryption of information using the institution's information processing resources. This key recovery function would assure an institution that it can always have access to information within its information processing resources; for example, such recovery service may be essential in disaster recovery. It may also satisfy law enforcement regulations in some jurisdictions enabling an institution to produce such a key or encrypted information in answer to a lawful court order.

6.3.1.3 Network of TTPs

The guidelines, in recognising that the TTP concept is relatively new and a network of co-operating TTPs must be developed before the full potential of TTPs will be realised, warn financial institutions that they must be particularly vigilant in insisting that their TTP function maintain its assurances. Competition between suppliers may reduce costs at the risk of offering reduced levels of service or assurance. It is of paramount importance to preserve confidence in the institution and the financial service sector.

6.3.1.4 Legal Issues

The document highlights a number of legal issues which are of special concern to financial institutions.

- **Archival and retrieval**
Financial institutions generally have higher level requirements for record retrieval. The contract with a TTP should be specific about issues relating to maintenance of keys used for encryption, authentication, and digital signatures, as these may need to be reproduced many years after the transactions for which they were used.
- **Liability**
Liability for the misfeasance, malfeasance, or non-feasance of the TTP to include direct and consequential damages must also be fully understood and agreed upon. The TTP must have adequate financial reserves or insurance to meet any liability.
- **Privacy**
Financial institutions in many jurisdictions are obliged to protect the privacy rights of individuals, especially safeguarding personal data. These obligations are sometimes at odds with the requirement of law enforcement to access information. The contract with an external TTP, or the operating procedures of an internal TTP must address both these concerns.

6.3.2 Certificate profile

TC 68 is developing a document entitled, "Banking - Certificate Management", which combines two ANSI documents, X9.55 and X9.57, and provides additional information useful for the financial community. A profile of the X.509 certificate has been prepared as an appendix to this document, and will appear in the next revision. It is intended that the document will soon be assigned an ISO number.

6.4 EDIFACT — Syntax Development Group of the United Nations Economic Commission for Europe (UN/ECE)

This group is responsible for the production of the International Standard 9735. ISO 9735 currently consists of ten parts, under the general title Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules:

The following parts are particularly concerned with security of EDI:

- ISO DIS 9735-5 - Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)
- ISO DIS 9735-6 - Secure authentication and acknowledgement message (message type - AUTACK)
- ISO "9735-7" - Security rules for batch EDI (confidentiality)
- ISO DIS 9735-8 - Associated data in EDI (confidentiality)
- ISO "9735-9" - Security key and certificate management message (message type - KEYMAN)
- ISO "9735-10" - Security rules for interactive EDI

Part 5 - Security rules for batch EDI (authenticity, integrity and non-repudiation of origin), Part 6 - Secure authentication and acknowledgement message (message type - AUTACK) and Part 8 Associated data in EDI (confidentiality), currently draft International Standards, have been submitted to ISO for fast-tracking to the status of an International Standard.

Part 9 - Security key and certificate management message (message type - KEYMAN) is about to be submitted to ISO for fast-tracking.

It is planned to submit Part 7 - (Security rules for batch EDI (confidentiality)) and Part 10 - (Security rules for interactive EDI) to ISO for fast-tracking before the end of September 1997.

Part 9, which deals with key and certificate management describes a model for key management, the basic assumption of which is that public key techniques for security services are used. In addition, an architecture according to the X.509 standard is assumed.

Within this part a number of TTP services relevant to EDI are listed:

- Independent time-stamping
- Attribute certificates
- Notary functions
- Document repository
- Non-repudiation of submission/delivery
- Translation/validation of certificates.

Part 5, which deals with authenticity, integrity and non-repudiation of origin, describes how trusted third party services can be used to support those services.

6.5 CEN

6.5.1 TC224 — Machine readable cards, related device interfaces and operations

TC224 is working with ISO TC68 on a study of the standards required to support card related, secure, commercial and financial transactions and related payments on open networks regardless of amount.

The study will cover the use of all major currently available card technologies (e.g. magnetic stripe cards, integrated circuit cards) and applications (e.g. debit-credit, electronic purse).

The study will cover application protocols, interface devices and appropriate software requirements to ensure implementation of the following functions and services in relation to customers, vendors and financial institutions:

- recognition and authentication of all parties (e.g. customer, vendor, etc.);
- ordering (including but not limited to order form, placement of order by the customer and acceptance of the order by the vendor);
- agreement on the means of payment and related authorisation to pay by the customer;

- payment authorisation (requested by the vendor to the financial institution);
- payment request and impact on settlement.

The study will also include the definition of a security architecture to provide appropriate integrity, confidentiality and, under certain circumstances, anonymity.

The results of the study will be submitted to the International and European standards bodies, in order to allow ISO, CEN and other bodies to undertake the required standardisation work.

6.5.2 TC251 — Medical Informatics

The standard Medical Informatics - Algorithm for Digital Signature Services was approved as ENV 12388 in July 1996. The standard defines the RSA algorithm for use within the European health care sector.

6.6 European Telecommunications Standards Institute — ETSI

The Security Technical Committee of ETSI is preparing a standard for Trusted Third Parties (TTP). The work is being done in a number of phases, starting with the production of a requirements report. The second phase is the production of the first standard. Current plans are to produce a standard for TTP services covering key management and key escrow/recovery.

6.6.1 Requirements

The Requirements Report identified requirements for a TTP Scheme under three headings:

- general requirements, including the services to be provided
- security requirements to be met by a TTP scheme
- functional and interface requirements to be standardised.

These requirements are now to be submitted to the ETSI membership for their endorsement, which should include confirmation that the stated requirements fully correspond to the market needs.

6.6.2 Proposed first standard

It is planned that the first standard will define TTP services for key management, and key escrow/recovery.

6.7 Internet Engineering Task Force (IETF)

Within the IETF, a number of working groups have published and are preparing specifications of major relevance to different aspects of implementing Trusted Services. The following sections consider those specifications. The specifications are important both as users of trusted services and as enabling components.

- Internet Public Key Infrastructure
- Generic Security Services API

- Lightweight Directory Access Protocol
- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- PGP/MIME (MIME Security with Pretty Good Privacy)
- Secure Sockets Layer
- Simple Public Key Infrastructure
- Domain Name System Security Extensions
- Security Architecture for the Internet Protocol

6.7.1 Internet Public Key Infrastructure

A four part standard is planned for development of a Public Key Infrastructure for the Internet. The standard has been published in draft form:

- Part 1: X.509 Certificate and Certificate Revocation List Profile
- Part 2: Operational Protocols
- Part 3: Certificate Management Protocols
- Part 4: Certificate Policy and Certification Practices Framework

6.7.1.1 Part 1: X.509 Certificate and Certificate Revocation List Profile

This specification profiles the format and semantics of certificates and certificate revocation lists for the Internet PKI. Procedures are described for processing of certification paths in the Internet environment. The specification presents profiles of the X.509 version 3 certificate and version 2 certificate revocation lists, work on which has been completed by ISO. This specification also includes path validation procedures.

Finally, the specification describes procedures for identification and encoding of public key materials and digital signatures. Implementations are not required to use any particular cryptographic algorithms. However, conforming implementations which use the identified algorithms are required to identify and encode the public key materials and digital signatures as described.

The goal of the specification is to develop a profile and associated management structure to facilitate the adoption and use of X.509 certificates within Internet applications for those communities wishing to make use of X.509 technology. Such applications may include WWW, electronic mail, user authentication, and IPSEC, as well as others. In order to relieve some of the obstacles to using X.509 certificates, this document defines a profile to promote the development of certificate management systems; development of application tools; and interoperability determined by policy, as opposed to syntax.

Some communities will need to supplement, or possibly replace, this profile in order to meet the requirements of specialised application domains or environments with additional authorisation, assurance, or operational requirements. However, for basic applications, common representations of frequently used attributes are defined so that application developers can obtain necessary information without regard to the issuer of a particular certificate or certificate revocation list (CRL).

6.7.1.1.1 Architectural model of the Internet PKI

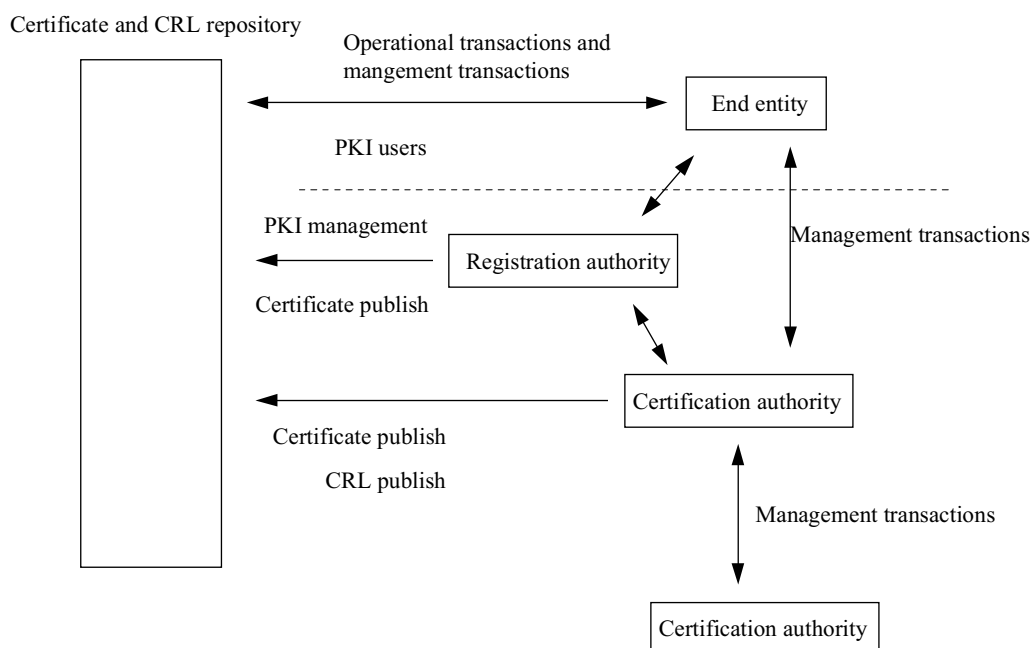


Figure 1 Internet PKI Model

The above figure shows the Internet PKI model. The components in this model are:

- end entity: user of PKI certificates and/or end user system that the PKI certifies;
- certification authority;
- registration authority, i.e., an optional system to which a certification authority delegates certain management functions;
- repository: a system or collection of distributed systems that store certificates and CRLs and serve as a means of distributing these certificates and CRLs to end entities.

6.7.1.1.2 The development of the Internet PKI

The Internet Privacy Enhanced Mail (PEM) proposals, published in 1993, include specifications for a public key infrastructure based on X.509 v1 certificates (RFC 1422). The experience gained in attempts to deploy RFC 1422 made it clear that the v1 and v2 certificate formats were deficient in several respects. Most importantly, more fields were needed to carry information which PEM design and implementation experience had shown were necessary. In response to these new requirements, ISO/IEC JTC/1 developed the X.509 version 3 (v3) certificate format. The v3 format extends the v2 format by adding provision for additional extension fields. Particular extension field types may be specified in standards or may be defined and registered by any organisation or community.

ISO/IEC JTC/1 has also developed a set of standard extensions for use in the v3 extensions field. These extensions can convey such data as additional subject identification information, key attribute information, policy information, and certification path constraints.

Because the extensions are very broad in their applicability, in order to develop interoperable implementations of X.509 v3 systems for Internet use, it is necessary to specify a profile for use of the X.509 v3 extensions tailored for the Internet. It is the goal of this specification (Part 1) to define a profile for Internet WWW, electronic mail, and IPSEC applications. Other environments with additional requirements may build on this profile or replace it.

6.7.1.1.3 Trust model

A Trust model is the organisation of certification authorities which provides a user of a security service with confidence in using that service. A user of a security service requiring knowledge of a public key generally needs to obtain and validate a certificate containing the required public key. If the public-key user does not already hold an assured copy of the public key of the CA that signed the certificate, then it might need an additional certificate to obtain that public key. It might be necessary to follow a chain of multiple certificates, comprising a certificate of the public key owner (the end entity) signed by one certification authority, and zero or more additional certificates of certification authorities signed by other certification authorities. Such chains, called certification paths, are required because a public key user normally has been initialised with only one assured certification authority public key.

The PEM (RFC 1422) specification defined a rigid hierarchical structure of certification authorities. This was a three level structure containing:

- Internet Policy Registration Authority (IPRA) at the top of the hierarchy
- Policy Certification Authorities (PCAs): distinct PCAs aim to satisfy different user needs and follow different policies.
- Certification Authorities (CAs): which certify user entities

PEM also has a name subordination rule which requires that a certification authority can only issue certificates for entities whose names are subordinate (in the X.500 naming tree) to the name of the certification authority itself.

The PEM certification authority hierarchical model has been found to be too restrictive and constraining.

These PKIX specifications propose a more flexible trust model, which is possible because of the extensions provided in X.509 v3. The changes in X.509 v3 which provide this flexibility are the inclusion of certificate extensions for certificate policies and alternative names; and the inclusion of constraint specifications in the certificates of CAs which provides for effective cross-certification of one CA by another CA.

6.7.1.2 Part 2 Operational protocols

The first draft of the second part of the PKIX specification, entitled "Operational protocols" defines two protocol profiles for retrieving certificates and certificate revocation lists from an information repository. The document also describes a protocol for ascertaining the status of a certificate from a CA. The protocols profiled for retrieval are:

- the Lightweight Directory Access Protocol (LDAP) and
- the File Transfer Protocol (FTP).

The protocol specified for communicating directly with a CA about the status of a certificate is called the On-line Certificate Status Protocol (OCSP). OCSP is, in this draft, specified to use HTTP as its access method.

6.7.1.3 Part 3: Certificate Management Protocols

Management protocols are specified to support on-line interactions between Public Key Infrastructure (PKI) components, as shown in figure 1.

The management protocols include the following functions:

- between the end entity and the certification authority
 - initial registration and certification
 - key pair recovery
 - key pair update
 - certificate update
 - revocation request.
- between two certification authorities:
 - cross-certification
 - cross-certificate update.
- between the end user and the repository
 - certificate publication
- between the certification authority and the repository
 - publication of certificates and certificate revocation lists

Development of this specification is in progress.

The requirements to be satisfied by the protocols defined in this specification include:

- PKI management must conform to ISO 9594-8 and the associated draft amendment (DAM) (X.509 v3)
- the use of confidentiality in PKI management protocols must be kept to a minimum in order to ease regulatory problems
- PKI management protocols must allow the use of different industry-standard cryptographic algorithms, (specifically including, RSA, DSA, MD5, SHA-1) - this means that any given CA, RA, or end entity may, in principle, use whichever algorithms suit it for its own key pair(s)
- PKI management protocols must not preclude the generation of key pairs by the end entity concerned, an RA or a CA
- PKI management protocols must support the publication of certificates by the end entity concerned, an RA or a CA
- PKI management protocols must support the production of CRLs by allowing certified end entities to make requests for the revocation of certificates
- PKI management protocols must be usable over a variety of "transport" mechanisms, specifically including, mail, HTTP, TCP/IP and ftp.

6.7.1.4 Part 4 Certificate Policy and Certification Practices Framework

The purpose of this document "Certificate Policy and Certification Practices Framework" is to present a framework that identifies the elements that may need to be considered in formulating a certificate policy or a Certification Practice Statement (CPS). The purpose is to assist the writers of certificate policies or CPSs with their task, but not to define particular certificate policies or CPSs. The eventual RFC will be published as an Informational RFC.

It is intended that the framework will contain nine top-level elements:

- community definition and applicability
- identification and authentication policy for subjects, Registration Authorities and Certification Authorities
- key management policy
- non-technical security policy
- technical security policy
- operational requirements
- legal & business provisions
- certificate and CRL profiles and
- policy administration.

The degree to which a certificate user can trust the binding in a certificate between a name and a public key depends on such factors as the Certification Authority (CA) policy and procedures for authentication of end entities, the CA operating policy, procedures and security controls, and the policy and procedures of the end entity for handling private keys.

The liability assumed by certificate issuers and end entities also plays a role in the degree of trust.

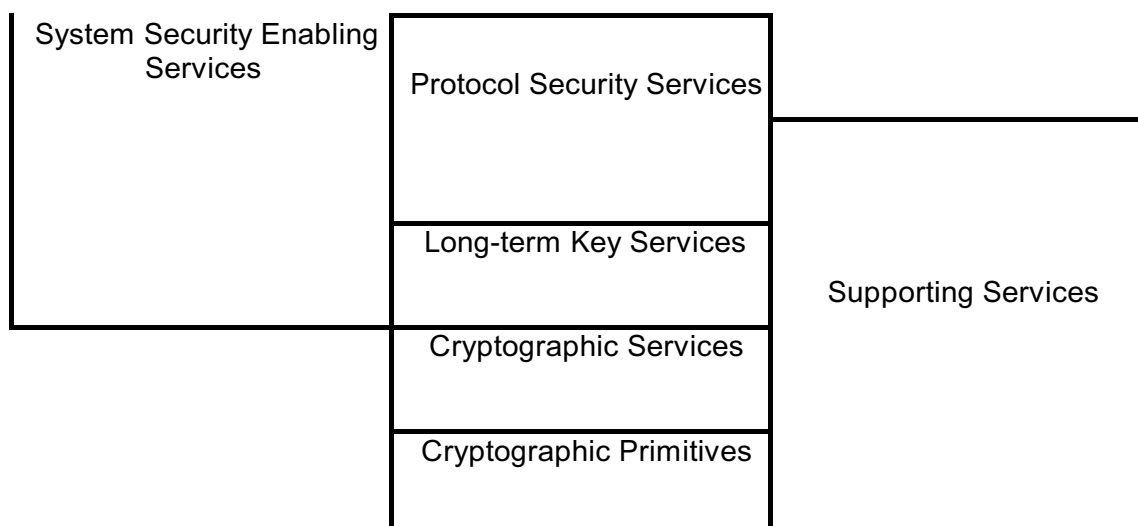
A certificate policy allows the users of a certificate to decide how much trust to place in the certificate, i.e., in the binding of the entity's identity and the entity's public key. A detailed description of how certificate policies are implemented by a particular CA is called a Certification Practice Statement (CPS). According to the American Bar Association (ABA), "a CPS is a statement of the practices which a certification authority employs in issuing certificates." When negotiating a cross certification, CAs examine and compare each other's CPS.

6.7.1.5 Architecture

The Open Group has produced an Internet Draft — Architecture for Public-Key Infrastructure. This document describes Requirements and an Architecture for Public-Key Infrastructure components, identifies which elements of the architecture should (in the opinion of the authors) be standardised, and identifies candidate interface and protocol specifications which might serve as base documents for standardisation.

The Architecture is described in the document as follows:

[Applications]		
	Secure Protocols	Security Policy Services



PKI Architecture

Where:

- System Security Enabling Services provide the functionality which allows a user's or other principal's identity to be established and associated with his actions in the system.
- Cryptographic Primitives and Services provide the cryptographic functions on which public-key security is based (including secret-key primitives such as DES).
- Long-term Key Services permit users and other principals to manage their own long-term keys and certificates and to retrieve and check the validity of other principals' certificates
- Protocol Security Services provide security functionality (data origin authentication, data integrity protection, data privacy protection, non-repudiation) suitable for use by implementors of security-aware applications such as secure protocols.
- Secure Protocols provide secure inter-application communications for security-unaware and "mildly" security-aware applications.
- Security Policy Services provide the policy-related information which must be carried in secure protocols to enable access control, and provide access-control checking facilities to security-aware applications which must enforce policy.
- Supporting Services provide functionality which is required for secure operation, but is not directly involved in security policy enforcement.

Elements of the architecture which are candidates for standardisation include:

- Cryptographic Service Interfaces
- Long-term Key Services - protocols for
 - user workstation or smartcard to certificate management component
 - local registration authority to CA agent
 - public key delivery and verification
 these are included in the Internet PKI proposal

- Long-term Key Services - interfaces for
 - virtual smartcard service
 - communication with hardware security tokens
 - public key delivery and verification interface
 - CA agent
 - local registration authority
 - publication authority (of certificates and CRLs)
- Protocol Security Services - interfaces
 - session oriented services, GSS-API is preferred
 - store and forward services, IDUP-GSS-API is preferred
 - non-repudiation services, IDUP-GSS-API is preferred.

6.7.2 Generic Security Services API

The Generic Security Service Application Program Interface (GSS-API) provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. This specification defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment, and is to be complemented by other, related specifications:

- documents defining specific parameter bindings for particular language environments
- documents defining token formats, protocols, and procedures to be implemented in order to realise GSS-API services above particular security mechanisms.

The document contains an example illustrating use of the GSS-API in conjunction with public-key mechanisms, consistent with the X.509 Directory Authentication Framework.

The specification entitled IDUP-GSS-API (draft-ietf-cat-idup-gss-07.txt) extends the GSS-API for applications requiring protection of a generic data unit (such as a file or message) in an "off-line" or store and forward environment, such as secure email. IDUP stands for Independent Data Unit Protection. The specification describes interfaces to services such as:

- data origin authentication with data integrity
- data confidentiality with data integrity
- non-repudiation services.

After being protected, the data unit can be transferred to the recipient(s) or stored in an archive, for later processing.

6.7.3 Lightweight Directory Access Protocol (LDAP)

LDAP, a simplification of the X.500 directory access protocol (DAP), defines a reasonably simple mechanism for clients to query and manage a hierarchically structured database of attribute/value pairs over the Internet. The LDAP

directory service model is derived from the X.500 model; use of LDAP does not require the existence of an X.500 directory. LDAP is a protocol for use between parties executing transactions on any hierarchical, attribute-based directory. The latest version of LDAP (version 3), which is currently a draft (draft-ietf-asid-ldapv3-protocol-03.txt), includes use of authentication mechanisms: password protection using a hash function, and certificate-based digitally signed token. Version 3 of LDAP can be carried over the Secure Socket Layer (SSL) protocol.

6.7.4 S/MIME (Secure/Multipurpose Internet Mail Extensions)

The specification for S/MIME (Secure/Multipurpose Internet Mail Extensions) (S/MIME Message Specification - draft-dusse-smime-msg-00.txt and S/MIME Certificate Handling - draft-dusse-smime-cert-00.txt) describes a protocol for adding cryptographic signature and encryption services to Internet MIME electronic mail messages:

- authentication, message integrity and non-repudiation of origin (using digital signatures) and
- privacy and data security (using encryption).

The Internet MIME standard (RFCs 2045-2049), provides a general structure for the content type of Internet mail messages and allows extensions for new content type applications. The S/MIME draft defines an application type which specifies that a MIME body part has been cryptographically enhanced according to PKCS #7. It also defines an application type which can be used to transfer a PKCS #10 certification request. The specification makes use of data structures, such as digital signature, specified in PKCS #9.

The latest draft requires use of RSA. SHA-1 should be used when sending mail. Mail receiving requires support for MD5 and SHA-1.

Open issues include:

- whether or not the PKCS-*nn* documents will be IETF RFCs or simply be referenced as external documents.
- references to the encryption and hash algorithms.
- use of the S/MIME trademark.

6.7.5 PGP/MIME (MIME Security with Pretty Good Privacy)

PGP/MIME (RFC2015) recently completed the final phase of the IETF's standards-track process. This document defines three new content types for implementing security and privacy with PGP:

- application/pgp-encrypted,
- application/pgp-signature and
- application/pgp-keys.

The specification is based on RFC1847 - "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", which defines security multipart formats for MIME. The security multiparts clearly separate the signed message body from the signature, and have a number of other desirable properties.

6.7.6 Secure Sockets Layer

The SSL Protocol (Version 3.0) described in the Internet draft draft-ietf-tls-ssl-version3-00.txt has as its goal to provide privacy and reliability between two communicating applications, in a client/server relationship. The protocol is composed of two layers. At the lowest level, above a reliable transport protocol such as TCP, is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can execute on top of the SSL Protocol transparently.

The SSL protocol provides connection security with three basic properties:

- the connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES), RC4)
- the peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS)
- the connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations.

SSL is widely used to provide secure communication over the World Wide Web.

6.7.7 Simple Public Key Infrastructure (SPKI)

Two developments which have been progressing separately are now merging. They are proposals for a Simple Distributed Security Infrastructure and a Simple Public Key Certificate. A proposal for a Simple Public Key Infrastructure is now being developed.

A Simple Distributed Security Infrastructure -- SDSI

This is a proposal for a new distributed security infrastructure. SDSI principals are public digital signature verification keys with individuals controlling the associated private keys. No global hierarchy is necessary, but there is support for common roots such as DNS, Verisign and others. Each principal is a "certification authority" and manages a local name space with which he can refer to other principals.

There are three types of certificate: identity certificate, name/value certificate, and membership certificate. Identity certificates have human-readable content and the process for creating them is manual.

A key can delegate the authority to sign certificates on behalf of the key. The delegation can be limited to certificates that match a template. Certificates can time out, and they can be reconfirmed by an on-line agent acting for the issuer. SDSI is optimised for an on-line Internet environment in which clients can interact with servers to learn what credentials are needed to satisfy a request, and can retrieve the needed credentials from other servers.

Simple Public Key Certificate

An SPKI certificate has been defined as an authorisation certificate. It grants a specific authority to a public key rather than binding an "identity" (such as a person's name) to that key. For example, one SPKI certificate might grant permission for a given public key to authenticate logins over TELNET as user CME on host CYBERCASH.COM for some period of time.

Requirements for a SPKI

A defining characteristic of an SPKI certificate is that it is a text based structure which does not use ASN.1 to define its data structures. The main purpose of an SPKI certificate is to authorise some action, give permission, grant a capability, etc. The first requirement for an SPKI certificate is then to bind a meaningful or useful attribute to a public key (and therefore to the keyholder of the corresponding private key). In many cases, the attribute would not involve any recognisable name.

The definition of attributes or authorisations in a certificate is up to the author of the application code which uses the certificate. The creation of new authorisations should not require interaction with any other person or organisation but rather be under the total control of the author of the code using the certificate.

The main driving forces behind the proposal are the desire to keep down overheads arising from use of an ASN.1 based certificate and an infrastructure supporting a global directory, the search for an efficient implementation, and freedom and flexibility to develop structures for a growing number of applications.

6.7.8 Domain Name System Security Extensions

The Domain Name System (DNS) is a critical operational part of the Internet infrastructure but it has no strong security mechanisms to assure data integrity or authentication. This document describes extensions to the DNS which provide these services to security aware resolvers or applications through the use of cryptographic digital signatures, which are included in DNS files. The extensions also provide for the storage of authenticated public keys in the DNS. This storage of keys can support general public key distribution service as well as DNS security. The stored keys enable security aware name resolvers to learn the authenticating key of name zones in addition to those for which they are initially configured. Keys associated with DNS names can be retrieved to support other protocols. The document provides for a variety of key types and algorithms.

6.7.9 Security Architecture for the Internet Protocol

This document describes the security mechanisms for IP version 4 (IP v4) and IP version 6 (IP v6) and the services that they provide. It focuses on IP-layer security. This document also describes key management requirements for systems implementing the security mechanisms. The document is not an overall Security Architecture for the Internet.

The document describes two mechanisms: the "IP Authentication Header (AH)" and the "IP Encapsulating Security Payload (ESP)". There are a number of ways in which these IP security mechanisms might be used. The IP Authentication Header is designed to provide integrity and authentication without confidentiality to IP datagrams. The IP Encapsulating Security Payload (ESP) is designed to provide integrity, authentication, and confidentiality to IP

datagrams. The document develops the concept of a "Security Association" which is fundamental to both the IP Encapsulating Security Payload and the IP Authentication Header. The Security Association includes a number of parameters such as:

- authentication algorithm and algorithm mode being used with the IP Authentication Header
- key(s) used with the authentication algorithm in use with the Authentication Header
- encryption algorithm, algorithm mode, and transform being used with the IP Encapsulating Security Payload
- key(s) used with the encryption algorithm in use with the Encapsulating Security Payload
- lifetime of the key or time when key change should occur
- lifetime of this Security Association
- sensitivity level (for example, Secret or Unclassified) of the protected data.

Standard default algorithms (keyed MD5, DES CBC) are specified to ensure interoperability in the global Internet.

A key management scheme has still to be standardised. The latest proposal is in draft-ietf-ipsec-isakmp-oakley-03.txt (February 1997).

6.8 Object Management Group

The Object Management Group (OMG) has defined an architecture: the Object Management Architecture (OMA), which is supported by detailed interface specifications. The goal is to promote the development by industry of interoperable, reusable, portable software components with standard and open object-oriented interfaces.

The Object Management Architecture Guide (OMAG) provides the conceptual infrastructure for the component specifications. Among the specifications are the Common Object Request Broker Architecture (CORBA) and the CORBA services.

CORBA Security is specified in the CORBA services specification. It includes a reference model and architecture. Facilities and interfaces are specified for application developers, administrators and implementors of Object Request Brokers (ORBs). The CORBA security services include support for:

- authentication
- audit of security relevant events
- access control
- message protection, such as integrity and confidentiality
- non-repudiation, that is generation and verification of evidence of actions.

The CORBA specification describes how Object Request Brokers can interoperate securely. CORBA Security does not mandate particular security mechanisms; it can be implemented using existing suitable mechanisms.

6.9 Microsoft CryptoAPI

The Microsoft CryptoAPI is a generalised interface to lower level cryptographic service providers (CSPs). One of the goals of the architecture is to isolate within the CSPs the cryptographic processing. Applications using the API cannot directly access keying material, cannot specify the details of cryptographic operations and do not handle user authentication data. The CSP alone generates keying material, carries out cryptographic operations and authenticates the user. A number of different types of CSP are defined. A type is a class of CSP, defined by such attributes as the following:

- Key exchange algorithm
- Digital signature algorithm
- Key blob format
- Digital signature format
- Session key derivation scheme
- Key length

Within a system, one or more CSPs may be registered of a particular type, with one nominated as the default CSP for that type. A number of provider types have been defined with a specified minimum functionality; some CSPs may support extra features.

The CSP may provide its functionality by software alone or with hardware.

The API is algorithm independent, because the data types it defines are generalised, for example "key blob". The interpretation of "key blob" is for the CSP.

The Microsoft CryptoAPI is a relatively low level interface and requires a high degree of cryptographic awareness.

Functions to which the API provides an interface include:

- key generation
- storing and exchanging keys
- encrypting and decrypting data
- producing a message digest of data or a session key
- signing a message digest
- verifying a digital signature of a message digest.

6.10 The Open Group

The Cryptographic Working Group of The Open Group has created a set of APIs and mechanisms to provide security services (primarily cryptographic and key management) to applications. This API, published as a Preliminary Specification for comment, is called the Generic Cryptographic Services API (GCS-API). The GCS-API is presented in two major sections, a Basic section and an Advanced section.

The first part, the Basic section, presents a simple overview of the types of cryptographic functions, a simplified model of the GCS-API architecture, and

the minimum set of generic cryptographic functionality that can support the requirements of general applications wishing to use cryptographic services. It is expected that the majority of the cryptographic service needs of most application developers can be met by the Basic GCS-API functionality. It is designed for both cryptographically aware and unaware applications. A common set of functions is required to support all types of callers. These comprise the following:

- data encipherment and decipherment
- integrity checkvalue generation and verification
- production of irreversible hash of data
- generation of random numbers.

Key management applications require the following additional functions:

- generation, derivation and deletion of keys
- export and import of keys.

Non-functional objectives of the specification include:

- application independence
- independence of cryptographic algorithm and subsystem: that is, appropriate to both hardware and software implementations, and implementable on top of any cryptographic technology or cryptomodule
- no constraints on future extensibility.

The second part of the specification, the Advanced section, presents a more detailed description of the concepts, detailed data structures and additional sets of functions that would only be used by applications that are developed to manage cryptographic policy and provide long term management of keys and the cryptographic service itself. The scope of the current specification considers only services to support cryptographic aware callers, who are aware of whether data are being enciphered or a checkvalue generated; they may be unaware of the algorithm details or cryptographic policy. An additional function in the Advanced section is:

- inquiry of available keys and key related data.

Additional or enhanced key management support functions are:

- generation, derivation and deletion of keys, including public parameters
- storage and retrieval of keys and associated information
- archive and retrieval of keys and key related data.

A Cryptographic API at this level of cryptographic awareness is designed to be used as an underlying layer to higher level security APIs like GSS/IDUP, or for security applications that use cryptography in ways not accommodated by higher level APIs.

6.11 Public Key Cryptography Standards (PKCS)

The Public Key Cryptography Standards (PKCS) are not what is normally understood as standards. Standards are normally defined and agreed by a number of organisations working together; the PKCS are controlled by RSA DSI. However, this may change: a process to review and update some of the

standards has been initiated; and it has been proposed that the PKCS be published as IETF documents, although not under the control of the IETF. However, whatever happens in the future, the PKCS currently occupy an important place in the development of trusted services. The particular standards most relevant to trusted services are:

- PKCS #1: RSA Encryption Standard
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Syntax Standard

6.11.1 PKCS #1: RSA Encryption Standard

PKCS #1 describes how data is encrypted using the RSA public-key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes, as described in PKCS #7. For digital signatures, before signing the content is first reduced to a message digest with a message-digest algorithm (such as MD5); signing is done by encrypting with the signer's RSA private key the message digest. For digital envelopes, the content to be enveloped is first encrypted under a content-encryption key with a content-encryption algorithm (such as DES), and then the content-encryption key is encrypted with the RSA public key(s) of the recipient(s) of the content. PKCS #1 also describes a syntax for RSA public keys, which is identical to that in both X.509 and PEM, and for RSA private keys. The public-key syntax would be used in certificates.

6.11.2 PKCS #3: Diffie-Hellman Key Agreement Standard

PKCS #3 describes a method for implementing Diffie-Hellman key agreement, whereby two parties, without any prior arrangements, can establish a secret key which can then be used, for example, to encrypt further communications between the parties.

6.11.3 PKCS #6: Extended-Certificate Syntax Standard

PKCS #6 describes a syntax for extended certificates, consisting of an X.509 public-key certificate and a set of attributes, collectively signed by the issuer of the X.509 public-key certificate. Following the recent amendments to X.509, it has been suggested that there is no longer a need for this standard.

6.11.4 PKCS #7: Cryptographic Message Syntax Standard

PKCS #7 describes a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes. The syntax supports recursion, so that, for example, one envelope can be nested inside another, or one party can sign some previously enveloped digital data. Other attributes, such as signing time, can be authenticated along with the content of a message, and countersignatures can be associated with a signature.

PKCS #7 does not cover issues such as the public key infrastructure, what entities certificate issuers are authorised to certify, what distinguished names

are considered acceptable, and the policies certificate issuers must follow (such as signing with secure hardware, or requiring entities to present specific forms of identification). Dissemination of certificate-revocation lists is not covered.

6.11.5 PKCS #9: Selected Attribute Types

PKCS #9 specifies various data structures used in other PKCS documents. The data structures include:

- for use in extended certificates
 - electronic-mail address
 - unstructured name
 - unstructured address
- for use in digitally signed messages
 - content type
 - message digest
 - signing time
 - countersignature
- for use in certification requests
 - challenge password
 - extended certificate attributes.

6.11.6 PKCS #10: Certification Request Syntax Standard

PKCS #10 describes a syntax for certification requests, which are sent to a certification authority, which using the information received produces an X.509 public-key certificate. The certification request contains a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. The set of attributes can be information such as:

- the postal address to which the signed certificate should be returned if electronic mail is not available
- a "challenge password" by which the entity may later request certificate revocation;

6.12 Secure Electronic Transaction

Secure Electronic Transaction (SET) is a message specification for the secure transmission of sensitive personal and financial information over public networks, such as the Internet. SET is being developed by an industry consortium headed by MasterCard and Visa International. It uses RSA encryption and authentication technologies to support secure payment transactions. The focus of SET is payment by credit or debit cards. SET does not cover the parts of the commercial transaction such as browsing the product catalogue, formulating the order, including agreeing prices for merchandise and setting delivery parameters, tracking delivery, confirming receipt. The goal of SET is "to set an open standard for secure bankcard

transactions over the Internet, while preserving the cardholder-issuer and merchant-acquirer relationships". The stated requirements for SET are:

- confidentiality of card account number
- integrity of payment data
- authentication:
 - buyer knows seller is a secure merchant
 - seller knows buyer has a valid card account
- interoperability between different brands of card

6.12.1 The participants

Cardholder

The holder of a card issued by an Issuer.

Issuer

The financial institution which establishes an account for the Cardholder and issues the card. The Issuer guarantees payment for authorised transactions made using the card in accordance with the regulations of the card association and local legislation.

Merchant

The merchant sells in exchange for payment. A merchant who wishes to enable his customers to pay electronically and securely must first have a relationship with an Acquirer.

Acquirer

An Acquirer is the financial institution that establishes an account with a merchant and processes card authorisations and payments.

Payment gateway

A payment gateway is a device operated by an Acquirer or a designated third party which processes merchant payment messages (including cardholders' payment instructions).

Association

A grouping of financial institutions which promotes and protects the card brand, sets and enforces rules for the use and acceptance of the cards and provides networks connecting the financial institutions.

Third parties

Issuers and Acquirers sometimes assign the processing of card transactions to third parties. SET does not distinguish between the financial institution and the party processing the card transactions on its behalf.

6.12.2 The processes

SET uses two asymmetric key pairs: one set is used as a "key exchange" pair in the process of encrypting and decrypting messages; the second pair is used as a "signature pair" for the creation and verification of digital signatures.

For each key pair, a SET participant has a certificate issued by a Certification Authority.

Cardholder certificates are not required in the draft version of the specification.

6.12.2.1 Purchasing with SET

1. The cardholder has identified what he wants to purchase with which brand of card and communicated that to the merchant; he now requests the merchant to initiate payment with a particular brand of card.
2. The merchant returns a transaction identifier and the merchant and payment gateway certificates for the brand of card.
3. The cardholder software:
 - verifies the merchant and gateway certificates by traversing the trust hierarchy to the root key;
 - creates the Order Information (OI) (NOTE This is NOT the description of goods or payment terms — that has already been communicated to the merchant) and payment Instructions (PI), including the transaction identifier and the cardholder signature certificate;
 - computes the message digest of the OI and the PI; concatenates the two digests, computes the message digest of the result and encrypts it with its private signature key, this is called “a dual signature”;
 - generates a random symmetric encryption key, encrypts the PI with it, then encrypts the symmetric encryption key and the cardholder’s account number with the Payment Gateway’s key exchange public key;
 - sends to the merchant the dual signature, the message digests of the OI and PI, the OI and the encrypted PI.
4. The merchant software:
 - verifies the cardholder signature certificate by traversing the trust hierarchy to the root key;
 - uses the cardholder signature public key and the message digest of the PI (sent with the OI) to check the digital signature (“dual signature”) to ensure that the OI has not been tampered with and that the signature is valid;
 - generates and digitally signs a purchase response message including the merchant’s signature certificate to indicate receipt of the order; the response is then sent to the cardholder.
5. The merchant can carry out payment authorisation before or after responding to the cardholder. The merchant software:
 - generates and digitally signs an authorisation request including the amount of money; encrypts it with the Payment Gateway’s key exchange public key;
 - sends the request and the PI from the cardholder to the Payment Gateway.

6. The Payment Gateway:
 - decrypts both the authorisation request and the PI;
 - verifies the certificates of the merchant and cardholder;
 - checks the integrity of the PI, using the message digest of the OI, which is sent with the PI, and the “dual signature”;
 - checks that the authorisation request and PI correspond;
 - sends an authorisation request to the Issuer via a card association network;
 - when a response has been received from the Issuer, the Payment Gateway generates and digitally signs an authorisation response message which is encrypted and sent to the merchant.
7. The merchant generates and digitally signs a payment capture request which is encrypted and sent to the Payment Gateway.
8. The Payment Gateway decrypts and verifies the request and sends a clearing request to the Issuer via the card association network. The Payment Gateway generates and digitally signs a capture response message which is encrypted and sent to the merchant.

6.12.3 Issues, status and standards

A vulnerability in SET is that no measures are specified to protect the local PC environment where the cardholder is executing his part of the transaction. The PC is a vulnerable component in the payment system: it is standard, well known and could host a program which could extract data used in the payment process.

Procedures for the assurance of SET application software need to be established and put into operation. A SET Mark is proposed for assured applications.

Interoperability between the various systems used by the different card brands is to be tested in trials.

A number of live demonstrations of SET have been carried out, including in Denmark.

Cardholders may carry out transactions without certificates as a temporary measure.

One root or top-level Certification Authority for SET whose key is used in the validation of all certificates.

Cryptographic algorithms specified for use are: RSA, DES and SHA.

The certificate format used by SET is intended to be X.509 v3.

7. PROJECTS AND STANDARDS

This section reviews a number of projects, both longer and shorter in duration. The objective is to show which standards are being used and what new standards may be produced from these projects.

7.1 General Projects

7.1.1 ICE-TEL

7.1.1.1 Objectives

The objective of the ICE-TEL project, which is part of the EC Telematics programme, is to provide solutions for secure use of the Internet by members of the industrial and academic research communities. The solutions will be:

- secure components as a toolkit for integration with applications, where users need to be certified;
- a large scale public key certification infrastructure in a number of European countries.

7.1.1.2 Application areas

Three applications have been selected to demonstrate how the toolkits can be applied and how usable the resulting application is. The three selected applications are:

- secure communication between administrations and electronic request and delivery of documents in the region of Turin, co-ordinated within the EU-sponsored "Information Society Network",
- secure communication between national Computer Emergency Response Teams (CERTs) and other distributed network support groups
- provision of a security enabled electronic Directory service for a large British research agency.

The requirements to be addressed are:

- secure e-mail
- secure directory access
- secure file transfer.
- secure use of the World Wide Web.

These user needs translate into mechanisms:

- which prove the authenticity of communicating partners,
- which protect the integrity of communication data,
which protect communication data from unauthorised access.

Another essential security requirement for reliable business communication is non-repudiation of the origin and receipt of information; this can be derived from authentication and integrity mechanisms.

7.1.1.3 Certification Authority Infrastructure

To meet these security requirements using public-key encryption and signature schemes, a widely distributed infrastructure for public key certification needs to be established. It is the major task of the ICE-TEL project to establish a prototype network of certification authorities (CA).

These CAs are interrelated by mutual certificates of their public-keys. A client of any of these CAs will be able to communicate securely with any other client of any of these CAs, in that both communication partners can trust in the certified binding of their names and related public keys. There is no need to check public keys on another communication path (like the exchange of finger prints over the telephone or by exchange of business cards) before the secure communication can be made.

7.1.1.4 Mail and Directory user agents, key management tools

ICE-TEL will equip the users with mail and directory user agents with integrated security functions for digital signature and encryption of their data. ICE-TEL will also develop and distribute easy-to-use tools for users which allow them to communicate with their certification authorities. With these tools, users can easily maintain their encryption keys and related information, e.g., to retrieve certificates, certification paths, black lists, and all information needed to verify the public keys of other users. ICE-TEL will also equip certification authorities with management tools which allow them to maintain their information bases, to communicate securely with their clients and other certification authorities, and to exchange all information necessary for responsible key management.

7.1.1.5 Securing the World Wide Web

The World Wide Web (WWW) is the technology platform on which most network developments are being based whether on the Internet or intranets restricted to an organisation. A number of security features need to be provided in the WWW environment, including:

- restriction of access to specific WWW pages;
- authentication of users who wish to make commercial transactions or access data on the WWW;
- in a commercial transaction, binding commercial terms from one source (e.g. a supplier) to a user, having all parties authenticated and making the transaction confidential and non-repudiable;
- non-repudiable pages from the WWW available to clients.

7.1.1.6 Software verification

The above facilities need to be provided by programs which are fully available in source form, to ensure that the security implications, and the strength of the algorithms used, can be verified.

7.1.1.7 Directories

ICE-TEL aims to develop a product named a Guardian DSA which will enable organisations which are concerned with privacy to connect to public directory

infrastructures. The Guardian DSA will provide a secure gateway to such public structures while supporting secure (confidential and authenticated) communications for users inside the organisation.

7.1.1.8 The project and standardisation

The deliverable from the project entitled "Architecture and General Specifications of the Public Key Infrastructure" relates the project to a number of standardisation activities.

The report contains a chapter on models of trust, from a completely general model of trust to a simplified "web of hierarchies" model. This chapter is planned to be submitted to the IETF-PKIX working group as an informal Internet Draft. An annex to the report was submitted to the IETF-PKIX working group as an Internet draft "Internet Public Key Infrastructure, Part III: Certificate Management Protocols".

Other parts of the specification — the chapter on security policies that the ICE-TEL PKI will follow and the chapter on operational modes and guidelines of Certification Authorities (CAs) — could be developed and used to establish generally agreed standards for Security Policies for PKIs and Guidelines for the operation of Certification Authorities.

7.1.1.9 Standards and technology used

The ICE-TEL project uses the relevant Internet technology (World Wide Web, secure HTTP, Secure MIME (S/MIME), PKCS) and OSI technology (X.500), and makes use of established cryptography (RSA, DSS, DES, IDEA).

The security toolkits for integrating public key based security services into applications will support the use of specialised hardware, e.g. smartcards, to store and process securely the sensitive security information objects, such as private keys, trusted public keys of communication partners and top-level public verification keys.

The toolkits will provide standardised security APIs at various levels, as for example GSS API on the level of authentication and confidentiality functions and ISO SC17 standards on the level of smartcard access, in order to maximise portability of components and interworking capabilities between components.

Tools will be developed for secure document exchange on the basis of S/MIME and X.400 Security, integrated into various mail user agents.

7.2 Electronic Commerce

7.2.1 *Secure Electronic Marketplace for Europe (SEMPER)*

The goal of the SEMPER project, funded under the ACTS programme of the EC, is to provide open and comprehensive solutions for secure commerce over the Internet and other public communications networks. The project is for three years, September 1995 - August 1998 with a budget of 9 million ECU.

The project has published a document entitled "Basic Services, Architecture and Design" (September 1996).

7.2.1.1 The SEMPER model for electronic commerce — The players

The players in the SEMPER electronic commerce model consist of two categories:

- users of the marketplace, that is buyers and sellers
- third parties who enable the business between the users.

A real life entity may be both a user and a third party, for example a bank selling a home banking service.

The third parties who enable electronic commerce are:

Network

The providers of the information infrastructure.

Directory

A database mapping a name to other attributes such as address, certified public keys etc..

Registration Authority

A Registration Authority verifies a user's real identity.

Certification Authority

A Certification Authority certifies a public key of a user.

Arbiter

An Arbiter considers digital evidence and follows defined procedures to reach decisions on what the evidence leads him to conclude happened.

Broker

A Broker is similar to a directory but is more intelligent in its classification, cf. yellow pages versus white pages.

Mall

A Mall is a grouping together of sellers, acting as an intermediate interface between buyer and seller.

Payment

Those third parties, such as banks, card issuers etc. who provide a means whereby the seller is paid by the buyer

Notary

Notaries provide such services as:

- time-stamping
- contract witnessing
- long term archiving
- fair exchange of values.

7.2.1.2 Concepts in the SEMPER model

The SEMPER model uses the concepts of **transfer** and an **exchange** to describe a business session. **Transfer** is the sending by one party to one or more other parties of a **container**. The sending party can define security

requirements such as confidentiality, anonymity, non-repudiation of origin, non-repudiation of delivery. An **exchange** is a number of combined transfers, whereby parties transfer to others something specific and receive something specific. After each transfer or exchange the parties are either satisfied and willing to continue to the next transfer or exchange or they are dissatisfied, in which case an **exception** or **dispute handler** is invoked. A **container** is a general data structure which may be:

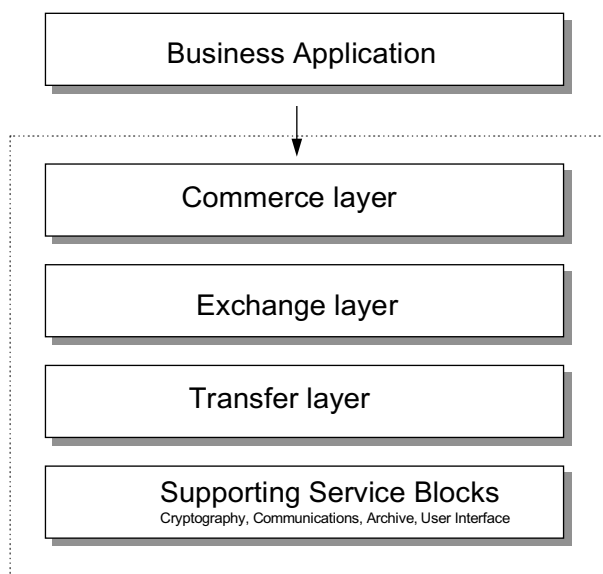
- signed documents, such as certificates, orders, receipts
- information, such as digital goods, a cryptographic key for enabling access to a video transmission (information is not processed as part of the transfer)
- electronic money.

Exception and dispute handling

The difference between exception handling and a dispute is taken to be that in the former case, both parties are honest. By use of audit trails, the parties can resolve exceptions. In a dispute, the audit trail has to contain evidence such as non-repudiation tokens, which can be verified by an arbiter using a decision procedure.

7.2.1.3 SEMPER Architecture

The SEMPER architecture defines a set of service layers:



The **Business Application** running in the top layer uses services in the lower layers, generally in the **Commerce layer**, to provide SEMPER services. The **Commerce layer** provides services which implement particular business protocols such as how specific types of merchant handle transactions with customers — for example, registration, offer, order, payment, delivery. This layer may offer features such as display and completion of standardised order forms. The **Exchange layer** provides services for the fair exchange of containers. The **Transfer layer** provides services for composing, sending and receiving containers, including security requirements. This layer contains the transfer manager, which splits up container processing among the payment service block, the statement service block and the certificate service block.

The Transfer layer can also provide services such as managing an electronic purse or communicating with a third party, such as a payment service. The **Supporting Services Block** includes:

- the **Cryptographic Services**, which provide message encryption and decryption, hash functions, message authentication codes, digital signatures and key generation;
- the **Communication Services**, which support communication in a network and protocol independent way
- the **Archive Services**, which provide local storage of all persistent data such as digitally signed messages, certificates, cryptographic keys, transaction and evidence objects; data can also be stored securely e.g. using encryption or in tamper-resistant memory on a smart card
- the **Trusted Interactive Graphical User Interface Services** provide a distinct user interface to emphasise that this and not the regular interface, such as a web-browser, is the interface, for critical inputs, e.g. account numbers, and outputs, e.g. confirmation of the seller's identity
- the **Access Control Services**, which implement access control to the various blocks of the SEMPER architecture.

The architecture must take account of the need to use, as much as possible, trusted hardware on small mobile devices such as smart cards and PDAs.

7.2.1.4 Trust and SEMPER

In order to use SEMPER with confidence, a user must trust its design and implementation. In order to establish this trust, the SEMPER project, in its initial stages, will follow an open design process, capable of security evaluation, will digitally sign issued software and will support use of tamper-resistant hardware.

7.2.1.5 Certificates in SEMPER

SEMPER defines a certificate to be any signed statement about a person and distinguishes three types:

a **key certificate**, which links a particular public key to a particular identity;

an **attribute certificate**, which certifies attributes of either a person or a key, such as this person is willing to accept legal responsibility for signatures made with this key.

a **hybrid certificate**, which contains both a public key and attributes describing what the key can be used for.

SEMPER provides services for registration and certification and use of certificates, but does not prescribe who can carry out the role of registration or certification authority nor for what purposes registration and certification are required. SEMPER supports a variety of user trust scenarios; however it does recognise the need to register and certify any third parties who may need to be trusted.

7.2.2 End-to-End Security over the Internet — E2S

The goal of this ESPRIT project is to develop, test and install end-to-end security mechanisms for commercial transactions using the Internet. The focus will be on:

- exploring the multicultural and multicountry aspects of the architectural model for business
- building prototype application packages on components developed elsewhere
- user assessment and evaluation of the model
- secure commercial and business operations over the Internet
- development of user security policies and reference models suitable for commercial and business use.

The project plans to use components such as the Verisign and ICE-TEL certification infrastructure, services using the Secure Electronic Transaction specification, Java, and smart cards supporting a number of algorithms and application data storage.

7.2.3 OSM, an Open Service Model for Global Information Brokerage and Distribution

This is an ACTS project in which the OSM Consortium are building a series of electronic commerce and brokerage products around an open architecture. The principal objective of the OSM Consortium is to initiate the creation of an open electronic trading market for product and service offerings delivered through on-line systems and other means. The project has three phases:

- specification of an Open Architecture for Information Brokerage and Distribution;
- development of a supporting implementation of that architecture;
- validation of the architecture and implementation under public trials

The architecture reflects the background of the OSM Consortium, ongoing development by the OSM team, and the introduction of standard components based on the consensus of opinion amongst Object Management Group (OMG) member organisations. The development of the open model will involve standardisation of:

- payment and security facilities;
- transactions and persistent asynchronous communications;
- catalogues, and services.

The project will support standardisation of infrastructure interfaces within the Object Management Group de facto standardisation process.

Trials will be undertaken in the area of news media content management and delivery involving organisations in Germany and France. There will also be trials focusing on professional service catalogues across a group of competitive suppliers involving organisations in Austria, France, Germany and the United Kingdom.

7.3 . The World Wide Web

The World Wide Web is the most important and rapidly developing medium for the dissemination of digital information, of all types, over the Internet. Two programmes of particular importance to trusted services are being carried out by the World Wide Web Consortium:

- Platform for Internet Content Selection (PICS)
- Digital Signature Initiative.

7.3.1 PICS (*Platform for Internet Content Selection*)

PICS represents the first specification to address this requirement, focusing on the classification of information according to its content. Implementations of this specification have concentrated on classifying information content in order to protect children from being exposed to inappropriate material. The PICS specification has been approved by the W3C as a Recommendation.

Key concepts in the PICS specification are:

rating service, where a third party provides content labels for information

rating system, which specifies the criteria used in the labels, the scale of allowable values for each criterion, and a description of the criteria.

content label, which contains the ratings for a particular document.

If the information object is a story with pictures, PICS enables an answer to be given to the question: "Is it suitable for viewing by a nine year old child?" It thus has a similar function to the V-chip.

PICS also specifies a means for ensuring the integrity of a page of information, using a message digest, and the authenticity of labels produced by a rating service, using a digital signature.

PICS also defines a label bureau, where a third party can be the holder of label information about documents held on a number of servers. This service can be linked to an information broking service enabling documents to be found according to their classification.

7.3.2 *Digital Signature Initiative*

As well as knowing something about the content of information resources, users want to know more so that they can decide whether or not to retrieve an information object. For example, if the information object is a report, who has reviewed the report and given it a "seal of approval"? Does the information really originate from the claimed author? If the information object is a software program, who has checked it to see that it does what it claims to do and does not contain any viruses? what computing resource does it need? what support is available for it? Users require information about the information ("meta-information") so that they can reach conclusions about trusting what the World Wide Web provides. In response to these requirements and in order to provide an infrastructure in which a number of solutions could interoperate, the World Wide Web Consortium (W3C) has launched a Digital Signature Initiative project.

The W3C goals for the project are:

- Cryptographic Format. To define an agreed format for digital signatures for information objects on the WWW.
- Awareness of Trust Issues. To help organisations taking part in the Digital Signature Initiative learn what the issues and problems are in the management of trust. In particular to realise the importance of a common architecture for managing trust in different application areas, such as software, product descriptions, press reports, academic reports and the value of building a reusable solution for trust management.
- Common Trust Management Environment. The major goal is to establish a shared, industry-wide trust management infrastructure enabling users and providers to create Web wide trust policies.

The deliverables from the project are planned to be:

- a Digital Signature Label Architecture (see below);
- a Trust Management Architecture, which will enable users to state their security policies with respect to information objects and process, in the most part automatically, assertions about information objects and so decide what to trust and on what basis.

The feasibility of the approach will be demonstrated by implementation of test systems, which will also be the basis for further development of the Trust Management Architecture. While the first part of the project's specifications, the Digital Signature Label Architecture, will be produced as a Recommendation of the World Wide Web Consortium and may be put into the industry standards process, the second part, on Trust Management will not be sufficiently mature — a reflection of the general state of experience in running trust- based systems.

Digital Signature Label Architecture

This architecture can be described as a realisation of the statement:

A Public key holder, identified by a digital signature, makes assertions, expressed in a formal, processable language, about information resources.

Each part of the statement translates into a specification:

- the key holder's identity will be expressed using a signature block, which will say who signed the information resource, when, and using what algorithms;
- the assertions about the information will be contained in a *signature label*, which is an extension of the PICS label;
- the information resources will be listed in a manifest.

7.4 Healthcare — TrustHealth

TrustHealth is a project within the Health Telematics sector of the European Commission 4th framework programme. The objectives of the project are to provide:

- A set of specifications for security services and interfaces.

- A trusted third party service infrastructure with operational systems in some countries and publicly available specifications.

The project partners are users, research institutions, providers of security technology and health care applications and infrastructure service providers.

Three assumptions about the environment in healthcare have influenced the project's work on security services and interfaces:

- the PC work station will continue to be the major type of terminal
- healthcare professionals are very mobile in their work pattern
- control of keys and certificates makes the smart card an ideal storage medium.

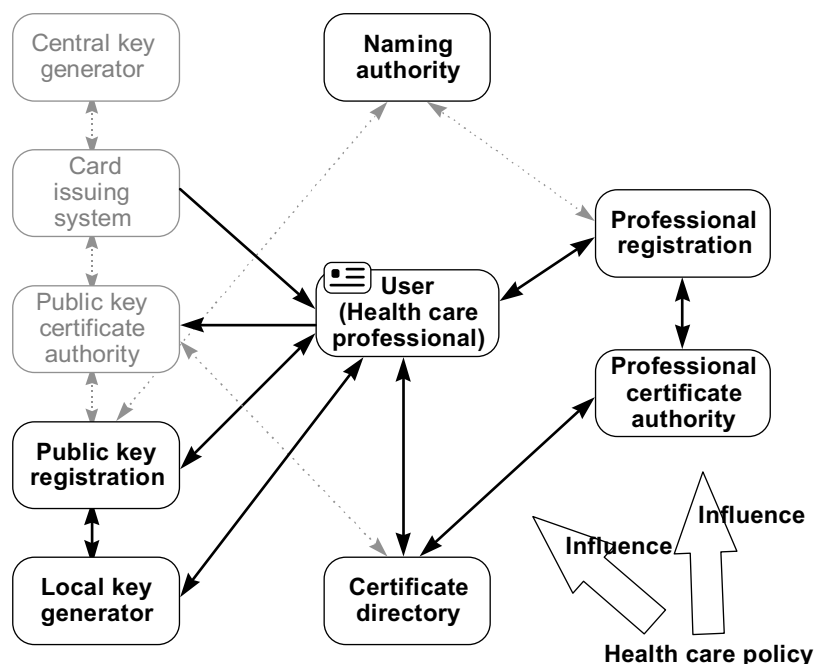
The work on trusted third parties took as its starting point requirements identified in the "Trusted Health Information Systems" (THIS) project, which reported on the need for a number of cryptographically based security services. It particularly emphasised the need for European guidelines to be developed for the establishment of an infrastructure of Trusted Third Parties with national control of operations and the importance of an electronic professional registration system which operated throughout Europe.

The project has produced a number of deliverables:

- Selection of Security Services and Interfaces — functional requirements for common security services and a specification of a TrustHealth Security Platform
- Guidelines for Implementation of Security Services and Interfaces — detailed interface specifications and implementation guidelines
- Functional Specification of TTP Services — functional requirements of services including Naming, Public Key and Professional Certification, Card Issuing and Directory Services.

TrustHealth and Trust Services

The report — Functional Specification of TTP Services — contains a model of TTP services and identifies those services which are of special importance to the health care sector. In the figure below, these services are in bold. It should be noted that the other services are also of relevance.



The following scenario shows the roles of the services which are more important to the health care sector:

- a *User* with a name and some additional number sufficient to identify him uniquely wishes to acquire a Health Care Professional (HCP) card enabling him to access restricted services, digitally sign documents and communicate confidentially with fellow professionals;
- he approaches a *professional registration authority* with a request for a HCP card;
- the user's identity, a *distinguished* name, obtained directly or indirectly from a naming authority, is registered with a *public key registration authority*;
- the user then receives:
 - from a *key generator*, three pairs of keys: one for digital signing, one for key encryption and one for identification and authentication. (Organisational issues might lead a local key generator to be preferred to a central key generator);
 - *public key certificates* (one for each key pair), generated by a public key certification authority, linking his identity to each public key;
 - an *electronic professional certificate*, recording his identity and his professional status, authorisations and so forth;
 - a *HCP card*, containing three private keys, the respective public key certificates and the professional certificate.

The public key and professional certificates would be stored in a *Certificate Directory*.

In addition to security requirements, there are also particular issues concerning the operation of the registration authorities and the directory services. The relationships between the professional registration authority, the public key registration authority and the naming authority may also be more important in health care than in other sectors.

A particular issue may be the degree of health care users' control required over TTP functions which require unconditional trust, for instance, in the generation of key pairs.

Naming

TrustHealth proposes to use an hierarchical naming scheme with a number of trees per country to support existing national practices. Three attributes: unique number (UN), numbering system (D) and country (C) uniquely identify a name. For readability a common name (CN), organisation name (O) and organisation unit (OU) may be present. The unique name is used within an X.509 v3 certificate. The TrustHealth naming scheme uses the name constraint extensions described in the Internet draft — Internet Public Key Infrastructure – Part I: X.509 Certificate and CRL Profile.

Professional Certificates

TrustHealth defines an X.509 v3 certificate with the Subject directory attributes extension used to contain health care professional data. This data defines within each country's professional structure the capabilities of an individual, such as their specialisations.

7.5 Telecommunications

7.5.1 Advanced Security for PErsonal Communications Technologies — ASPeCT

One of the objectives of this ACTS project is to investigate, implement and trial solutions for Trusted Third Parties for end-to-end services in Universal Mobile Telecommunications Systems (UMTS), including secure billing and end-to-end encryption services. Secure billing will be done using digital signatures to provide non-repudiable evidence of use of a value-added service by a mobile user. ASPeCT TTPs will generate, distribute and manage public/private key pairs for users and value-added service providers (VASPs). To support end-to-end encryption services, an ASPeCT TTP will act as a secret key generation and distribution centre, with a key escrow facility to enable lawful interception.

The architecture of an ASPeCT TTP has four layers:

- external communication: floppy disk driver, graphical user interface, communication subsystem
- TTP security control: database, containing keys, user information and event information (e.g. for audit); and security functions
- TTP functions and operation: provides security services to the layer above via an application programming interface based on Generic Security Services-API and Key Management Framework- ISO/IEC 11770-1
- cryptographic functions: provides cryptographic services to the layer above via an application programming interface based on Generic Cryptographic Services-API published by the Open Group.

The project also intends to use interfaces for client-TTP and TTP-TTP communication specified in the ETSI TTP standard which is being developed.

Because space on a smart card and bandwidth of mobile communications are limited, the project has defined a non-standard, compact certificate format. There are two types of certificates, depending on the signature mechanisms used:

- Rivest-Shamir-Adelman (RSA) signature based on ISO/IEC 9796-2 Digital signature scheme giving message recovery - Mechanisms using a hash-function
- Agnew-Mullin-Vanstone (AMV)-signature based on ISO/IEC 14888-3 Digital signatures with appendix - Certificate-based mechanisms.

7.6 Electronic mail

The European Electronic Mail Association (EEMA) is undertaking a project called Challenge.97@Electronic.Commerce.Europe. The purpose of this project is to demonstrate a secure messaging infrastructure which can be used for secure and reliable commercial transactions. In addition to the secure messaging infrastructure, the project will demonstrate a directory infrastructure in which security information will be stored and which can be used to provide both White and Yellow pages services. One of the project's objectives is to facilitate the adoption of the EEMA Security Framework.

Demonstrations will be given at the EEMA conference in June 1997. Three business scenarios have been defined:

- directory business scenario: yellow pages will be used to locate an individual to whom a message is to be sent
- digital signature business scenario: using S/MIME format a signed document will be sent to a customer
- encrypted message business scenario: using S/MIME an encrypted and signed document containing a contract will be sent by a customer to a supplier.

Specific technical security issues include X.400/SMTP inter-working using gateways and the management of security keys.

7.7 Electronic publishing, information broking, copyright management

7.7.1 *Architecture for information Brokerage Service — ABS*

The ABS project, funded by the ACTS programme, is focusing on the design, specification, implementation and validation of an open broker system to permit the efficient provision of on-line information services over the European Information Infrastructure. The project has three main objectives:

- to design, implement and validate a prototype of the broker system by conducting significant international trials;
- to contribute to relevant standardisation activities, especially on the topics of broker/trader services, broker architecture, federation of broker systems, broker information models, particularly to support international deployment of the services;

- to exploit the trials results in order to produce a comprehensive technical and economic evaluation of the potential market development in different business areas.

The project plans to investigate the use of TTPs in 1997 and expects to use the results of the SEMPER project in achieving its own goals.

7.8 Chip - Secure Electronic Transaction — C-SET

Cartes Bancaires(CB), the French bank card association, has developed this solution, the C-SET (Chip-Secured Electronic Transaction) protocol. In the first phase, existing smart cards issued by the French banks will be used. The solution will provide security to national and international payment transactions in electronic commerce and interoperates fully with SET, which is developed by CB's international partners Visa and MasterCard. It is identical to the generic architecture of CB remote payment, except that the connection between the cardholder and the merchant is established through an open network.

7.8.1 Differences between C-SET and SET

Security in the C-SET architecture relies on the use of the smart card with the active participation of the cardholder. The cardholder has to key in his PIN to authorise his card to sign a transaction.

In contrast, the SET architecture, implemented entirely in software, does not support the use of a smart card. Security relies on software secure mechanisms and therefore depends on the environment in which the software executes, the cardholder's PC. In C-SET all the sensitive sequences of the cardholder's software are executed in a trusted environment: the PIN-pad reader and the smart card.

The integrity of the PIN-pad reader is protected, it is a Tamper Evident Device. It does not contain any secret but protects the PIN (Personal Identification Number). In C-SET, all sensitive information going through the PC (card data and payment instructions) are protected for confidentiality and integrity.

Secret keys are kept in secure devices such as the smart card.

7.8.2 Interoperability with SET

Compatibility with SET is a major requirement, but the implementation of SET in the CB remote payment process would introduce SET weaknesses, arising from the software-only environment. Therefore, interoperability between C-SET and SET is provided by specific converters.

A converter serving the C-SET cardholder acts on the one hand as a payment gateway (using the CB Acquirer key) to check the C-SET payment instructions, and on the other hand as a SET certification authority (using the Visa/MasterCard certification key) to grant SET certified identities to cardholders.

A converter serving C-SET merchants acts on the one hand as a SET certification authority to grant SET certified identities to merchants, and on the other hand as a SET payment gateway to check SET payment instructions.

7.8.3 *Future plans*

Once the first phase has been completed, a second phase will comprise the development of a new French smart card which conforms to the international EMV '96 (Europay MasterCard Visa) standards. The card will contain SET related functions, among others, and will provide a model for other countries implementing smart card technology.