SANDIA REPORT

SAND97–2901 • UC–705
Unlimited Release
Printed November 1997

Final Report for the Integrated and Robust Security Infrastructure (IRSI) Laboratory Directed Research and Development Project

Robert L. Hutchinson, Victoria A. Hamilton, Gabi G. Istrail, Juan Espinoza, Martin D. Murphy

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A04
Microfiche copy: A01

SAND97-2901
Unlimited Release
Printed November 1997

Distribution
Category UC-705

Final Report for the Integrated and Robust Security Infrastructure (IRSI) Laboratory Directed Research and Development Project

Robert L. Hutchinson
Network Systems Surety Department

Victoria A. Hamilton, Gabi G. Istrail
Information Systems Surety Department

Juan Espinoza, Martin D. Murphy
Software Systems Surety Department

Sandia National Laboratories
P. O. Box 5800
Albuquerque, NM 87185-0449

Abstract

This report describes the results of a Sandia-funded laboratory-directed research and development project titled "Integrated and Robust Security Infrastructure" (IRSI). IRSI was to provide a broad range of commercial-grade security services to any software application. IRSI has two primary goals: application transparency and manageable public key infrastructure. IRSI must provide its security services to any application without the need to modify the application to invoke the security services. Public key mechanisms are well suited for a network with many end users and systems. There are many issues that make it difficult to deploy and manage a public key infrastructure. IRSI addressed some of these issues to create a more manageable public key infrastructure.

1. Introduction

Information security is becoming increasingly important as the public, private, and government sectors become more connected through modern computer networking. Users of today's networks require a wide range of security services. Before two users share information, they may need to authenticate each other's identity. If the information is private, they will want confidentiality. They may also want to ensure that the information was not modified since origination. There are many other security services a user may desire. Many software vendors are providing security solutions but these solutions require modifications to existing applications. For example, Kerberos, a network security product, requires the software application to invoke the security services. Existing software applications must me modified to use the Kerberos security services.

Basic information security requires a user to authenticate the identity of other users or sources of information. Public key cryptography provides a conceptually scaleable method of authenticating users and entities. There are many issues that make it difficult to implement practical public key infrastructures. Consider a valid user who has been initialized into a public key infrastructure. That user is given a secret which if exposed could compromise the system. It is impractical to believe that the secret will remain unexposed for the life of the system. The public key infrastructure must have a mechanism to inform all other users in the event of a compromised secret (revoke the key). This mechanism must be secure itself. If it is not, an adversary could revoke a valid user's key. This type is attack is called a denial of service.

The purpose of this laboratory-directed research and development project was to provide an integrated security solution for today's information systems and networks. Our goal was to eliminate the need to modify existing software applications and provide an easily managed public key infrastructure using commercial operating systems. We did not seek to provide a security infrastructure which enabled multilevel secure computing. IRSI sought to provide robust, commercial-grade security service with flexible access control policies. We also investigated the use of secure tokens to store the user's long term secret. Our motivation for using this approach was to prevent compromise of the long term secret by limiting its exposure to the system.

IRSI was originally funded for two years. After the first year of investigation, we concluded that it would be necessary to modify the

software application or the operating system to meet our goals. This modification is inconsistent with the intent of IRSI. The LDRD technical assessment team chose not to continue IRSI into the second year. This report describes our findings in the areas of application transparency, public key infrastructure, and secure tokens. This report has three primary sections: section 3 describes the team's research, section 4 details our research findings, and section 5 provides some conclusions and recommendations.

2. Acronyms and Abbreviations List

AH	authentication header
CA	certification authority
DCE	distributed computing environment
ESP	encapsulating security payload
IPSec	internet protocol security
IRSI	integrated and robust security infrastructure
LDRD	laboratory directed research and development
MD5	message digest 5 (hash algorithm)
NRL	Naval Research Laboratory
OSI	open system interconnection
PKI	Rivest, Shamir, and Adleman (public key algorithm)
PKM	public key management
SDSI	simple distributed security infrastructure
SPKI	simple public key infrastructure
SSL	secure sockets layer
TCP/IP	transmission control protocol / Internet protocol

3. Integrated Security Services

The goal of this project was to investigate mechanisms to provide integrated security services which were nearly transparent to the user, transparent to applications, and did not require special purpose, highly secure and often costly operating systems. The IRSI team believed that integrated security at a system level rather than ad hoc or patchwork security features provided several advantages. Integrated system security is the only way to successfully implement a unified security policy. Implementation of a unified security policy is often the only way to implement complex access controls to a variety of objects that might exist in a distributed manner throughout the system. Without a unified or integrated implementation, the system will almost assuredly include weaknesses or backdoors that would allow unauthorized access to these objects. In addition, security features like all other parts of a dynamic system will require maintenance. This maintenance will include bug fixes, feature enhancement, and perhaps even implementation of new security algorithms. Integrated and unified system security will simplify the maintenance requirements and it is well known that the cost of system maintenance almost always outweighs the cost of system development by several factors.

The IRSI development team also believed that system security should be an integrated system feature, but should also be viewed as a separate system attribute. The reasoning behind this belief is that the field of system security is a specialized field just as is operating system development or database development. Implementation of security features in a complex system is best left to those developers who have an understanding of the issues and the tools available to address these issues. However, system security features clearly cannot be implemented in a vacuum. System security requirements must be met as part of a well-managed system engineering process.

3.1 Commercial Grade Security

It should be noted that the goal of this project was not to investigate system security at the national security level, but to address security at a level that might be reasonably required in a commercial environment. For instance, when data security is required, this requirement might be met by some publicly available, well-tested encryption algorithm using keys of some reasonable length. The team recognizes that this goal is very loosely stated. Without a lot of difficulty, one can easily see that different

commercial industries could have wildly different security requirements. Electronic banking applications must clearly meet stringent and exacting security requirements. These requirements may or may not be excessive in a general intra-company email application. However, the IRSI team was only interested in security solutions that could be provided by publicly available technologies regardless of the severity of an application's security requirements.

3.2 Description of Security Services

The following table defines and describes the various security services that were of interest to this project.

Security Service	**Definition**
Privacy	• the prevention of access to information by unauthorized users • the protection of resources from access by the unauthorized and limiting access by the authorized
Integrity	• the correctness and appropriateness of the content of a piece of information • the property that an object is changed only in a specified and authorized manner
Authenticati on	• the condition that the claimed identity of a user, device, or any other entity in a system is genuine • the condition that the data stored, transmitted, or otherwise exposed to possible unauthorized modification has integrity • the condition that the claimed identity of an entity in a computer system is genuine and that the data generated by that entity has integrity
Non-repudiation	• the ability to prove to a third party the authenticity of data • an authentication that with high assurance can be asserted to be genuine, and that cannot subsequently be refuted • a condition whereby the author of data cannot deny the validity of the result of the process used to authenticate data
Anonymity	• the quality or state of being not named or identified (can be applied to all entities within a system, e.g.,

	users, machines, nodes, etc.) • lacking individuality, distinction, recognizability, traceability
Availability	• the ability to access a specific resource within a specific time frame • the ability to use or access objects and resources as required • the prevention of the unauthorized withholding of information or resources
Access Control	• the process of limiting access to the resources a system only to authorized users, programs, processes, or other systems in a network • the limiting of rights or capabilities of a subject to communicate with other subjects or to use functions or services in a computer system or network • restrictions controlling a subject's access to an object
Audit	• independent review and examination of records and activities to determine compliance with established usage policies and to detect possible inadequacies in system security policies and their enforcement • a mechanism used to provide traceability and/or system recovery

Note that some of these services are related to each other. Integrity, authenticity and non-repudiation are related services that in some sense build on each other. Non-repudiation and anonymity are services which directly conflict with each other. Access control is often implemented using some sort of privacy mechanism. An audit service often supports all other security services. Unfortunately, a good audit service is rarely completely automated. Some trusted human review is generally required.

There are many reasons why these security services may or may not be needed in a particular system. Individual systems will have specific requirements. However, many systems do require some combination or combinations of these services. For example:

- many systems require secure communications to and from database servers or web sites to limit access to data,
- many systems require privacy for email or file transfer services,
- almost all systems require integrity during data transfer,
- some systems will require authentication to prove the claimed originator of data is indeed the data originator,

- some systems will require that the originator of data may not at some later date deny originating that data (e.g., some banking applications),
- some critical systems will require that the system always be available (e.g., some medical applications), and
- a few systems may need to provide anonymity (e.g., electronic commerce systems that mimic cash transactions).

The mechanisms used to implement these features can often be quite different and these mechanisms can have a tremendous impact on system architecture requirements. For instance, while a privacy security service might be implemented using a private key mechanism, non-repudiation often requires public-key mechanisms.

Two basic terms necessary for an understanding of cryptographic techniques are symmetric (private key) and asymmetric (public key). Symmetric mechanisms require that all parties involved in the use of a cryptographic technique (encryption, authentication, etc.) use the same key and that this key be kept secret from parties not involved in the use of that technique. Asymmetric mechanisms require that only one party hold a key that must be kept secret. All other parties hold a mathematically related and openly available key. The availability of the secret is more limited in asymmetric mechanisms and therefore makes asymmetric mechanisms more appealing for certain applications. However, in general, symmetric mechanisms are far less computationally intensive than asymmetric mechanisms.

Unfortunately, asymmetric cryptographic mechanisms also require an extensive certification infrastructure since a given public key must be certified to belong to a specific entity. Usually, this means that the system must have a policy defined for proving identity and must include, at the very least, an off-line certification authority.

3.3 The Long Term Secret

Critical to any security service is the ability to authenticate the user or end system element. Consider a system that provides perfect confidentiality. Users of such a system could send messages to one another with no possibility of eavesdropping. This system can still be easily exploited if users are not able to authenticate each other. How useful is a system with a perfectly secure communication channel if a user is unable to determine the identity of the distant user? We chose to solve this problem using public key cryptography.

Users are enrolled into the system by registering a public key. The public key must be available to other users. The user's secret key must be protected or the system can be compromised. We refer to this secret as the long term secret since it may have a useful lifetime of a year or more.

If a user's long term secret is compromised, an adversary can masquerade as that user and gain all of that user's privileges. It could be difficult or impossible to know that an adversary has broken into the system. Therefore, it is critical that the user's long term secret be protected.

It is difficult to protect the user's long term secret if it is stored on a user's workstation. Commercial operating systems have lists of vulnerabilities that will allow a clever adversary to extract information. There are even programs that look at the workstation's memory or keyboard buffers. Most of these attacks require the adversary to have access to the workstation. No commercial operating system or computer architecture can protect the long term secret from a reasonably capable adversary with physical access.

There may be many users with access to a single workstation. This makes it even more difficult to protect any individual's long term secret. An adversary with access to the workstation requires less skill than a remote adversary to extract the long term secrets. Finally, there are many known network attacks which give an adversary access to restricted workstations. Firewalls help minimize these attacks, but most system administrators are always one step behind hackers. Without proper network configuration and management, an adversary could extract the long term secret over the Internet.

One of the IRSI team's goal was to minimize exposure of the long term secret. We chose to investigate and implement secure tokens using smart cards. A smart card has the same physical dimensions as a credit card but contains integrated circuit technology. The face of the card has an area with metal contacts that provide a standard electrical interface with the integrated circuit. The user inserts the smart card into a card reader that is attached to the workstation. The workstation communicates with the smart card through the card reader. The smart card we chose is a Data Key SignaSURE cryptographic smart card. This particular card has a micro-controller with a hardware cryptographic processor. The cryptographic processor supports RSA or DSA. We chose to implement RSA public key cryptography.

The IRSI team chose to store the user's long term secret (private key) on the smart card. The long term secret never leaves the smart card during normal operation. This prevents exposure of the long term secret to the workstation and network. Each user would receive a smart card

containing her long term secret at the time she is enrolled in the system. The user would not have the ability of viewing the long term secret. Smart card manufacturers have designed many features that make it difficult for all but an extremely capable adversary to extract a secret from the smart card. The smart card and the user's long term secret would be used primarily to authenticate the user's identity to the system. We chose RSA digital signature using MD5 as an authentication algorithm.

Digital signatures provide a mechanism for users to *sign* a message in a way that other users can positively verify. An RSA digital signature of a message requires two steps. First the messaged is transformed into a relatively short fixed size message digest using a one way hashing algorithm such as MD5. Second, the message digest is transformed with the user's private key (long term secret). Once received, other users can hash the message into a message digest using MD5 then reverse transform the signature using the correct public key. If the signature is identical to the verification transformation, then the message had to be signed by the owner of the public key.

Our approach to signing messages is to take advantage of the two steps necessary to create an RSA/MD5 digital signature. The smart card is capable of creating the entire signature itself, but it is very slow. We decided to create the message digest on the workstation using the MD5 hash. Once we hash the message, we send the message digest to the smart card to be transformed with the long term secret. This solution protects the long term secret and maintains a reasonable level of performance.

In conjunction with another LDRD project titled "Highly Secure Smart Card System", we demonstrated this method of creating a digital signature. The digital signature performance was limited by the smart card. The smart card took about one and a half seconds to generate a signature. Current smart card vendors claim to be able to perform an RSA signature in less than one second. The time required to perform an RSA signature will continue to decrease as the speed of smart cards increases.

3.4 Public Key Infrastructure

Consider the following incomplete, very simplified scenario. Alice wishes to exchange information with Bob in a particular domain in a confidential manner such that the origin of the communication can be authenticated (that is, Alice knows Bob is sending the information and vice versa). Alice acquires a (possibly unique) key pair for each cryptographic service she

wishes to exercise (authentication, confidentiality, etc.). The key pair is associated with Alice's identity. Alice wants to send a confidential memo to Bob. Alice retrieves Bob's public key, checks that it has not expired and that it has not been revoked, encrypts the memo with Bob's public key, signs the encrypted message with her private key and sends it on its way. Bob retrieves and checks Alice's public key and decrypts the signature. If this is successful, he knows that Alice did indeed send the message, and that he can trust the origin of the message. He then decrypts the message with his private key. There are complications to this scenario. In the case where both Alice and Bob live in distinct hierarchies, their respective hierarchies may not have a workable trust relationship yet. What should Alice or Bob do if they discover that the other's key has expired or been revoked? Finally, there are no attackers in this idealized description.

How is all of this managed? How are keys created, associated with an identity, and distributed to a new principal? How does Alice go about getting a key to communicate with Bob? How and when are keys archived? How is new keying material generated and distributed? How are compromised keys indicated and removed from use? These questions are addressed by public key infrastructures (PKI) and the management thereof (PKM).

The key infrastructure provides the structure by which the secrets (and their associated identity, lifetime, validity, etc.) are managed. Specifically, PKM should provide the following capabilities [65]:

1. initialization of system users within a domain;
2. generation, distribution, and installation of keying material;
3. controlling the use of keying material;
4. update, revocation, and destruction of keying material; and
5. storage, backup/recovery, and archival of keying material.

While there is agreement on the functionality that should be provided, there is no such agreement on the implementation. This disagreement roughly parallels the current debate about deployment of cryptographic tools to the public and revolves around the entity or entities which should be trusted.

The core of a key infrastructure is the key. A necessary requirement to manage keys is that the system bind the key to an identity. Expiration dates, key issuer, access controls, attributes, algorithms used, and other information is optionally included in this binding. For this discussion, the binding of a key, identity and optional information will be called a certificate for all instances of the PKI. The certificate is issued by an authority. In this paper, the certificate authority (CA) will simply mean the entity that supplies the certificate. In the general case, the certificate

(key plus identity plus miscellaneous information) could refer to a person, computer, process, transaction or any number of other things. The object with which a key is associated may also be called a principal.

3.4.1 Establishing Identity

The use of cryptographic solutions to provide confidentiality, data integrity, authenticity, etc., is often based on the assumption that the identity of the entity called Alice really is the Alice intended. If this association can be made with an acceptable degree of risk, most of the cryptographic requirements can be met (simple, but likely not easy). If it is necessary that this identification be absolutely accurate, then out of band techniques will be necessary (e.g., couriers, in person meetings). This appears to be the only way to ensure that the identification is perfect. Out of band techniques also appear to be the only sure way to distribute initial secret keying material to a principal.

The discussion in the previous paragraph does not mean that establishing identity is always necessary. There is a large set of transactions, activities, and processes that only require that some identity be bound to a key right now and that it remain known. There is even a school of thought that believes that rigorous identity establishment is never necessary. For example, if Alice wishes to withdraw money from her bank, then all that is really required is that the Alice that wants to withdraw the money is the same one that deposited the money. If Bob wants to initiate a relationship with a party met on the Internet, his only concern is that a key be bound to the identity of the new party when he initially encounters them. Bob doesn't care if the other party is Klingon, canine or human; only that the key he is assigning to the other party can be associated with them from now on. If the key is compromised or eavesdroppers are encountered, then, of course, Bob has some problems to address. However, these issues exist whether identity was rigorously established or not.

3.4.2 The Spectrum

Two philosophies illustrate the ends of the spectrum with respect to public key infrastructures and management. One extreme holds that a single hierarchical infrastructure is appropriate. The standard that describes this extreme is the ITU-T Recommendation. One example of an implementation of this hierarchical approach and standard is SPX: The other end of the spectrum holds that every entity/principal should be able to control all aspects of their keys and that trust should be distributed. A

standard that describes this philosophy is the merger of the Simple Distributed Security Infrastructure and the Simple Public Key Infrastructure standards (SDSI/SPKI). MIT and Microsoft have developed implementations of the SDSI/SPKI specification.

In addition to the technical issues surrounding PKIs, there are significant "human factors" issues that cloud the any discussion of PKIs. These are exactly the same issues that cloud the cryptography debate in general. These issues are brought up when one asks the question "why should anyone dictate to a person who they should trust or not trust as the protector of their secrets?" These very important issues are not easily (if at all) addressed by technical means. The recognition of their existence is the extent of their discussion in this paper.

3.4.3 Pros and Cons/Issues

Managing a truly global infrastructure is a huge task. Considering the five billion people on the planet, the services they may wish to protect with cryptographic methods (television, telephony, computing at home, computing at work, automation of household appliances, credit and financial services, electronic commerce to name a few), that multiple keys may be necessary for each application (signature and encryption as a minimum for most cases), and that these same services will be provided to businesses, it is conservative to suggest that a PKI be able to handle 500 billion principals. To emphasize, managing a global infrastructure will be a monumental task. Of course simply agreeing upon a group or agency responsible for managing the global PKI may be impossible in itself.

The X.509 specification does not of itself dictate a hierarchical PKI. However, its dependence on a distinguished name leads to a hierarchical solution. Some positive aspects of this (for some people) are that every principal is accounted for in the same way and that there is centralized control. The negative aspect is that the centralized control produces a system with a very risky single point of failure. The specification and data structures used to develop the distinguished name have also been deemed to be difficult to use and understand. It is impossible to create access control lists in X.509. Access control lists specify a principal's set of permissions to use or access processes, objects, activities, etc.

On the other hand, the SDSI/SPKI approach allows each principal to act as its own certificate authority and there is thus no single point of failure. Currently pending federal legislation may make this illegal, but the option exists today in the SDSI/SPKI specification. SDSI/SPKI makes specific

provision for groups which then lead to a natural implementation of access control lists. The syntax of their implementation is easier to understand and implement than that in the X.509 standard. That there is no single point of failure decreases the risk in the system, but is a downside in that finding a particular principal may be difficult (especially the first time). It will also be difficult to establish trust relationships because of the lack of centralized certification. In general, determining if a certificate has been revoked is more difficult in the distributed case than in the hierarchical case. This distributed, end-user control makes SDSI/SPKI look like the "Internet model of cryptography," an approach that is very appealing to many people.

Neither the hierarchical nor the distributed approach is flawless. Government interactions between municipalities, states or countries implies a hierarchical infrastructure. Personal communications between Bob and Alice implies an infrastructure strictly dependent on the trust relationship between them. Business activities may have additional unique, or at least more stringent, requirements (international banking transactions of billions of dollars require much higher levels of protection than personal communications between Bob and Alice). The legitimate needs of law enforcement agencies yield even more requirements that may be difficult to balance with the protection of personal freedoms. Key escrow is currently the most hotly debated of these requirements.

3.4.5 A Perfect World

An integrated and robust security infrastructure would provide the services discussed in the introduction to this section. In a perfect world, these services would be provided seamlessly, without regard to whether the principals live in a digital world dictated by a hierarchical philosophy or a distributed philosophy. Clearly, a perfect world isn't. As discussed above, there are arguments for and against both philosophies. For distinct implementations of the same philosophy, compatibility has yet to be demonstrated. These inconsistencies and incompatibilities are similar to those experienced by the computer-aided drafting (CAD) industry when they were first asked to exchange drawings between vendors. The CAD vendors eventually solved many of their problems. The PKI "industry" is now in a similar position, different only in the magnitude and seeming urgency of the task. It is very likely that the pieces of the PKI/PKM puzzle that result will have distributed (Internet-like) and hierarchical attributes and features; a hybrid solution is a distinct possibility when the many diverse needs of the users are considered.

3.5 Transparency to the Application

Application transparency hides the details of the security services from the application. Any off the shelf application could use the security services for inter-process and network communications without the need to modify the application The goal was to develop a security layer transparent to the application which would provide data separation by user authorization level. Existing middle-ware security products such as Kerberos require that the application be modified to invoke the Kerberos security services. Our research goal was to develop integrated security services that could be installed on a workstation without modifying the operating system or existing applications. This approach requires the security services to intercept inter-process communications and apply the correct security services.

Given a client-server type data-base application (data-base server servicing queries clients running on the same or different machines), devise an application transparent security layer that will ensure communication security (confidentiality, data integrity, authentication, availability and enforcement of the access control policy established by the security policy authority). The authentication should be done on a user basis (user oriented keying). Computer security need not be addressed; consequently, the security services need not protect against malicious users. Application transparency is defined as follows:

- no modifications of the application's code should be needed in order to integrate the security services
- no modifications of the operating system should be needed
- application re-linking might be acceptable
- it might be acceptable to recompile the application if source code is available.

The way application-dependent security parameters would be set is by having the system administrator enter this information into a per-application or per-user security table. The solution should be portable to different platforms. The products available so far (Kerberos, DCE, etc.) pose many constraints on systems: some require secure operating systems, others require a lot of processing overhead, storage, synchronized clocks, etc. Most of them use a symmetric-key key management infrastructure, which is not scaleable and has a single point of attack (the key server). The ideal security layer should employ a public key based key management infrastructure and be easy to install and maintain. There are European public key security products, but they are not available in the U.S.

4. Research Findings

This section of the report describe this year's findings. We had two primary focuses: a broad range of security services that are transparent to the application, and manageable public key infrastructure.

4.1 Application Transparency

Today's security middle ware products require modification of an application to invoke the security services. Our goal was to develop a security product that could be loaded on a workstation without having to alter the application in any way. Our security services would act as a proxy for the application and apply the necessary security services to network and inter-process communications.

4.1.1 Architectural Placement of Security Services

For the purpose of defining communication protocols between real systems, the OSI standards introduce the concept of a model of a real system, known as an open system. The model system is considered to be structured in layers. The pair of communicating entities in some layer N provide a service to the entities in the layer N+1. This service includes carrying data. The entities at the N-th level communicate with each other via an (N)-protocol, which is conveyed by making use of a service provided by the (N-1)-entities. The OSI reference model defines seven layers. Protocols from each of the layers are grouped together into what is known as the OSI layer stack. An OSI layer stack fulfills the communication needs of an application-process, which is part of a real system that performs information processing for a given application purpose. The Internet (TCP/IP) protocol suite spans virtually the same range of functionality as the OSI reference model. The four levels at which distinct requirements for security protocol elements arise are:

- Application level: security protocol elements that are application-dependent.
- End-system level: security protocol elements providing protection on an end-system to end-system basis. It maps into the Network Layer (IP).
- Sub-network level: security protocol elements providing protection over a sub-network which is considered less trusted than other parts of the network environment. It maps into the Data Link layer.
- Direct-link level: security protocol elements providing protection internal to a sub-network, over a link which is considered less trusted than other parts of the sub-network environment. It maps into the Physical Layer.

The direct-link and sub-network level are not acceptable for our goal. These layers secure a logical or physical communication link and are not associated with a user or an application process. Therefore, it is not possible to perform user-oriented keying. Implementing security services at the application layer (a library which could be linked with any application) or at the Network Layer seem to be the two acceptable approaches.

4.1.2 Secure Sockets Layer (SSL)

SSL is an application layer library. It provides most of the services we need. The problem with SSL is that the application needs to be re-written to incorporate the SSL application program interface calls.

4.1.3 IP Layer Security

The IP security architecture is defined in Internet request for comments RFC 1825, RFC 1826 and RFC 1827. IPSec is logically defined at the IP layer. Two cryptographic security mechanisms have been defined for IPv6, which is the next version of IP, implementing the IP security specifications. One, known as the Authentication Header (AH), provides authentication without confidentiality. The second, known as the Encapsulating Security Payload (ESP), provides confidentiality through encryption of packet contents. ESP has two modes. The first mode, known as the transport-mode, encrypts only the upper-layer header and data and leaves the IP header in the clear. The second mode, known as the tunnel-mode, encrypts an entire IP datagram, prepending an additional clear text IP header outside the encrypted IP datagram so that the packet can be routed. A fundamental concept behind IP security is the Security Association. A Security Association contains all of the configuration data for a particular secure session between two or more systems communicating via IP. IPSec (and probably any IP level security specification) can be implemented at three levels:

- Above the IP layer. Only transport-mode ESP is possible with this choice. Requires source code to be available and an implementation of the logical interface between TCP and IP. Any additional protocols (i.e. user datagram protocol) would have to have their own implementation as well. Under Solaris, SunOS, BSD the TCP protocol is part of the kernel.

- Within the IP layer. Requires IP layer source code to be available. Under Solaris, SunOS, BSD the IP protocol is part of the kernel.
- Below the IP layer. This choice is independent of the TCP/IP protocol stack implementation and does not require TCP/IP code. One must re-implement the fragmentation and reassembly of datagrams and IP header checksum computation. This is how Belovin's implementation for DOS was done.

IPSec provides all services we need. Most implementations seem to be based on the Naval Research Laboratory (NRL) implementation for BSD. In this implementation, by setting the default system policy in a certain way, one could achieve application transparent, user-oriented keying security services. The problem is that TCP/IP is logically in the kernel, and the key management system is implemented inside the kernel.

4.1.4 Remarks

We have discovered that in general the philosophy of standards authors and middle-ware implementers is that the application should be security-aware, since this way it could dynamically tailor its security needs. A security-unaware application could not, for example, use different security parameters for different sockets, or adjust the security options depending on the applications it talks to. If security was transparent to the application, those parameters would have to be manually set by a system administrator to the highest security level that could be required by an application. That would incur a lot of unnecessary overhead. SSL has a number of shortcomings (bad random generator, no non-repudiation..), some of which might get fixed in future releases, but what makes it especially unattractive for this project is the alternate BSD socket calls needed to support it. If application recompilation were allowed, the compiler could be modified so as to replace the old socket calls with the new ones. Parameters needed for the calls could be passed to the compiler. If we are willing to give up the "no OS modification" requirement, which seems more reasonable than giving up application transparency, IPSec could provide user-oriented keying and probably (implementation dependent and some hacking required) application transparency. Giving up the OS requirement seems more reasonable for Solaris users, since future releases will probably come with IPSec included.

4.2 *Public Key Infrastructure*

Public key infrastructures (PKI) consist of supporting services that are needed if technologies based on public key cryptography are to be used on a wide scale. Certification authorities and related certification management facilities constitute the core of public key infrastructures. However, when we try to apply these certificate management concepts in real-world environments, especially environments involving highly diverse organizations and communities which need to work together in complex ways, many interesting and subtle issues arise. A range of other supporting infrastructural services of both a technological and legal nature, are also needed to effectively exploit public key technologies to their fullest potential.

To have an effective and efficient PKI, we need to understand the necessary operational requirements so that we may come up with a complementary design and implementation. However, the operational requirements are not merely technical in nature but must account for the legal, social, economic, security, and technological issues. These issues are highly interrelated and cannot be easily separated and treated independently.

4.2.1 What's Out There

There is an incredible amount of activity happening in the world concerning public key infrastructures:

- Many standards, either complementary or competing, are being created, implemented, or under review all around the world, particularly in the United States, Canada, Europe, and Australia.
- Many public key infrastructure prototypes are being implemented, primarily at the national government level in the United States, Canada, and Europe. Many of these governments are attempting to build the necessary infrastructure for government-wide secure communications, procurements, building access control, benefits transfer to their constituency, among many other government services.
- Many reports have been available or are now in progress discussing the legal and technological ramifications of public key infrastructures.
- There are several timely books discussing the legal, technological, and operational aspects of public key infrastructures.

We have attempted to provide an extensive listing of information pertinent to public key infrastructure. This section summarizes the results of our search for active work and publications on public key infrastructure.

Search Methods

To understand the current state of public key infrastructures, we performed both an intensive and extensive literature search to gather information on the ongoing research and development efforts in public key infrastructures.

The literature search consisted of the following techniques and methods to locate books, articles, reports, and web sites on PKI:

- SNL Technical Library search using their Horizon search program.
- On-line book search through the web sites of Barnes & Noble, Amazon, McGraw-Hill and Prentice Hall.
- Internet search using the following six major search engines — AltaVista, Yahoo, Excite, Infoseek, Lycos, and AOL NetFind.

The following sets of keywords were used:

1. "public key infrastructure"
2. "trusted third parties"
3. "cryptography"
4. "electronic commerce"
5.

The phrase, "electronic commerce" was also used as public key cryptography and public key infrastructures are considered by many a necessary and fundamental basis for electronic commerce.

Search Results

The technical library search turned up only three relevant as the library's book inventory is primarily limited to basic science and engineering textbooks and reports.

The on-line book search turned up hundreds of books but only the six books listed in the book reference contained any significant information on public key infrastructures. Reference 64 has yet to be published (expected out in November 1997) but was available as on-line "betabook" from McGraw-Hill's web site.

The combined efforts of the six Internet search engines using the above keyword phrases literally turned up thousands of sites. Performing the search was easy, the laborious manual browsing through the various sites for relevant information was the difficult part. In all, the number of relevant documents was narrowed down to less than a hundred. Many of

the web sites linked back to the same set of sites and/or documents. The final list of relevant web sites is provided in the next section.

The following paragraphs describe the significant PKI efforts that are in progress around the world and their related web sites and/or documents.

AT&T, "Security Software -- Public Key Infrastructure."

January 1997. <http://www.att.com/secure_software/pki/> (September 29, 1997).

AT&T describes their security solutions, in particular, an enhanced version of SecretAgent, their encryption and authentication software, working with Novell Directory Services. According to AT&T, the combination of the two products provides an effective, affordable alternative to purchasing an entirely new X.500-compliant directory system as part of an enterprise-wide Public Key Infrastructure.

Avellan, Juan. "Digital Signature Links."

June 1997. <http://www.qmw.ac.uk/~tl6345/index.htm> (September 29, 1997).

Juan Avellan, a researcher at the Information Technology Law Unit, Queen Mary and Westfield College, University of London developed this page as part of the work on the "Study on the Legal Aspects of Digital Signatures" being done for Directorate General XV of the European Commission.

Avellan, Juan. "Certification Authority Survey (DGXV Project)."

June 1997. <http://www.qmw.ac.uk/~tl6345/ca.htm> (September 29, 1997).

Another set of pages prepared by Juan Avellan. The links on this page are based on a survey of certification authorities, trusted third parties and other entities related to the use of digital or electronic signatures. The survey covers all continents except Antarctica. He also points to another set of CA URLs prepared by the German Research Network (DFN-PCA).

Branchaud, Marc. "Public Key Infrastructure References."

August 1997. <http://www.xcert.com/~marcnarc/PKI/References.htm> (September 29, 1997).

Marc Branchaud, now with Xcert Software, Inc., compiled an on-line bibliography in support of his thesis for his Computer Science Master's degree. It is very extensive and covers a broad range of topics (X.509, non-X.509, PKI issues, Internet RFC's and Drafts, papers, books, *etc.*).

CertCo. "E–Commerce 101."

June 1997. <http://www.certco.com/ecomm101/ecomm101.htm> (September 29, 1997).

This site is a short tutorial on electronic commerce, or in their parlance, E-Commerce.

As per CertCo:

"CertCo, the leader in trustworthy electronic commerce, combines technology and services to provide the infrastructure supporting the rapidly growing electronic commerce market. The company integrates its experience in cryptography, risk management, law, technology and banking, with its experienced management team, to deliver fast, cost effective and secure on-line transaction solutions. CertCo enables banks and other financial institutions to build a trustworthy infrastructure to support large-scale, international, secure electronic commerce..."

Community Research and Development Information Service. "INFOSEC: Description of the 8 studies starting January 1997."

July 1997. < http://www.cordis.lu/infosec/src/prep2.htm> (September 29, 1997).

CORDIS, the Community Research and Development Information Service, is a European Commission information service providing efficient access to complete information on EU research and exploitation possibilities. CORDIS is the information focal point for the EAGLE project. EAGLE is a joint European project tasked with studying the use and co-operation of Trusted Third Parties. It is funded by Directorate General Thirteen (DG XIII) of the European Commission, under their INFOSEC (information security) program and is scheduled to run during 1997.

The partners working on this project are:

- Telia Promotor, Sweden (Project leader)
- Deutsche Telekom, Germany
- France Telecom - CNET, France
- KPN Research, NL
- Racal Research, UK
- Vodafone, UK

Eight studies are in progress and are discussed in greater detail in the following paragraphs.

Community Research and Development Information Service. "INFOSEC: EUROTRUST — ETS."

July 1997. <http://www.cordis.lu/infosec/src/study7.htm> (September 29, 1997).

As quoted from the EUROTRUST - ETS web site:

Objectives and Scope

Baltimore Technologies Limited has been awarded a contract from the European Commission to operate a pilot Certification Authority (CA)/ Trusted Third Party service.
Certification Authorities issues digital certificates which "notarize" or certify that a user's public key belongs to that user. That public key can then be used to securely encrypt messages or data over an insecure network such as the Internet.
EuroTrust will allow full CA facilities to be accessible by a number of different methods. Using EuroTrust, systems such as E-mail, EDI, Web Browsers etc. can verify communications without user intervention. Individuals can issue requests to EuroTrust to certify their public keys interactively using any Web browser.

Community Research and Development Information Service. "INFOSEC page from DGXIII of the European Commission."

September 1997. <http://www.cordis.lu/infosec/home.html> (September 29, 1997).

This site is the INFOSEC page from DGXIII of the European Commission. It documents the results of activities which have been supported during the last four years. These activities range from the ITSEC recommendation to the implementation of pilots for Trusted Third Parties.

Community Research and Development Information Service. "INFOSEC: Design and Implementation of infrastructure for TTP."

July 1997. <http://www.cordis.lu/infosec/src/study8.htm> (September 29, 1997).

As quoted from the OSCAR web site:

Purpose and Scope

The work is split into three main bodies: Design study, Pilot, and Assessment. The design of the TTP infrastructure will be based on investigation of requirements involving users. The TTP specifications will be subject to a vigorous validation process.
The emphasis of the pilot is on certification in support of European Internal Market: how is it possible to certify business of users, to support secure messaging and any other communications services inside a country and across Europe.

Community Research and Development Information Service. "INFOSEC: EAGLE."

July 1997. <http://www.cordis.lu/infosec/src/study13.htm> (September 29, 1997).

EAGLE is a joint European project tasked with studying the use and co-operation of Trusted Third Parties. It is funded by Directorate General Thirteen (DG XIII) of the European Commission, under their INFOSEC (information security) program and is scheduled to run during 1997. This site summarizes the activities to support the EAGLE project. Sweden is the project leader.

Community Research and Development Information Service. "INFOSEC: Key Recovery in Secure Information Systems."

July 1997. < http://www.cordis.lu/infosec/src/study9.htm> (September 29, 1997).

As quoted from the KRISIS site:

Purpose and Scope

The project will try to define a key recovery scheme accepted by the commercial sector that also provides the means government agencies can use for controlled interception needed for law enforcement. Demonstrating such a scheme in 5 different European countries should help to define a scheme acceptable to all involved parties. The additional requirements determined in this project will be taken into account for new versions of the key recovery product used within the pilot. The project will also analyze the interoperability requirements when the schemes adapted to national regulations are used in international communication.

Community Research and Development Information Service. "INFOSEC: MANDATE II."

July 1997. <http://www.cordis.lu/infosec/src/study10.htm> (September 29. 1997).

As quoted from the MANDATE II web site:

Objectives and Scope:

There is an enormous benefit both to Banks and their customers if the traditional paper check and other negotiable instruments can be replaced by an electronic equivalent with the same functionality as its predecessor, while significantly more secure and at the same time more easily transferred and settled. In addition the burgeoning commercial use of the Internet is creating a significant demand for secure electronic payment methods, operable within the framework of Internet use.

Funded under the EC DGXIII ETS (Electronic Trusted Services) program, MANDATE uses a functionally Trusted Third Party to provide the confidence needed for a new electronic financial negotiable instrument. Designed as a generic solution to electronic negotiability, MANDATE will ultimately be built on tamper-resistant hardware, known as a DOC-carrier, and using public-key cryptography to provide the security required. The purpose of the hardware is to prohibit what is known as "double-spending", i.e. that the same electronic negotiable document is sold twice.

Community Research and Development Information Service. "INFOSEC: Operational & Architectural Aspects of TTPs for Europe."

July 1997. <http://www.cordis.lu/infosec/src/study6.htm> (September 29, 1997).

As quoted from the OPARATE web site:

Purpose and Scope

The aim of the project is to investigate operational and architectural aspects of TTP service provision. The project will concentrate in particular on the investigation of the following specific issues:

- how a TTP should be organized and operated in order to provide TTP services effectively;
- how different TTP systems may be combined or made to interwork together, and in particular:
  1. how an ES/TTP network may be extended to provide confidentiality/key recovery services
  2. how interworking may be achieved between heterogeneous TTP networks

Community Research and Development Information Service. "INFOSEC: Study on the legality of encrypted electronic messages, signed by digital signature and certificated by a TTP as proof of evidence in criminal litigations."

July 1997. <http://www.cordis.lu/infosec/src/study11.htm> (September 29, 1997).

As quoted from the AEQUITAS web site:

Purpose and Scope

In the progress of the study specifications will be done for:

- judicial and technological possibilities to ensure that encrypted messages be decrypted,
- the juridical rules to fulfil by a TTP

The study will establish on the experience made during one year by a public -experimental - TTP. This TTP will act as service of

certification of the established relations made by a group of lawyers, judges and prosecutors in their daily practice.
The study will be restricted by the geographic dimension of the experimence of the TTP. This will be in three European countries: France, Spain and Portugal. From the juridical perspective, the reflections will center the study on the legality of encrypted messages. Object of study will be also real cases occurred in other countries.

Community Research and Development Information Service. "INFOSEC: Trusted Third Party Services for Health Care in Europe."

July 1997. <http://www.cordis.lu/infosec/src/study12.htm> (September 29, 1997).

As quoted from the EUROMED ETS web site:

Scope-Objectives-Approach

As the number of telemedical applications over the World Wide Web (WWW) grows, security becomes an indispensable service for exploiting and utilizing these applications in real environments. Guidance on security issues in the health care sector is provided by various European projects (e.g. THIS, SEISMED, SESAME, TrustHealth, ISHTAR, etc.).
From the above projects it is derived that Trusted Third Party Services (TTPs) is the new approach to the security problems facing the open systems and the complex infrastructure of health care. Establishment of TTPs ensuring that all health care actors can communicate in a secure way is among the tasks of many of these projects.

The first objective of this proposal is using the experts' experiences and findings to identify, define and verify operational, technical, regulatory and legal aspects of the TTPs for telemedical applications over the WWW. The second objective is to implement the above adjusted findings in EUROMED's configuration, which is a telemedical application over the WWW, with regards to effectiveness, economics and acceptability.

EUROMED is a European Commission DG III/B pilot project. Its aim is to collaboratively exploit, combine and support HPCN activities to enhance and standardize visualization techniques to be used in telemedicine applications throughout Europe.

This project compliments EUROMED by concentrating on, and tackling, the issues of security in a telemedical information society supporting regional development.

Ellison, Carl M. "Establishing Identity Without Certification Authorities." July 1996.

<http://www.clark.net/pub/cme/usenix.html> (September 29, 1997).

This paper was presented at the 6th USENIX Security Symposium, in San Jose, July 22-25, 1996 by Carl M. Ellison of CyberCash, Inc. The thrust of his paper is the binding of identities to a pair of public keys without using certificates issued by a trusted CA.

As quoted from the Introduction:

It is commonly assumed that if one wants to be sure a public key belongs to the person he hopes it does, he must use an identity certificate issued by a trusted Certification Authority (CA). The thesis of this paper is that a traditional identity certificate is neither necessary nor sufficient for this purpose. It is especially useless if the two parties concerned did not have the foresight to obtain such certificates before desiring to open a secure channel. There are many methods for establishing identity without using certificates from trusted certification authorities. The relationship between verifier and subject guides the choice of method. Many of these relationships have easy, straight-forward methods for binding a public key to an identity, using a broadcast channel or 1:1 meetings, but one relationship makes it especially difficult. That relationship is one with an old friend with whom you had lost touch but who appears now to be available on the net. You make contact and share a few exchanges which suggest to you that this is, indeed, your old friend. Then you want to form a secure channel in order to carry on a more extensive conversation in private. This case is subject to the man-in-the-middle attack. For this case, a protocol is presented which binds a pair of identities to a pair of public keys without using any certificates issued by a trusted CA.

The apparent direct conflict between conventional wisdom and the thesis of this paper lies in the definition of the word "identity" -- a word which is commonly left undefined in discussions of certification.

Entrust Technologies. "Resource Library: White Papers."

September 1997. <http://www.entrust.com/library.htm> (September 29, 1997).

This site points to a large source of white papers from Entrust Technologies. In particular, the paper, "The Scalability of Public Key Infrastructures, " by Dr. Tim Moses is noteworthy. The report abstract is as follows:

Abstract

Public Key Infrastructures are required to serve very large communities of users, and the standards that apply in this area have been developed with this in mind. However, individual components of a PKI contain finite resources. Therefore, the size of community that they can serve will, inevitably, be limited. In this paper we explore this limit and derive quantitative values applicable to a representative implementation architecture which is based upon a two-tier communications architecture. We discover that the limit for this architecture is imposed by the finite computational resource of the Certification Authority, and is on the order of one million users per physical instance of the Certification Authority. A larger scale can be achieved by using multiple Certification Authorities in an appropriate trust relationship.

Froomkin, A. Michael, "The Essential Role of Trusted Third Parties in Electronic Commerce."

University of Miami School of Law, October 1996. <http://www.law.miami.edu/~froomkin/articles/trusted.htm> (September 29, 1997).

"This Article aims to describe what CAs do, explain why they are important to electronic commerce, and suggest that they are likely to provoke some interesting legal problems. It does not attempt to describe a complete legal regime for the regulation of CAs in electronic commerce.{4} The coming wave of faceless electronic commerce presents a number of challenges; opportunities for fraud and error and for the prevention of fraud and error are interwoven with the solutions to these difficulties. Although accounts of fraud in commercial electronic transactions (as opposed to simple theft of data or services by a stranger) on the Internet remain very rare, this may reflect the low level of Internet commerce today more than any virtues of the medium.{5}"

General Services Administration. "Federal Security Infrastructure."

April 1997. <http://www.gsa.gov/fsi/default.htm> (September 29, 1997).

"On September 7, 1993, Vice President Al Gore issued the Re-engineering Through Information Technology National Performance Review. In this report the need for a Secure Information Infrastructure was stressed. The FSI Program was chartered in April 1995, on the recommendation of the National Information Infrastructure Task Force and the Government Information Technology Services Working Group. The FSI Program will coordinate, operationally oversee, monitor, implement, and report on the development of an information

security infrastructure to support electronic commerce, electronic messaging, other applications and support services to users."

General Services Administration. "The Paperless Federal Transactions for the Public Project."

February 1997. <http://www.gsa.gov/fsi/paprles.htm> (September 29, 1997).

"This project, based on Vice President Gore's vision, establishes a Federal Public Key Infrastructure pilot initially focused on World Wide Web technology. The developed security infrastructure will permit Federal agencies to deploy World Wide Web applications accessible to the public using standard security services (identification, authentication, access control, integrity, confidentiality, and non-repudiation.)"

Gerck, Ed. "Overview of Certification Systems: X.509, CA, PGP and SKIP."

July 1997. <http://novaware.cps.softex.br/mcg/cert.htm> (September 29, 1997).

Abstract

Cryptography and certification are considered necessary Internet features and must be used together. This paper deals with certification issues and reviews the three most common methods in use today, which are based on X.509 Certificates and Certification Authorities, PGP and, SKIP. It concludes that none of these methods are adequate, because they are partially incoherent within their own basic assumptions, may give a false impression of a high level of security and, worse, the user — who is at risk — has no firm ground on which he can base his decision of trust. The implicit assumption of this conclusion has led governments to try to establish restrictive Internet regulations on certification, such as TTP, which actions have raised questions on international jurisdiction, privacy rights and other issues. This paper argues that the conflict is in its essence based on the single fact that all three methods need centralized certification control — whereas the Internet is not centralized. The solution would be to construct a decentralized certification method — a par with the Internet architecture — which could: (i) guarantee certification with an arbitrary degree of safety, (ii) interoperate with current standards or be used by itself and, (iii) legally avoid the issues of TTPs and key escrow. A specification of a suitable solution, tentatively called the Meta-Certificate, is being drafted by an open non-profit international group, the MCG, which invites participation from the Internet community. The main motivation for this paper, besides a comparative

review of the three chosen methods, is to serve as a basis for the evaluation of Meta-Certificates vis-a-vis the other solutions available in the market.

GMD – TKT.SIT. "Interworking Public Key Certification Infrastructure for Europe."

June 1996. <http://www.darmstadt.gmd.de/ice-tel/> (September 29, 1997).

As quoted from the ICE-TEL web page:
ICE-TEL is funded by the TELEMATICS for Research Initiative within the European TELEMATICS APPLICATIONS Programme and is supported by the SCIMITAR project of TERENA. The CONCORD project provides a directory to the Telematics Applications Programme. EuroDemo aims at providing a demonstration facility in Brussels.

Project Objectives, Summary Description and Anticipated Results

The aim of the ICE-TEL project is to offer solutions to the problem of security on the Internet as used by industrial and academic research. This will be achieved by support for the usage of secured applications where users need to be certified, by providing a large scale public key certification infrastructure in a number of European countries and by providing all the necessary technology components which allow the deployment. In particular, the project will:

- Develop and deploy the necessary tools for both the provision of the **security infrastructure** and the **support of users** of the infrastructure for a variety of platforms (Unix, PC, Macintosh),
- Develop and deploy **security toolkits** which allow to integrate **public key based** security services into virtually any application, and which make use of the security infrastructure,
- Develop and deploy security enabled **user services** which immediately allow to use the certification infrastructure without further application integration,
- Support the integration of security services into applications, and provide **secure testbeds** for applications.

Government of Canada, Communications Security Establishment. "Government of Canada Public Key Infrastructure."

August 1997. <http://www.cse-cst.gc.ca/cse/english/gov.html> (September 29, 1997).

The Communications Security Establishment (CSE) is a federal government lead agency that delivers Information Technology

Security (ITS) solutions to the government of Canada. Its web site describes the Government of Canada's effort in a federal-wide public key infrastructure.
As quoted from the GOC Public Key Infrastructure web site:
The Government of Canada Public Key Infrastructure (PKI) will allow the federal government to:

- provide more efficient delivery of services to Canadians;
- provide electronic commerce and confidentiality services to public servants; and
- better protect privacy of information used in Government business.

Government of Canada, Dobranski, Lawrence. "The Government of Canada's Public Key Infrastructure."

May 1997. <http://www.governmentsource.com/focus5.3/08Cse.html> (September 29, 1997).

Lawrence G. Dobranski is the Manager, ITS Industrial Programs, Standards and Initiatives at the Communications Security Establishment. He presents what appears to be a report on the GOC's federal PKI.

Government of Canada. "CAR ITS Strategy."

July 1997. <http://www.cse.dnd.ca/cse/english/car.html> (September 29, 1997).

This site represents a snapshot on the PKI efforts of the Government of Canada. This site presents the Final Report of the Information Technology Security (ITS) Strategy Steering Committee as submitted to the Council for Administrative Renewal (CAR), February 1996, in part:
"provide the business rationale for investing in the component parts of the IT Security Framework, including Advanced Card Technology, Electronic Authorization and Authentication, Confidentiality and Privacy, Firewall and Gateways, as well as a *Government Public Key Infrastructure* already approved by Treasury Board;..."

Grant, Gail. Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks.

The McGraw-Hill Companies. November 1997. <http://www.betabooks.mcgraw-hill.com/grant/> (September 29, 1997).

As quoted from the preface of the "betabook" available from the web site:
Preface:

Digital Signatures are one of the most difficult technologies for anyone to understand, whether or not they have a technical computer background. For the businessperson, this is especially daunting, since some of the words that are used to describe this technology - keys, certificates, signatures - are different enough from their physical counterparts to make grasping the subject even more difficult. Add to the mix unfamiliar terms like asymmetric cryptographic methods, key pairs and message digests, then stir in the infrastructure necessary to make it all work and you have a great recipe for confusion.

Yet understanding is critical, because the dream applications possible over the Internet require strong authentication and privacy. While the executive who signs the purchase order for "certification authority" services or products doesn't need to know all the algorithms involved, they do need to understand how it works in broad terms and the implications for their business. They need to understand the issues involved in committing to this technology and how they can mitigate the risks and reap the rewards.

If digital signatures are so complex, why not use something simpler? Because using simpler technology means either increased overhead or additional risk. Nothing else available today is robust enough for broad scale usage.

If you want to have confidence that the person sending you an order for a million widgets isn't a hormone-driven hacker getting their latest thrill, you need digital signatures and certificates or "digital ID's" that vouch for that person or corporation's identity.

Understanding digital signatures requires big thinking, but it can be done in small digestible bites. This book is an attempt to carve digital signatures -- and the infrastructure that is needed to truly trust them -- down to a manageable portions that any business executive can digest.

Organization

This book is divided into five parts. Each section builds upon the topics discussed in previous sections, but has been written to allow the more advanced reader to skip over known material to the sections most pertinent to them. The first part defines the problem space and the technology used to solve the problem. The second part explains how companies are using or plan to use the technology. The third explains the issues from a business, legal and technical standpoint. Part IV enumerates the companies offering products that implement the technology and the final section looks at some of the future possibilities of usage.

IBM. "IBM Registry and World Registry."

1997. <http://www.internet.ibm.com/commercepoint/registry/index.html> (September 29, 1997).

World Registry and IBM Registry are IBM's digital certificate and the public key infrastructure products. PKI provides digital authentication, digital signatures, and security functions for global application over the Internet and other networks.

INESC. "INESC ICE-TEL page."

March 1997.
<http://www.di.fc.ul.pt/departs/informatica/investigacao/projectos/ice/> (September 29, 1997).

Instituto de Engenharia de Sistemas e Computadores (INESC) of Portugal is one of the participants in ICE-TEL project and this is their home page.
As quoted from the web site:
The aim of the ICE-TEL project is to provide a large scale public key certification infrastructure in a number of European countries for the use of public key based security services, and to provide all technology components which allow the deployment of user tools and applications with a common integrated public key security technology. The participants are coming from all over Europe.
The work in the project is divided into different work-packages (WP). INESC will contribute in the following:

- WP2: activity with external groups
- WP3: architecture and general specifications of the public key infrastructure

  National Security Regulations - template (draft)

  National Security Regulations and the Use of Cryptography for Trans-border Communication
- WP6: secured document tools
- WP11: CA service provision and security support

  Certification Authority of Universidade de Lisboa
- WP12: secure communication of the CERTs

Information Resource Engineering. "Cipher College 103."

June 1997. <http://www.ire.com/CYPHER/CC_103.HTM> (September 29, 1997).

Information resource Engineering, Inc. has prepared this a site as an on-line tutorial on Internet Virtual Private Networks Key

Management: Essentials, Methods and Public Key Standards. The goals of the tutorial are to:

- Discuss the importance of key management
- Describe types of key management - secret key and public key
- Provide an update on the status of public key standards for Internet Virtual Private Networks
- Outline considerations in selecting a key management approach for VPNs

Internet Engineering Task Force. "Public-Key Infrastructure (X.509) (pkix) Charter."

September 1997. <http://www.ietf.org/html.charters/pkix-charter.html> (September 29, 1997).

The task of the PKIX Working Group is to develop Internet standards needed to support an X.509-based PKI. The goal of this PKI will be to facilitate the use of X.509 certificates in multiple applications which make use of the Internet and to promote interoperability between different implementations choosing to make use of X.509 certificates. The resulting PKI is intended to provide a framework which will support a range of trust/hierarchy environments and a range of usage environments (RFC1422 is an example of one such model).

Internet Engineering Task Force. "Public-Key Infrastructure (X.509) (pkix)."

September 1997. <http://www.ietf.org/ids.by.wg/pkix.html> (September 29, 1997).

Internet-Drafts on Public Key Infrastructures based on X.509 prepared by the PKIX working group.

Internet Engineering Task Force. "Simple Public Key Infrastructure (spki) Charter."

September 1997. <http://www.ietf.org/html.charters/spki-charter.html> (September 29, 1997).

The task of the SPKI Working Group is to develop Internet standards for an IETF sponsored public key certificate format, associated signature and other formats, and key acquisition protocols. The key certificate format and associated protocols are to be simple to understand, implement, and use. For purposes of the working group, the resulting formats and protocols are to be known as the Simple Public Key Infrastructure, or SPKI.

Internet Engineering Task Force. "Simple Public Key Infrastructure (spki)." September 1997. <http://www.ietf.org/ids.by.wg/spki.html> (September 29, 1997).

Internet-Drafts on the Simple Public Key Infrastructure not based on X.509 prepared by the SPKI working group.

Jozef Stefan Institute, "IJS ICE-TEL page." May 1997. <http://www.e5.ijs.si/security/ice/ice.html> (September 29, 1997).

Another European participant in the ICE-TEL project. As quoted from their web-site:

Objectives

The aim of the ICE-TEL project is to provide a large scale public key certification infrastructure in a number of European countries for the use of public key based security services, and to provide all technology components which allow the deployment of user tools and applications with a common integrated public key security technology. In particular, partners in this project will

- develop and deploy the necessary tools for both provision of the infrastructure and the support of users of the infrastructure for a variety of platforms (Unix, PC, Mac),
- develop and deploy security toolkits which allow to integrate public key based security services into virtually any application, and which make use of the security infrastructure,
- develop and deploy user tools (secured e-mail, secured WWW clients, secured X.500 DUAs) which immediately allow to use the certification infrastructure without further application integration
- support the integration of security services into applications, and provide test beds for applications.

Our Contribution

The work in the project is divided into different work-packages. Jozef Stefan Institute will contribute in the following:

- architecture and general specifications of the public key infrastructure
- CA tool development
- secured document tools
- CA service provision and security support
    - SI-CA - Slovenian Policy Certification Authority
- secure communication of the CERTs

Kelm, Stefan. "Comprehensive list of Public Key Infrastructure (PKI) links."
September 1997. <http://www.pca.dfn.de/eng/team/ske/pem-dok.html> (September 29, 1997).

Kelm, Stefan. "PKI related internet drafts."
September 1997. <http://www.pca.dfn.de/eng/team/ske/drafts/> (September 29, 1997).

As quoted from the German Research Network (DFN) site on documents about Email Security and PKI:
"Stefan studied computer science at Hamburg University. In 1995, he finished his diploma thesis that describes secure communications via PEM and PGP within the (insecure) Internet. The focus of his thesis is on the applications used by the German Computer Emergency Response Team (DFN-CERT).
In January 1996 Stefan has become a member of the new research *project A Policy Certification Authority (PCA)* for the German Research Network (DFN)."

Keywitness Canada. "Welcome to Keywitness Canada."
July 1997. <http://www.keywitness.ca/english/keywitness.htm> (September 29, 1997).

Keywitness Canada is a Canadian commercial firm that provides the services of a CA.

Long, J. P. "Public / Private Key Certification Authority and Key Distribution — A White Paper."
September 1995. <http://www-irn.sandia.gov/organization/div4000/ctr4600/dpt4621/ppkeycert/encwhtt.html#I> (September 29, 1997).

This paper exists in the SNL Internal Restricted Network and therefore is only available if you have access to it. As quoted from the Introduction of the web-based report:
"Traditional encryption, which protects messages from prying eyes, has been used for many decades. Our concepts of encryption are built from that heritage. Utilization of modern software-based encryption techniques implies much more than simply converting files to an unreadable form. Ubiquitous use of computers and advances in encryption technology coupled with the use of wide-area networking completely changed the reasons for utilizing encryption technology. The technology demands a new and extensive infrastructure to support these functions. Full understanding of these functions, their utility and value, and the need for an infrastructure, takes extensive exposure to

the new paradigm. This paper addresses issues surrounding the establishment and operation of a key management system (i.e., certification authority) that is essential to the successful implementation and wide-spread use of encryption."

Masse, David G. and Andrew D. Fernandes. "Economic Modelling And Risk Management In Public Key Infrastructures — The Business Case for A Broadly-based Highly Scalable Public Key Infrastructure."

Chait Amyot Virtual Library. January 31, 1997. <http://www.chait-amyot.ca/docs/pki.html> (September 29, 1997).

As quoted from the start of the web version of the report: "This is version 3.0 of this paper. This revision of April 15, 1997 updates references to the German Digital Signature Act in note 80. This paper was presented at the 1997 RSA Data Security Inc. annual symposium. The authors eventually intend to submit this paper for law review publication and they welcome the reader's comments. This paper was available before presentation and will remain available at least until law review publication on the Chait Amyot Web site at http://www.Chait-Amyot.ca and will be continually updated to reflect the comments the authors receive. Persons providing comments are kindly asked to refer both to the version number of the paper and to the paragraph number to which the comment pertains."

McConnel, Bruce W. and Edward J. Appel. "Draft Paper, 'Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure.'"

May 1996. <http://www.isse.gmu.edu/students/pfarrell/nist/kmi.html> (September 29, 1997).

This site presents, as a public service, a draft report that is distributed by NIST and is described by the following cover letter:

SUBJECT: Draft Paper, "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure"

FROM: Bruce W. McConnell [Initials]

Edward J. Appel [Initials]

Co-Chairs, Interagency Working Group on Cryptography Policy

Attached for your review and comment is a draft paper entitled "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure." It presents a vision and course of action for developing a cryptographic infrastructure that will protect valuable information on national and international networks.

The draft paper is the result of the many discussions we have had with interested parties concerning the use of encryption.

While those discussions have explored the use of both key recoverable encryption and non-recoverable encryption, the draft paper addresses an infrastructure which uses key recoverable encryption.

We believe such a key management infrastructure, voluntary and supported by *private sector* key management organizations, is the prospect of the near future. It would permit users and manufacturers free choice of encryption algorithm, facilitate international interoperability, preserve law enforcement access, and, most importantly, provide strong system security and integrity.

Recognizing that a robust infrastructure is not yet a reality, we are also considering measures to liberalize export policy for some non-escrowed products. Appendix II of the draft paper begins to summarize current policy, and we intend to expand and improve that section.

We believe that clearly articulating such a vision will accelerate the ability of the United States to realize the full advantages of the global network for commerce, security and public safety. However, such a vision cannot become a reality unless it is widely shared. Therefore, rather than being a finished product, the attached paper is a draft which we ask you to help us improve. We hope it will contribute to constructive discussion and promote a clearer understanding of each others' needs and concerns regarding the use of encryption.

We welcome your comments and look forward to further discussion. Written comments may be sent to our attention, Room 10236, NEOB, Washington, D.C. 20503.

Mestré, Patrick. "Patrick Mestré Page."

August 1997. <http://www.dice.ucl.ac.be/~mestre/pme.htm> (September 29, 1997).

Mestré, Patrick. "PKI References."

August 1997. <http://www.dice.ucl.ac.be/~mestre/index_2.htm> (September 29, 1997).

Patrick Mestré is working for the Belgacom project ASTRA, relating to Certification Authorities. He has collected information on the topic at his web site in support of his research for the Microelectronics Laboratory of the Catholic University of Louvain.

National Information Infrastructure Security Issues Forum. "NII Security: The Federal Role."

June 1995. <http://www.sevenlocks.com/NIISecurityTheFederalRole.htm> (September 29, 1997).

The Information Infrastructure Task Force's (IITF) National Information Infrastructure Security Issues Forum released for public comment a draft report, "NII Security: The Federal Role." The draft report summarizes the Forum's findings concerning security needs in the National Information Infrastructure (NII), presents an analysis of the institutional, legal, and technical issues surrounding security in the NII; and proposes Federal actions to address these issues.

National Institute of Standards and Technology. "PKI Technical Working Group (PKI-TWG)."

September 1997. <http://csrc.ncsl.nist.gov/pki/twg/twgindex.html> (September 29, 1997).

The PKI-TWG is an open group focusing on technical obstacles to implementation and use of public key infrastructures by government agencies. NIST chairs the TWG, which is composed of technical representatives from Federal agencies and industry. Active since October 1994, the TWG has developed initial versions of a requirements document, a concept of operations, a technical security policy, an X509 v3 certificate profile, and an interoperability report. These documents are available at the site.

National Institute of Standards and Technology, "Public Key Infrastructure."

September 1997. <http://csrc.ncsl.nist.gov/pki/> (September 29, 1997).

The National Institute of Standards and Technology (NIST) is taking a leadership role in the development of a Federal Public Key Infrastructure that supports digital signatures and other public key-enabled security services. In doing this, NIST is coordinating with industry and technical groups developing PKI technology such as the Federal PKI Steering Committee and its Technical Working Group (TWG), CommerceNet, Internet's PKIX, and the Open Group. NIST chairs the TWG, which is composed of technical representatives from Federal agencies and industry. Active since October 1994, the TWG has developed initial versions of a requirements document, a concept of operations, a technical security policy, an X509 v3 certificate profile, and an interoperability report. These documents are available below. NIST is represented in the Federal PKI Steering Committee chaired by the Government Information

Technology Services (GITS) IT10.03 and maintains contact with the Federal PKI Business Working Group.
In addition to work within the TWG, NIST has several laboratory-based activities. The first activity is developing a Minimum Interoperability Specification for PKI Components (MISPC). This activity involved industry participants through Cooperative Research and Development Agreements (CRADAs). During this activity the NIST PKI Team (1) exercised implementations of PKI components provided by CRADA participants and examining their features, (2) identified a minimum set of desirable features, and (3) drafted the specification. Industry participants had a review period to examine the draft specification and comment on its feasibility. The PKI Team evaluated the comments received, made appropriate changes. and released a draft for public comment. Additional laboratory activities include the development of a Reference Implementation and the initial implementation of a root Certification Authority (CA) for the Federal PKI. The purpose of the Reference Implementation is to have a proof of concept for the MISPC that will be available for testing of commercial implementations. The Reference Implementation need not be as efficient and robust as an operational system but it must be well-behaved and function correctly. The initial implementation of a root CA involves the development of a procurement specification for a CA based on the MISPC and the procurement of an operational CA. The purpose of this root CA is to examine hierarchical and non-hierarchical CA relationships, scalability, and other operational issues. In addition, the minimum interoperability specification will be available to companies and to Government agencies developing their own procurement specifications for PKI components and/or services.
NIST envisions a follow on activity that will develop a test suite for conformance to the MISPC. The test suite may be used in establishing an interoperability validation service for PKI components. Although many details regarding this service remain to be defined, it is likely that independent commercial entities would be accredited to perform the tests.

Network Working Group. "RFC 1422."

February 1993. <http://sunsite.auc.dk/RFC/rfc/rfc1422.html> (September 29, 1997).

As quoted from the Request for Comments 1422:

Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management
1. Executive Summary
This is one of a series of documents defining privacy enhancement mechanisms for electronic mail transferred using Internet mail protocols. RFC 1421 [6] prescribes protocol extensions and processing procedures for RFC-822 mail messages, given that suitable cryptographic keys are held by originators and recipients as a necessary precondition. RFC 1423 [7] specifies algorithms, modes and associated identifiers for use in processing privacy-enhanced messages, as called for in RFC 1421 and this document. This document defines a supporting key management architecture and infrastructure, based on public-key certificate techniques, to provide keying information to message originators and recipients. RFC 1424 [8] provides additional specifications for services in conjunction with the key management infrastructure described herein.
The key management architecture described in this document is compatible with the authentication framework described in CCITT 1988 procedures and conventions for a key management infrastructure for use with Privacy Enhanced Mail (PEM) and with other protocols, from both the TCP/IP and OSI suites, in the future...

Network Working Group. "RFC 1424."

February 1993. <http://sunsite.auc.dk/RFC/rfc/rfc1424.html> (September 29, 1997).

As quoted from the Request for Comments 1424:
Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services
1. Executive Summary
This document describes three types of service in support of Internet Privacy-Enhanced Mail (PEM) [1-3]: key certification, certificate-revocation list (CRL) storage, and CRL retrieval. Such services are among those required of an RFC 1422 [2] certification authority. Other services such as certificate revocation and certificate retrieval are left to the certification authority to define, although they may be based on the services described in this document.
Each service involves an electronic-mail request and an electronic-mail reply. The request is either an RFC 1421 [1] privacy-enhanced message or a message with a new syntax defined in this document. The new syntax follows the general RFC 1421 syntax but has a different process type, thereby

distinguishing it from ordinary privacy-enhanced messages. The reply is either an RFC 1421 privacy-enhanced message, or an ordinary unstructured message.
Replies that are privacy-enhanced messages can be processed like any other privacy-enhanced message, so that the new certificate or the retrieved CRLs can be inserted into the requestor's database during normal privacy-enhanced mail processing.
Certification authorities may also require non-electronic forms of request and may return non-electronic replies. It is expected that descriptions of such forms, which are outside the scope of this document, will be available through a certification authority's "information" service.

Open Group. "Open Group -... at a glance."

1997. <http://www.rdg.opengroup.org/press/glance.htm> (September 29, 1997).

As quoted from their web site:
Dedicated to the advancement of multi-vendor information systems, The Open Group is an international consortium of vendors, ISVs and end-user customers from industry, government, and academia.
Mission
To enable customer choice in the implementation of multi-vendor information systems.
Founded
The Open Group was formed in February, 1996 by the consolidation of the two leading open systems consortia, X/Open Company Ltd. (X/Open) and the Open Software Foundation (OSF). Under the Open Group umbrella, OSF and X/Open work together to deliver technology innovations and wide-scale adoption of open systems specifications.
OSF
Founded in 1988, OSF hosts industry-wide, collaborative, software research and development for the distributed computing environment.
X/Open
Founded in 1984, X/Open's brand mark is recognized worldwide as a guarantee of compliance to open systems specifications.

Open Group. "Public Key Infrastructure."

1997. <http://www.rdg.opengroup.org/public/tech/security/pki/index.htm> (September 29, 1997).

As quoted from their web site:

"A robust, flexible, standard, and open Public-Key Infrastructure Architecture is critical to the success of secure systems based on Public-Key technology.
The Open Group have begun to work with experts in other organizations, (IETF, CommerceNet, European Commission funded projects, etc.), to define a common architecture for a public key infrastructure. This will make use of existing standards in The Open Group and the IETF for instance, and will identify gaps in the infrastructure that need to be filled. The Open Group also intends to work with other organizations to encourage early commercial implementations and pilot trials."

Open Group. "Architecture for Public-Key Infrastructure (APKI)."
May 1997. <http://www.rdg.opengroup.org/public/tech/security/pki/apki_1-0.pdf> (September 29, 1997).

This is a key report that was published by the Open Group in support of their PKI efforts. A synopsis of the document is provided by the following excerpt from the report:

This Document

This document is a Guide (see above).

- Chapter 1 describes the requirements on a Public-Key Infrastructure.
- Chapter 2 presents the high-level structure of the PKI Architecture by grouping the architecture's components into broad functional categories.
- Chapter 3 on page 111
  - enumerates the components in each of the Architecture's functional categories
  - describes the functionality of each component and lists existing specifications which could serve as candidate standards for each component's interfaces and protocols (To be considered a "candidate" for purposes of the public-key infrastructure architecture, an interface or protocol must:
    1. be described by a publicly-available specification, and
    2. support a significant fraction of the functionality of the PKI component for which it is proposed as a candidate.

  It is assumed that the candidate interface and protocol specifications identified in this document will serve as base documents for open standardization processes, which will produce finalized PKI component interface and protocol specifications.)

- identifies where negotiation facilities are required to deal with the probable existence of a
- multiplicity of security mechanisms enumerates important public-key-related protocols and discusses the need for environment-specific profiles

- Chapter 4 discusses the use of hardware security devices in the architecture.
- A glossary and index are provided.
- The Open Group PKI TG continues to refine and extend these requirements; comments should be sent by electronic mail to pki-tg@opengroup.org.

Open Group. "Latest proposals for an HMG PKI."

1997. <http://www.rdg.opengroup.org/public/tech/security/pki/cki/index.htm> (September 29, 1997).

This site contains the latest proposals for an HMG PKI submitted by the Communications Electronic Security Group (CESG). HMG is Her Majesty's Government for the United Kingdom.

PKI.org. "PKI Clearinghouse."

September 1997. <http://www.pki.org/home.html> (September 29, 1997).

A fledgling site that is attempting to be the ultimate source and clearinghouse for all PKI-related information and activities.

Politecnico di Torino. "ICE-TEL Italian PCA Policy."

July 1997. <http://www.polito.it/ice-tel/pca-it/policy/> (September 29, 1997).

This site constitutes the ICE-TEL Italian PCA policy and describes the procedures and the requirements of its operations. It is tailored to Phase I of the ICE-TEL Project.

Povey, Dean. "PKI resources."

July 1997. <http://www.dstc.qut.edu.au/MSU/projects/pki/index.html> (September 29, 1997).

This site provides an extensive set of links to PKI-related sites compiled by the Distributed Systems Technology Centre (DSTC).

DSTC has recently completed the design and implementation of a Public Key Infrastructure and is documented in the report, "Design Issues in a PKI." This paper presents the issues identified from the implementation of this prototype and discusses some of the design options available.

The Distributed Systems Technology Centre is a joint venture supported by the Australian Government's Cooperative Research Centres Program and over 25 participating organizations developing the technological infrastructure for tomorrow's global distributed systems. DSTC also hosts part of the Research Data Network CRC.

Sandy Bay Software, Inc. "PKI — PC Webopaedia Definition and Links." August 1997. <http://www.pcwebopaedia.com/PKI.htm> (September 29, 1997).

The PC Webopaedia is an Internet resource that acts as an on-line encyclopaedia on computer-related subjects. It provided a concise definition for PKI and several links to very useful PKI-related web sites.

TeleTrusT Sweden. "Welcome to TeleTrusT Sweden." June 1997. <http://www.teletrust.se/defaulte.htm> (September 29, 1997).

As quoted from their report **CA–Policies in practical use**:
The Swedish TeleTrusT Association, founded in 1987, has during its lifetime managed to run a number of projects in order to enhance the understanding and implementation of digital documents produced with the help of digital signatures. There are two documents written in Swedish which explain the basic ideas. The name of the documents are **TeleTrusT-konceptet (1993)** and **Utgivning och hantering av nyckelbärande kort (1994)** This means in English The TeleTrusT Concept and The issue and administration of keys in smart cards. In the latter there is an Appendix D in English: **Issuing of cards - an example.** The document in front of you **CA-policies in practical use** (English version) is the latest contribution in the area. Together with the earlier mentioned documents, this form a trilogy which explains the ideas behind TeleTrusT - from idea to practical use. This process was important for the Swedish debate which has formed the basic input to i e the public investigation of the Department of Justice (SOU 1996:40) aiming at the introduction of legal acceptance of digital documents in public agencies. Always emphasized by TeleTrusT, solutions must build on equal parts of *social acceptance, legislation and good technical implementations.*
The document **CA-policies in practical use** is also formally given to the non-profit making organization SEIS (Secured Electronic Information in Society). To achieve the most efficient way to introduce the use of basic security services, The Swedish

TeleTrusT Association has decided to fulfil its task in co-operation with the SEIS organization.

University College London. "UCL ICE-TEL Project."

September 1997. <http://www.cs.ucl.ac.uk/research/ice-tel/> (September 29, 1997).

University College London is involved in the ICE-TEL project and is setting up and running the UK Academic Policy Certification Authority.

"UCL is contributing the latest version of the OSISEC X.509 toolkit and secure applications to the ICE-TEL project. A preliminary 'zero release' for project partners has now been made, with a general release in the middle of the year."

Verisign, Inc.. "VeriSign."

September 1997. <http://www.verisign.com/> (September 29, 1997).

As quoted from their web site:

Founded by RSA Data Security and other industry leaders, VeriSign is the only company focused entirely on digital authentication products and services. VeriSign Digital IDs use today's strongest cryptographic techniques to provide a reliable means of authenticating the identity of each party in an electronic transaction. VeriSign follows strict verification and security protocols-as outlined in its Certificate Practices Statement (CPS)-for every Digital ID it issues. To ensure the integrity of the Digital IDs it issues, VeriSign's facility features state-of-the-art security systems, including multi-level physical access controls, biometric scanners, infrared monitors, and the latest firewall technology. (For more information on VeriSign's security practices, consult the VeriSign CPS, section 3, at www.verisign.com/repository/cps.)

The Internet is rapidly gaining acceptance as a marketing and distribution medium for a wide variety of businesses. It provides an inexpensive and ubiquitous platform for conducting commerce, enabling both business-to-business and consumer exchange of goods, services, and information. Increasingly, organizations are turning to the Internet as a way to reduce costs, extend their reach, and develop a competitive edge. However, security remains the primary inhibitor to electronic commerce on the Internet-the ability to send and receive secure data is a fundamental requirement. A mechanism is needed that prevents unauthorized access to the information exchanged with users, such as credit card and account information. Furthermore, in this "faceless" environment, a business or

organization needs a way to establish its identity and credibility to protect itself and its customers from impostors. VeriSign's Server Digital IDs address both of these needs. Server Digital IDs enable companies and organizations to:

- Establish secure sessions with site visitors. These private communications sessions cannot be penetrated by external parties, protecting sensitive information from unauthorized access.
- Establish the authenticity of the website. Site visitors can verify the site's Digital ID and be assured that VeriSign has established the company or organization's identity.

Digital certificates such as VeriSign's Digital IDs are the standard for server authentication. Over 16,000 commercial sites are using VeriSign Server Digital IDs to create secure communication channels with customers.

Xcert Software Inc. "Xcert Software Inc."

September 1997. <http://www.xcert.com/> (September 29, 1997).

"Xcert provides Public Key Infrastructure (PKI) for IT managers, Fortune 500 corporations and independent software vendors."

Zimmermann, Philip. "PGP User's Guide, Volume I: Essential Topics —How to protect public keys from tampering."

May 1996. <http://www.chemistry.mcmaster.ca/pgp/pgpdoc1/how-to-protext-pk-from-tamp.html#0> (September 29, 1997).

Excerpts from Zimmerman's PGP user Guide as to how to protect public keys from tampering to ensure authenticity.

4.2.2 Where do the Standards Fall Short

The many PKI-related standards that are out and available all discuss either specific implementations or specific issues dealing with PKIs. However, the literature search did not find any comprehensive standard that provided a full discussion on the complex enterprise aspects of a PKI that could be customized for a specific environment or business need.

4.2.3 What Needs to be Implemented

Though there is a great deal of material on public key infrastructures, there is no one comprehensive source that covers all of the different viewpoints and issues dealing with public key infrastructures. Some sources come very close such as Ford's book, *Secure Electronic Commerce*, and the as-yet unpublished book by Gail Grant coming out in November

1997, *Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks*. Both book are highly recommended for budding and seasoned PKI architects.

What is needed is an integrated enterprise model of public key infrastructures. This model would integrate all of the different relevant points of view and act as a comprehensive requirements document that could be used to develop a customized PKI for a specific implementation. For example, the requirements for a treaty-verification system would differ greatly for a commercial private e-mail system but be similar to the needs for secure electronic commerce over the Internet. The basic components of a PKI are common to all potential implementations; however, the system security requirements vary greatly.

4.2.4 Models

As mentioned in the previous section, we recommended that an enterprise model of a public key infrastructure be implemented that would satisfy a wide range of applications, from treaty verification to electronic commerce to personal private communications and so on. We had proposed such an effort during the summer of 1997 but seriously underestimated the required effort to create such a model. We estimate that the development of generic PKI enterprise model would, at a minimum, require a 2FTE effort. As a compromise, this section will discuss what goes into an enterprise model.

An enterprise model is an abstract representation of enterprise objects and their dependencies based on functional, structural, and behavioral similarities. It describes consistently all relevant views (world of discourse) on an enterprise (real world). These views are characterized by an abstraction reducing the world's complexity. An integrated enterprise model then consists of a redundancy-free conjunction of partial models. In order to design information systems, the following has to be specified:

- all activities that have to be necessarily performed with the context of order processing;
- the connecting information flows;
- the describing data;
- the sequence of process steps; and
- the organizational responsibilities for carrying out these process steps.

These views can be classified as belonging to partial models. Each one of them refers to different aspects of the real enterprise and also affects the different phase of a system life-cycle:

- Conception
- Requirements
- Design
- Implementation
- Test
- Maintenance
- Retirement

An excellent textbook on the subject is *Getting Results with the Object-Oriented Enterprise Model* by Thornton Gale and James Eldred.

In summary, the most appropriate step that can be taken is to for us to develop an integrated enterprise model of a public key infrastructure that would act as a framework for a diverse set of PKI implementations (*e.g.*, treaty verification systems, secure electronic commerce, global communications and entertainment).

5. Conclusions and Recommendations

Early on in fiscal year 97, the IRSI team realized that the scope of the LDRD was too broad. However, the team believed that there were some interesting areas open to investigation. These were:

- secure tokens,
- public-key infrastructures, and
- application transparency.

The team investigated the system security features which could be provided by secure tokens. Quite a lot of interest in this area is being exhibited in the commercial world. The capability of secure tokens is constantly increasing. Tokens are available to perform most of the cryptographic mechanisms that might be required by an integrated and secure system. However, there are issues regarding the security of the token reader. There are difficulties with system integration in this area, but this issue is being researched. In addition, better methods for securing information on the token are being addressed.

Public-key technology can provide several security services including privacy, integrity, authentication and non-repudiation. While other technologies including private-key mechanisms can provide some of these features, non-repudiation requires public-key techniques. Given this requirement, a system employing public-key techniques must also provide an infrastructure in support of these techniques. In particular, certification of identity must be reliably furnished. The IRSI team investigated new and emerging standards in this area. The team found some of these standards difficult to understand and not particularly scaleable. Some of the standards implicitly define a hierarchical certification model that may not be appropriate for many distributed systems. However, the team found that much effort is going into improving these standards. The two emerging standards are the SDSI/SPKI standard and the X.509 standard. They are quite different from each other and show no signs of merging in the near future. SDSI/SPKI is more appropriate for the distributed environment, but X.509 is more widely supported. There is no infrastructure of either type to speak of available on the Internet. There are merely small implementations, usually within single companies. Depending on the system requirements, this may be adequate for the time being.

Finally, the team investigated the possibility of providing application transparency. Application transparency would allow users to purchase

and use less costly commercial-off-the-shelf application software and rely on the underlying system to provide integrated security. This area of investigation led to a dead end. The team found that it would be extremely difficult if not impossible to provide application transparency without significant changes to the underlying operating systems. Even if changes to the operating system were possible, which is not always the case, the security provided might be quite weak. In the case of the UNIX operating system, providing the security features described in previous sections of this document would require the UNIX kernel to be rebuilt, a risky prospect especially when attempting to develop an integrated and easily maintainable system. In the case of Windows NT and/or Windows 95, transparency could be provided but the resulting system security would be quite weak. The only recommendation that the team can make in this area is that commercial operating system developers should begin to address security as an important operating system attribute. Without advancements in this area, integrated system security does not appear to be an achievable goal.

6. References

1. AT&T. "Security Software – Public Key Infrastructure." January 1997. <http://www.att.com/secure_software/pki/> (September 29, 1997).
2. Avellan, Juan. "Certification Authority Survey (DGXV Project)." June 1997. <http://www.qmw.ac.uk/~tl6345/ca.htm> (September 29, 1997).
3. Avellan, Juan. "Digital Signature Links." June 1997. <http://www.qmw.ac.uk/~tl6345/index.htm> (September 29, 1997).
4. Branchaud, Marc. "Public Key Infrastructure References." August 1997. <http://www.xcert.com/~marcnarc/PKI/References.htm> (September 29, 1997).
5. "CAR ITS Strategy." July 1997. <http://www.cse.dnd.ca/cse/english/car.html> (September 29, 1997).
6. CertCo. "E–Commerce 101." June 1997. <http://www.certco.com/ecomm101/ecomm101.htm> (September 29, 1997).
7. Communications Security Establishment. "Government of Canada Public Key Infrastructure." August 1997. <http://www.cse-cst.gc.ca/cse/english/gov.html> (September 29, 1997).
8. Community Research and Development Information Service. "INFOSEC: Description of the 8 studies starting January 1997." July 1997. < http://www.cordis.lu/infosec/src/prep2.htm> (September 29, 1997).
9. Community Research and Development Information Service. "INFOSEC: EUROTRUST — ETS." July 1997. <http://www.cordis.lu/infosec/src/study7.htm> (September 29, 1997).
10. Community Research and Development Information Service. "INFOSEC page from DGXIII of the European Commission." September 1997. <http://www.cordis.lu/infosec/home.html> (September 29, 1997).
11. Community Research and Development Information Service. "INFOSEC: Design and Implementation of infrastructure for TTP." July 1997. <http://www.cordis.lu/infosec/src/study8.htm> (September 29, 1997).
12. Community Research and Development Information Service. "INFOSEC: EAGLE." July 1997. <http://www.cordis.lu/infosec/src/study13.htm> (September 29, 1997).
13. Community Research and Development Information Service. "INFOSEC: Key Recovery in Secure Information Systems." July 1997. < http://www.cordis.lu/infosec/src/study9.htm> (September 29, 1997).
14. Community Research and Development Information Service. "INFOSEC: MANDATE II." July 1997. <http://www.cordis.lu/infosec/src/study10.htm> (September 29, 1997).

15. Community Research and Development Information Service. "INFOSEC: Operational & Architectural Aspects of TTPs for Europe." July 1997. <http://www.cordis.lu/infosec/src/study6.htm> (September 29, 1997).
16. Community Research and Development Information Service. "INFOSEC: Study on the legality of encrypted electronic messages, signed by digital signature and certificated by a TTP as proof of evidence in criminal litigations." July 1997. <http://www.cordis.lu/infosec/src/study11.htm> (September 29, 1997).
17. Community Research and Development Information Service. "INFOSEC: Trusted Third Party Services for Health Care in Europe." July 1997. <http://www.cordis.lu/infosec/src/study12.htm> (September 29, 1997).
18. Dobranski, Lawrence. "The Government of Canada's Public Key Infrastructure." May 1997. <http://www.governmentsource.com/focus5.3/08Cse.html> (September 29, 1997).
19. Ellison, Carl M. "Establishing Identity Without Certification Authorities." July 1996. <http://www.clark.net/pub/cme/usenix.html> (September 29, 1997).
20. Entrust Technologies. "Resource Library: White Papers." September 1997. <http://www.entrust.com/library.htm> (September 29, 1997).
21. Froomkin, A. Michael, "The Essential Role of Trusted Third Parties in Electronic Commerce," University of Miami School of Law, October 1996, <http://www.law.miami.edu/~froomkin/articles/trusted.htm> (September 29, 1997).
22. General Services Administration. "Federal Security Infrastructure." April 1997. <http://www.gsa.gov/fsi/default.htm> (September 29, 1997).
23. General Services Administration. "The Paperless Federal Transactions for the Public Project." February 1997. <http://www.gsa.gov/fsi/paprles.htm> (September 29, 1997).
24. Gerck, Ed. "Overview of Certification Systems: X.509, CA, PGP and SKIP." July 1997. <http://novaware.cps.softex.br/mcg/cert.htm> (September 29, 1997).
25. GMD – TKT.SIT. "Interworking Public Key Certification Infrastructure for Europe." June 1996. <http://www.darmstadt.gmd.de/ice-tel/> (September 29, 1997).
26. Grant, Gail. *Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks*. The McGraw-Hill Companies. November 1997. <http://www.betabooks.mcgraw-hill.com/grant/> (September 29, 1997).
27. IBM. "IBM Registry and World Registry." 1997. <http://www.internet.ibm.com/commercepoint/registry/index.html> (September 29, 1997).

28. INESC. "INESC ICE-TEL page." March 1997. <http://www.di.fc.ul.pt/departs/informatica/investigacao/projectos/ice/> (September 29, 1997).
29. Information Resource Engineering. "Cipher College 103." June 1997. <http://www.ire.com/CYPHER/CC_103.HTM> (September 29, 1997).
30. Internet Engineering Task Force. "Public-Key Infrastructure (X.509) (pkix) Charter." September 1997. <http://www.ietf.org/html.charters/pkix-charter.html> (September 29, 1997).
31. Internet Engineering Task Force. "Public-Key Infrastructure (X.509) (pkix)." September 1997. <http://www.ietf.org/ids.by.wg/pkix.html> (September 29, 1997).
32. Internet Engineering Task Force. "Simple Public Key Infrastructure (spki) Charter." September 1997. <http://www.ietf.org/html.charters/spki-charter.html> (September 29, 1997).
33. Internet Engineering Task Force. "Simple Public Key Infrastructure (spki)." September 1997. <http://www.ietf.org/ids.by.wg/spki.html> (September 29, 1997).
34. Jozef Stefan Institute, "IJS ICE-TEL page." May 1997. <http://www.e5.ijs.si/security/ice/ice.html> (September 29, 1997).
35. Kelm, Stefan. "Comprehensive list of Public Key Infrastructure (PKI) links." September 1997. <http://www.pca.dfn.de/eng/team/ske/pem-dok.html> (September 29, 1997).
36. Kelm, Stefan. "PKI related internet drafts." September 1997. <http://www.pca.dfn.de/eng/team/ske/drafts/> (September 29, 1997).
37. Keywitness Canada. "Welcome to Keywitness Canada." July 1997. <http://www.keywitness.ca/english/keywitness.htm> (September 29, 1997).
38. Long, J. P. "Public / Private Key Certification Authority and Key Distribution — A White Paper." September 1995. <http://www-irn.sandia.gov/organization/div4000/ctr4600/dpt4621/ppkeycert/encwhtt.html#I> (September 29, 1997).
39. Masse, David G. and Andrew D. Fernandes. "Economic Modelling And Risk Management In Public Key Infrastructures — The Business Case for A Broadly-based Highly Scalable Public Key Infrastructure." Chait Amyot Virtual Library. January 31, 1997. <http://www.chait-amyot.ca/docs/pki.html> (September 29, 1997).
40. McConnel, Bruce W. and Edward J. Appel. "Draft Paper, 'Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure.'" May 1996. <http://www.isse.gmu.edu/students/pfarrell/nist/kmi.html> (September 29, 1997).
41. Mestré, Patrick. "PKI References." August 1997. <http://www.dice.ucl.ac.be/~mestre/index_2.htm> (September 29, 1997).

42. Mestré, Patrick. "Patrick Mestré Page." August 1997. <http://www.dice.ucl.ac.be/~mestre/pme.htm> (September 29, 1997).
43. National Information Infrastructure Security Issues Forum. "NII Security: The Federal Role." June 1995. <http://www.sevenlocks.com/NIISecurityTheFederalRole.htm> (September 29, 1997).
44. National Institute of Standards and Technology. "PKI Technical Working Group (PKI-TWG)." September 1997. <http://csrc.ncsl.nist.gov/pki/twg/twgindex.html> (September 29, 1997).
45. National Institute of Standards and Technology, "Public Key Infrastructure." September 1997. <http://csrc.ncsl.nist.gov/pki/> (September 29, 1997).
46. Open Group. "Architecture for Public-Key Infrastructure (APKI)." May 1997. <http://www.rdg.opengroup.org/public/tech/security/pki/apki_1-0.pdf> (September 29, 1997).
47. Open Group. "Latest proposals for an HMG PKI." 1997. <http://www.rdg.opengroup.org/public/tech/security/pki/cki/index.htm> (September 29, 1997).
48. Open Group. "Open Group -... at a glance." 1997. <http://www.rdg.opengroup.org/press/glance.htm> (September 29, 1997).
49. Open Group. "Public Key Infrastructure." 1997. <http://www.rdg.opengroup.org/public/tech/security/pki/index.htm> (September 29, 1997).
50. PKI.org. "PKI Clearinghouse." September 1997. <http://www.pki.org/home.html> (September 29, 1997).
51. Politecnico di Torino. "ICE-TEL Italian PCA Policy." July 1997. <http://www.polito.it/ice-tel/pca-it/policy/> (September 29, 1997).
52. Povey, Dean. "PKI resources." July 1997. <http://www.dstc.qut.edu.au/MSU/projects/pki/index.html> (September 29, 1997).
53. Sandy Bay Software, Inc. "PKI — PC Webopaedia Definition and Links." August 1997. <http://www.pcwebopaedia.com/PKI.htm> (September 29, 1997).
54. Network Working Group. "RFC 1422." February 1993. <http://sunsite.auc.dk/RFC/rfc/rfc1422.html> (September 29, 1997).
55. Network Working Group. "RFC 1424." February 1993. <http://sunsite.auc.dk/RFC/rfc/rfc1424.html> (September 29, 1997).
56. TeleTrusT Sweden. "Welcome to TeleTrusT Sweden." June 1997. <http://www.teletrust.se/defaulte.htm> (September 29, 1997).
57. University College London. "UCL ICE-TEL Project." September 1997. <http://www.cs.ucl.ac.uk/research/ice-tel/> (September 29, 1997).
58. Verisign. "VeriSign." September 1997. <http://www.verisign.com/> (September 29, 1997).

59. Xcert Software Inc. "Xcert Software Inc." September 1997. <http://www.xcert.com/> (September 29, 1997).
60. Zimmermann, Philip. "PGP User's Guide, Volume I: Essential Topics — How to protect public keys from tampering." May 1996. <http://www.chemistry.mcmaster.ca/pgp/pgpdoc1/how-to-protext-pk-from-tamp.html#0> (September 29, 1997).
61. Ahuja, Vijay. "User Certification." *Secure Commerce on the Internet.* AP Professional. Boston, MA. November 1996.
62. Ford, Warwick and Michael S. Baum. "Public Key Infrastructures." *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption.* Prentice-Hall. Upper Saddle River, NJ. April 1997.
63. Garfinkel, Simon and Gene Spafford. "Digital Identification Techniques." *Web Security & Commerce.* O'Reilly and Associates. June 1997.
64. Grant, Gail. *Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks.* The McGraw-Hill Companies. November 1997. <http://www.betabooks.mcgraw-hill.com/grant/> (September 29, 1997).
65. Menezes, Alfred J., Paul C. van Oorschot, Scott A. Vanstone. "Key Management Techniques." *Handbook of Applied Cryptography.* CRC Press. Boca Raton, FL. 1996.
66. Wright, Benjamin, "Emerging Topic 1: Legal Identity and Signatures on the Information Highway." and "Emerging Topic 2: Internet Security Breaches—The Meaning for Electronic Commerce." *The Law of Electronic Commerce — EDI, E-mail, and Internet: Proof, and Liability,* 2nd Edition, Aspen Law & Business. New York, NY. November 1996.
67. T. Alto. A Unix Streams Implementation of the Internet Protocol Security. Master's Thesis, Helsinki University of Technology, Dept. of Computer Science.
68. T. Alto, P. Nikkander. A Modular, STREAMS based IPSEC for Solaris 2.x Systems
69. R. Atkinson. *IP authentication header.* Request for Comments (Proposed Standard) RFC 1826, Internet Engineering Task Force, August 1995.
70. R. Atkinson. *IP encapsulating security payload (ESP).* Request for Comments (Proposed Standard) RFC 1827, Internet Engineering Task Force, August 1995.
71. R. Atkinson. *Security Architecture for the internet protocol.* Request for Comments (Proposed Standard) RFC 1825, Internet Engineering Task Force, August 1995.
72. R. Atkinson, D. McDonald, B. Phan, C. Metz, K. Chin. *Implementation of IPv6 in 4.4 BSD.*1996 USENIX Technical Conference - January 22-26, 1996.

73. S. Bellovin. *Problem Areas for the IP Security Protocols.* Proceedings of the Sixth Usenix UNIX Security Symposium, July 22-25, 1996.
74. D. Wagner, S. Bellovin. *A "Bump in the Stack" Encryptor* for MS-DOS Systems.
75. R. Glenn (rob.glenn@nist.gov) e-mail reply to IPSec implementation transparency question, June 1997.
76. R. Moskowitz (rgm3@chrysler.com) e-mail reply to IPSec implementation transparency question, June 1997.
77. C. Metz (cmetz@inner.net) e-mail reply to IPSec implementation transparency question, July 1997.
78. B. Trost (trost@cs.pdx.edu) e-mail reply to IPSec implementation transparency question, Sept. 1997.
79. D. Keromytis (angelos@dsl.cis.upenn.edu) e-mail reply to IPSec implementation transparency question, Sept. 1997.
80. B. Phan (phan@itd.nrl.navy.mil) e-mail reply to IPSec implementation transparency question, Sept. 1997.
81. W Ford, *Computer Communications Security, Principles, Standard Protocols and Techniques.* Prentice Hall, 1994.

7. Distribution

1	MS 0188	C. E. Meyers, 4523
1	MS 0431	S. G. Varnado, 6200
1	MS 0449	S. R. Copus, 6231
1	MS 0449	P. L. Campbell, 6231
1	MS 0449	J. Espinoza, 6231
1	MS 0449	M. D. Murphy, 6231
1	MS 0449	J. H. Moore, 6234
2	MS 0449	V. A. Hamilton, 6234
1	MS 0449	G. G. Istrail, 6234
1	MS0449	R. S. Tamashiro, 6236
5	MS 0449	R. L. Hutchinson, 6236
1	MS 0806	M. R. Sjulin,
3	MS 0661	T. M. Meeks, 4612
1	MS 9018	Central Technical Files, 8940-2
5	MS 0899	Technical Library, 4414
2	MS 0619	Review and Approval Desk, 12690 For DOE/OSTI