NISTIR 5234

Report of the NIST Workshop on Digital Signature Certificate Management December 10-11, 1992

Dennis K. Branstad
Editor

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

NIST

NISTIR 5234

Report of the NIST Workshop on Digital Signature Certificate Management December 10-11, 1992

Dennis K. Branstad
Editor

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

October 1993

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arati Prabhakar, Director

TABLE OF CONTENTS

1. Executive Summary

1.1 Purpose of the Workshop

The purpose of the workshop was to review the existing and required technologies for digital signature certification authorities and to develop recommendations for certificate contents, formats, generation, distribution and storage. The results of the workshop will be provided to MITRE Corporation as input to its federally sponsored study of signature certification authorities.

Invited participants represented various constituencies including the federal government, commercial organizations, standards organizations, and international interests.

1.2 Structure of the Workshop

The workshop was organized as a sequence of presentations on selected topics, including: certificate infrastructure and technology, planned security offerings, needs of government organizations, international and commercial interests in digital signature technology, international standards for security in the context of X.509, and specific certificate contents and formats. Discussion about particular topics such as the contents of a certificate or a proposed hierarchy of certificate management authorities was not confined to any particular presentation but rather occurred in a continuous fashion throughout the two days of the workshop.

This report provides a summary of the major discussion points. It is organized chronologically by presentation.

1.3 Summary of the Major Issues

The major topics of discussion were certificate format, certification revocation lists (CRL's), possible certificate management hierarchies, and the difference between authentication and authorization certificates. Also discussed were the possibility of multiple signatures on a single certificate, liability, trust, cross certification, and different levels of assurance.

What follows is a summary of the major issues identified by workshop participants that must be addressed by any proposed certificate management solution.

1. <u>Certificate Revocation Lists</u>
Certificate Revocation List management is of utmost importance to certificate users and must be done correctly. The following questions were discussed: Who is responsible for reporting a compromise or change of attribute?; Within what time frame should that reporting be done?; If it is a shared responsibility of the user and the CA (Certification Authority), how exactly will that responsibility be shared? How often will CRL's be issued? What will their format be, (e.g. PEM, X9F, X.509)?

2. Certificate Management Hierarchies
An integrated Certificate Authority structure must be a hierarchy. What will that hierarchy be for the federal government? Will it be formed along organizational lines or communities of interest? A naming schema for the federal government needs to be worked out. Who will do this? Will the choices in naming need to be restricted?

3. Costs
What are the cost estimates for each choice of hierarchy? What metrics can be used?

4. Certificates
Should we standardize requests for certificates or is this a local matter? Should we have multiply signed certificates and are these another kind of certificate in addition to authentication and authorization. What will be the format of an authorization certificate? Will the new work in security information objects be of use for authorization certificates? How should the unique id field of the 1992 X.509 certificate be used?

1.4 Workshop Recommendations

The following list represents consensus on several of the major issues:

1. Use the X.509 certificate format for authentication (identification) certificates.

2. At least two kinds of certificates should be supported:
   a) Authentication certificates; and
   b) Authorization certificates (for access control)

3. An individual should have multiple certificates corresponding to different roles.

4. International standards should be utilized.

5. A certificate management hierarchy should include strict name subordination (in the X.500 sense) below the level of a CA.

6. CA's should support different assurance levels and they should publicize their policies.

7. An authorization certificate should contain the minimum amount of information which serves the purpose and this information should be closely coupled with the owner of the certificate (i.e., authentication information). This reduces the need to reissue certificates when authorities change.

2. Workshop Participants

Aiken, Dina
Ankney, Rich, Fischer International
Barker, Elaine, NIST
Baum, Michael
Branstad, Dennis, NIST
Chamberlain, Chuck, U.S. Postal Service
Chang, Shu-Jen, NIST
Crocker, Steve
Dusse, Steve, RSA Data Security, Inc.
Fischer, Addison
Galitzer, Shari, MITRE Corporation
Geiter, Jisoo
Gill, Dave, MITRE Corporation
Greenlee, Blake, M. Blake Greenlee Associates, Ltd.
Humphreys, Ted, Commission of the European Communities
Kent, Steve, BBN Communications
Moreau, Jean-Maurice, Communications Security Establishment, Canada
Shomo, Larry, NASA
Smid, Miles, NIST
Williams, Al, GSA
Williams, Peter, University College London

3. Day 1 --- Morning Presentations

3.1 Digital Signature Certificate Infrastructure Study

Dave Gill, MITRE, Deputy Task Leader for the NIST sponsored digital signature certificate infrastructure study, presented an overview of that study, including the following topics: why an infrastructure is needed; one possible hierarchy; how the study is being conducted; a time table for deliverables; and who is funding and participating in the study.

An infrastructure is clearly needed to manage the public keys and provide some level of assurance as to their authenticity. The number of keys is potentially quite large (consider the IRS using this for electronic submission of 1040 forms). The potentially large number of keys implies the need for some sort of hierarchy of certificate authorities. Potential hierarchies that MITRE is considering include one used by the North American Directory Forum (NADF), one based on organizations, or one based on communities of interest, i.e. groups with the same security policies or requirements. The question of who will manage the US Government portion of the hierarchy is open for debate. MITRE's current thinking going into this workshop is that the responsibility may be divided among different agencies based primarily on different security requirements.

The methodology used in the study involves obtaining input from private organizations, federal agencies, standards organizations, and security experts and using that input to derive a set of user, legal and technical requirements.

Draft requirements in these three areas are due at the end of January, 1993. After that time, more interviews with federal agencies will take place regarding their intended application of digital signature technology. Infrastructure alternatives will be proposed by mid-March and the infrastructure analysis will be complete by June, 1993.

Eight federal agencies are funding the study; NIST is the coordinating agency. Dennis Branstad, the workshop coordinator, pointed out that the agencies funding the study are very interested in digital signature technology and the supporting infrastructure. He stated that the recommendation of the MITRE study will go to OMB who will be asked to act on it.

3.2 MITRE Certificate Technology Findings

Shari Galitzer presented MITRE's view of the current certificate technology. She discussed specific issues that need to be addressed in defining a certificate management infrastructure that can be extended easily and can support many different applications. She focussed on four separate areas: architecture, security policy, functional components and resource requirements.

The hypothesis that the infrastructure must be a hierarchy was reinforced. A question of organization is, "Should the infrastructure be formed along organizational lines or communities of interest?" Interviews with various federal agencies about their user and legal requirements will be used to guide the final recommendation. It was suggested by several participants that MITRE ask the STU-III support people about the choices that were made regarding the key management structure for the STU-III system. Why is it flat? Does the structure relate to the security policy? Would they do it differently next time? MITRE was reminded that it is important to put the STU-III work in the context of the environment in which it operates; while some of the STU-III experience may be relevant to the digital signature infrastructure, it would be unwise to duplicate the STU-III choices without analysis.

The discussion then centered on the scope of MITRE's study. Their charter is to recommend an infrastructure for government agencies. The scope of NIST's responsibilities does not include telling private industry what to do. However it is recognized that the recommended digital signature support infrastructure must work in an international environment and with the private sector. There is a strong interest in maintaining interoperability and compatibility with recognized standards. If the design is good, others may wish to duplicate it.

The issue of trust was then raised. One of the questions addressed was, "Which organizations could be trusted and what should be required of certifying authorities so that their certificates can be trusted?" The idea that there are different kinds of certificates and that a single certificate will not satisfy all needs was introduced.

Major issues under the topic of security policy included: who should generate the keys; how to manage CRL's; what are the security requirements for managing a CA (certification authority); and how to deal with multiple roles of individuals. The ultimate goal is an infrastructure that will support a variety of security rules (i.e. policies) that any organization might want to impose/adopt.

A lot of discussion centered around the question of how to provide for the multiple roles that an individual may hold at any one time. Should the same public key be in multiple authorization certificates? Should the same certificate be used for multiple roles? If the certificates or roles are associated with different organizations with different security policies and levels of assurance, it is unlikely that either of these alternatives will work. If one certificate has multiple authorizations with respect to the various roles bound into it, anytime one of the roles changes the whole certificate must be reissued. If those authorizations were all from different organizations, who would sign it? It was recognized by the participants that authentication and access control are two fundamentally different operations and that there is a need for different kinds of certificates. It was pointed out that X.509 is deficient in the aspect of handling multiple roles. New standards work is in progress on defining a more generic syntax for a "security certificate" that will be an extension to X.509 and allow different security services to be provided.

A discussion was held regarding who is responsible for making it known that a certificate has been revoked. A typical approach to answering a question like this is to look at how it is done now in paper and then to look at the technical and legal ramifications encountered when the manual procedure is automated. In the current revocation practice for credit cards, there is a split responsibility for financial liability between the credit card holder and the credit card issuer. The participants agreed that a split approach will probably be used electronically as well, with responsibility for notification and for liability shared between the user and the certification authority.

The costs of the certificate management alternatives will be considered in the study. MITRE is eager for input on metrics to be used for analyzing costs. Cost is clearly an important issue. At least two ways of looking at costs were articulated. One is the business viewpoint which says, "What cost is acceptable so that a digital signature will be used?". The lower the cost the better (twenty-nine cents per signing was suggested). If the cost of the infrastructure is amortized over the total usage, then the cost per transaction is lower. However, if low value transactions dominate and there is no need for a signature on them, then the cost per signature will go up. The other viewpoint on costs is the futuristic approach, also referred to as the "certification field of dreams." This view is that we cannot anticipate today all the possible applications that may use certificates in the future. Therefore we cannot do a pure cost analysis. Rather we build the system in anticipation that other uses will occur. An analogy was drawn here to the work that has been done in computer communications. There is a need to balance these two viewpoints.

3.3 CEC Certificate Workshop Report

Ted Humphreys of the Commission of the European Communities (CEC) presented the results of a workshop held in Brussels on December 1-2, 1992. The title of the workshop was "Electronic Signature: The Key to Mobility". Ted explained the process by which a "Call for Ideas" was issued in May, 1992, and then the responses summarized in a document published in October, 1992. There was an overwhelming response to the Call for Ideas from the international community. Many application areas for electronic signatures were identified, including medical informatics, transportation, aerospace and personal communications. The workshop in Brussels was held to further explore the issues raised by the respondents.

Ted reinforced the idea that X.509 is applicable for a number of different security services (primarily related to authentication) but needs to be expanded to handle the very important idea of access control. He stressed the importance of using international standards and not reinventing what already exists.

A question was asked about the requirement for a license to import cryptography in some European countries. This and other legal issues are being addressed. Not only are there legal differences internationally, but also internally within the European community. Ted gave an example of unique identifiers which are acceptable in some countries in Europe and not acceptable in others. Another question was asked about the differences between the legal systems in Europe with regard to cryptography. A study is being done that addresses the various European legal perspectives on intellectual property rights issues. Dennis Branstad announced that NIST is sponsoring a study on export laws and other legal topics related to cryptography in the United States and other countries.

Ted finished his presentation by pointing out that the British Post Office is looking at digital signatures and how to link up with their counterparts in other countries.

3.4 International Interests

3.4.1 Communications Security Establishment (CSE), Canada

An informal report was given by Jean-Maurice Moreau of the CSE. CSE is the Canadian government agency that provides advice on communications security. Its scope of authority is both "low-grade" and "high-grade" applications, or what we would call unclassified and classified. CSE wants agencies to implement electronic authentication and authorization for electronic transfers. They are now in the definition state, looking at the user requirements. A requirements paper will be produced by the end of February, 1993. The architecture should be defined by the summer.

3.4.2 University College London (UCL)

Peter Williams talked about the security related work being done at UCL that is funded by the CEC. It is a pilot project that by the end of 1993 will have 30 sites in three different countries exchanging X.400 (Message Handling Systems) and X.500 (Directory) services and have a certification infrastructure in place. They are using existing Open System Interconnection (OSI) protocols and are not involved in a discussion of what should be in certificates. In this project, UCL is taking a different approach. Instead of defining and analyzing the requirements for an infrastructure first, they are implementing a prototype infrastructure first and will perform the analysis afterwards.

The countries involved are using their own implementations of the OSI protocols and security toolkits to avoid import and export rules. It was commented that using multiple implementations is a good way to check out the protocol specifications. In response to a question about possible U.S. involvement in this project, Peter said that UCL welcomed U.S. participation; just bring your own software.

4. Day 1 —— Afternoon Presentations

4.1 Federal Interests

4.1.1 NASA Digital Signature and Security Services System

Larry Shomo described NASA's need to replace paper documents with electronic ones and to do so in a uniform way across the organization. While financial applications were the impetus to the original idea, there is an interest in developing a much broader infrastructure that will support many applications. Providing a complete electronic document environment for NASA would go beyond just security features and would include the ability to (1) read documents prepared with previous versions or types of software, (2) maintain electronic archives, and (3) perform search and retrieval of documents. NASA interacts with businesses and universities throughout the world and any solution must work in this context. Furthermore, it must be capable of operating on and with a diverse set of hardware and software.

With those requirements stated, Larry went on to describe an ambitious set of objectives that the system should meet and services it should provide. He stated that NASA's Information Research Management (IRM) council has adopted this system as a standard for NASA. He also hopes that if done right, other government agencies may adopt it as well. He expects an interagency agreement to be signed with NIST by early January; a prototype system developed within 11 months; and 6 months later, the technical specifications should be available for a Request for Proposal (RFP).

4.1.2 GSA Perspective

Al Williams stated GSA's objective: to replace a number of paper documents with electronic equivalents (the same as NASA). They would like to see a government-wide, classified and un-classified, integrated solution that provides many different types of security services. He recognized that trust is required in those providing the security services. His comment that this should be "integrated" provoked much discussion. This discussion paralleled a similar discussion in the morning session on how to figure cost. The question is, "Can you design a complete system that anticipates every future requirement and every application's need, or should you start with one area, e.g. the certificate infrastructure for supporting digital signatures, and design it without the applications already developed and in place?" There is considerable feeling that it is possible and a good idea to focus on a single area, do a good job and learn from the experience. There is a danger that too large a project will not succeed. Another comment concerned the feasibility of expecting vendors to incorporate specific security services into their products, such as secure logins in the operating system, and in so doing make those services available for off the shelf purchase. While it may be possible for the government to hire a contractor to build security services at the application level, it is difficult, if not impossible, to get vendors to change their operating system or network protocol in response to government requirements.

4.2 Commercial Interests

4.2.1 RSA, Inc.

Steve Dusse described RSA Data Security, Inc.; its history, its customers, its concerns, and then stressed their interest in supporting not just the RSA algorithm but also other "cryptographic solutions" including DES, DSS, etc. He described their work on PKCS (Public Key Cryptography Standards). The certificate used in this standard is compatible with PEM (Privacy Enhanced Mail) certificates and in tune with the 1992 X.509 standard. The PKCS will be used by several vendors, including Apple and Microsoft, to produce office workgroup software. He described a new product for CA's to be used for issuing certificates. This product includes a database to be used by the CA's for certificate management, tracking and querying. It also includes a signing unit, built by BBN, that is tamper proof (the private key is destroyed if the box is tampered with), makes a public-private key pair for signing certificates where the private key remains inside the unit, and is controlled by "user-friendly" software.

Steve stated that while we know a lot about certificates and their format, their use is still new in the business world and we lack experience in certificate management. He further asserted that certificates provide assurance of identity but little is understood about liability. For these reasons, a continuance of pair wise agreements may be required among cooperating organizations in order to conduct business.

The discussion then moved to X.509 certificates and the need for authentication and authorization certificates. X.509 certificates were developed to satisfy a need for strong authentication in the context of the Directory. There are now applications that need wider services and X.509 is being improved to offer more generic certificates.

It is useful when discussing possible authorization certificates to consider how access control is accomplished in operating systems. Access control can be done by using access control lists (which represent the columns of an access control matrix) or by using capabilities (which represent the rows of the same matrix). They both perform equivalent functions but have unique tradeoffs. Access control lists consist of all the entities that have a right to access a particular resource. Capabilities are tickets that an entity presents when accessing a resource that say the entity has the proper access rights. It is possible to build an identity based access control scheme using X.509 certificates as entries in an access control list. One potential drawback is the cost of managing those lists. Another one is that while one CA may be trusted to vouch for someone's identity, another CA or organization may need to authorize that identified individual. Certificates could have multiple signatures, but as soon as one item in the certificate changes, the entire certificate must be reissued. If the capability approach is chosen instead of an ACL approach, then a new certificate format is needed for an authorization certificate. This format should be sufficiently general so that it can be used by any application.

Another topic which arose from the previous discussion was how to make an identity unique. Your name is guaranteed unique only if enough context is provided to differentiate you from others with the same name, e.g. your home address or your employer and position in that company. Much of that information may be of no interest for the purposes of certificate management. On the other hand, if using identity based access control, the application may wish to use the related information supplied with the name to make a decision about authorization.

4.2.2 Fischer International

Addison Fischer, president of Fischer International, introduced his company and his primary concerns as a software producer for an international market. His company produces four RSA based products, including a PEM implementation. They use the X.509 certificate format. His message was that since his company does software for many customers, not just the government, the government should stay with the standards that everyone else is using if they want to buy products off the shelf. He also expressed a concern over supporting multiple cryptographic algorithms. It was pointed out that many algorithms could coexist within a particular certificate infrastructure. In particular, the X.509 certificate format gives the ability to select different algorithms or key lengths.

4.3 What's in a Public Key Certificate?

Steve Kent explained his view of what should be in a public key certificate and why. He explained that it is difficult to get one certificate to fit all needs. There are different attributes that are of interest to different applications (e.g clearance levels in the military or financial authority in business), there are different entities to vouch for these attributes, and there are different validity time frames. All these reasons suggest that there will be more than one certificate for each individual, as well as more than one type of certificate (e.g. authentication and authorization). Concern was voiced that the certificates would proliferate rapidly and we would have the electronic equivalent of a thick billfold. It was agreed that while one certificate per individual will not work, in part because organizations want to control their authorizations and because differing levels of assurance of identity may be needed, it is important not to have too many certificates since the management would become unwieldy.

It was again mentioned that X.509 is being extended to handle a wider range of applications. Standards work is progressing on defining "security certificates" to support security information objects. It was asserted that certificates of a more general type could be used for rule-based authorization where identity was not important or desired.

The next discussion centered on the issue of trust and levels of trust. First, we must trust the issuer to vouch for the validity of the attributes that are bound in the certificate and that they have been accurately bound. Second, how will a CA identify any entity and to what level of assurance? Will there be different levels of assurance offered by a single CA, that is, will a single CA offer different levels of checking attributes; or will there be different levels of CA's, that is, will some CA's require higher validity assurance of the attributes presented to them? It was agreed that there would be different levels of CA's, that they would make their policies known, and anything signed by them would comply with that standard of checking. For instance, a CA signing certificates in a classified environment would do a higher level of checking than a CA in an unclassified environment.

Steve's last point about trust was that "A certificate vouching for an identity binding does not imply trust in the identified entity." It is important not to get confused about what we are trusting and what is being certified.

Another issue regarding certificates is that of revocation. If we use the capability analogy from operating systems to describe a certificate, then we know that revocation is difficult. You cannot, in general, find all the certificates and "pull" them back. It was suggested that when certificates are used as authorization, then a combination of a "push" and "pull" model must be used, especially as the number of users gets larger. In particular, revocation lists could be periodically published ("push") and also the most current version could be available online for checking if the transaction is valuable enough ("pull").

The discussion then went back to authorization certificates vs. identification certificates. Concerns were raised that having too many different formats for certificates would make implementation difficult. It was suggested that an appropriately general format for an authorization certificate could be developed that would represent a compromise between fixed fields required for all applications and some flexibility to define new attributes for particular applications. It was agreed that binding too much unrelated information about an individual into one authorization certificate would be a bad idea for several reasons. One, there may be privacy concerns associated with some of the identifying information. Two, if one piece of information changes then the entire certificate must be reissued. If identification is separated from authorization, then changing an authorization certificate would occur less often. By binding less information into a certificate, certificates could support the principle of least privilege or need to know.

The issue of individual names was raised. The X.509 subject field is a distinguished name. This format is well-defined, however, the naming hierarchy for the United States (C=US) is not yet worked out. The NADF (North American Directory Forum), a self-appointed group, is working on one schema for an X.500 directory project. This does not address certificates directly. Steve Kent suggested that the names would separate an individual's role from his/her unique identity. If we assume that people change roles frequently within an organization, then this would minimize name changes and subsequent reissuing of identification certificates. On the other hand, if movement is rare in an organization this may not be needed. It seemed clear that some guidance should be provided on the schema for the U.S. Government, but it was not clear what that would be.

4.4 Initial Recommendations

Based on the discussions on certificate contents that had taken place throughout the day, two recommendations were endorsed by the participants. They were:

- There should be at least two types of certificates, an identification certificate and an authorization certificate. They may have different contents and formats because they have a different set of requirements.

- The format for the identification certificate should be X.509. The format for the authentication certificate is unknown at this time but will be different from the id certificate.

A participant pointed out that certificates may not always be the proper choice for authorization. In some situations, other mechanisms could be used. It was clarified that the "security certificate" is a general term not to be confused with authorization certificate.

4.5 X.509 Certificate Format

Ted Humphreys presented a summary of identified deficiencies in the 1988 version of the X.509 certificate format and in the revocation list format. Some, but not all of these defects, are addressed in the 1992 version of the standard. The particular deficiencies relating to the format of the certificates are listed in his paper "Security Certificates". They include concerns over reuse of Distinguished Names, how to distinguish between a user certificate and a CA certificate, and how the certificate is stored.

The defects in the revocation list format and/or suggested repairs include: a change in the ASN.1 syntax from a SIGNED SEQUENCE OF SEQUENCE to a SEQUENCE OF SIGNED SEQUENCE; there is a difference in the date at which a user requests revocation and when it is actually done; there is no indication of when the next revocation list will be issued; and the management of a potentially very large revocation list. Steve Kent explained the difference between the proposed way of doing revocation lists (SEQUENCE OF SIGNED SEQUENCE) and the way that PEM does it. In X.509, when a notice of a revoked certificate is signed by the issuer of that certificate and stored in a revocation list, it is acceptable for the issuer of the revocation list to be different from the issuer of the notices of revoked certificates within it. The PEM group did not adopt this, since a CA should not be able to revoke a certificate that someone else signed, and therefore they chose a different structure (SIGNED SEQUENCE OF SEQUENCE). The syntax of the revocation lists is significantly different in PEM and X.509. The question was asked, could one group accept the other's proposal. Steve Kent replied that for PEM, putting in the next date of issue for a CRL is a security issue and could not be negotiated. This feature is still lacking in the 1992 standard. Ted suggested that future work on security services not arising in the context of the Directory will be handled in other groups as a general security problem. Work on more general security information objects may overcome this difference between the two groups.

A further incompatibility surfaced when the group was told that the ANSI X.9 revocation list format uses the basic PEM format but then adds a reason code that tells why the certificate was revoked. The reasoning behind this is that in the financial community, if it were a serious key compromise, they would want to move quickly to limit damage. On the other hand, less serious reasons, such as a change of affiliation might result is a more measured response.

4.6 General Discussion of Certificate Revocation Lists and Naming

Some of the issues regarding CRL management were discussed. One issue is how the CRL's can be used to provide a nonrepudiation service. In order to show that a signature was valid at a particular time, it is not sufficient to store just the CRL that is in use at that time. Rather, an updated CRL must also be stored when it is next issued, in case the key is compromised between the time of issue of the first and second CRL. How often CRL's will be published is not yet specified and will probably be a local management decision by a CA.

A question was asked about how many certificates would be on a CRL. It appears that the number of certificates will be a function of how much information is bound into a certificate. For instance, if attributes such as the position held in the company are in the DistinguishedName and that position is likely to change often, then the list could get very large.

Other issues include: who is responsible for reporting a compromise or change of attribute and within what time frame should that reporting be done. If we follow the credit card model, then the reporting should be done by the user in a timely fashion (e.g. within three days). Specifying what is a timely fashion may not be easy. And while limiting financial liability may work in the credit card case, the analogy may not hold with certificates. It was suggested that a company may need to buy employee bonds in order to limit their liability. Also, some steps may be taken manually to limit damage by checking recent orders or signed contracts and determining if it is possible to cancel them. These types of action are outside the nonrepudiation service.

Peter Williams opened a discussion on naming by asserting that because of the deficiency in X.509 (88) it is possible for a user to pose as a CA, and in order to combat this threat a strict hierarchy must occur in the naming scheme. Steve Kent responded that there is no requirement that the certification hierarchy follow the X.500 naming hierarchy and offered the PEM approach as an example solution. The subject name must be in a strict subordinate relationship to the issuer, but the issuer (CA) may be anywhere in the naming tree. It is clear that a hierarchy is needed as a way of managing certificates, it's just not clear which one. One assertion is that if C=US is controlled by ANSI, then if the certification hierarchy must be identical to the X.500 hierarchy, no one could issue certificates until ANSI set up a certification granting authority. There is a problem identifying the root of the certification hierarchy; no organization has indicated they are ready to assume that role and no organization has been approved for that role. There is also a social acceptability issue associated with naming. If the objects named contain great semantic content, people want more choice over the names assigned to those objects. Objects such as ethernet addresses or internet protocol (ip) addresses do not generate the same strong emotional response. One suggestion is to have a number of different domains, i.e., several public and multiple private domains. Another was that one certification hierarchy specified as a preferred model could convey benefits such as increased trust in the certification path. Further, having a single model will promote (but not guarantee) interoperability.

The day's sessions ended with a brief cost/benefit analysis of implementing security. Both business and government may find security unattractive if the estimated cost of the cure exceeds expected savings. Some participants said that losses could escalate in an electronic environment. Some would like a complete analysis of a threat model. MITRE stated that they needed more input on how to measure the costs of managing certificates.

5. Day 2 --- Morning Presentations

5.1 ANSI X9 Certificate Format

5.1.1 X9F1 Standards Activities: An Introduction

Blake Greenlee presented an overview of the security standards activities involving the financial services industry. The ANSI X9F1 group is working on two sets of public key standards, one using irreversible algorithms (X9.30) and one using reversible algorithms (X9.31). Both of these standards include four parts, the signature algorithm itself, the associated hash algorithm, certificate management and management of symmetric keys. He discussed briefly some of the requirements for managing hot lists (CRLs) and what the hot lists should contain.

He defined some requirements placed upon a CA regarding liability and responsibility. Items such as identifying the requestor and protecting the CA's private key are on the list. Also included is a stringent requirement that the CA's private key be generated inside a crypto-module and NEVER appear outside that module in either plaintext or enciphered form. From these requirements and from the implementation of sound management practices, it follows that the CA will be trusted by its subscribers.

The final viewgraph contained a table of actions to be taken upon revocation of a certificate. How a reason code for revocation would be used in practice and the actions to be taken by the entity certified, the CA, and the users of the certificate were presented in detail.

The status of the proposed standards was discussed. The secure hash algorithm for the irreversible algorithm is in draft form and should be an ANSI standard by the end of the first quarter of 1993. The certificate management portion of the standard should be voted on by the summer. Other parts of X9.31 will be reviewed at the March meeting.

5.1.2 Credentials

Elaine Barker of NIST showed the ASN.1 specifications for what a certificate requesting party would present to the CA to put into the certificate. These are called credentials. The required attributes have been brought into alignment with the X.509 certificate contents. The issue of whether there were additional restrictions placed on the values of these attributes, such as subject name, was raised. For the banking community this has been deliberately not specified, leaving maximum flexibility. It is anticipated that these will be private systems with a relatively flat hierarchy. It was noted that national systems may in fact wish to narrow down the choices of naming schema and so remove some of this flexibility.

The ASN.1 specification for a multiply signed certificate was presented. The ANSI X9F1 members perceive a possible requirement for multiply signed certificates in applications such as syndicated loan agreements. The multiple signatures are computed just on the certificate information; it is not a signature on a signature, although that may be a future operation. A lot of discussion occurred over the difference between signing a document and signing a certificate and the need to keep these two ideas differentiated.

Other issues that were identified and discussed, but not resolved, include: how to sequence multiple signatures in order of time; how to indicate how many signatures you need; how changes can be made after a signature is applied (this relates to documents not certificates); and how many primes are needed for multiple signatures.

Elaine finished by showing the ASN.1 specs for the Certificate Revocation List and for the Attribute Certificate. There was considerable discussion over what would be revoked in the case of CA compromise. If we stop using the compromised CA key, do we also need to stop using a user's key in any certificate signed with that (now) compromised key? It was pointed out that we must differentiate between the idea that we are revoking certificates and not revoking keys. That is, it is not in general necessary to reissue a user's public/private key pair due to CA compromise. After an appropriate investigation, you may reissue certificates signed in error, or hot list certificates as necessary, but the keying material may still be valid.

The discussion then returned to the liability of the CA. The requirements presented by Mr. Greenlee were very detailed, very specific. A question was asked, who would step up to those requirements, given the concerns over liability? Blake asserted that he anticipates a CA at each Federal Reserve District and that having these rules and policies in place will help clarify their responsibilities. The CA is clearly liable for doing its job properly, that is, binding the attributes correctly. It was suggested that MITRE consider these liability discussions when it produces its report.

5.2 Certificate Format Discussion

Rich Ankney led the discussion on certificate format. He presented a list of discussion points and went over each of them. The first point established that the X.509 certificate is indeed used as a base for PEM and X9F activities and would be suitable for use by the government as an authentication certificate. The 1992 version of the X.509 certificate is preferable; it has a unique id field that will be useful for a variety of purposes. It was felt that while the exact semantics of the User Identifier (UID) field should be left somewhat open, additional guidance should be given to minimize the flexibility and potential confusion. That guidance is not yet determined. One possible use is to determine, in the case of multiple certificates for one subject, which private key of the CA signed a particular certificate. Another question was how to convey the necessary Digital Signature Algorithm (DSA) parameters for use with a certificate. It was felt that conveying them in each certificate in the SubjectPublicKeyInfo field was appropriate. Even though it requires a certain amount of bandwidth, that is a reasonable tradeoff when one goal of using certificates is to avoid prenegotiations and to have all the information necessary to use the certificate in the certificate itself.

Point two on the list related to the attribute certificate defined by X9F and whether that kind of certificate would be useful for the government. It was suggested that it might be too early to decide on specific attributes, since we lack experience in this particular area. The security information object work that is going on in ISO SC 27 Working Group 1 appears to be the right mechanism to use for future development. It was also pointed out that the CA that does the authentication, and the CA that issues the authorization, may not be the same; in fact, they should not be the same CA.

The next point was about multiple signatures on certificates, another feature provided in X9F. This provoked a great deal of discussion. Many of the concerns about multiple signatures may lie outside the scope of the certificate discussion, as they are application specific. For instance, is the order of signing relevant, can there be substitute signers, can you annotate documents or change them after signing, how will you indicate that multiple signers are needed. MITRE was directed to look at the possibility of using multiple signatures on certificates or if necessary, using multiple certificates to sign one public key. It was asserted that no one government CA may want to take complete responsibility. On the other hand, it was also pointed out that if there are doubly signed authentication certificates, the CA's may not be acting as a CA should if they are unwilling individually to vouch for the validity of a certificate. Also, if we are talking about doubly signed X.509 certificates, then they are no longer X.509 certificates, but in fact, are an additional type of certificate. There was no consensus on this issue.

Point four regarded other security services that might make use of the infrastructure. Peer entity authentication was an easily agreed upon service. It was felt that other services might be outside the scope of MITRE's report, and while important and useful to specify these services more fully, given our time constraints at this workshop, discussion was postponed.

Point five addressed which format to use for the CRL's: X.509, PEM or X9F? The use of the reason code by X9F was (again) explained. The use in PEM of a next update time was viewed favorably by the participants. In the interests of compatibility, Rich Ankney said he would see if the X9F group would accept an "optional" designation for the reason code. A request was made to consider including a version number. That was also considered a good idea, but would have to go back to the various standards groups. There was some concern about retaining the ability to revoke a user's certificate if the issuer's private key were lost. Since none of the proposed CRL formats contain any keying material, this was not felt to be a problem.

A question was asked about why we should standardize the certificate request. There are two ways of looking at this. The first position says that each CA operates independently based on the needs of the community it serves and so these decisions should made be locally. The second position says that in the interest of buying off the shelf software to do the request for a certificate, we should have one standard format.

5.3 Demo of RSA Certificate Issuing System

Steve Dusse of RSA, inc. gave a demonstration of a system to do RSA key pair generation and issue certificates. This system is scheduled for release early in 1993. It consists of: a certificate signing unit manufactured by BBN in which the RSA key pair is generated, a data base component for certificate management, and some "user-friendly" software that allows the issuer to enter and view various attributes associated with a transaction. The system is set up to issue "subordinate" certificates, in that the user's Distinguished Name will be strictly subordinate to the issuer. He emphasized that while the strict subordination is required in the naming, other attribute/value pairs are not restricted. However, a particular organization may wish to enforce some restrictions based on their policies. This is acceptable as long as it does not conflict with the standards. Another feature that was mentioned was the ability to generate the user's public key inside or outside of the box. This ability might be useful in a smart card environment.

5.4 U.S. Postal Service Security Offerings

Chuck Chamberlain described how the postal service is planning to transition from a hard copy world to an electronic world, and what value-added services they might provide. He began with a brief overview of what happens in the paper world today with registered and certified mail. He moved quickly to a description of three services that they could provide in support of electronic commerce for the federal government. These include identity authentication, an electronic postmark and an audit trail and integrity check of certificates.

To provide the first service, identity authentication, the postal service would act as a certification authority. In his example, a government employee dials in to a post office computer and requests a certificate. Once the employee has entered the appropriate data, a certificate is built. An application form is then printed on the employee's local printer. This form can be presented at any post office where the requestor's identity is verified and the form signed. The certificate is then activated and sent to the requestor via email.

The second service provides the equivalent of a trusted timestamp. Some anticipated uses include verifying the date of submission and integrity of bids, proving intellectual property and sealing files for subsequent IRS audit. A related discussion about the semantic difference between proof of delivery (it got to someone) and proof of receipt (it got to the designated recipient) occurred at this time.

This led to a discussion of naming and hierarchies and their relation to the international standards, e.g. X.400 and X.500. It was suggested that the standards require management domains and no organization has really addressed that need by establishing a national policy or by providing a national authority. The PEM model was proposed as a useful way to view things. The USPS could be a PCA (Policy Certification Authority) with established policies that may prove useful to a wide variety of applications. There could be other PCA's serving the banking industry or other agencies with different security requirements. The important thing to remember with the PEM model is that it does not require a strict adherence to the naming hierarchy except below the level of the CA. In that sense, the Post Office would not be "higher" in the naming hierarchy than other agencies that might use it services; no name will start with "org=usps"!

Chuck stated that he thought other agencies would want to do their own authentication and that they (the postal service) might provide a cross certification service or a common root. The USPS could also assist with managing the CRL's between them. He looks to the work on X.500 implementations to help their efforts, particularly the NADF work on a central authority for synchronizing the directories.

A question about how well the PCA idea scales was raised. It was felt that scaling does not pose an assurance problem but rather a human interface problem with deciding if a particular CA should have signed a particular certificate. If a certain locality of reference holds, and you deal with only a few CA's on a normal basis, then this affect may be mitigated.

5.5 Report on the EC

Ted Humphreys reported on activities in support of the European Community and European policies in contrast to national policies in Europe. He presented the action plan associated with the only council decision issued in the area of security. This decision was ratified in March 1992. Another decision on data protection is expected to be ratified soon.

The action plan had five points: identify user requirements; look at solutions for intermediate and interim needs; develop long-term specifications and standards; look at operational deployment; and ultimately the provision of security. Under this action plan they have various activities going on, including some pilot projects. There is a firm commitment to international standardization with the associated procurement implications.

The topic of universal electronic addressing was discussed. It was pointed out that in Europe, the directories are maintained by the telecomm companies and are their property. Further, the telephone companies have not gotten together to offer a Pan European directory service due to competition, regulation, etc. This holds back development of certification authorities. They are looking at the postal codes and the postal systems as a way of setting up a certification system.

The legal issues remain difficult to sort out in Europe. Ted hopes new legislation at the European level will help this situation. MITRE was reminded that we may need legislation here as well to solve some of the issues regarding name changes in case of death, marriage, incapacity, bankruptcy, etc.

5.6 Certificate Management Discussion

Steve Kent presented an example of a certification hierarchy, the one currently being set up for the PEM effort. The PEM hierarchy has three levels, a root, the PCA's and the CA's. The root is needed so that the international standards "work" and to register the Policy Certification Authorities. The root sets some minimum standards that all PCA's must follow, that is, what information a PCA must tell its customers so that they can compare the services offered by different PCA's. The root must also verify that applicants for a PCA are who they claim they are. After verification, the root will sign a certificate for the PCA.

The specific criteria for various levels of assurance will not be set by the root. Each PCA will have a policy statement that specifies, for instance, how it protects its keys, how often it issues CRL's, etc. It is anticipated that there will be a range of PCA's from high quality with rather stringent requirements to a low end, persona PCA which offers an anonymous service with no verification of identity, only a guarantee of uniquely named certificates. A draft policy statement for a high quality PCA will be circulated on the PEM-DEV list early in the first quarter of 1993. It will include many of the things listed about responsibilities of a CA with regard to CRL's as stated earlier in the X9.F standards activities presentation.

A question was asked about how an infrastructure for the federal agencies would fit into this particular hierarchy. The response was that they could be another PCA. It was again emphasized that there is no relationship between the name of the PCA and the rest of the certification tree below it. In principle, it would be possible to have a PCA for each domain and have the PCA's cross certify themselves. This leads to the problem of determining the exact assurance that one has in any given certificate chain. Having one root solves a number of problems, it provides a certain level of confidence by specifying the rules that a PCA must follow and you only need one public key, the key of the root, to build correct certificate paths. Steve asserted that having a level in the hierarchy that incorporates the idea of policy would be useful in supporting communities of interest and that the only remaining choice is how to implement it, either by using a root or by relying on cross certification. And if a root is seen as a useful feature, who will pick that root?

Some clarifications were made regarding how the PEM hierarchy worked. Anyone who is willing to abide by the rules that are common to all PCA's and pay the management fee to the root can become a PCA. The naming depth is arbitrary. Below the CA, all names are constrained to be subordinate to that CA. An individual may have multiple certificates representing different assurance levels and issued by the same CA (who is certified by two different PCA's). This can be accommodated with the 1992 format by using the UID field. It is also clear that a high assurance CA will charge more for its services. The hierarchy will be extended to include process names; a draft RFC discussing this will be released soon.

At this point, the meeting was adjourned, time had run out! Dennis

Branstad thanked all the attendees for coming and gave a special thanks to Steve Kent for being the workshop facilitator.

6. List of Acronyms

ACL	Access Control List
ANSI	American National Standards Institute
ADMD	Administrative Management Domain
CA	Certificate Authority
CCITT	International Telegraph and Telephone Consultative Committee
CEC	Commission of the European Communities
CRL	Certificate Revocation List
CSE	Communications Security Establishment
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
IRM	Information Resources Management
IP	Internet Protocol
ISO	International Organization for Standardization
NADF	North American Directory Forum
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
PCA	Policy Certification Authority
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standard
RFP	Request for Proposal
RSA	Rivest, Shamir, and Adleman
Stu-III	Secure Telephone Unit
UID	User Identifier

APPENDIX A

PUBLIC KEY INFRASTRUCTURE STUDY

CERTIFICATION WORKSHOP

David L. Gill

MITRE Corporation

Public Key Infrastructure Study
Certification Workshop

David L. Gill

10 December 1992

MITRE

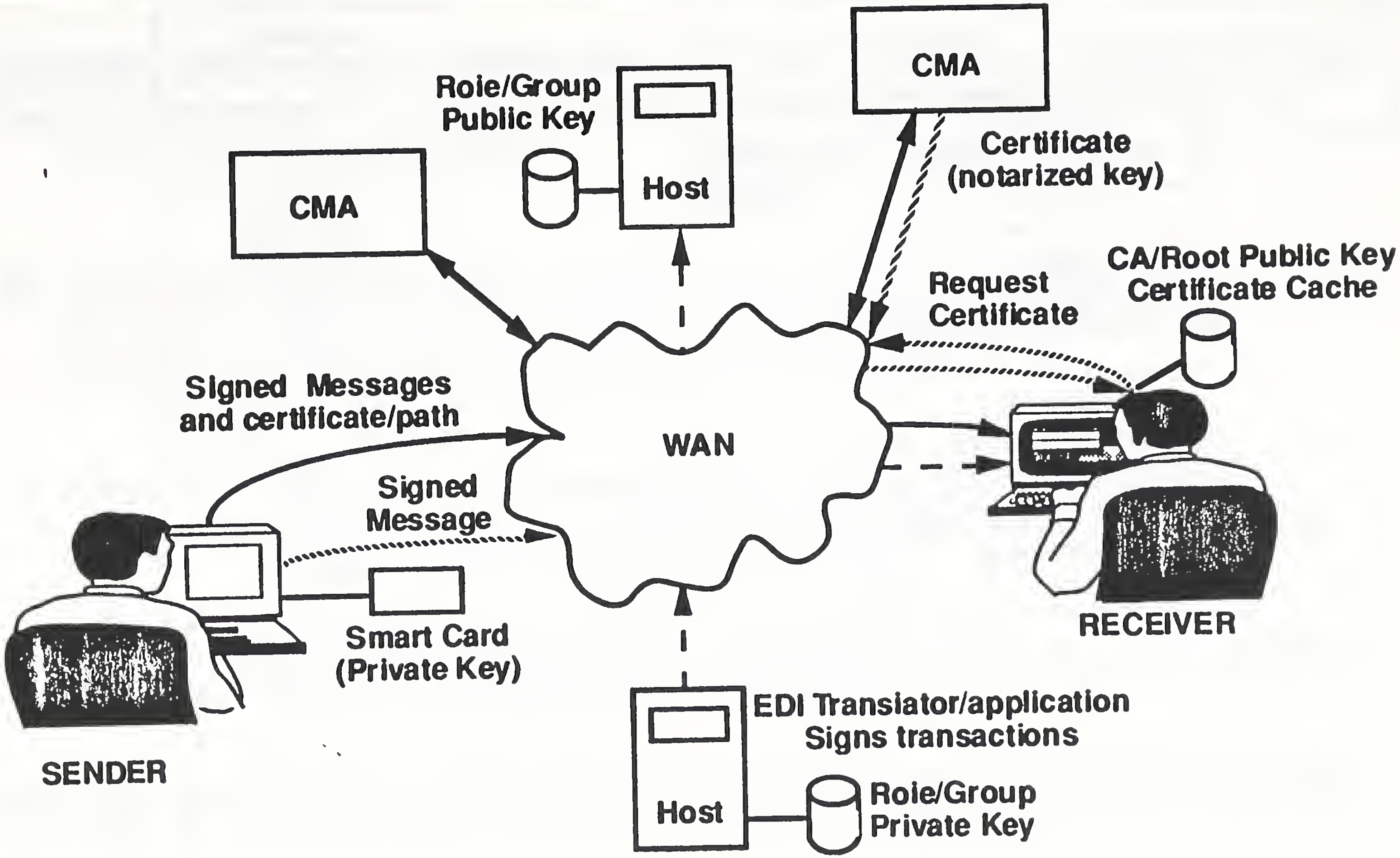
Overview

- Background of Public Key Cryptography Technology
- Public Key Infrastructure Study Overview

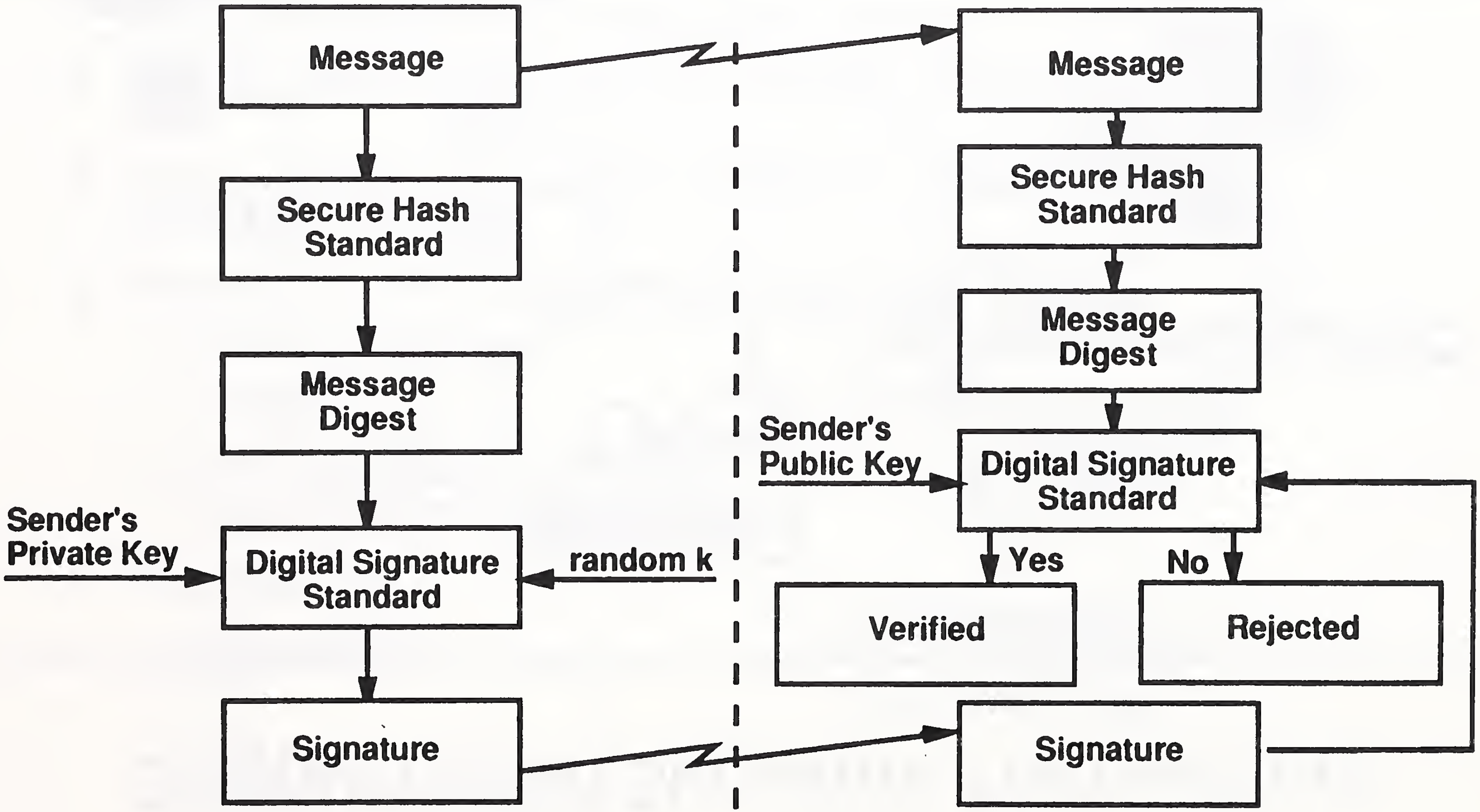
Key Aspects of Public Key Cryptography

- Based on mathematics of prime numbers
- Pair of related numbers (one public, one private) for each user
- Uses large prime numbers to counter the threat of exhaustive attacks
- Protocols used to provide following services:
  - Authentication
  - Integrity
  - Non-repudiation (sender)
  - Non-repudiation (receiver)
  - Secrecy/privacy
  - Sender anonymity
- Applications
  - Encryption
  - EFT
  - EDI
  - Digital Signature
  - Virus Protection
  - Key Exchange

Sample Digital Signature Transactions



Draft Digital Signature Standard Overview



Message

Secure Hash Standard

Message Digest

Sender's Private Key

Digital Signature Standard

random k

Signature

Message

Secure Hash Standard

Message Digest

Sender's Public Key

Digital Signature Standard

Yes

No

Verified

Rejected

Signature

MITRE

Need for the Infrastructure

- Need a means to accurately bind an individual's identity and public key. ⟹ Strong user authentication at the time of public key registration.

- Need a means for the receiver of a transaction to get sender's public key (Integrity of Public Key). ⟹ Use trusted certificate management authorities.

- Need to manage large number of public key certificates. ⟹Use a hierarchy of certificate management authorities.

- Need to deal with certificate invalidation due to private key compromise ⟹ Implement Hot lists.

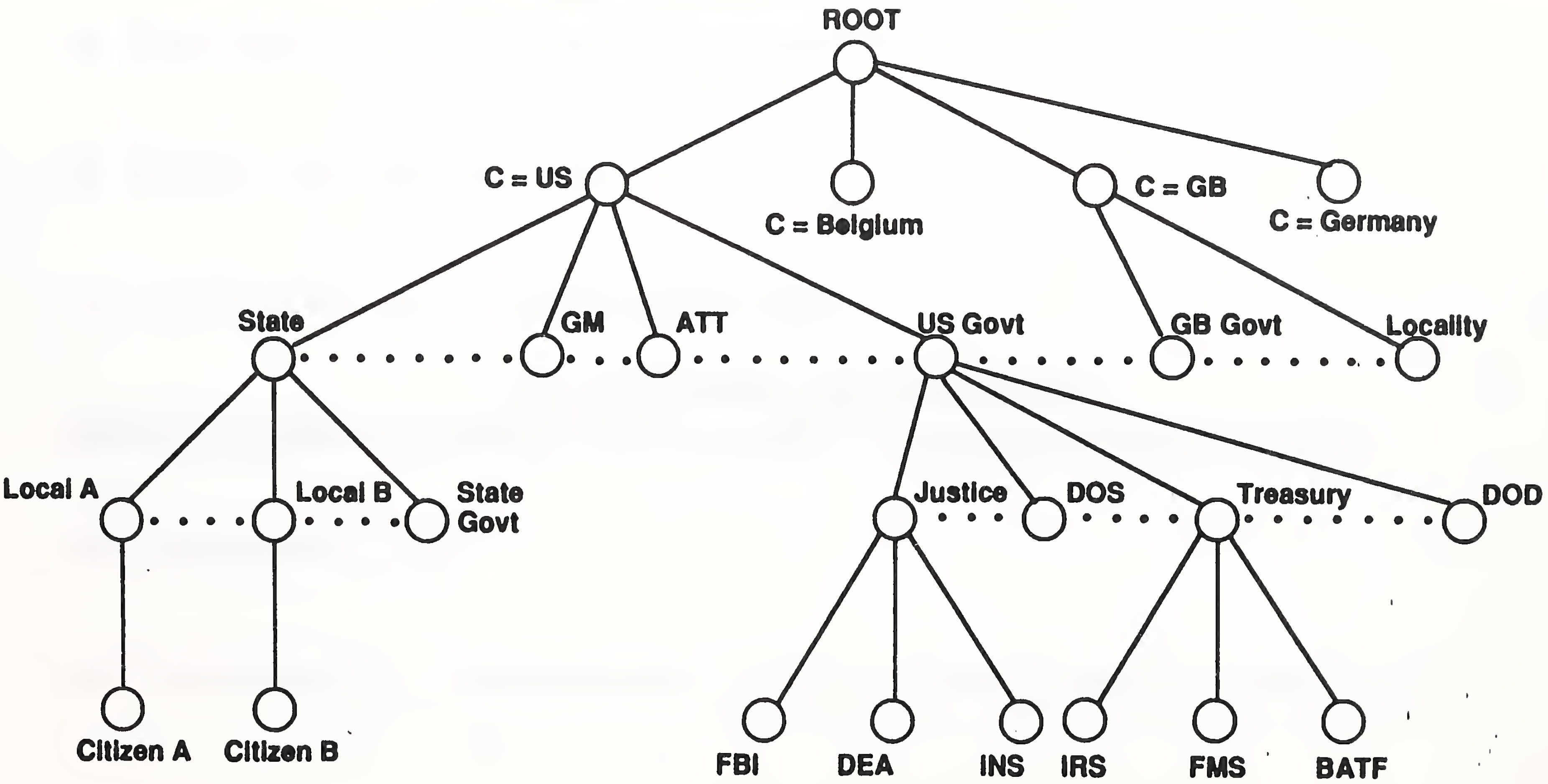
MITRE

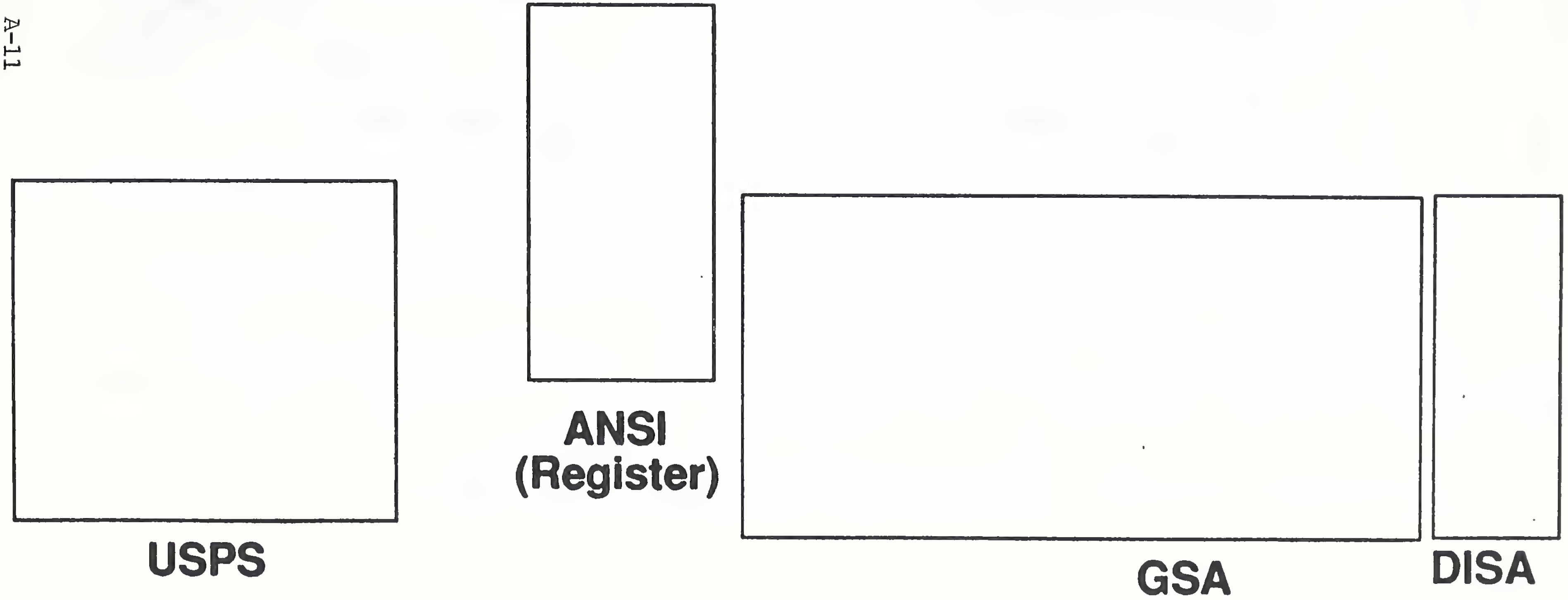
Possible Functions of a Certificate Management Node

- User Identification and Authentication
- Public Key Registration
- Certificate Notarization/Signature
- On-line Certificate Service
- On-line Hot List
- Centralized or Distributed Computer System Implementation

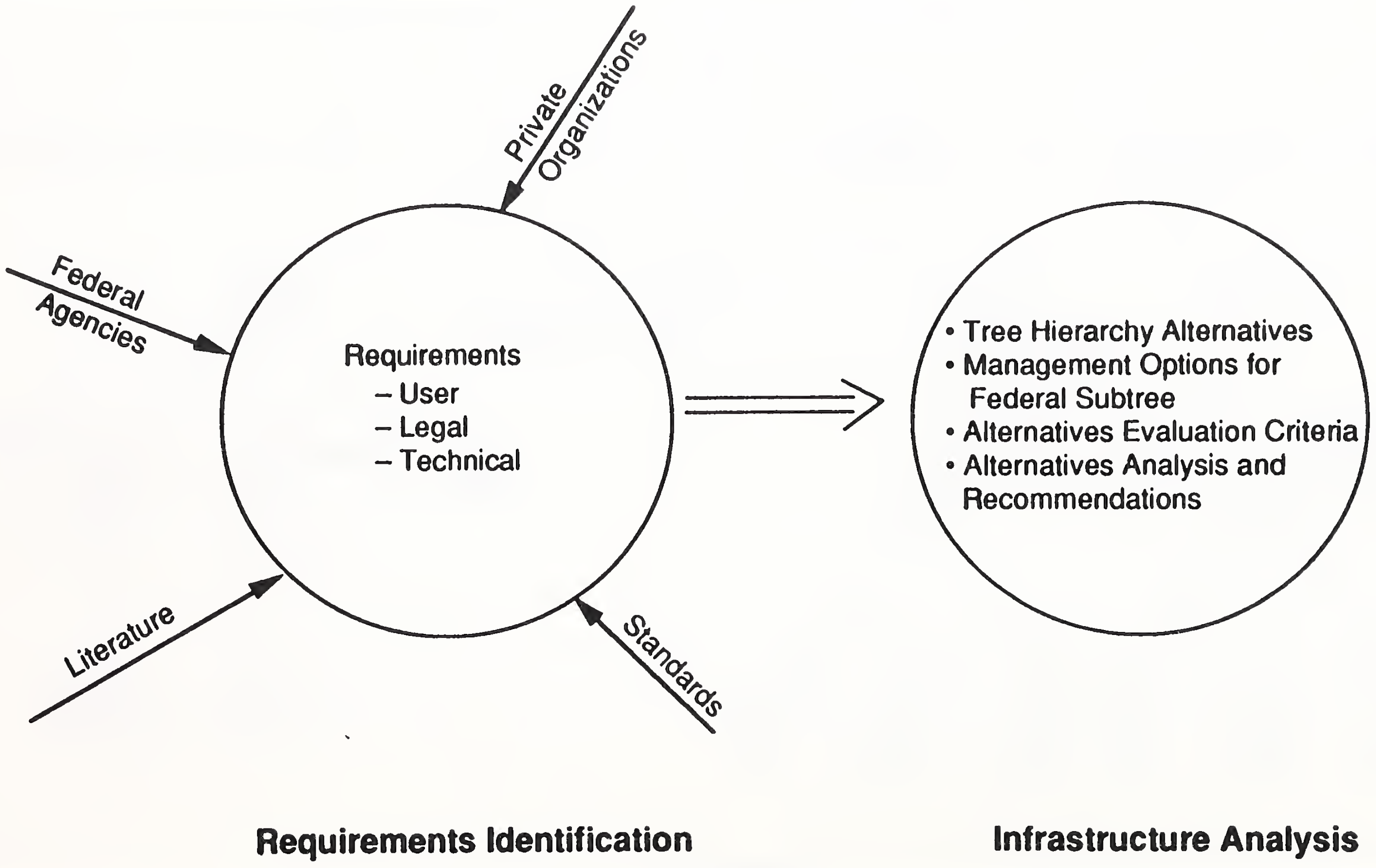
Infrastructure: Hierarchy of "trusted" Certificate (Public Key) Management Organizations.

Sample Infrastructure




ANSI
(Register)
USPS
GSA
DISA

Study Methodology



Federal Agencies

Private Organizations

Literature

Standards

Requirements
- User
- Legal
- Technical

- Tree Hierarchy Alternatives
- Management Options for Federal Subtree
- Alternatives Evaluation Criteria
- Alternatives Analysis and Recommendations

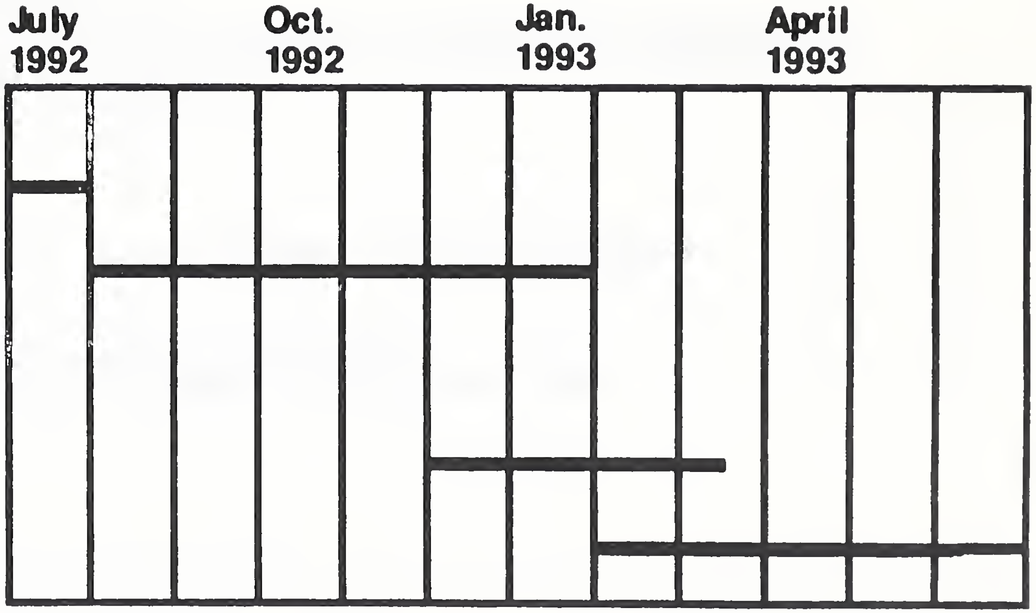
Requirements Identification

Infrastructure Analysis

MITRE

Overall Schedule

- Task Plan (Phase I)
  - Task Planning
  - Infrastructure Requirements
- Task Plan (Phase II)
  - Infrastructure Alternatives
  - Infrastructure Analysis



Players

- NIST
  - Lynn McNulty, Contracting Officer's Technical Representative (COTR)
  - Miles Smid, Dr. Dennis K. Branstad, Vicki Howard
- Participating Agencies (Funding)
  - Defense Advanced Research Projects Agency (DARPA)
  - Department of State (DOS)
  - Department of Treasury [Internal Revenue Service (IRS)]
  - Federal Bureau of Investigation (FBI)

Players (Concluded)

- Participating Agencies (Concluded)
  - General Services Administration (GSA)
  - National Security Agency (NSA)
  - United States Postal Service (USPS)
  - NASA

- Participants
  - Office of Management and Budget (OMB)

- MITRE
  - Dr. Santosh Chokhani, Task Leader
  - David L. Gill, Deputy Task Leader
  - Dr. Shimshon Berkovits, Judith A. Furlong, Shari B. Galitzer, Shirley T. Kawamoto, Judith R. Messing

MITRE

APPENDIX B

CERTIFICATE TECHNOLOGY FINDINGS

Shari Galitzer

MITRE Corporation

Certificate Technology Findings

Shari Galitzer

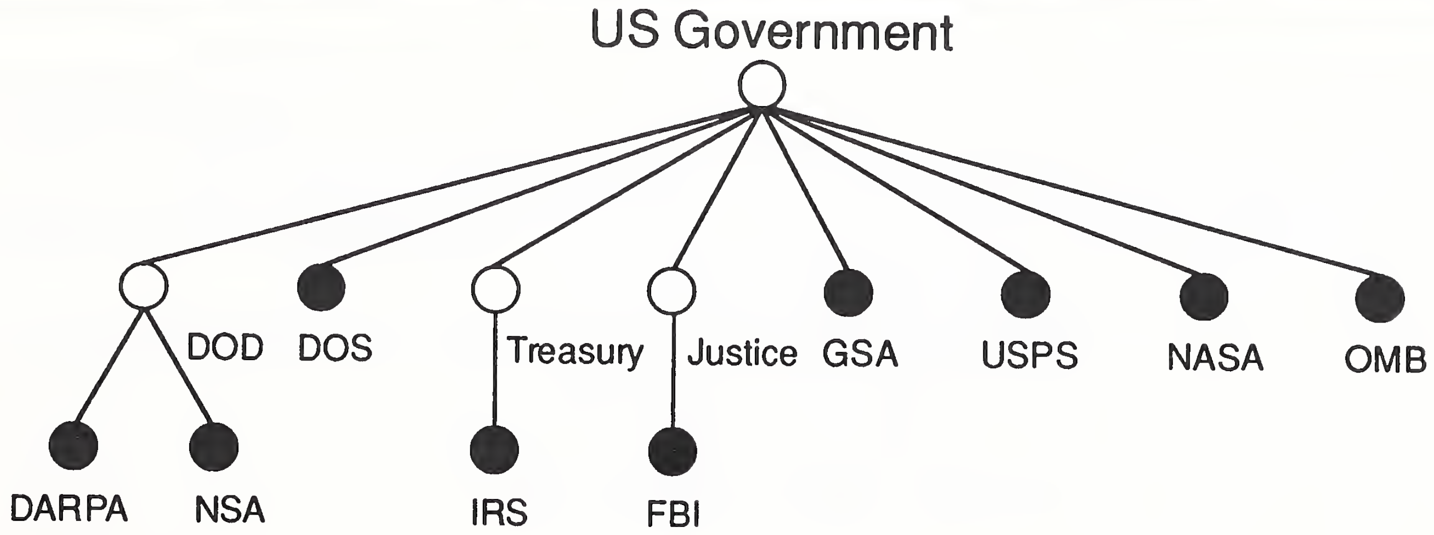
10 December 1992

MITRE

Outline

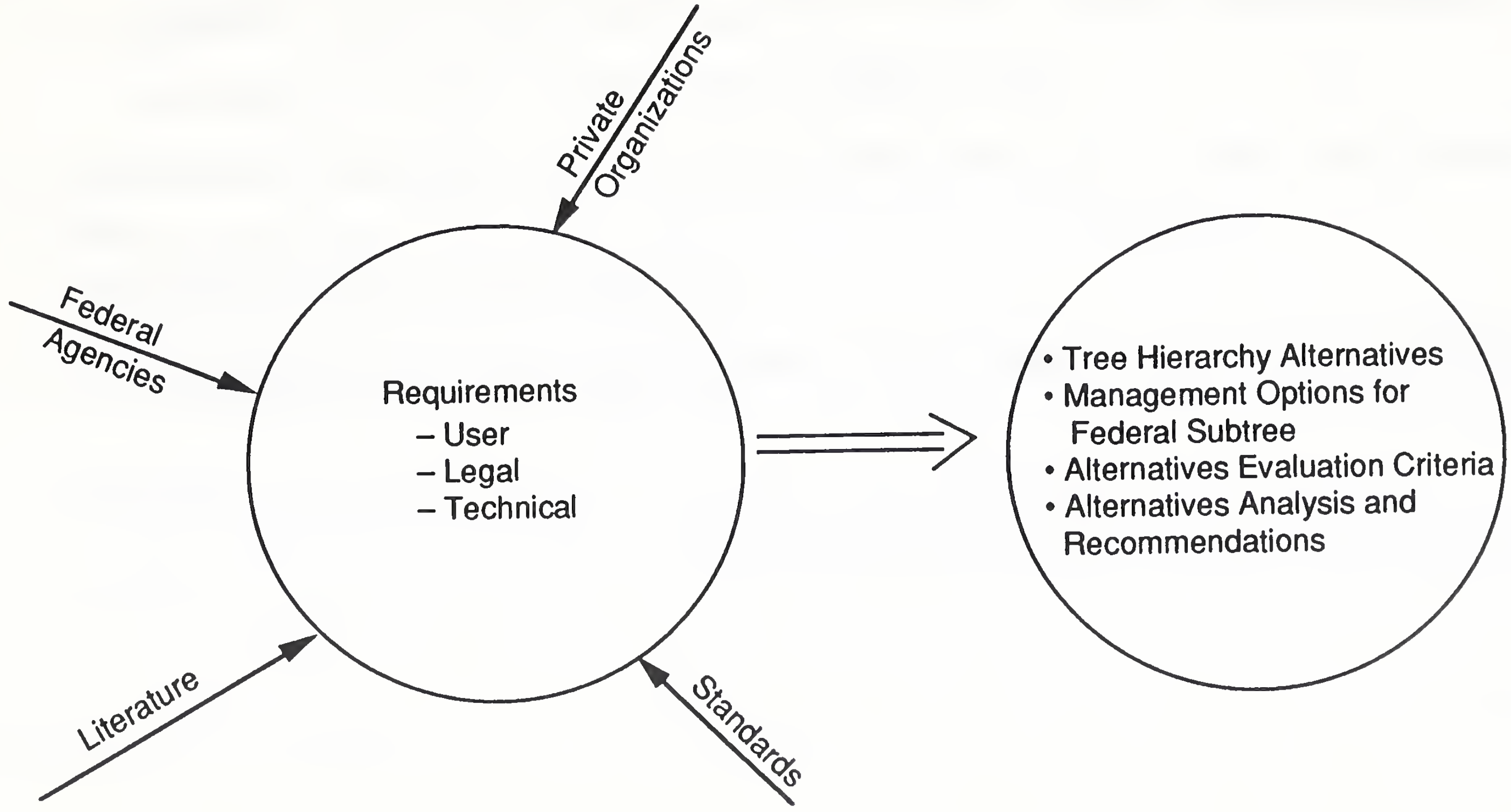
- The Scope of the Technology Study
- Issues to Address
- The Issues

The Scope of the Technology Study



- Analyze alternative infrastructures for managing public key certificates to support the Federal Agencies' applications that require digital signatures.
- Provide the base of the Infrastructure, and ensure it is able to evolve.

Study Methodology



Federal Agencies

Private Organizations

Literature

Standards

Requirements
- User
- Legal
- Technical

- Tree Hierarchy Alternatives
- Management Options for Federal Subtree
- Alternatives Evaluation Criteria
- Alternatives Analysis and Recommendations

Requirements Identification

Infrastructure Analysis

MITRE

Issues to Address

- The Infrastructure is a management (the policies that govern a CA) and a data management problem.
- First identify and address the issues, and then apply the appropriate technology.
- Current findings are encompassed in a set of issues:
  - Architecture, e.g., the hierarchy
  - Policy and Security Policy, e.g., key generation
  - Functional components, e.g., the certificate contents
  - Resource requirements, e.g., the processing required

Architectural Issues

- How should the Infrastructure be formed?
  - Should it be a hierarchy? - yes
  - Should the infrastructure form along organizational lines?
  - Should the infrastructure form along communities of interest and the security requirements of these groups?

Architectural Issues (cont.)

* Groupings of similar functions, and functions with similar requirements will evolve from the analysis of the user and legal requirements.
* This analysis will also provide the basis for the certification revocation list (CRL), storage, and retrieval requirements.
* The communities of interest will be formed by the applications' requirements, analogous to PEM's Policy Certification Authorities (PCAs).

Architectural Issues (concl.)

- How does the infrastructure accommodate transactions with commercial and private entities?
  - The infrastructure could provide a "business partner" certification service.
  - The security requirements (i.e. policy) for an application may determine the most appropriate cross-certification mechanism for privately generated certificates.
    - * CRL management
    - * Other aspects of security required for managing the privately generated certificates.

Security Policy Issues

- Who should generate the keys?
- Security requirements for private key storage
- What should the infrastructure require regarding multiple roles of individuals?
  - Same public-key in multiple certificates
  - Same certificate for multiple roles
  - How to create the multiple distinguished names

Security Policy Issues (concl.)

- Security requirements for managing a CA
  - Providing the service, e.g., authentication requirements
  - Supporting functions, e.g., secure storage
- CRLs
  - Reporting
  - Availability, both distribution and real-time access
- Storage, Archival, and Retrieval of public keys and CRLs

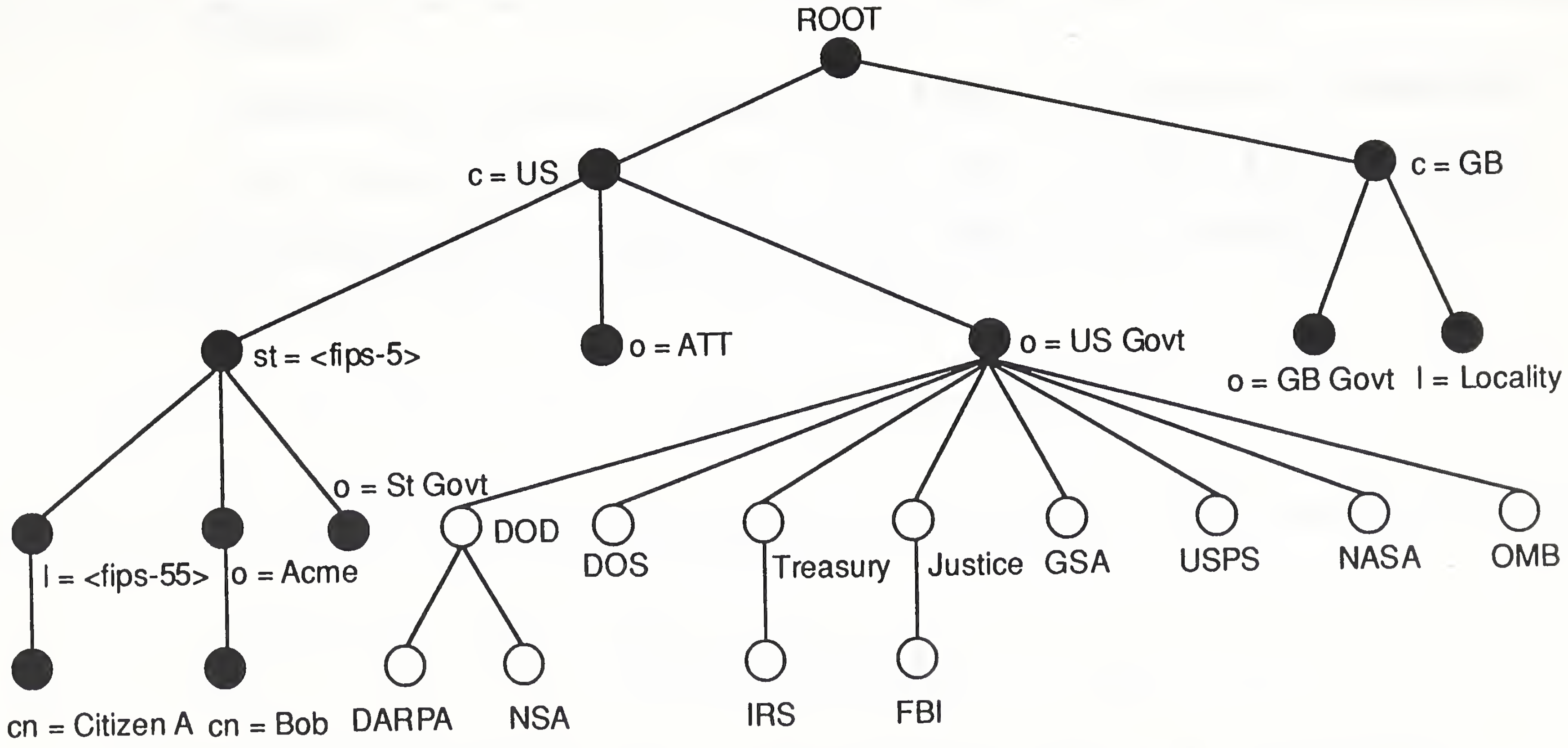
The Functional Components Issues

- Certificate contents - standard X.509

- Given no ubiquitous Directory Service, how do interim solutions impact the infrastructure?
  - Use existing databases, local applications, and out-of-band means
  - CRL management is viewed as the biggest challenge

- What to use as Distinguished Names
  - North American Directory Forum (NADF)

NADF



8-DEC-92

MITRE

The Functional Components Issues (concl.)

- The naming scheme for the USGovt branch:
  - * One consideration is FIPS 95, Codes for Identification of Federal and Federally-Assisted Organizations.
  - * Who is going to decide?

The Resource Requirements of the Technologies

- The cost in time and dollars is the driving factor when considering various technologies.
- What are the most useful cost metrics?
  - Pilot projects:
    - certificate management
    - directory services
  - Other internetwork management functions

APPENDIX C

ELECTRONIC SIGNATURE

THE KEY TO MOBILITY

Commission of the European Communities

Results of the Call for Ideas

October 1992

COMMISSION OF THE EUROPEAN COMMUNITIES
Directorate-General XIII Information Technologies and Industries
and Telecommunications
Directorate B RDT Actions: Telecommunications

S

Electronic Signature
The Key to Mobility

Results
of the
Call for Ideas

October 1992

COMMISSION
OF THE EUROPEAN
COMMUNITIES

Brussels, 2 October, 1992
XIII/B5 InfoSec

Directorate-General XIII
Information Technologies and Industries, and Telecommunications
Directorate B - Actions RDT: Telecommunications

Electronic Signature

The Key to Mobility

Results of the Call for Ideas

TABLE OF CONTENTS

The views put forward in this report are those extracted from the contributions received under the "Call for Ideas". This report should not be viewed as presenting the formal view of the Commission of the European Communities.

1. INTRODUCTION

The Council of Ministers adopted on March 31 1992 an action in the field of Security for Information Systems. This action is now implemented in close collaboration with the administrations of the Member States via the Senior Officials Group on Information Systems Security, SOG-IS.

As part of its work, SOG-IS agreed on a consultation of interested sector actors on the concept of *Electronic Signature - The Key to Mobility.*

As a first step, it was decided that the current views on the use and functions of such a capability should be identified through a 'Call for Ideas'. To facilitate this process, an initial Reflection Note was distributed in May 1992, as a first indication of the scope under consideration.

A large number of contributions were received in response to this 'Call for Ideas'. This present document provides an indication of the important comments and ideas with respect to the Reflection Note and some of the issues requiring further consideration. Also included in the Annex of this present draft are a selection of those contributions that provided the most interesting feedback.

This document and the contributions identified in the Annex will be used as the basis of the workshop that is being scheduled. This workshop will assist in the consolidation of the contributions received and a clarification of the scope and action with regard to an Electronic Signature capability.

The emphasis in this document is on the ideas received. This document, therefore, does not present results from other Community activities, of which there are several, related to the concept of an Electronic Signature; for example results from the TEDIS programme (see TEDIS Programme 1988-89 Activity Report COM(90) 361 Final, the Reports of the TEDIS Workshops June 1989, and the Report "Service Infrastructure for EDI Security", etc.) or other actions related to data protection, legislation and regulatory issues .

The views put forward in this report are those extracted from the contributions received under the "Call for Ideas". This report should not be viewed as presenting the formal view of the Commission of the European Communities.

2. SUMMARY OF CONTRIBUTIONS

2.1 Overview of Responses

The Reflection Note on Electronic Signatures (ESs) resulted in an overwhelming response from a wide cross-section of interested parties. The written responses provided a wealth of ideas, some old ideas presented in a different form and some completely new ideas. In addition, these contributions raised a number of issues.

There was a general feeling that an ES capability has a significant part to play in public, private and commercial life. It was also felt that the ES concept is one of the early steps towards the long term use of information security technology satisfying a broad base of application needs.

Despite the lack of an exact definition for an ES, there was no shortage of responses with feasible interpretations of the ES concept. There were a number of contributions that defined an ES as a concept capable of offering 'personal identification', 'originator authentication' and 'equipment / resource identification'.

Other contributions were less broad in their approach focusing on a more restrictive set of functionality. Some contributions quite simply equated the ES concept with digital signatures, smart cards and existing products and technology. Whatever the finally agreed definition is, the wealth of ideas as a result of the call reflects considerable interest and concern in this area.

As one might expected user requirements, legal and regulatory issues, technology and operational aspects featured high in many of the contributions. What follows is a summary of the major issues that appear in the contributions. This list of issues is not exhaustive and the planned ES workshop will no doubt identify possibly more issues.

2.2 General Comments

Requirements, Economics, Markets, Legal & Regulatory Aspects

o A high level model is required to match user requirements and application needs against the technological possibilities for an ES capability

o Early action is required to distil an agreed long-term vision of the expected role of ESs within society

o It is important to have as wide a view as possible with regard to the possible application of an ES capability, current attempts at providing an ES capability often satisfy narrow operational requirements, in particular the significance of mobility is less pronounced

o The significance of mobility for economic success and positioning is increasing: there is a need for a socio-economic reference model for the use of ESs

o Need to develop specific users scenarios illustrating the role of an ES in real areas of application

o Greater awareness and application of an ES capability is needed before establishments will be ready to accept them

o Legal acceptance and admissibility of the ES methodology is a major prerequisite and in some areas of ES application of paramount importance

- Work on legal and regulatory aspects should be given a high priority complementing all other areas of activity exploiting existing work on digital signature

- Different ES applications may have different legal and regulatory demands

- Legislation associated with electronic documents (e.g. in Sweden) uses the concept of signature to prevent document forgery

Functional Capabilities, System Concept & Technology

- Agreement is required on the following - What range of functions should the ES have? What are the minimum desirable security requirements for each type of function? Which functions are technically feasible?

- The ES capability should be part of the comprehensive open systems architecture currently being developed, taking into account existing standards and technology were they exist?

- ES and distributed system security go hand in hand, and so the ES concept should be an integral part of future distributed system strategy and policy

- It is important to consider what connects, and not what divides (which often is the case when commercial interests are involved)

- Standardisation is a major technical problem with regard to signature technology e.g. establishing an open systems approach to ES facilities

- The ES technology should be developed to an acknowledged level with regard to functionality and assurance, in particular the concept should be developed consistent with the ITSEC approach

Operational & Management Aspects

- Potentially ES technical issues are of less complexity compared to those concerned with the administration and management of an ES capability

- A user-organisation design concept needs to be developed

- Information flows, data linking and their system re-evaluation e.g. in the area of medical informatics information labelling

- Lost cost solutions are required for the management of ESs with supporting operational infrastructure

- There is a need for one access device to access many services and so it is necessary to manage different services within different application segments

- The method of management should have high integrity

Verification of ES Concept

- First prototypes should be well focused on areas of immediate significance to ES to validate early user acceptance and to show the benefits and opportunities provided by ES in a realistic environment

- Such verification of the ES concept is required at an early stage of the ES activity before large scale implementation and introduction can take place

3. OVERVIEW OF ISSUES

3.1 Specific Issues and Ideas

The following issues and ideas have been extracted from the contributions received. This is not a definitive list of the issues and ideas on those presented. However, they do represent a large sample of the major issues identified by the contributors.

Use and Application of the ES Capability

o The following is a list of suggested uses of the ES capability compiled from the contributions received (NB because of the wide range of terms used to mean different things or to illustrate different concepts, the list below does not differentiate between the terms used):

- 'personal identification', 'originator authentication' and 'equipment / resource identification'.
- applications requiring the use of non-repudiation services
- electronic passports / ID cards
- product stamping to ensure its integrity and authenticity (e.g. software stamping, together with its development / updating / maintenance history)
- electronic document security / copy management and protection
- use in personal communications
- electronic mail folder
- electronic purse / wallet
- road transport payments (parking, fuel stations, tolls, information services, road haulage payments)
- access to databases and more general to telematic services
- applications requiring use of remote control capabilities (e.g. in safety critical and hazardous environments)
- physical access

o The following is a list of suggested areas of application compiled from the contributions received:

- telecommunication & broadcast systems (e.g. GSM, satellite services, television services)
- personal mobile appliances (e.g. PDAs, personal communicators, personal information, personal payments etc)
- aerospace systems
- medical systems (e.g. patients records, medical databases, primary care systems, distributed decision and executive support systems, telemedicine services (home care & mobile), communications, drug administration, general administration, access to restricted areas)

- transport systems (e.g. airport environment - aircraft maintenance, customs & VAT, duty free, access to restricted areas, ticketing and reservations, baggage control etc)

- industry in general (e.g. for production control, mobile data gathering (PDAs), sales)

- social services & local government systems (e.g health, welfare, taxation, passports, Customs & Excise etc)

- police systems (e.g. communications, access to restricted areas, electronic police records)

- banking & payment systems, retail systems

- EDI-based trading systems & other VAN systems

- teleshopping / telebanking

o The broad scope of ES suggests that it might not be feasible to produce a unique universal ES solution (but it is essential to define a broader approach which defines a conceptual framework (i) allowing for a variety of ES solutions on a per application domain(s) basis, (ii) for ensuring upward compatibility between ES solutions of varying complexity and (iii) open to simple solutions that are technically and economically feasible)

o A need to consider the requirements of personal data protection and the prevention of data linking

o There is a need for users to be on an equal footing with application / service providers - current systems do not offer the same level of protection to users as to the providers of services and products

o The legal and logical aspects of security must be looked at together from a business point of view (commercial interests), a personal point of view (data privacy interests) and a public point of view (society and the quality and safety of life)

Functions of the ES Capability

o The following is a list of suggested functions of the ES capability compiled from the contributions received (NB because of the wide range of terms used to mean different things or to illustrate different concepts, the list below does not differentiate between the terms used):

- user / data origin identification and authentication

- copy management

- user access control

- data / file / document access control

- the integrity / authentication of data / documents / messages / resources etc

- confidentiality

- authorisation, audit and accountability

- electronic personal organisers, notebooks, pen computers and Personal Assistants (PAs) / Personal Data Assistants (PDAs)

o The ES capability as a new technology versus the use of current smart card technology

o Notarisation techniques need to be considered

o Tamper proofing techniques are important

o Biometric techniques should be considered (voice, finger print etc)

o Commensurate with the scope of the ES capability the memory capacity could be significantly large (secret / private information, control information, work space, program memory etc) - this may be a practical limitation to its final definition

o The ES capability must be user / owner / closed group activated only

o The ES capability should have a keyboard and display as suggested in the Reflection Note

Operational and Management Aspects

o An easy to use, cost-effective solution is needed for ES

o Multi-system portability and interworking is essential in multi-application and service environments

o ES product related security evaluation is important

o The security management of the ES functionality should be as simple as possible without compromising the security of the ES overall

o Control of the use and issue of ESs are an important concerns needing practical solutions (economic, legal and personal issues). What are the requirements on trusted mechanisms and processes for the deployment and maintenance of ES capabilities? There are important issues concerned with the personalisation of ES related products

o What international aspects need to be considered e.g. public-key certificates in the case of digital signature techniques, directory services for certificates?

o The establishment and operation of some of the technical / legal aspects for handling repudiation / non-repudiation claims etc

o ES solutions must aim to exploit future technology

o Is there a need for ES related product identifiers as in the case with GSM ?

ANNEX A LIST OF CONTRIBUTORS

Thanks are due to the following individuals and organisations for their contributions in response to the Call for Ideas.

ABI, UK	P W Lever
Alcatel Telecom, Norway	K Presttun
Alcatel TITN Answare, France	B Passagez
Allianz, Germany	B Senff-Schöne
Anitra Medienprojekte GMBH	W Boc
Ascom Tech AG, Switzerland	A Beuchat
Association Belge des Banques, Belgium	J Van den Nieuwenhof
Bakkenist, The Netherlands	P van der Meijs
Baltimore Technologies, Ireland	Dr M Purser
Bancamatica, Italy	A Biasiotti
Banesto, Spain	J D Lifante
British Bankers' Association, UK	A A Kettley
British Computer Society, UK	Dr F E Taylor
British Telecommunications Plc, UK	D Willetts
Bull, France	D Pinkas
Bull CP8, France	J Patarin
Bundesverband deutscher Banken, Germany	N Schmitz
CAP debis GEI, Germany	F-P Heider
CAP SESA Finance, France	P de Kervasdoue
CEC DG XIII/D-5, Belgium	P Husson
CEPIS, UK	P Walmisley
Comatlas, France	A Dubreuil
Computer Audit Specialist Group - BCS, UK	Dr J A Mitchell
Computer & Systems Telecommunications Ltd., UK	Dr S Castell
Data Security Consultant, UK	D Watts Davies
Der Landesbeauftragte für den Datenschutz N-W, Germany	Dr P S Pütter
DCE Nederland B.V., The Netherlands	H Wierenga
Digital, France	Y Le Roux
EDP Audit Pool, The Netherlands	H de Zwart RA
EDS, Belgium	H Ardies
EDS Scicon, UK	T C R Nicholson
ENST Bretagne, France	P Rolin
Fern Universitat , Germany	Prof.Dr-Ing F Kaderali
Fraunhofer-IAO, Germany	H Meitner
Gemplus Card International, France	O Trebucq
Genesis, Austria	Ms I Schaumüller
Geneva Management Group, Switzerland	R I Polis
Gesellschaft für Mathematik und Datenverarb., Germany	M Agi
Gesellschaft für Mathematik und Datenverarb, Germany	Prof Dr E Raubold
Giesecke & Devrient GmbH, Germany	Prof Dr E Klein
Hewlett-Packard Labs, UK	Dr V Varadharajan
IBM European Networking Center, Germany	Dr H Fanderl
IBM Semea S.p.A., Italy	F Zanon
Information Security Corporation, USA	T J Venn
Information & Systems Management Ltd, UK	E T Peers
Inforama, France	R Guillaumot
Innenministerium Baden-Württemberg, Germany	Dr Frömel
Intercai Advanced Telematic Skills, The Netherlands	R van Eijk
via Internet	Dr J Linn (USA)
via Internet	Mr Kent (USA)
via Internet	B Kaliski (USA)
ITS, Sweden	P Hoving
Johan Wolfgang Goethe - Universität Frankfurt, Germany	Prof C P Schnorr

K&M Technologies	HJ Kugler
The Kingswell Partnership,UK	W List
KPMG, The Netherlands	H Roos
KPMG Consultants Ltd, London, UK	Dr B Collins
Kryptokom & P3K, Germany	C Ruland, J Fernandez
Logica Defence & Civil Government Ltd, UK	J Wilde
Logica Finance Ltd, UK	G Smith
The Management Consulting Group, UK	R Horrocks
Marinade Ltd, UK	J King
Math RiZK, University of Louvain, Belgium	J-J Quisquater
Matra Marconi Space, France	B Hurt
MHP B.V. Associates , The Netherlands	Ir A A van Kranenburg
Ministry of Defence, UK	D Hughes
Ministry of Finance SAMS, Sweden	P Svenonius
The Mitre Corporation, USA	J Edelheit (USA)
National Physical Laboratory, UK	F Williams
Nationale Raad voor de Volksgezondheid,The Netherlands	L Ottes
Northern Telecom, UK	J E Ettinger
O.C.T	JM Castellet Mart
Ott Technology Software Sprl, Belgium	K-W Ott
PBS, Denmark	P Terp / P Fjelbye
Philips MBLE, Belgium	Dr M de Soete
Philips/TRT, France	F Petit
Protexarms, France	A Brignone
PTT Research, The Netherlands	M van Zoelen
Royal Holloway & Bedford New College, London	Prof. F Piper
RWTUV, Germany	Dr R Baumgart
SAP AG, Germany	K Tschira
Saritel s.p.a. Sarin Telematica, Italy	M Saponaro
Security Engineering, Switzerland	Dr R A Rueppel
Security & Standards Consultancy Ltd.UK	J Ross
SEMA Group Consulting Ltd, UK	R P J Winsborrow
SEPT (France Télécom-La Poste), France	E Delacour
Siemens AG, Germany	Y Léauté
Siemens Nixdorf, Germany	D Kruse
Stockholm University, Sweden	Prof Dr S Muftic
Swedish Committee on Computer Related Crime, Sweden	P Furberg
Swedish National Police Board, Sweden	J F Wester
TeleTrust Deutschland e.V	H Reimer
Thomson-CSF/RGS, France	J Lebidois
Triple P. Management B.V., The Netherlands	J Raak
TSC, Spain	L Tudanca
UCL, UK	P Kirstein
University College Dublin, Ireland	A Patel
University Computer Laboratory	Anderson / Kelman / Lomas
Universität Hildesheim, Germany	A Pfitzmann
University of Patras, Greece	Prof A A Sissouras
Universitat Karlsruhe, Germany	Dr M Waidner
UTI Maco Belgium	M Mergeay
XP Conseil, France	P-L Refalo
Zergo Consultants Ltd. UK	Dr J Leach

ANNEX B. SUMMARY OF INTEREST

B.1 Main Areas of Interest

	Number of papers	Requirements	Political & Legal Issues	System Concept	Technology	Operation & Management	Others
Austria	1						
Belgium	7	3		4	4	3	3
Denmark	1	1		1	2	1	
France	15	5	1	10	9	3	1
Germany	21	8	5	16	13	7	4
Greece	1	1		1	1		
Ireland	2			2	2	2	
Italy	3	1	1	3	1	1	
Netherlands	9	8	3	10	7	5	2
Norway	1			1	1		
Spain	2					2	1
Sweden	5	1	2	4	2	4	3
Switzerland	3	2	1	2	2	1	1
UK	25	14	6	15	18	14	8
USA	5			5	6	6	6
Totals	101	44	19	74	68	49	29

B.2 Sector Responses

	No of contributions
Academic institutions	20
Financial institutions	2
Government Depts.	10
Management Consultants	23
IT Manufacturer	25
System Houses	16
Telecommunications Operators & Equipment suppliers	5

ANNEX C SOME CONTRIBUTIONS OF INTEREST

The following contributions are a selection of those received from the individuals and organisations listed in Annex A.

Bakkenist, The Netherlands	P van der Meijs
British Telecommunications plc, UK	D Willetts
CAP debis GEI, Germany	F-P Heider
EDS Scicon, UK	T C R Nicholson
Fraunhofer-IAO, Germany	H Meitner
Geneva Management Group, Switzerland	R I Polis
IBM European Networking Center, Germany	Dr H Fanderl
KPMG Consultants Ltd, London, UK	Dr B Collins
Logica Defence & Civil Government Ltd, UK	J Wilde
The Kingswell Partnership,UK	W List
Marinade Ltd, UK	J King
Nationale Raad voor de Volksgezondheid,The Netherlands	L Ottes
Northern Telecom, UK	J E Ettinger
Ott Technology Software Sprl, Belgium	K-W Ott
Philips/TRT, France	F Petit
Royal Holloway & Bedford New College, London	Prof. F Piper
SEMA Group Consulting Ltd, UK	R P J Winsborrow
Siemens Nixdorf, Germany	D Kruse
Swedish Committee on Computer Related Crime, Sweden	P Furberg
Thomson-CSF/RGS, France	J Lebidois
UTI Maco Belgium	M Mergeay
Zergo Consultants Ltd. UK	Dr J Leach

APPENDIX D

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION DIGITAL SIGNATURE AND SECURITY SERVICES (DS^3) SYSTEM

Lawrence P. Shomo

NASA

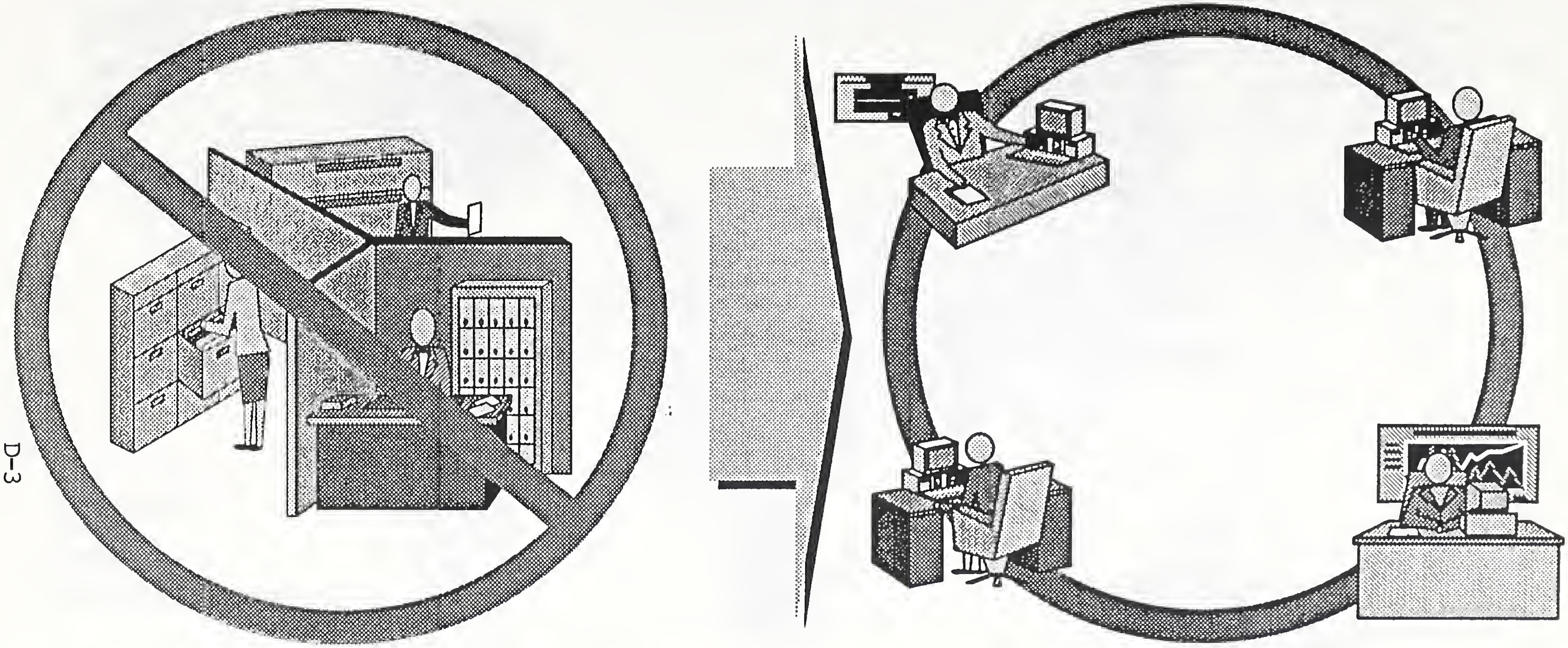
National Aeronautics and Space Administration

NASA
Digital Signature and Security Services (DS^3) System

Lawrence P. Shomo

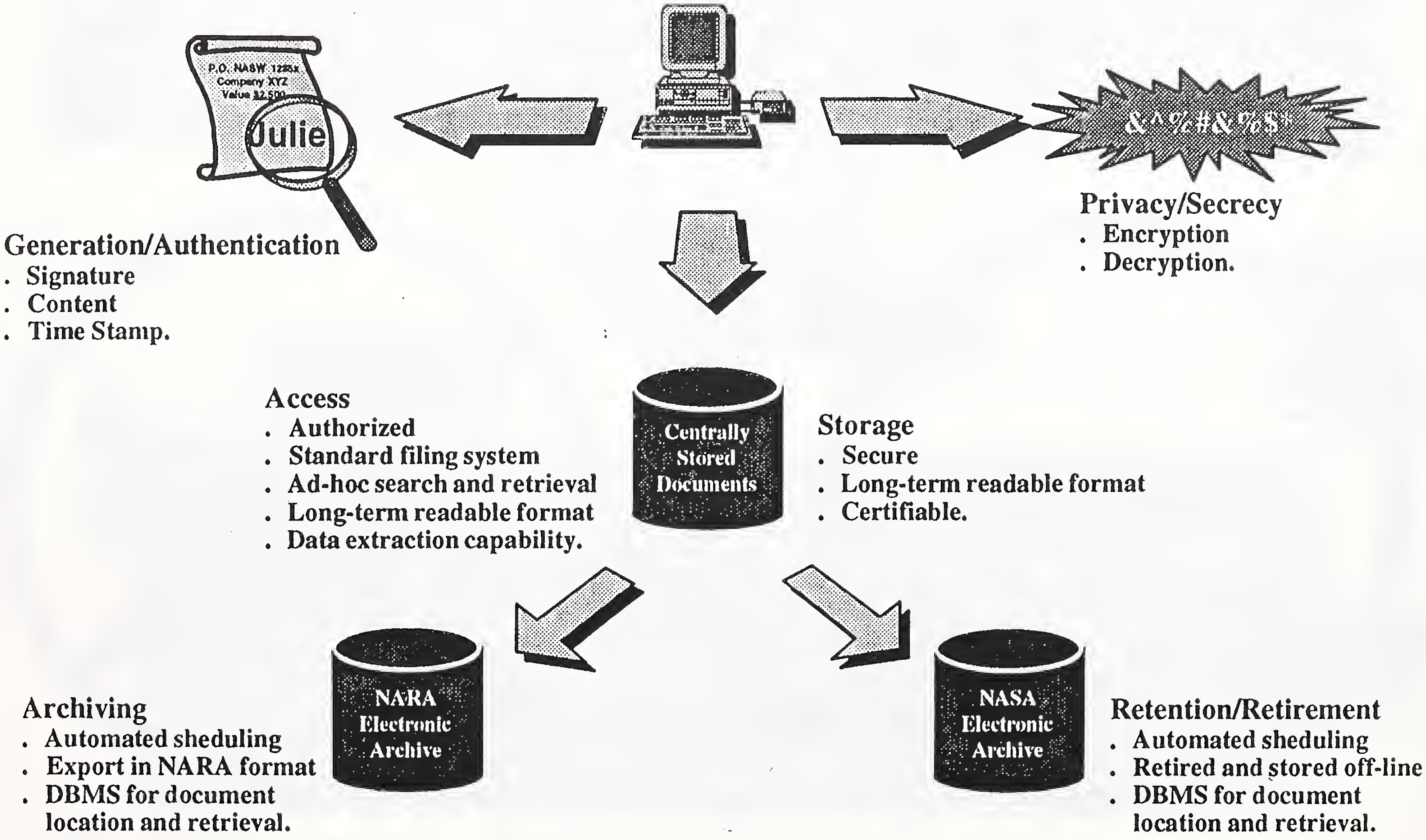
December 1992

Why Does NASA Need An Electronic Document Environment?



An Electronic Document Environment is required to allow NASA to replace paper documents and manual flows with electronic documents and automated flows, while maintaining or enhancing existing levels of security.

Requirements For An Electronic Document Environment



Generation/Authentication
. Signature
. Content
. Time Stamp.

Privacy/Secrecy
. Encryption
. Decryption.

Access
. Authorized
. Standard filing system
. Ad-hoc search and retrieval
. Long-term readable format
. Data extraction capability.

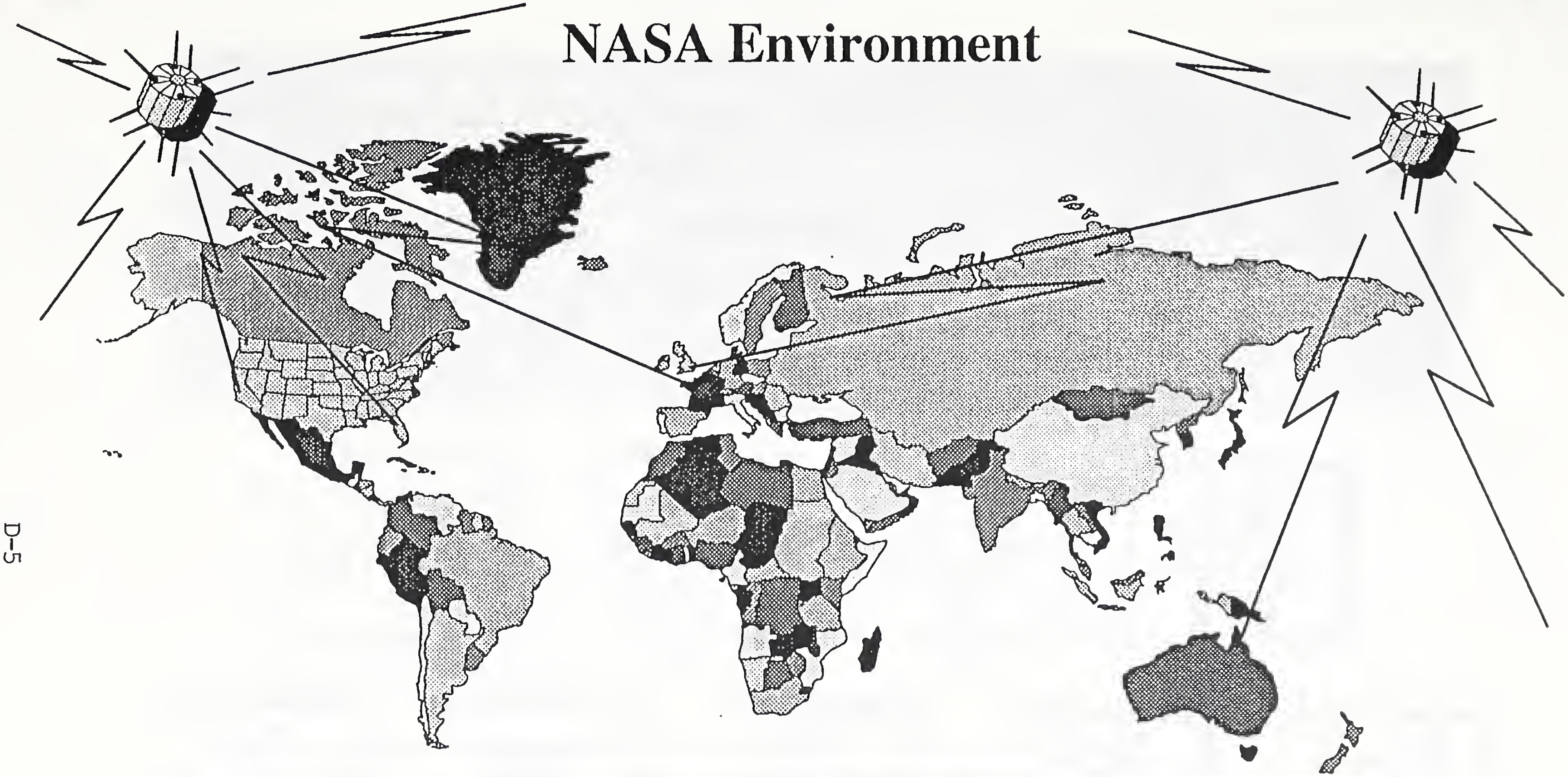
Storage
. Secure
. Long-term readable format
. Certifiable.

Archiving
. Automated sheduling
. Export in NARA format
. DBMS for document
location and retrieval.

Retention/Retirement
. Automated sheduling
. Retired and stored off-line
. DBMS for document
location and retrieval.

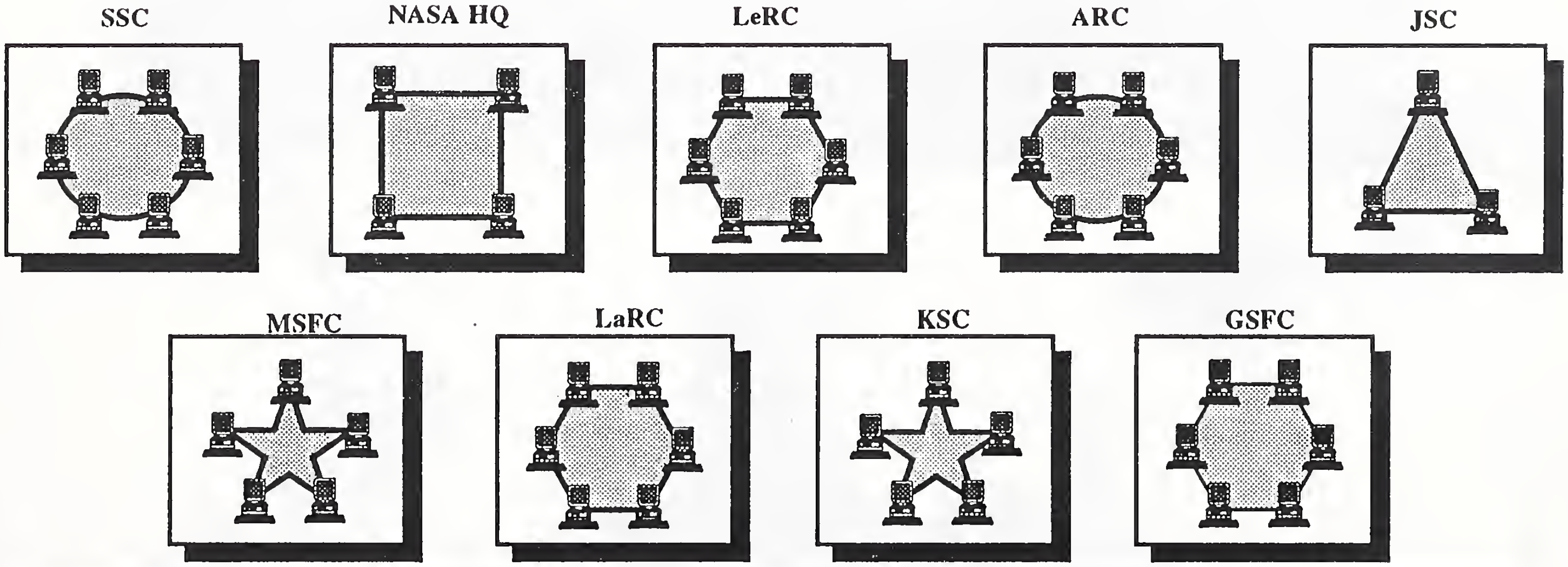
NASA Digital Signature And Security Services (DS^3) System

NASA Environment



- World-wide interactions in support of:
  - NASA contractors and businesses
  - Government departments, agencies, etc...
  - University and science communities.

NASA Environment (cont.)



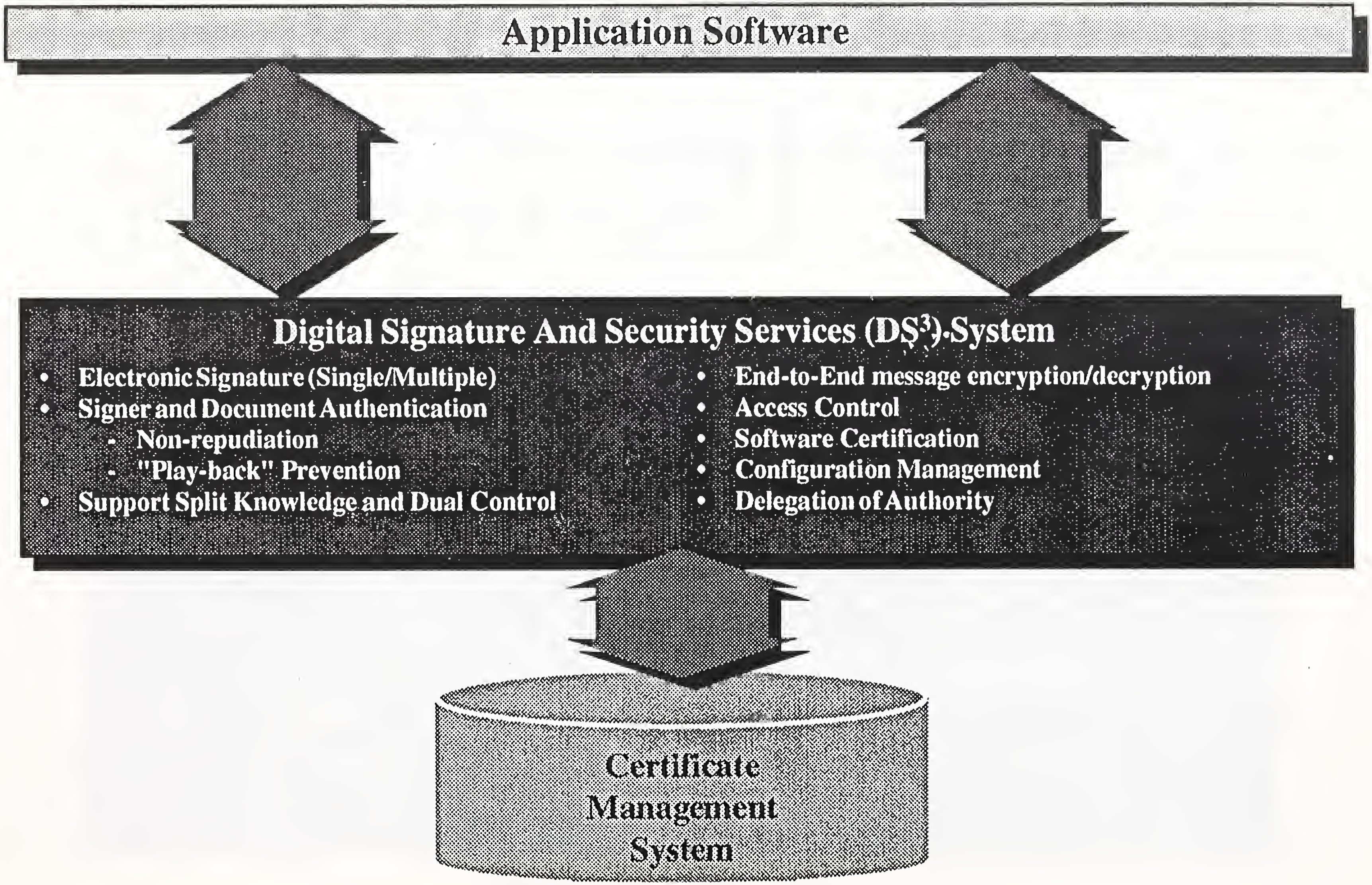
Operate In NASA's Heterogeneous Computing Environment:

- Mainframe, Minicomputer and Microcomputer application development environments
- PC platforms and operating systems
- Network environments.

DS^3 Objectives

- Single NASA-wide system
- Standard system which can be used by any application and Government Agency
- Portability across platforms
- Adhere to Government standards and policy
- Sanctioned in writing by GAO for Government use
- Public-Private Key-based (DSS)
- Interoperable with other mainstream Public-Private Key-based systems (e.g., RSA)
- Key Certificate Management
- Implementable in software-only and hardware configurations
- Cost effective.

DS^3 Services



Application Software

Digital Signature And Security Services (DS^3) System

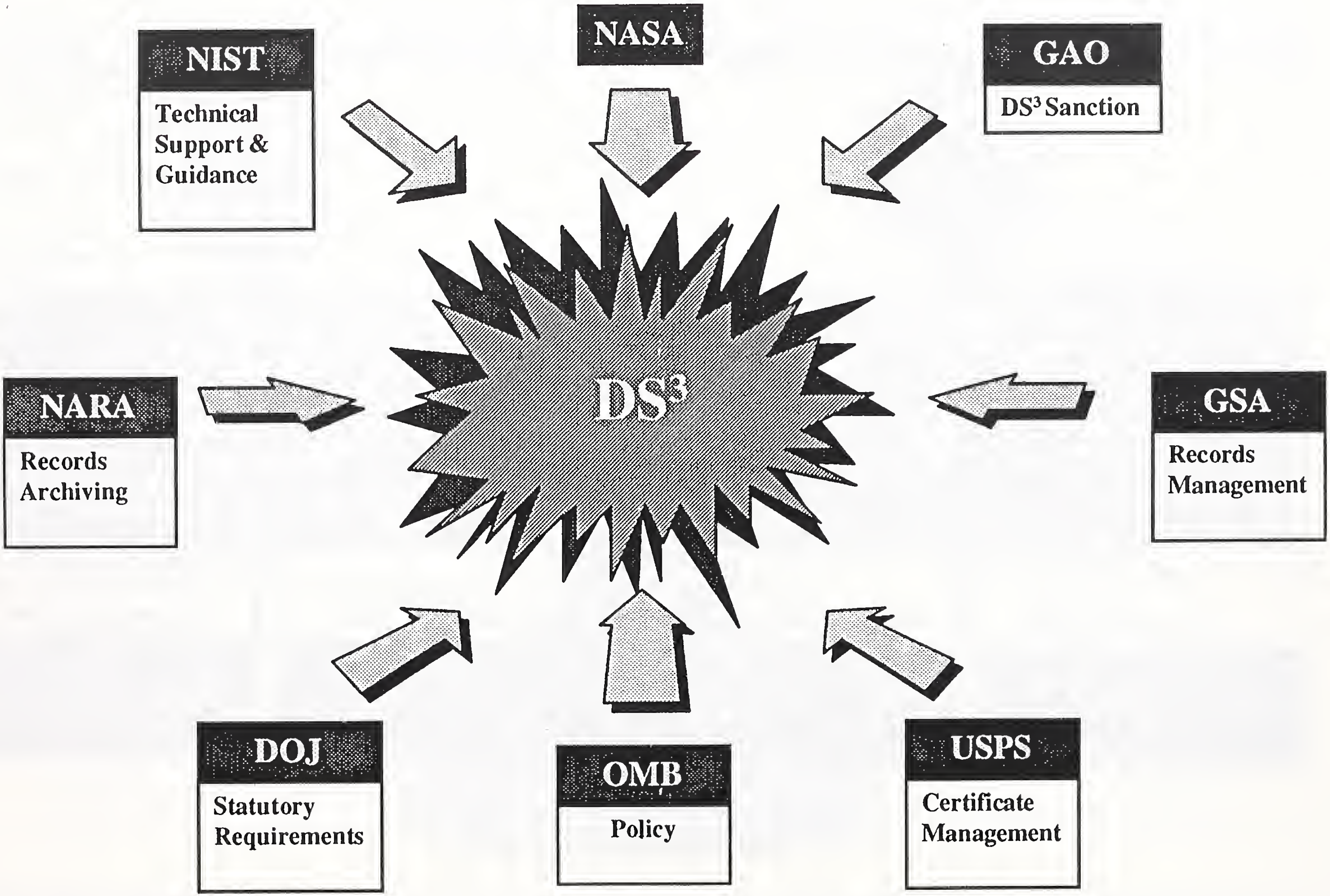
- Electronic Signature (Single/Multiple)
- Signer and Document Authentication
  - Non-repudiation
  - "Play-back" Prevention
- Support Split Knowledge and Dual Control
- End-to-End message encryption/decryption
- Access Control
- Software Certification
- Configuration Management
- Delegation of Authority

Certificate Management System

DS^3 Components

Certificate Management System Module	Distribution and Management System Module	Access Control Module	DS^3
• Provide information to and receive information from higher and lower level certification authorities • Publish Public Key directories • Issue certificates • Revoke certificates • Publish hot list directories • Maintain database • Hierarchical to allow center certification of center employees.	• Distribute Smart Cards and initial PINs • Distribute DS^3 software • Maintain database • Configuration control • May be hierarchical (NASA and centers).	• Provide a standard user logon interface • Authenticate user • Identify user access level and capabilities • Maintain audit trail.	• Standard services • Standard calls • Operate on a variety of platforms • Called by: - Application software - Terminal emulation software - Standalone DS^3 PC Interface software.

Interagency Involvement



NASA

NIST
Technical Support & Guidance

GAO
DS^3 Sanction

NARA
Records Archiving

DS^3

GSA
Records Management

DOJ
Statutory Requirements

OMB
Policy

USPS
Certificate Management

APPENDIX E

WHAT'S IN A ~~NAME~~ PUBLIC-KEY CERTIFICATE?

Stephen Kent

BBN Communications

What's in a ~~Name~~ Public-Key Certificate?

- A public-key certificate binds attributes to a public key using a digital signature to effect the binding
- Much of the debate is about which attributes are bound to the public key
- Not all applications are interested in the same attributes; not all attributes are vouched for by the same authority nor have the same time frame
- An entity (user/role/device/process ...) could possess more that one certificate to bind different attributes for use by different applications (X.509, PACs, X9,...)

Candidate Certificate Attributes

- subject name
- issuer name
- validity interval
- subject clearance
- fiduciary authorization
- application/device privileges

Certificates: The More the Merrier?

- A baseline certificate can bind identity information to a public key and is generally useful in many contexts
- Additional certificates can be used to bind additional, application-specific attributes to the base certificate
- If different authorities are responsible for different attributes, and/or different attributes have different lifetimes, using multiple certificates may simplify administration

Certificates & Trust

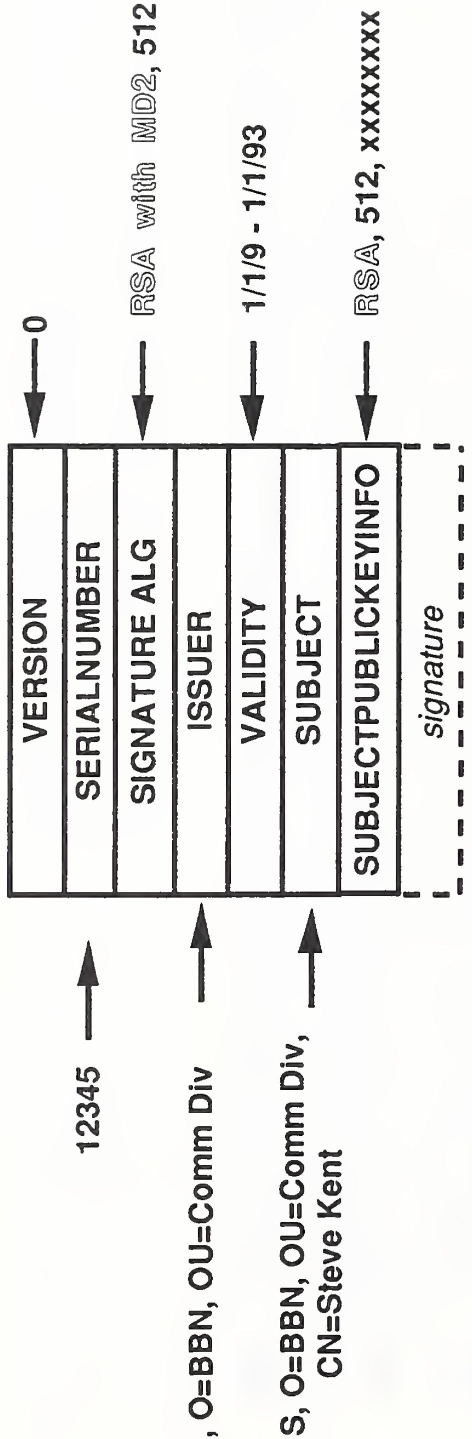
- A certificate implies that its issuer is trusted to vouch for the attribute binding expressed in the certificate
- A certificate implies that the attributes contained therein are correctly bound to one another (e.g., to a subject)
- A certificate may imply that an entity is trusted within the context of some application
- In general, a certificate vouching for an identity binding does not imply trust in the identified entity

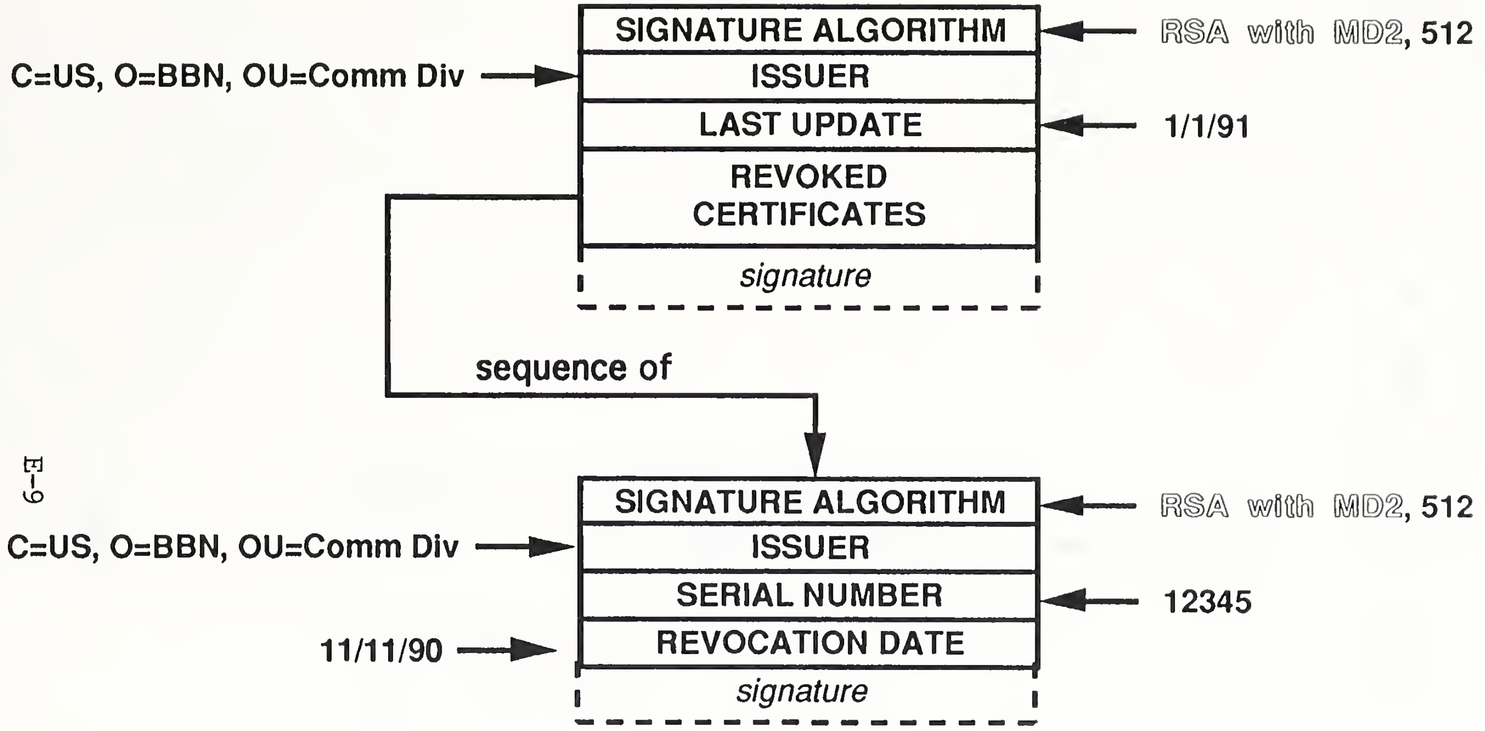
Revocation: The Ugly Side of Certificates

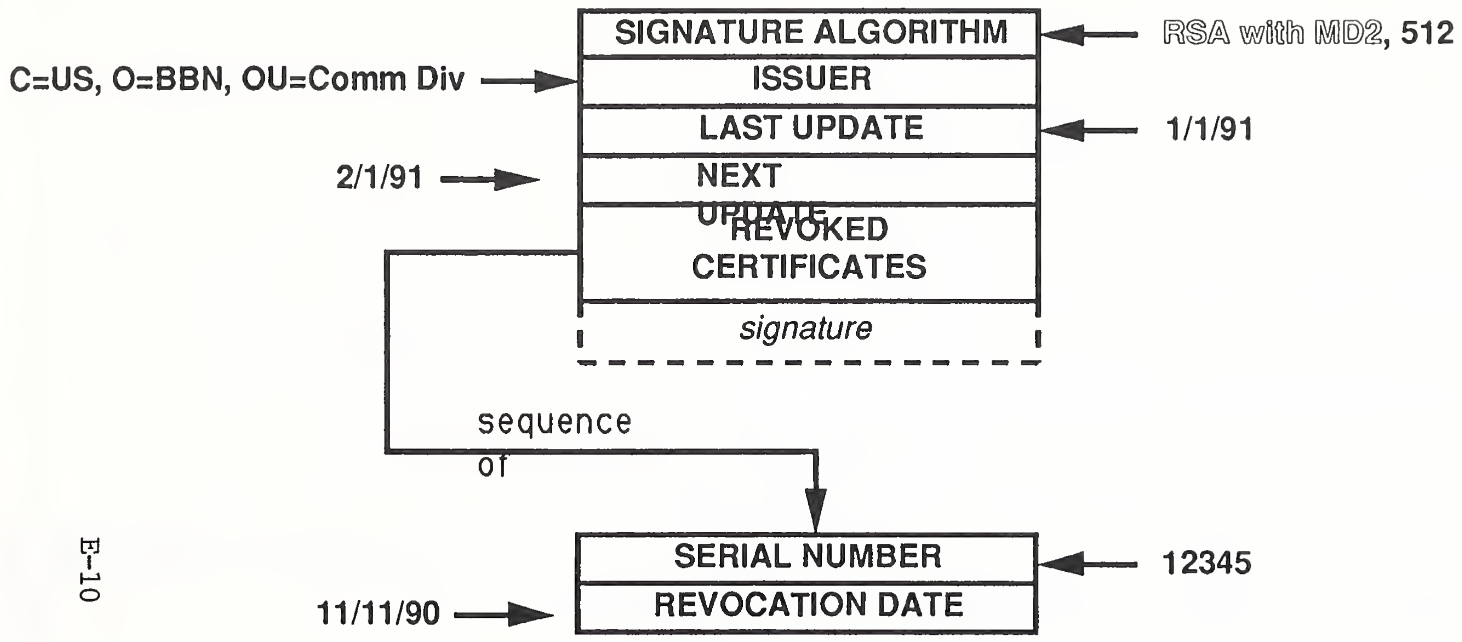
- Certificates are revoked because the private key is presumed compromised or because the attributes bound to the public key are invalid
- A Certificate Revocation List (CRL) is the primary means of distributing information about which certificates have been revoked
- CRLs can be "pushed" or "pulled" to disseminate the revocation information, but in large open systems neither approach is quick and complete

Comprehensive Non-Repudiation

- Hashed & signed message/document
- Timestamp applied to message by a notary
- Certificate(s) of signer and any superior CAs
- Timely CRLs for signer and superior CAs
- Timestamp applied to CRLs by a notary
- A "meaningful" message (not too context specific)


VERSION
0
12345
SERIALNUMBER
SIGNATURE ALG
RSA with MD2, 512
C=US, O=BBN, OU=Comm Div
ISSUER
VALIDITY
1/1/9 - 1/1/93
C=US, O=BBN, OU=Comm Div, CN=Steve Kent
SUBJECT
SUBJECTPUBLICKEYINFO
RSA, 512, xxxxxxxx
signature


SIGNATURE ALGORITHM
ISSUER
LAST UPDATE
REVOKED CERTIFICATES
signature
RSA with MD2, 512
C=US, O=BBN, OU=Comm Div
1/1/91
sequence of
SIGNATURE ALGORITHM
ISSUER
SERIAL NUMBER
REVOCATION DATE
signature
RSA with MD2, 512
C=US, O=BBN, OU=Comm Div
12345
11/11/90


SIGNATURE ALGORITHM
RSA with MD2, 512
C=US, O=BBN, OU=Comm Div
ISSUER
LAST UPDATE
1/1/91
2/1/91
NEXT UPDATE
REVOKED CERTIFICATES
signature
sequence of
SERIAL NUMBER
12345
11/11/90
REVOCATION DATE

APPENDIX F

SECURITY CERTIFICATES

BSI, United Kingdom

TITLE: Security Certificates

SOURCE: BSI, UK

DATE: 2nd March 1992

IST/21 has identified a need for a single definition of the common features of a security certificate, and a method to customise this definition to specific applications. This definition would be referenced by all SC21 standards that require security certificates.

IST/21 considers that such a standard should be developed by SC27, as part of the work item on defining Security Information Objects. SC27 should attempt to extract the common features of all security certificates into one syntactic structure, and provide a means to customise it to specific applications.

Several existing SC21 standards define their own form of security certificate. These definitions are summarised below, to give examples of the types of information carried in certificates. The definition to be developed need not use a ASN.1 representation compatible with these current definitions, but should be capable of providing equivalent functionality.

We note that implementations of the Directory Authentication Framework (ISO 9594-8 1988) are coming into widespread use. All future versions of the Directory specification will permit use of security certificates in the format described in the 1988 version. In the event that the security certificate format developed by SC27 does not encompass this format as a special case, then both should be registered as separate security information objects.

1 Relation to the Security Framework

The Security Frameworks Overview (WD, to become ISO 10181-1) describes the common features of security certificates as follows:

1.1 Introduction

A security certificate contains security control information (SCI) relating to one or more security services. It is used to convey SCI from an authority to entities which require this information to perform a security function.

In general a security certificate may contain the following SCI:

- access control information
- authentication information
- integrity control information
- confidentiality control information
- non-repudiation information
- audit information
- key management information

as described in the the other frameworks, plus protection information as described in clause [1.3].

All the SCI carried within a security certificate is protected to provide integrity and data origin authentication. The SCI may also be confidentiality protected.

1.2 Chaining of Security Certificates

Where an entity may not have the SCI needed to verify a security certificate, then it may use a security certificate from another authority to provide this SCI. This process can be repeated to provide a chain of security certificates. These carry SCI which provides a secure path from a known authority (ie, one for which SCI has already been established) to the entity requiring certified SCI.

1.3 Security Certificate Protection Information

The general form of a security certificate is in three fields containing:

1. SCI which is confidentiality and integrity protected
2. SCI which is integrity protected
3. information which provides the security itself

where security protection includes:

Data origin + integrity protection (eg. digital signature)

Replay protection (eg. unique token id., timestamp)

Audit information (eg. timestamp)

1.4 Protection Features of a Security Certificate

The information which protects the security certificate itself will include items that support integrity and data origin authentication (such as a checkvalue or digital signature).

It may also include:

1. items required for confidentiality
2. attributes that describe the characteristics of the entities that can submit the security certificate.
3. attributes that describe the characteristics of the entities which can receive the security certificate.
4. a validity time period or an expiration time derived from the creation time which prevents the indefinite re-use of the security certificate.
5. the security policy under which the security certificate must be used.
6. cryptographic parameters to protect the security certificate from unauthorised use.
7. the identity of the authority and the identity of the agent that issued the security certificate (so as to establish the security certificate's origin).
8. information used for replay detection (eg. creation time)

1.5 Detection and Recovery Features of Security Certificates

This section describes the security features that can be used upon detection of a security relevant event involving a security certificate as well as the features that can be used when security recovery takes place.

The detection features of a security certificate may include:

- a security certificate reference number which is unique to this security certificate with respect to all security certificates of the same authority and agent.
- an identity field which allows audit of the entity to which the security certificate was originally issued.

Recovery features of the security certificate include:

- A reference which can be used to revoke a specific security certificate.
- A reference which can be used to revoke a group of security certificates.

2 Additional Requirements for Security Certificates

The security certificate format used by the Directory (ISO 9594-8) is perceived to have the following deficiencies:

- In the event that DistinguishedNames are re-used over time, the certificate should also contain a unique numeric identifier to indicate which holder of the name was intended to be the certificate subject. (This will be added in ISO 9594-8 (1992)).
- In the event that different keys are used for integrity and confidentiality, the certificate should included multiple keys, and indicate which security services each key may be used for.
- It is not currently possible to distinguish user certificates from CA certificates. Thus, there is a risk of unauthorised users posing as certification authorities.
- When the certificate is a CA certificate, there should be a means for the issuer to indicate which part of the name-space has been delegated to the subject.
- The algorithm identifier used to identify the signature algorithm should also identify the encoding rules which were used to translate the presentation data value to be signed into a sequence of octets for input to the signature algorithm.
- When a certificate is stored, the concrete syntax used to encode the certificate should be held with it.

The revocation list format used by the Directory is perceived to have the following deficiencies:

- The SIGNED SEQUENCE OF SEQUENCE should be replaced by SEQUENCE OF SIGNED SEQUENCE. This would allow individual revoked certificates to be signed. This is particularly useful when non-repudiation of the revocation is required. (See directory defect report 9594/033).
- If there is a difference between the date at which a user requested the CA to revoke their certificate and the date at which the CA carried out the revocation, the revoked certificate should contain both dates. (See SC21 N1734, summary of voting on extensions to 9594-8, AFNOR comments).

- There is no indication of when the next revocation list will be issued. Without this information, it is difficult to tell whether the revocation list is the most recent. (For example, an attacker knowing a compromised key and revoked key might try to make the key valid again by replacing the current revocation list with an old one).

- The CertificateList structure is liable to become very large. It would be useful to have a more compact format.

3 Example SIO Definitions

The following sections describe the security certificates defined in ISO 9594-8 and CD 10164-9. These are provided as informative examples only: the format to be developed by SC27 need not be identical.

4 Certificate

4.1 Purpose

A Certificate information object is created by an issuing authority to bind security control information to an entity (the certificate subject).

4.2 Security Services Used

A data integrity service is used to prevent unauthorised modification of the certificate contents. A non-repudiation service is used so that if the authority issues certificates containing incorrect information, it is possible to demonstrate this to an adjudicator.

4.3 Fields

- version
- serialNumber
- issuer
- validity
- subject
- securityControlInformation

  In v1988 certificates, the security control information is restricted to the subject's public key. In v1992 certificates, the SCI is subject's public key and optionally a unique identifier which is the subject's identity for the purposes of access control. Other forms of certificate may define additional security control information.
- signature

  A digital signature is used to provide data integrity and non-repudiation.

4.4 ASN.1

```
-- Extracted from ISO 9594-8

Certificate ::=
       SIGNED SEQUENCE {
             version [0] Version DEFAULT v1988,
             serialNumber CertificateSerialNumber,
             signature  AlgorithmIdentifier,
             issuer Name,
             validity Validity,
             subject Name,
             subjectPublicKeyInfo SubjectPublicKeyInfo
}

CertificateSerialNumber ::=
    INTEGER

Validity ::=
    SEQUENCE {
```

```
              notBefore UTCTime,
              notAfter  UTCTime
    }

SubjectPublicKeyInfo ::=
    SEQUENCE {
              algorithm AlgorithmIdentifier,
              subjectPublicKey BIT STRING
    }

AlgorithmIdentifier ::=
    SEQUENCE {
              algorithm OBJECT IDENTIFIER,
              parameters ANY DEFINED BY algorithm OPTIONAL
     }
```

5 Revoked Certificate

5.1 Purpose

A RevokedCertificate information object is created by an issuing authority to indicate that a certificate which it had previously created should no longer be accepted.

5.2 Security Services Used

A RevokedCertificate is protected by a data integrity service (to prevent unauthorised entities issuing revocations) and a non-repudiation service (so that the certificate subject can complain to an arbitrator if it considers that its certificate was revoked unfairly).

5.3 Fields

- issuer

  The name of the certificate issuer.

- certificateSerialNumber

  The serial number of the certificate to be revoked.

- revocationDate

  The date at which the revocation takes effect.

- signature

  A digital signature is used to provide both data integrity and non-repudiation.

5.4 ASN.1

```
-- Extracted from ISO 9594-8 .

RevokedCertificate ::=
      SIGNED SEQUENCE {
         signature AlgorithmIdentifier,
         issuer Name,
   subject CertificateSerialNumber,
         revocationDate UTCTime
      }
```

6 RevocationList

6.1 Purpose

A RevocationList is created by an authority (A) to enumerate all "active" revoked certificates issued by a set of authorities, which may or may not include A. A revoked certificate is active if it has been issued and the expiry date of the certificate it revokes has not been reached. A Revocation List provides assurance that there are no other active Revoked Certificates issued by the named authorities.

6.2 Fields

- issuer

  The issuer of the revocation list (ie. authority A)

- lastUpdate

  The time at which the list of revoked certificates was known to be complete. (ie. the time at which the revocation list was constructed).

- revokedCertificates

  Details of the certificates which have been revoked.

6.3 ASN.1

```
-- Extracted from ISO 9594-8, with the correction in defect report 9594/033
-- applied.

CertificateList ::=
        SIGNED SEQUENCE {
             signature AlgorithmIdentifier,
             issuer Name,
             lastUpdate UTCTime,
             revokedCertificates SEQUENCE OF
                   RevokedCertificate OPTIONAL
        }
```

7 Access Control Certificate

7.1 Purpose

An AccessControlCertificate provides assurance of the association of specific ACI values with an entity (in CMIP, this will be either a CMIP initiator or a managed object).

7.2 Security Services Used

An access control certificate is protected by an integrity service and a non-repudiation service.

7.3 Fields

- proxy
- securityDomainAuthorityName
- securityDomainAuthoritySignature
- securityDomainName
- timeOfCreation
- validFrom
- validUntil
- validationIdentifier
- validationKey
- accessControlInformation
- cryptographicAlgorithm
- cryptographicChecksum

7.4 ASN.1

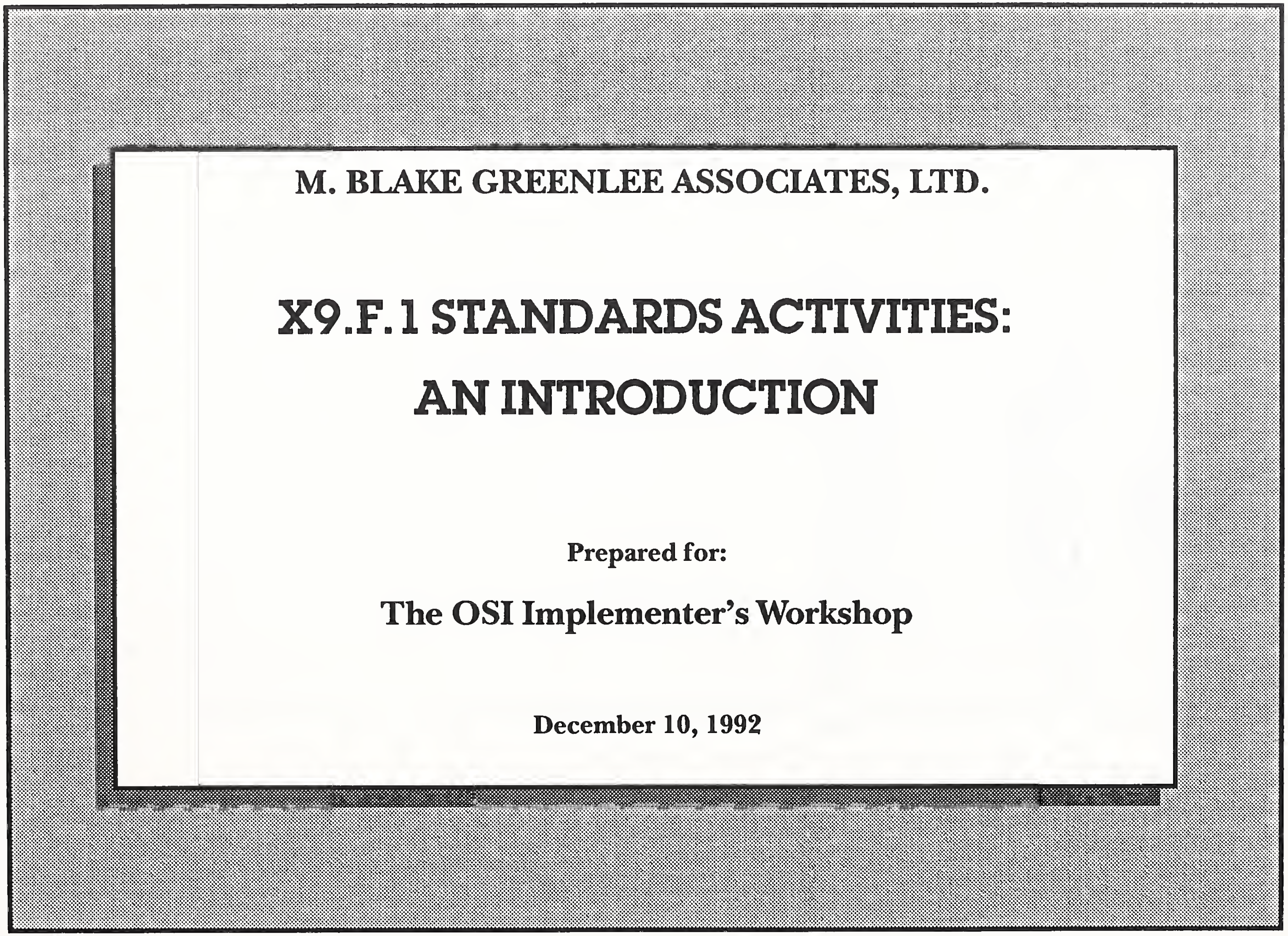
```
-- Extracted from CD 10164-9

AccessControlCertificate ::= SEQUENCE {
    proxy [0] IMPLICIT AccessControlCertificate OPTIONAL,
    securityDomainAuthorityName [1] IMPLICIT
          SecurityDomainAuthorityName OPTIONAL,
    securityDomainAuthoritySignature [2]
          SecurityDomainAuthoritySignature OPTIONAL,
    securityDomainName [3] IMPLICIT SecurityDomainName OPTIONAL,
    timeOfCreation [4] IMPLICIT GeneralTime OPTIONAL,
    validFrom [5] IMPLICIT GeneralTime OPTIONAL,
    validUntil [6] IMPLICIT GeneralTime OPTIONAL,
    validationIdentifier [7] IMPLICIT ValidationIdentifier OPTIONAL,
    validationKey [8] IMPLICIT ValidationKey OPTIONAL,
    accessControlInformation [9] SEQUENCE {
               capability [1] IMPLICIT SET OF Capability OPTIONAL,
               identity [2] IMPLICIT InitiatorName OPTIONAL,
               label [3] IMPLICIT SET OF SecurityLabel OPTIONAL }
    cryptographicAlgorithm [10] IMPLICIT CryptographicAlgorithm OPTIONAL,
    cryptographicChecksum [11] CryptographicChecksum OPTIONAL
   }

GeneralTime ::= GeneralisedTime

CryptographicAlgorithm ::= OBJECT IDENTIFIER

CryptographicChecksum ::= INTEGER

SecurityDomainAuthorityName ::= DistinguishedName

SecurityDomainAuthoritySignature ::= OCTET STRING

ValidationIdentifier ::= INTEGER

ValidationKey ::= INTEGER
```

APPENDIX G

X9.F.1 STANDARDS ACTIVITIES: AN INTRODUCTION

Blake Greenlee

M. Blake Greenlee Associates, Ltd.



M. BLAKE GREENLEE ASSOCIATES, LTD.

X9.F.1 STANDARDS ACTIVITIES: AN INTRODUCTION

Prepared for:

The OSI Implementer's Workshop

December 10, 1992

X9.F.1 IS DEVELOPING TWO SETS OF PUBLIC KEY STANDARDS; NEW WORK ITEMS ARE IN PROCESS

- X9.30-199x, Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry
- X9.31-199x, Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry.
- A proposal for a Guideline on Basic Encoding Rules (BER) and Abstract Syntax Notation (ASN-1) is in process.
- Authentication and Non-repudiation using symmetric algorithm cryptography is in the discussion phase.

X9.30-199X, PUBLIC KEY CRYPTOGRAPHY USING IRREVERSIBLE ALGORITHMS...

X9.30 CONTAINS THE FOLLOWING FOUR STANDARDS:

Part 1: The Digital Signature Algorithm (DSA) (mathematically identical to N.I.S.T.'s *Digital Signature Standard*).

Part 2: The Secure Hash Algorithm (SHA) (mathematically identical to N.I.S.T.'s *Secure Hash Algorithm)*.

This standard is in final ballot and should be issued by the end of the first quarter, 1993.

Part 3: Certificate Management for DSA

Part 4: Management of Symmetric Algorithm Keys Using Irreversible Cryptography

X9.31-199X, PUBLIC KEY CRYPTOGRAPHY USING REVERSIBLE ALGORITHMS...

X9.31 WILL CONTAIN THE FOLLOWING FOUR STANDARDS:

Part 1: The RSA Signature Algorithm

Part 2: Hash Algorithms (will include the SHA)

Part 3: Certificate Management For RSA

Part 4: Management of Symmetric Algorithm Keys Using RSA

X9.30, PART 3: CERTIFICATE MANAGEMENT

SCOPE

- certificate management, and
- an authentication framework for the financial services industry.

THE PROBLEM WITH SOME OTHER PUBLIC KEY-BASED STANDARDS IS THAT THEY DO NOT REQUIRE THAT AS SYSTEM BE STARTED AND MAINTAINED UNDER SECURE CONDITIONS (E.G., CD-11166).

LIABILITY ISSUES

- The entity or CA generating a public/private key pair shall be liable for the quality of that key pair and for ensuring the privacy and integrity of the private key.
- The CA shall be liable for the certification process.

THE CA SHALL BE SOLELY RESPONSIBLE FOR:

- Identifying the entity whose Certificate Request Data are presented for signature.
- Securing the certification process and the private key used to sign the Certificate Request Data.
- Advising the entity identified in the Certificate Request Data that a certificate has been issued.
- Ensuring that certificates are not issued to two entities with the same entity identity.

DISTRIBUTION OF A CA'S PUBLIC KEY

- It is the responsibility of the CA to distribute its public key and:
  - ensure the integrity of that key during distribution, or
  - to provide a mechanism for detecting its modification during the distribution process.
- It is the responsibility of each entity to ensure the integrity of the CAs public key is maintained once acquired.
- Multiple public keys may be distributed to provide for replacement upon the expiration of the cryptoperiod or for backup.
- It is the responsibility of an entity to use the correct CA public key.

SECURITY REQUIREMENTS FOR A CA'S PRIVATE KEY

- CA shall be implemented in a cryptographic module not shared by any subscribing entity.
- This private key shall be generated internally to the cryptographic module in which it shall be used.
- It shall never appear outside of that cryptographic module in any form (plain text or enciphered).
- The cryptographic module shall afford level 4 protection[1] to private keys.

[1] As defined in draft Federal Information Processing Standard 140-1.

THE CA IS “TRUSTED” BY ITS SUBSCRIBERS

TRUST IS BASED ON:

- using a cryptographic module designed to meet requirements for financial institution use,
- implementing sound management and control practices that are confirmed by an independent audit function (internal, external or both) which shall report audit results to the subscribers.

THE TRUST MODEL IS:

1. A user trusts all certificates issued by its CA;

2. If a user trusts some other CA, it trusts all certificates issued by that CA for that CA's users and superior CA. To trust another CA, it must be certified (directly or indirectly) by the user's CA (possibly via cross certification);

3. A CA is trusted to certify CAs subordinate to it in the hierarchy, its users, and its superior CA; and

4. A CA may be trusted to cross-certify other CAs not adjacent to it in the hierarchy.

NOTATION IS DERIVED FROM X.509

1. X_p = X's public key; X_s = X's private key

2. CA(X) = X's CA

3. $X_l<<X_2>>$ X_2's certificate, issued by X_1, i.e. $X_1\{X_2, X_{2P}, \ldots\}$

4. $X_l<<X_2>>X_2<<X_3>> \ldots\ X_{n-1}<<X>>$ = certificate chain (of arbitrary length) in which each item is the certificate for the CA which produced the next item. This chain is functionally equivalent to $X_l<<X_n>>$; possession of X_{1p} allows a user to extract the authenticated public key of X_n

5. $X_{1p}{\bullet}X_1<<X_2>)$ = Unwrapping of a certificate or chain, using the public key of the leftmost certifier, to extract the authenticated public key of the rightmost certificate; this example extracts X_{2P}

VALIDITY PERIOD

- Every public/private key pair shall have a validity period
- The period may be explicitly or implicitly defined.
- Where dates and times are used, the validity period shall be identified by "notBefore" and "notAfter" dates (and times), using the format for universal time type defined in ISO 8824, Section 31.

CERTIFICATE CONTENTS:

```
Certificate ::= SIGNED SEQUENCE {
   version              [0]     Version DEFAULT v1,
   serialNumber              CertificateSerialNumber,
   signature                 AlgorithmIdentifier,
   issuer                    Name, — CA's name
   validity                  Validity,
   entity                    Name,
   entityPublicKeyInfo          EntityPublicKeyInfo,
   issuerUniqueID   [1]     IMPLICIT BIT STRING OPTIONAL,
   entityUniqueID   [2]     IMPLICIT BIT STRING OPTIONAL }
```

ATTRIBUTES AND ATTRIBUTE CERTIFICATES

- Liability Limits
- Binding Information

WHEN HOT LISTS ARE USED, THESE LISTS SHALL BE:

- dated and signed by the CA so that entities can validate the integrity of the list and the date of distribution,
- issued by the CA at regular intervals, even if no changes have occurred since the last issuance, and
- accessible to all entities of the system except when precluded e.g., by law, regulation or court order,
- can also be made available by a Directory Service.

Flexibility: The Hot List distribution need not automatically include all entities.

THE HOT LIST SHALL BE:

```
CertificateRevocationList ::= SIGNED SEQUENCE {
   signature           AlgorithmIdentifier,
   issuer              Name,
   lastUpdate          UTCTime,
   nextUpdate          UTCTime,
   revokedCertificates  SEQUENCE OF CRLEntry OPTIONAL }

CRLEntry ::= SEQUENCE {
   certificate         CertificateSerialNumber,
   revocationDate      UTCTime,
   reasonCode          ENUMERATED CRLReason }

CRLReason ::= ENUMERATED {
   keyCompromise (0),
   caCompromise (1),
   affiliationChanged (2),
   superceded(3)
   cessation of operation (4)
   other (5) }
```

OTHER FEATURES OF THE DRAFT X9.30, PART 3

- When dual signatures are required for high-risk applications:
  - each of the signatures shall be from an independent cryptographic module, and
  - the two (or more) facilities shall not be collocated.
- Audit Journal Requirements

Table 1

Actions to be Taken on Revocation of a Certificate

Reason for Revocation	Actions to be Taken By Entity Certified[1]	Actions to be Taken by the CA_1	Actions To Be Taken By Users Of The Certificate
1. All reasons	1. Request that the signer's CA (CA_1) cancel the certificate, giving the CertificateSerialNumber to identify the certificate and the requested CRLEntry. 2. The entity requesting cancellation of one or more of its own certificates may communicate the identities of revoked certificates to other entities. 3. The entity shall update the Audit Journal to reflect the actions taken and the reasons for the actions. Revoked certificates shall be journalized.	1. The CA_1 shall : a. Optionally send a signed message to all entities which shall include an appropriate CRL, or b. Immediately update the Hot List(CertificateRevocationList). The certificate remains on the revocation list until its expiration date. 2. The CA_1 shall update the Audit Journal to reflect the actions taken and the reasons for the actions. Revoked certificates shall be journalized.	1. Any message requiring the use of the revoked certificate shall be rejected. 2. The user shall update the Audit Journal to reflect the actions taken and the reasons for the actions. Revoked certificates shall be journalized. 3. The user may also notify other entities.
2. Other than for: a. key compromise b. cessation of operations, or c. a change of affiliation.	1. If the entity is a CA, the CRL of the CA itself shall contain entries for all revoked certificates, with a reasonCode of superceded or other.	1. The reasonCode shall be superceded or other, as appropriate.	1. All keying material sent and protected by that certificate (without regard to type) should be replaced as soon as operationally convenient.

[1] The entity may be a CA.

Table 1

Actions to be Taken on Revocation of a Certificate (Continued)

Reason for Revocation	Actions to be Taken By Entity Certified[1]	Actions to be Taken by the CA_1	Actions To Be Taken By Users Of The Certificate
3. Compromise or suspected compromise of an entity's private key.	1. If the entity is a CA, the CRL of the CA itself may contain entries for all suspect certificates, with a reasonCode of keyCompromise or caCompromise. 2. The entity should conduct an investigation and take action to limit loss.	1. The reasonCode shall be caCompromise or keyCompromise, as appropriate. 2. The CA_1 should conduct an investigation and take action to limit loss.	1. All keying material ever sent and protected by that certificate (without regard to type) shall be discontinued immediately. 2. The user should conduct an investigation and take action to limit loss.
4. Request for revocation of entity's keys because of a cessation of operations.	1. If the entity is a CA, the CRL of the CA Itself may contain entries for all revoked certificates, with a reasonCode of cessationOfOperation. 2. The entity should take action to limit exposure.	1. The reasonCode shall be cessationOfOperation. 2. The CA_1 should take action to limit exposure.	1. All keying material sent and protected by that certificate (without regard to type) should be replaced as soon as operationally convenient. 2. The entity should take action to limit exposure.
5. Request for revocation of entity's keys because a change of affiliation of the entity (E.g., affiliation with a different CA_1)	1. If the entity is a CA, the CRL of the CA itself may contain entries for all revoked certificates, with a reasonCode of affiliationChanged. 2. The entity should take action to limit exposure.	1. The reasonCode shall be affiliationChanged. 2. The CA_1 should take action to limit exposure.	1. All keying material sent and protected by that certificate (without regard to type) should be replaced as soon as operationally convenient. 2. The entity should take action to limit exposure.

[1] The entity may be a CA.

CREDENTIALS

```
Certificate Request ::= SEQUENCE {
     subject                  Name,
     subjectPublicKeyInfo  SubjectPublicKeyInfo,
     validity                 [0] Validity,                 - requested validity
                                                             period
     attributes               [1] SET OF Attributes OPTIONAL }


Name ::= SEQUENCE OF RelativeDistinguishedName

SubjectPublicKeyInfo ::= SEQUENCE {
     algorithm                AlgorithmIdentifier,
     subjectPublicKey         BIT STRING }

Validity ::= SEQUENCE {
     notBefore                UTCTime,
     notAfter                 UTCTime }

Attributes ::= SEQUENCE {
     type                     OBJECT IDENTIFIER,
    values                    SET OF ANY DEFINED BY type }

AlgorithmIdentifier ::= SEQUENCE {
    algorithm                 OBJECT IDENTIFIER,
    parameters                ANY DEFINED BY algorithm OPTIONAL }

DSAParameters ::= SEQUENCE {
    prime1                INTEGER,                       -modulus p
    prime2                INTEGER,                       - modulus q
    base                  INTEGER,                       - base g
    seed                  BIT STRING OPTIONAL,           - for prime generator
    counter               INTEGER OPTIONAL }             - for prime generator
```

CERTIFICATE

```
Certificate ::= SIGNED CertificateInfo

SIGNED Data ::= SEQUENCE {
     databeing signed        ANY,
     algorithmIdentifier     AlgorithmIdentifier,
     signature               Signature }

CertificateInfo ::= SEQUENCE {
     version                 [0] Version DEFAULT v1,
     serialNumber            CertificateSerialNumber,
     signature               AlgorithmIdentifier,
     issuer                  Name,                              - CA's name
     validity                Validity,
     subject                 Name,
     subjectPublicKeyInfo    SubjectPublicKeyInfo,
     issuerUniqueID          [1] IMPLICIT BIT STRING OPTIONAL,
     subjectUniqueID         [2] IMPLICIT BIT STRING OPTIONAL }

Version ::= INTEGER { v(0), v(1) }

CertificateSerialNumber ::= INTEGER
```

```
Signature ::= SEQUENCE {
      s                    INTEGER,
      r                    INTEGER }
```

MULTIPLY SIGNED CERTIFICATE

```
MultiplySignedCertificate ::= SEQUENCE {
      CertificateInfo,
      Signatures }

Signatures ::= SEQUENCE {
      version                  Version,
      digestAlgorithms         SET OF AlgorithmIdentifier,
      contentInfo              ContentInfo,
      signerInfos              SET OF SignerInfo }

ContentInfo ::= SEQUENCE {
      contentType              OBJECT IDENTIFIER }

SignerInfo ::= SEQUENCE {
      version                        Version,
      issuerSerial                   IssuerSerial,
      digestAlgorithm                AlgorithmIdentifier,
      authenticatedAttributes        [0] Attributes OPTIONAL,
      digestEncryptionAlgorithm      AlgorithmIdentifier,
      encryptedDigest                EncryptedDigest,         - the sugnature
```

```
    unauthenticatedAttributes  [1] Attributes OPTIONAL }

IssuerSerial ::= SEQUENCE {
    issuer              Name,
    serial              CertificateSerialNumber }

IssuerSerial ::= SEQUENCE {
    issuer              Name,
    serial              INTEGER }           - certificate serial number

EncryptedDigest ::= OCTET STRING                     - encrypted DigestInfo

DigestInfo ::= SEQUENCE {
    digestAlgorithm         AlgorithmIdentifier,
    digest                  Digest }

Digest ::= OCTET STRING
```

CERTIFICATE REVOCATION

```
CertificateRevocationList ::= SIGNED CertificateRevocationListInfo

CertificateRevocationListInfo::= SEQUENCE {
     signature              AlgorithmIdentifier,
     issuer                 Name,
     lastUpdate             UTCTime,
     nextUpdate             UTCTime,
     revokedCertificates    SEQUENCE OF CRLEntry OPTIONAL }

CRLEntry ::= SEQUENCE {
     certificate            CertificateSerialNumber,
     revocationDate         UTCTime,
     reasonCode             CRLReason }

CRLReason ::= ENUMERATED {
     keyCompromise (0),
     caCompromise (1),
     affiliationChanged (2),
     superceded (3),
     cessationOfOperation (4),
     other(5) }
```

ATTRIBUTES CERTIFICATE

```
AttributeCertificate ::= SIGNED AttributeCertificateInfo

AttributeCertificateInfo ::= SEQUENCE {
    certificateID        IssuerSerial,
    attributes           SET OF Attributes }

CertificatePurpose ::= ENUMERATED {
    any (0),
    encipherment (1),
    signature (2) }

TrustedThirdParty ::= Name

LiabilityLimitation ::= CHOICE {
    no-liability              [0] NULL,
    full-liability            [1] NULL,
    monetary-limit            [2] MonetaryValue }

MonetaryValue ::= SEQUENCE {
    currency                  [0] PrintableString (SIZE 3)      - per ISO 4217
    amount                    [1] INTEGER }
```

```
BindingInformation ::= SEQUENCE {
     methodOfDelivery            [0] DeliveryMethod,
     methodOfIdentification      [1] IdentificationMethod,
     entityType                  [2] EntityType }

DeliveryMethod ::= ENUMERATED {
     not-present-in-person (0),
     present-in-person (1),
     presented-by-authorized-agent (2),
     split-knowledge (3),
     other (4) }

IdentificationMethod ::= ENUMERATED {
     reasonable-commercial-practices (0),
     verified-by-trusted-third-party (1),
     dual-control(2),
     other (3) }

EntityType ::= ENUMERATED {
     individual (0),
     corporation (1),
     government (2),
     other(3) }
```

Certificate Format Discussion
Discussion Points

1. X.509, PEM, and X9F all use the X.509 certificate as a base. X9F uses the 1992 version, while PEM uses the 1988 version. The 1992 version contains unique ID (UID) fields for issuer and subject, which are used to prevent name reuse (for the subject), and to indicate which certificate is needed to validate a signature (for the issuer). (In this second case, the UID serves as an identifier for the public key, in addition to distinguishing between multiple uses of a name; this may have some impact on the internal structure of the UID.)

   a) Is the X.509 certificate suitable for our purposes?

   b) Which version is preferable (1988 or 1992)?

   c) If 1992 certificates are used, what are the exact semantics of the UID?

   d) How will common DSA parameters (prime and generator) be managed? They could be conveyed in each certificate, per the ASN.1 presented previously, but this seems like a waste of storage/bandwidth. Alternatively, DSA parameters could be tied to a CA (and its subordinates), and retrieved from the CA's certificate (or distributed along with the trusted public key of a CA). Or the parameters could be tied to the (X.500) naming hierarchy in a similar manner.

2. X9F additionally defines an *attribute certificate* to contain other (optional) useful information, in the form of X.500-style attributes (type plus one or more values). The following attributes were felt to be useful for the financial community:

   - liability limitation,
   - binding information (method of identification, method of delivery),
   - certificate purpose (encipherment and/or signature),
   - names of any trusted third parties used to convey credential information, and
   - Common DSA parameters (for some "subtree" of the name space).

   a) Is a similar "extension" mechanism required in this case? If so, what attributes would be useful?

   b) Is the attribute certificate issued by the same CA which issues the public key certificate, or might separation of duties dictate that a different entity is responsible for issuing an attribute certificate (e.g. one with monetary transaction limits)?

3. X9F allows for the use of multiple signatures on certificates used with high value transactions. The multiple signature structure allows for joint signatures, as well as nested (counter)signatures, and is based on RSADSI's "PKCS #7: Cryptographic Message Syntax."

a) Is such a mechanism useful in this case?

b) Can this mechanism usefully be applied to individual messages/transactions, as well as to certificates?

c) Given a signature on a certificate or message, (how) does one indicate which other signatures are required?

4. Certificates as defined in X.509 are useful in providing the following security services: integrity, authentication, and non repudiation (of origin). It may be useful to examine other security services to determine whether they might make use of this infrastructure, particularly if the extension mechanism of point 2 is used.

- Peer Entity Authentication: The use of signatures for this purpose (generally using a challenge/response mechanism) is well documented in the literature and in existing standards (e.g., X.400 and X.500).

- Confidentiality: Symmetric key management can be performed using, e.g., RSA public keys to encrypt DES keys a la PEM, ISO CD 11166-1, etc. Certificates would be used in this case to hold the (trusted) public keys.

- Access Control and Authorization: The use of certificates to contain access control information is also well documented. (Note that we are referring to long-lived access control information, with a lifetime similar to that of the public key certificate. Other mechanisms, such as ECMA PACs, are defined for use on a short term, e.g. per connection, basis.) Two examples are:
  - ○ In the DoD environment, SDNS Access Control (SDN.802).
  - ○ In the commercial environment, Electronic Document Authorization (Proceedings of the 1990 NCSC).

- Non Repudiation: Additional non repudiation mechanisms beyond the use of (originator) signatures are discussed in the ISO Non Repudiation Framework (Working Draft). These include Time Stamping Services and Third Party Notaries.

a) What other security services should the infrastructure support?

5. The CRL format of X.509 was extended in PEM to include a "next update" time. This prevents attacks based on preventing delivery of CRLs to an entity. X9F further extended the CRL to include a revocation reason fo: each entry, since different actions are required of the entity and CA in different cases.

a) What CRL format is suitable for these applications?

APPENDIX H

ASN.1 STRUCTURES FOR CERTIFICATE MANAGEMENT

Rich Ankney

Fischer International

ASN.1 Structures for Certificate Management

Rich Ankney
Fischer International
(703) 818-0713
ankney@emc2-tao.fisc.com

This paper describes the various ASN.1 structures used in the X9F1 certificate management standards.

1 Signatures

A signature is generally represented as the output of the SIGNED macro, i.e. a BIT STRING. The macro is defined as:

```
SIGNED MACRO ::=
BEGIN
        TYPE NOTATION ::= type(ToBeSigned)
        VALUE NOTATION ::= value (VALUE
                SEQUENCE {
                        ToBeSigned,
                        AlgorithmIdentifier,
                        ENCRYPTED OCTET STRING } )
END

ENCRYPTED MACRO ::=
BEGIN
        TYPE NOTATION ::= type(ToBeEncrypted)
        VALUE NOTATION ::= value(VALUE BIT STRING)
END
```

So a **SIGNED DataToBeSigned** (with DataToBeSigned being an arbitrary type) expands to:

```
SEQUENCE {
        ToBeSigned.
        AlgorithmIdentifier,
        BIT STRING }
```

While an RSA signature, being a single integer, is mapped into a BIT STRING in the obvious way (MSB to LSB), the DSA signature consists of two integers, **r** and **s**. These need to be encoded into a BIT STRING for use as an ASN.1 signature. The signature should be interpreted as being (the BER encoding of) the type:

```
SEQUENCE {
        s       INTEGER,
        r       INTEGER }
```

That is, the encoding of the sequence is wrapped inside a BIT STRING.

2 Public Keys

Public keys are generally conveyed within a BIT STRING, as defined in the following section. Within the bit string, there is typically some additional structure. This will be represented as the BER encoding of the appropriate structure as defined in this section. A public key is always conveyed as a BER encoding, but the bit string *in which it appears* is encoded using the mechanism appropriate to the network.

```
DSAPublicKey ::= SEQUENCE {
key             INTEGER,        -- y (public key)
params          DSAParameters OPTIONAL }

DSAParameters ::= SEQUENCE {
        prime1              INTEGER,        -- modulus p
        prime2              INTEGER,        -- modulus q
        base                INTEGER,        -- base g
        seed                BIT STRING OPTIONAL,        -- for prime generator
        counter             INTEGER OPTIONAL }          -- for prime generator
```

For an RSA public key, this bit string is the ASN.1 encoding of the following structure, as defined in X.509:

```
RSAPublicKey ::= SEQUENCE {
        modulus             INTEGER,        -- n
        publicExponent      INTEGER }       -- e
```

3 Certification Requests

The **CertRequestData** include that information which the subject wishes to have certified.

```
CertReqData ::= SEQUENCE {
        subject                         Name,
        subjectPublicKeyInfo            SubjectPublicKeyInfo,
        validity                [0]     Validity,       -- suggested validity period
        attributes              [1]     SET OF Attribute OPTIONAL }

CertReqSubmission ::= SIGNED CertReqData

Validity ::= SEQUENCE {
        notBefore       UTCTime,
        notAfter        UTCTime }

SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm               AlgorithmIdentifier,
        subjectPublicKey        BIT STRING }
```

```
AlgorithmIdentifier ::= SEQUENCE {
        algorithm       OBJECT IDENTIFIER,
        parameters      ANY DEFINED BY algorithm OPTIONAL }

Name ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeValueAssertion

AttributeValueAssertion ::= SEQUENCE {
        type    OBJECT IDENTIFIER,
        value   ANY DEFINED BY type }

Attribute ::= SEQUENCE {
        type    OBJECT IDENTIFIER,
        values  SET OF ANY DEFINED BY type }
```

The **validity** field may be overridden by the CA in the certificate created from the credentials.

The **subjectPublicKey** field contains a bit string which is the public key of the subject. (This bit string may contain a BER encoding as discussed above.)

The **Name** follows the definition of X.500, but the structure rules (allowable name forms) need not follow the schema described in X.521.

The **attributes** component is a (possibly empty) set of other information whose association with the entity must also be certified by the CA.

5 Public Key Certificates

An X.509 (public key) certificate has the following contents:

```
Certificate ::= SIGNED SEQUENCE {
        version                 [0]     Version DEFAULT v1,
        serialNumber            CertificateSerialNumber,
        signature               AlgorithmIdentifier,
        issuer                  Name,                   -- CA's name
        validity                Validity,
        subject                 Name,
        subjectPublicKeyInfo    SubjectPublicKeyInfo,
        issuerUniqueID          [1]     IMPLICIT BIT STRING OPTIONAL,
        subjectUniqueID         [2]     IMPLICIT BIT STRING OPTIONAL }

Version ::= INTEGER { v1988(0), v1992(1) }

CertificateSerialNumber ::= INTEGER
```

The **version** is used to differentiate between versions of the certificate. The **validity** field indicates the period when the certificate is valid. (This may be different from that requested by the subject in the **Credentials.**) Note the CA's (issuer's) certificate indicates the validity of the CA's public key. The **signature** and **issuer** fields are added by the CA. The **certificateSerialNumber** field uniquely identifies this certificate among all those issued by the CA. (Thus the combination of issuer name and serial number will, ideally, uniquely identify a certificate, assuming proper procedural controls on serial number assignment by the CA.) The **subjectUniqueID** field is provided by the CA and may be used to distinguish between reused instances of a name. The **issuerUniqueID** field performs a similar function for the CA name.

6 Certificate Revocation Lists

The following "hot list" format is based on that of Internet RFC 1114, with the addition of a reason code.

```
        CertificateRevocationList ::= SIGNED SEQUENCE {
                signature               AlgorithmIdentifier,
                issuer                  Name,
                lastUpdate              UTCTime,
                nextUpdate              UTCTime,
                revokedCertificates     SEQUENCE OF CRLEntry OPTIONAL }

        CRLEntry ::= SEQUENCE {
                certificate             CertificateSerialNumber,
                revocationDate          UTCTime,
                reasonCode              ENUMERATED CRLReason }

        CRLReason ::= ENUMERATED {
                keyCompromise (0),
                caCompromise (1),
                affiliationChanged (2),
                superseded (3),
                cessationOfOperation (4),
                other (5) }
```

7 Attributes

The (optional) attributes associated with the subject / certificate are carried in a separate structure which is also signed by the CA. This structure is the attributes certificate.

```
AttributesCertificate ::= SIGNED SEQUENCE {
        certificateID           IssuerSerial,
        attributes              SET OF Attribute }

IssuerSerial ::= SEQUENCE {
        issuer          Name,
        serial          CertificateSerialNumber }
```

The issuer and serial number are those of the base X.509 certificate, and would be used to retrieve the attributes certificate in the event the **subjectUniqueID** field is not used for that purpose.

Following are some useful attributes for attribute certificates. (We only define the syntax for the attribute values; object identifiers are defined elsewhere.)

```
LiabilityLimitation ::= CHOICE {
        no-liability            [0]     NULL,
        full-liability          [1]     NULL,
        monetary-limit          [2]     MonetaryValue }

MonetaryValue ::= SEQUENCE {
        currency        [0]     PrintableString (SIZE 3),       -- per ISO 4217
        amount          [1]     INTEGER }
```

This attribute defines the limits of a CA's liability in the event of key compromise, etc. One might find this attribute in a CA's certificate.

```
BindingInformation ::= SEQUENCE {
        methodOfDelivery                [0]     DeliveryMethod,
        methodOfIdentification          [1]     IdentificationMethod,
        entityType                      [2]     EntityType }

DeliveryMethod ::= ENUMERATED {
        not-presented-in-person (0),
        presented-in-person (1),
        presented-by-authorized-agent (2),
        split-knowledge (3),
        other (4) }

IdentificationMethod ::= ENUMERATED {
        reasonable-commercial-practices (0),
        verified-by-trusted-third-party (1),
        dual-control (2),
        other (3) }

EntityType ::= ENUMERATED {
        individual (0),
        corporation (1),
        government (2),
        other (3) }
```

This attribute indicates the criteria used to bind the public key (and optionally attributes) to the identity of the entity being certified.

```
CertificatePurpose ::= ENUMERATED {
        any (0),
        encipherment (1),       -- key transport
        signature (2) }
```

This attribute indicates what functions the public key contained in the certificate may be used for.

```
TrustedThirdParty ::= Name
```

This attribute conveys the names of one or more third parties which were involved in the identification process. This would allow a complete trail to be constructed from top-level CA through all involved parties to the certificate subject.

Additionally, if a set of DSA parameters (*p*, *q*, and *g*) are associated with a given CA's users rather being common to the whole network or unique to a single user, this information could be carried as an attribute in the CA's certificate.

8 Multiple Signatures

For high-risk applications it may be desirable to require multiple signatures on the certificate by the CA, with the signatures being performed in independent cryptographic facilities (with different private keys).

We define a **MULTIPLY-SIGNED** macro:

```
MULTIPLY-SIGNED MACRO ::=
BEGIN
        TYPE NOTATION ::= type (ToBeSigned)
        VALUE NOTATION ::= value (VALUE
                SEQUENCE {
                        ToBeSigned,
                        Signatures } )
END
```

A multiply signed certificate is then:

```
MultiplySignedCertificate ::= SEQUENCE {
        CertificateInfo,
        Signatures }
```

The **Signatures** type is a subtype of **SignedData**, defined in "PKCS #7: Cryptographic Message Syntax", constrained to carry only signature information. **SignedData** is defined as follows:

```
SignedData ::= SEQUENCE {
        version                 Version,
        digestAlgorithms        SET OF DigestAlgorithmIdentifier,
        contentInfo             ContentInfo,            -- content type only
        certificates       [0]  SET OF Certificate OPTIONAL,
        crls               [1]  SET OF CertificateRevocationList OPTIONAL,
        signerInfos             SET OF SignerInfo }
```

```
ContentInfo ::= SEQUENCE {
        contentType             OBJECT IDENTIFIER,
        content                 ANY DEFINED BY contentType OPTIONAL }
```

We require that the **content** field of the **ContentInfo** be absent, and in addition that the **certificates** and **crls** fields be absent. The content types indicate what type of information is being signed. The object IDs are defined elsewhere, but might include **data** (messages), **public-key-certificate**, **attribute-certificate**, etc. Using the subtype notation of IS 8825:

```
Signatures ::= SignedData (WITH COMPONENTS
   {    ...,
        contentInfo (WITH COMPONENTS
                { contentType (FROM (id-pk-cert|id-attr-cert)),
                  content ABSENT },
        certificates ABSENT,
        crls ABSENT } )

SignerInfo ::= SEQUENCE {
        version                         Version,
        issuerSerial                    IssuerSerial,
        digestAlgorithm                 DigestAlgorithmIdentifier,
        authenticatedAttributes         [0]     Attributes OPTIONAL,
        digestEncryptionAlgorithm       DigestEncryptionAlgorithmIdentifier,
        encryptedDigest                 EncryptedDigest,        -- the signature
        unauthenticatedAttributes       [1]     Attributes OPTIONAL }

EncryptedDigest ::= OCTET STRING  -- encrypted DigestInfo

DigestInfo ::= SEQUENCE {
        digestAlgorithm         DigestAlgorithmIdentifier,
        digest                  Digest }

Digest ::= OCTET STRING
```

A **SignerInfo** contains the signed digest of the associated content, and identifies the algorithms used to compute and sign the digest. It may also contain other information in the authenticated attributes; this information, if present, is included in the signature computation. Attributes consist of a type and one or more values, as defined in and other standards.

The authenticated attributes contained in the **SignerInfo** might include timestamps, comments and annotations, etc. If present, they **must** include the content type of the **contentInfo** being signed, and the message digest of that content.

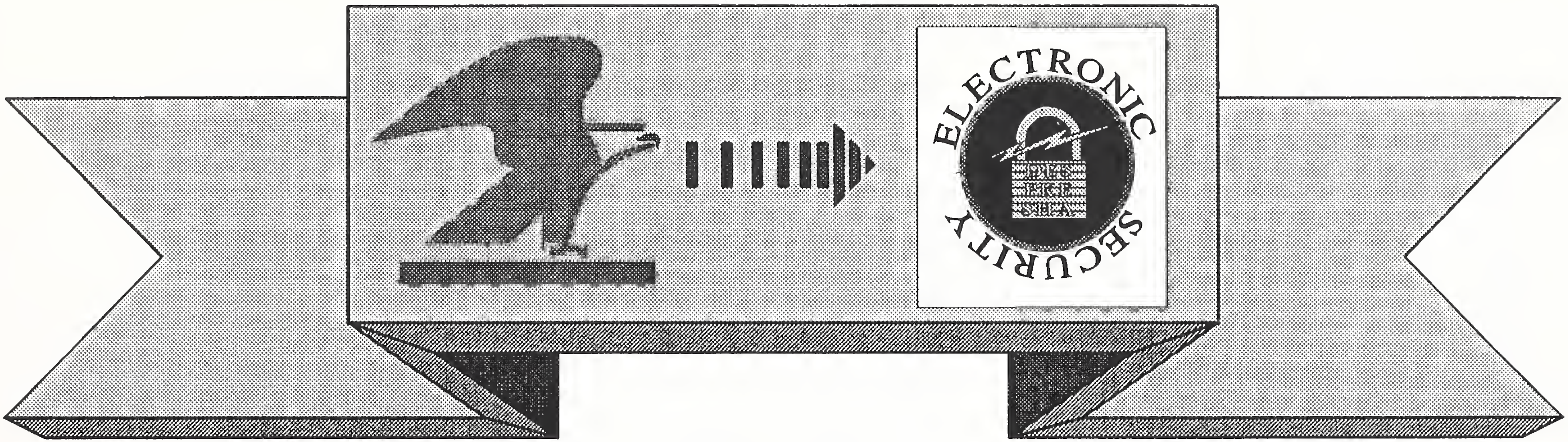
A useful unauthenticated attribute is the **countersignature**, whose format is simply a **SignerInfo**. Its signature is computed on the encrypted digest (i.e. signature field) of the enclosing **SignerInfo** (and any authenticated attributes which might be present in the countersignature). Since the countersignature is of type **SignerInfo**, it may itself contain countersignatures; this allows construction of arbitrarily long chains of countersignatures.

APPENDIX I

U.S. POSTAL SERVICE SECURITY OFFERINGS

Chuck Chamberlain

U.S. Postal Service



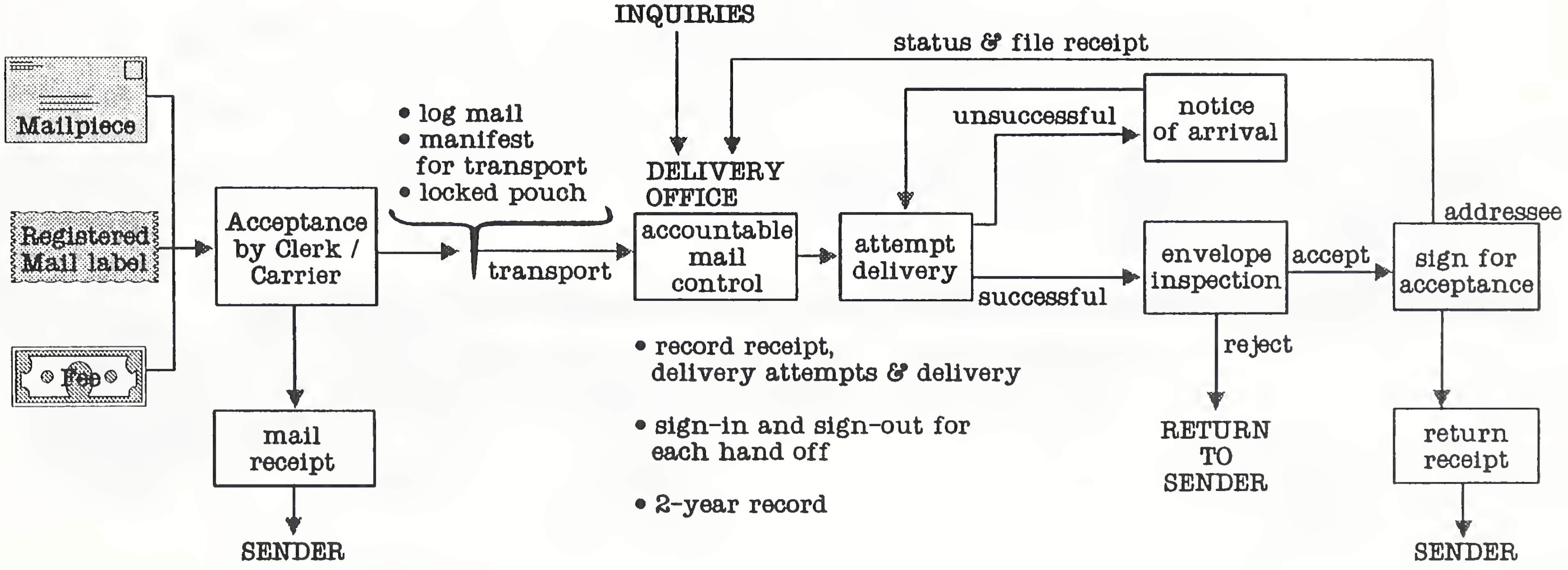
U.S. POSTAL SERVICE SECURITY OFFERINGS

Presentation to
"NIST Public Key Certification Technology Workshop"

December 10-11, 1992

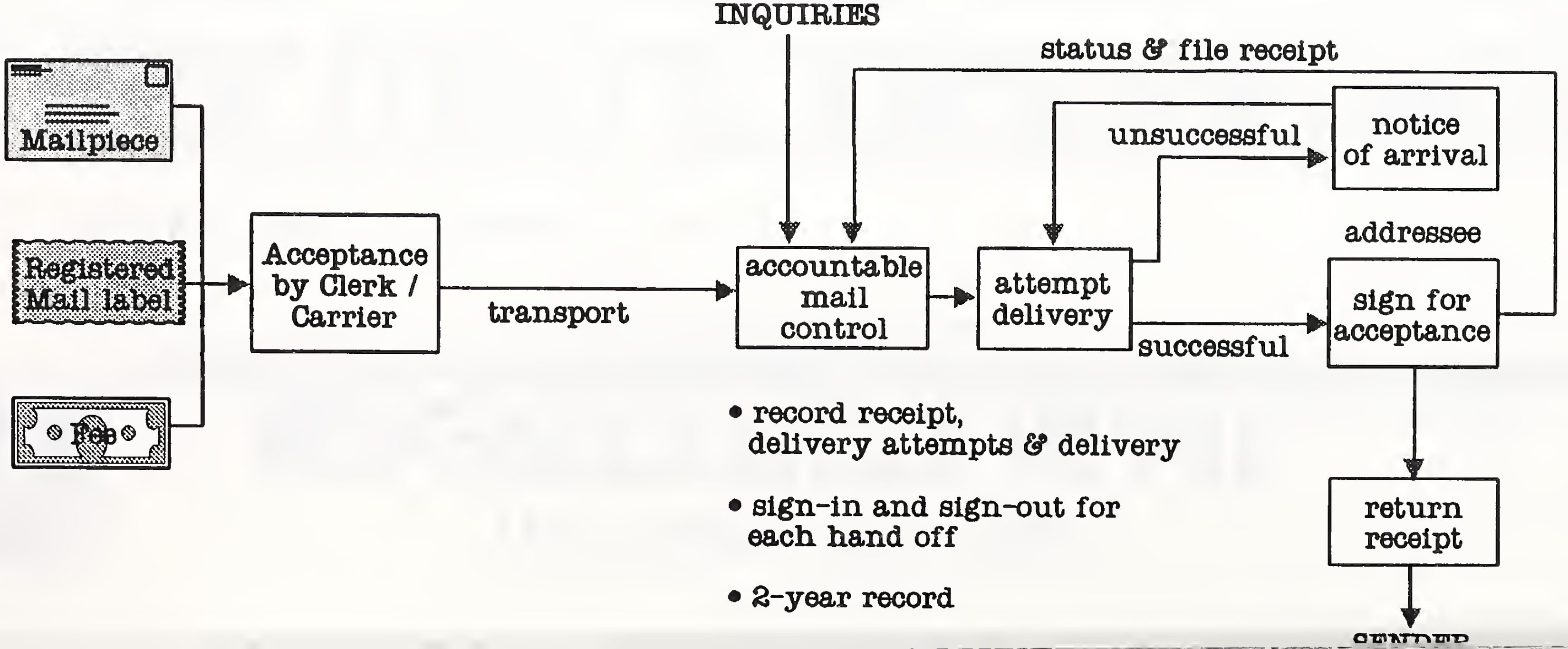
REGISTERED MAIL

- ✓ *USPS's Most Secure Service*
- ✓ *System of Receipts to Monitor Movement*
- ✓ *Insurance, Return Receipt and Restricted Delivery Options*
- ✓ *Secured Container for Transmit*



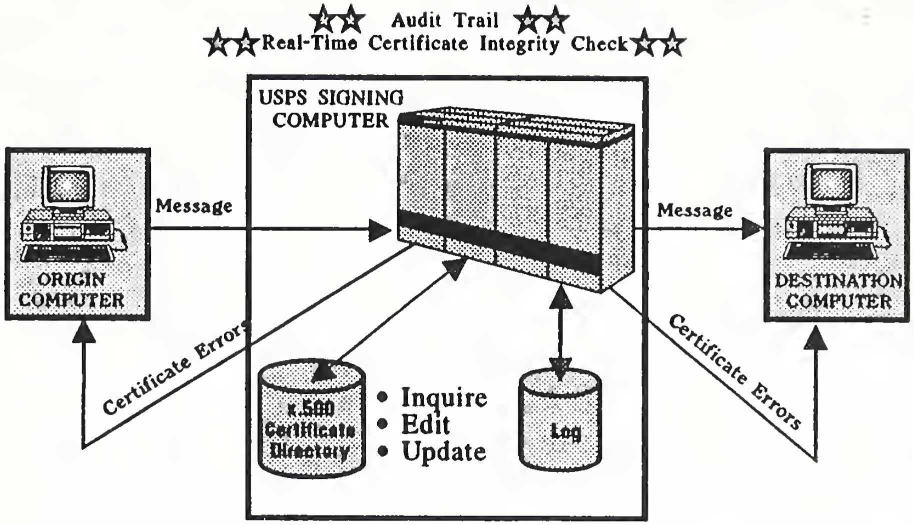
CERTIFIED MAIL

- ✓ *Mailing Receipt and Record of Delivery at Delivery Office*
- ✓ *Handled as Ordinary Mail in Transit*
- ✓ *Return Receipt and Restricted Delivery Options*



- record receipt, delivery attempts & delivery
- sign-in and sign-out for each hand off
- 2-year record

FEDERAL GOVERNMENT ELECTRONIC COMMERCE SERVICES



☆☆ Audit Trail ☆☆

☆☆Real-Time Certificate Integrity Check☆☆

USPS SIGNING COMPUTER

ORIGIN COMPUTER

Message

Message

DESTINATION COMPUTER

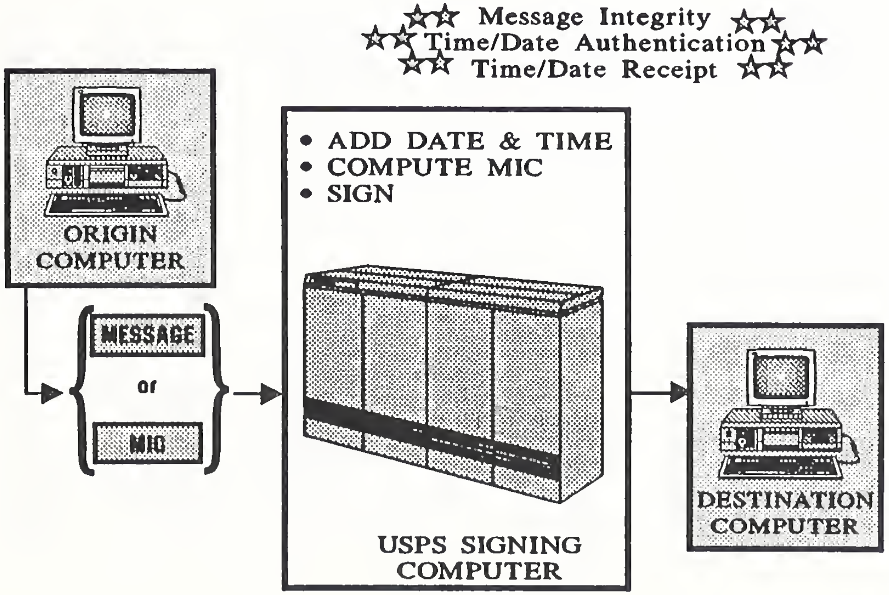
Certificate Errors

Certificate Errors

x.500 Certificate Directory

- Inquire
- Edit
- Update

Log



☆☆ Message Integrity ☆☆

☆☆ Time/Date Authentication ☆☆

☆☆ Time/Date Receipt ☆☆

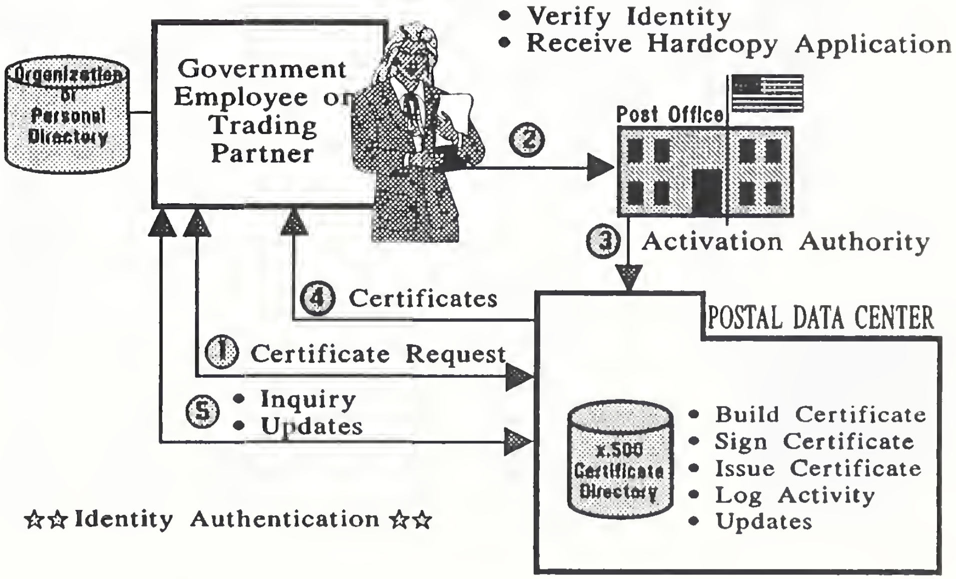
ORIGIN COMPUTER

MESSAGE or MIC

- ADD DATE & TIME
- COMPUTE MIC
- SIGN

USPS SIGNING COMPUTER

DESTINATION COMPUTER



Organization or Personal Directory

Government Employee or Trading Partner

- Verify Identity
- Receive Hardcopy Application

② Post Office

③ Activation Authority

④ Certificates

① Certificate Request

⑤
- Inquiry
- Updates

POSTAL DATA CENTER

x.500 Certificate Directory

- Build Certificate
- Sign Certificate
- Issue Certificate
- Log Activity
- Updates

☆☆ Identity Authentication ☆☆

USPS SECURITY ATTRIBUTES

	Reg 1C.	Regis.	Cert.	Express	Priority	Electronic
Control Totals & Manifesting	NO	YES	YES	YES	NO	NO
Criminal Investigations & Prosecutions	YES	YES	YES	YES	YES	TBD
Delivery Audit Trail	NO	YES	YES	YES	NO	YES
Delivery Notification	NO	YES	YES	YES	NO	NO
Employee Screening	YES	YES	YES	YES	YES	YES
Facility Security	YES	YES	YES	YES	YES	YES
ID Check for Pick-Up	N/A	YES	YES	YES	NO	YES
Machine Security	N/A	N/A	N/A	N/A	N/A	YES
Mailbox Protection	YES	YES	YES	YES	YES	NO
Message Encryption	NO	NO	NO	NO	NO	NO
Sealed						
- Envelopes	YES	YES	YES	YES	YES	YES
- Containers	NO	YES	NO	NO	NO	NO
- Transp.	YES	YES	YES	YES	YES	NO
Time/Date of USPS						
- Receipt	NO	YES	YES	YES	NO	YES
- Delivery	NO	YES	YES	YES	NO	YES(SAME)
Track & Trace	NO	NO	NO	YES	NO	NO

APPENDIX J

AMERICAN NATIONAL STANDARD X9.30-199X

WORKING DRAFT

1992 American Bankers Association

Accredited Standards Committee X9
Title: X9-Financial Services
Accredited by the
American National Standards Institute

N03 92, December 8, 1992

Dennis Branstad

WORKING DRAFT

AMERICAN NATIONAL STANDARD
X9.30-199X

PUBLIC KEY CRYPTOGRAPHY USING IRREVERSIBLE ALGORITHMS FOR THE FINANCIAL SERVICES INDUSTRY:

PART 3: CERTIFICATE MANAGEMENT FOR DSA©

Price per copy:

Notice -- Warning to readers of this document

This document is in the working document stage. It has not yet been processed through the consensus procedures of X9 and ANSI.

Many changes which may greatly affect the contents can occur before this document becomes an American National Standard. The developmental committee may not be held responsible for the contents of this document as it currently exists.

Implementation or design based on this working paper is at the risk of the user. No advertisement implying compliance with this "Standard" should appear as it is erroneous and misleading to so state.

Copies of the draft proposed American National Standard will also be available from the X9 Secretariat when the document is finally announced for two months public comment. Notice will be issued in the trade press.

Copies of this document are available from the X9 Secretariat at the price listed above. Please send a self- addressed mailing label with your order.

Secretariat: American Bankers Associatio

Standards Departme
1120 Connecticut Ave., N.W
Washington, DC 2003

Contents

X9.30

PART 3: CERTIFICATE MANAGEMENT

1. SCOPE

This Standard defines certificate management and an authentication framework for the financial services industry.

The binding association between the identity of the owner of a public key and that key shall be documented in order to prove the ownership of a public key. This binding is called a "Certificate". Certificates are generated by a trusted third entity known as a Certification Authority (CA).

The structure encompassing CAs and the entities that they certify is called an "Authentication Framework." To ensure interoperability and security, rules, procedures and the functions of the entities and CAs shall be agreed upon and managed.

This Standard specifies the contents of certificates, the credentials required to obtain a certificate, and procedures for certificate generation, validation, and revocation, for Digital Signature Algorithm (DSA) public key certificates. A related standard, X9.31-3, addresses the management of RSA certificates. DSA shall always be used to certify a DSA (or other irreversible algorithm) public key.

It also recommends some useful attributes, encoding schemes, and operational procedures (e.g., distribution mechanisms, and acceptance criteria for submitted credentials).

2. DEFINITIONS AND COMMON ABBREVIATIONS

2.1. Definitions

Accountability
The property that ensures that the actions of an entity may be traced uniquely to the entity.

Asymmetric Key System
A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

Attribute
Information, excluding the public key, which is provided by the entity or the CA and certified by the CA in an **AttributeCertificates**. Examples include the CA's liability limitations and binding information.

Attributes Certificate
A set of attributes along with a certificate identifier that is bound to an entity's certificate by the CA.

Audit Journal

A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

Audit Trail

See Audit Journal.

Data Origin Authentication

Corroboration that the identity of the originator of a data unit is as claimed. Data integrity is implied.

As used in this Standard, authentication shall be by means of a digital signature and certificates or the process of ANSI X9.9-1986[1].

Authorization

The granting of rights.

Certificate

A certificate contains the public key of a legal entity together with other information. The CA's digital signature renders the certificate unforgeable.

Certification Authority (CA)

A Center trusted by one or more users to create and assign certificates.

Certification Path

An ordered sequence of certificates of entities which, together with the public key of the initial entity in the path, can be processed to obtain the public key of the final entity in the path.

Certification Request Data

The "Certification Request Data" (**CertReqData**) of an entity includes the entity's public key, entity identity and other information included in the certificate or otherwise used in the certificate management process.

Certificate Revocation List

A list of revoked certificates.

Compromise

A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred.

Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Cross Certification

Cross certification is used by one CA to certify any CA other than a CA immediately adjacent (superior or subordinate) to it in a hierarchy.

[1] ANSI X9.9-1986, *Financial Institution Message Authentication (wholesale) (revised).*

In the X.509 trust model, a CA always certifies its superior and subordinates, and cross certifies other CAs.

Cryptographic Module

The set of hardware, firmware or software or some combination thereof, that implements cryptographic logic, cryptographic processes, or both.

Cryptography

The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

Cryptoperiod

The time span during which a specific key is authorized for use or in which the keys for a given system may remain in effect.

Cryptographic Key (Key)

A parameter that determines the operation of a cryptographic function such as:

1. the transformation from plain text to cipher text and vice versa,
2. synchronized generation of keying material,
3. digital signature computation or validation.

Cryptographic Keying Material

See Keying Material.

Data Integrity

Property that data has not been altered or destroyed.

Digital Signature

A cryptographic transformation of data which, when appended to a data unit, provides the services of:

1. origin authentication,
2. data integrity, and
3. signer non-repudiation

Dual Control

A process of utilizing two or more separate entities (usually persons), who are operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person shall be able to access or to utilize the materials (e.g., cryptographic key).

For manual key and certificate generation, conveyance, loading, storage and retrieval, dual control requires split knowledge of key among the entities. (Also see Split Knowledge)

Entity

A legal entity or an individual. Note that a Certification Authority is an entity.

Financial Message

A communication containing information which has financial implications.

Forgery

The fabrication of information by one individual, entity or process and/or the claim that such information was received in a communication from another individual, entity, or process.

Hash

A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A 'good' hash is such that the results of applying the function to a (large) set of values in the domain will be evenly (and randomly) distributed over the range.

A (cryptographic) hash function is a mathematical function which maps values from a large domain into a smaller domain, and has appropriated cryptographic properties (See X9.30-199x: *Part 2, Secure Hash Function*, Section 3). It may be used to compress a potentially long message in a representative message image ("hash value" or "message digest") sufficiently compact to be input into a digital signature algorithm (e.g., DSA, as defined in X9.30-199x: *Part 1, The Digital Signature Algorithm*).

Hot List

See Certificate Revocation List

Interoperability

The ability to exchange keying material, both manually and in an automated environment, with any other entity implementing this standard, providing that both implementations use compatible options of this standard and compatible communications facilities.

Key

See Cryptographic Key.

Keying Material

The data (e.g., keys, certificates and IVs) necessary to establish and maintain cryptographic keying relationships.

Key Management

The generation, storage, secure distribution and application of keying material in accordance with a security policy.

Key Pair

When used in public key cryptography, a public key and its corresponding private key.

Keying Relationship

The state existing between a communicating pair or between members of a group (logical entity) during which time they share keying material.

Legal Entity

A group or area that has legal recognition, e.g., a corporation, labor union, state or nation.

Message

A communication containing one or more transactions or related information.

Module

See Cryptographic Module.

Non Repudiation

The prevention of the denial by an entity of having participated in a communication, creation, or authorization of some data.

Optional

Not required by this standard or not required to meet an optional provision of this standard.

Originator

The person, institution or other entity that is responsible for and authorized to originate a message.

Private key

In an asymmetric (public) key cryptosystem, that key of a user's key pair which is known only by that user.

Public Key

In an asymmetric key system, that key of a user's key pair which is publicly known.

Recipient

The person, institution or other entity that is responsible for and authorized to receive a message.

Repudiation

The denial by a user of having participated in part or all of a communication. See non-repudiation which has the opposite meaning.

Security Life

The time span over which cryptographically protected data have value.

Split Knowledge

A condition under which two or more entities separately have key components which, individually, convey no knowledge of the resultant cryptographic key. The resultant key exists only within secure equipment as the automatically generated, exclusive-or'ed result of the full length key components which each individual entered separately and confidentially.

4. CERTIFICATE MANAGEMENT

4.1. General

This section defines a CA's controls and other management requirements for a CA and its subscribers. The CA has a public/private key pair and uses the Digital Signature Algorithm (DSA)and the Secure Hash Algorithm (SHA) to produce certificates.

The binding of an entity's public key and identity is verified by using the public key of one or more CAs. The certificate(s) and its validation shall be maintained by the verifier in an audit journal. A CA may issue certificates to entities or other CA's.

Entities or CAs can use these certificates to authenticate themselves to other entities and to CAs. Hence, authentication may involve a chain of certificates. The validator's CA's public key corresponding to the private key used by the validator's CA to sign the end certificate shall be obtained and authenticated by some means other than by the use of certificates. See Section 4.2 and Appendix A, Suggested Requirements for the Acceptance of Certificate Request Data.

Once a certificate has been generated, the integrity of its contents is protected. This Standard does not require that certificates be given confidentiality protection. A valid copy of the CA's public key is required by the verifier in order to validate a certificate. Given the assumption that the CA is a trusted third entity, this permits the verification of the binding between an entity's public key, its identity and other needed information.

Examples of CA relationships are illustrated in Figures 1 and 2.

Each group (such as a retail credit authorization network, a clearing house, a financial institution or a subgroup thereof) may have its own CA. To make inter-group authentication services possible, CAs shall either have a common CA to authenticate them, or the CAs shall cross certify each other. If a common CA is used, this common CA shall be a mutual point of trust for the entities.

An entity may have one or more valid certificates for backup or transition.

The information which an entity presents to a CA in order to obtain a certificate is:

- Certification Request Data.

  Certification Request Data includes the entity's public key, identity and other information used in the certificate management process.

FIGURE 1

A CERTIFICATION AUTHORITY HIERARCHY

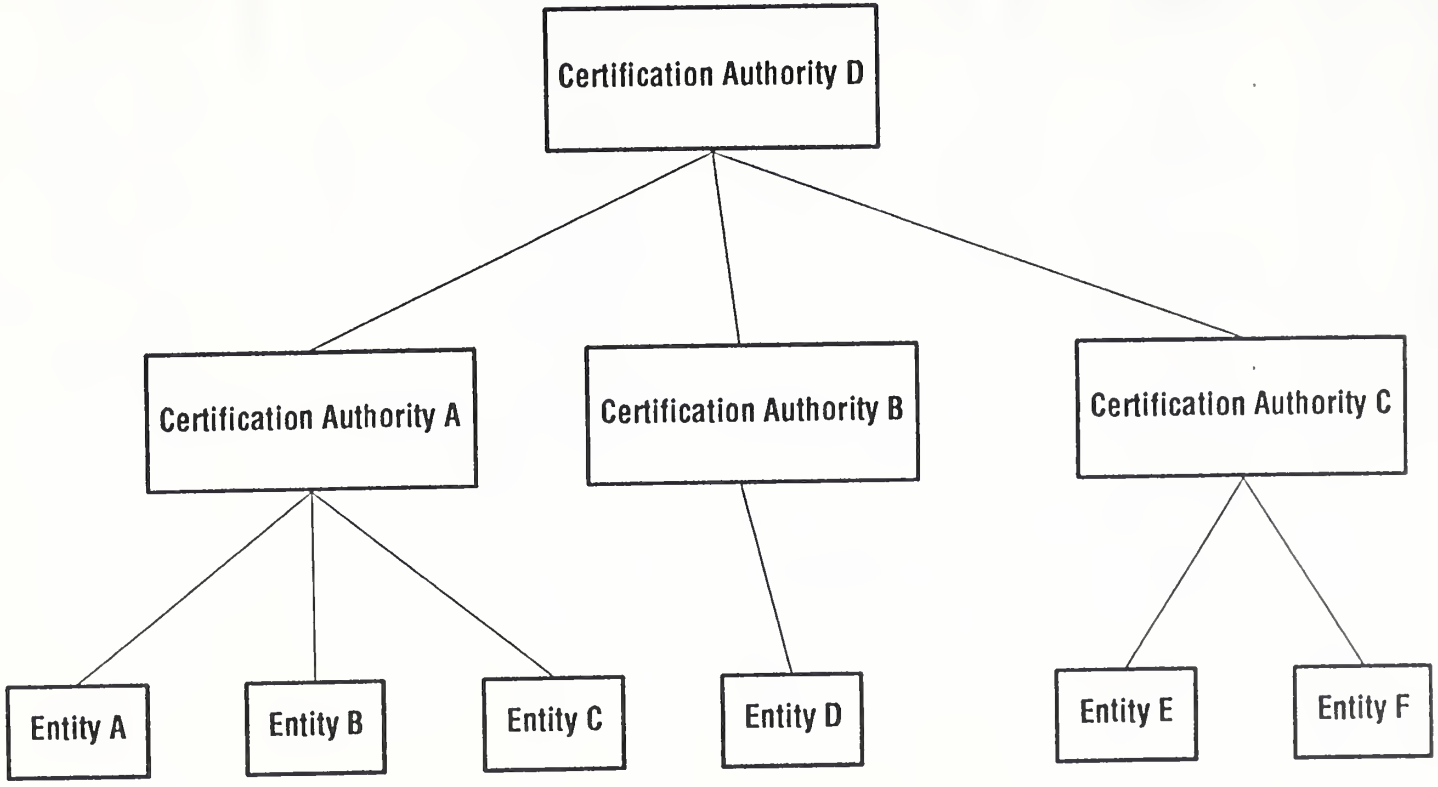
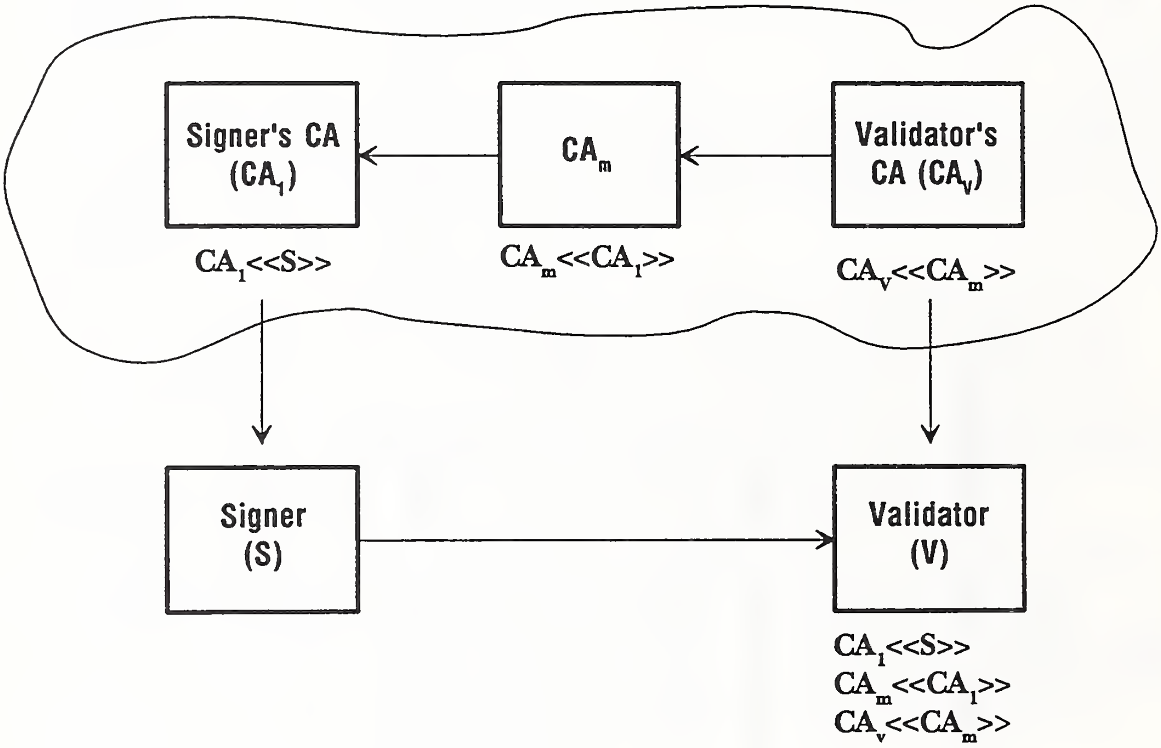

Certification Authority D
Certification Authority A
Certification Authority B
Certification Authority C
Entity A
Entity B
Entity C
Entity D
Entity E
Entity F

FIGURE 2

A NON-HIERARCHICAL CERTIFICATION AUTHORITY CHAIN



- V starts with an authenticated copy of the public key of CA_v
- V checks the signature of $CA_v<<CA_m>>$ $CA_m<<CA_1>>$ $CA_1<<S>>$

- additional data required for identification

  See Appendix A.

The CA issues a certificate containing an entity's public key and any other information added by the CA (See Section 5.5.5). The binding of the entity's public key to its identity is accomplished by having the CA generate the certificate, thereby attesting to the relationship of the information therein and ensuring its integrity.

Each entity shall generate its own public/private key pair(s) and shall be responsible for the quality of that key pair and for ensuring the privacy and integrity of the private key. The CA shall be responsible for the certification process.

4.2. The Certification Authority (CA)

4.2.1. Certification Authority Responsibilities

The Certification Authority shall be solely responsible for:

1. Verifying the identity of the entity requesting a certificate.
2. Securing the certification process and the private key used to generate the certificate.
3. Advising the entity identified in the certificate that a certificate has been issued. The means used to convey this advice shall be independent of the method used to convey the certificate to the entity.
4. Ensuring that certificates are not issued to two different entities with the same entity name.

Appendix A contains suggested requirements for the acceptance of Certificate Request Data. See Section 6 for audit journal requirements.

4.2.2. Distribution of a CA's Public Key

a. General

The integrity of a CA's public key is essential. When a hierarchy or chain of CAs is employed, the integrity of the hierarchy or chain depends on the integrity of the public key and confidentiality of the private key of every CA in the certification path. It is the responsibility of the CA to:

1. distribute its public key, validity period and the unique identity corresponding to Xp, and
2. ensure the integrity of that key during distribution, or

3. to provide a mechanism for detecting its modification during the distribution process.

   As in the case of the delivery of Certificate Request Data, a digital signature may be used to detect errors in the distribution process.

It is the responsibility of each entity to ensure that:

1. it possesses and uses the correct CA public key, and
2. that the integrity of the CAs public key is maintained once acquired.

Multiple public keys, each corresponding to a CA's public/private key pair, may be distributed to provide for replacement of a public key upon the expiration of the cryptoperiod of a given public/private key pair and for backup and recovery purposes.

CA public keys stored in such local caches should be protected against accidental or deliberate modification by either a digital signature or a Message Authentication Code[3].

b. Certified Delivery of a CA's Public Key

A CA's public key may be distributed using one or more of the following certified methods:

1. Direct electronic transmission from the root CA, or retrieval from a remote cache or directory service

   a) If an entity has an authenticated copy of a currently valid public key of the CA, say CA_np:

      (1) a new public key, CA_mp, may be sent by the CA to the entity by electronic transmission,

      (2) the message transmitting CA_mp shall be signed by the CA using CA_ns, and

      (3) on receipt, the entity shall authenticate the received public key, CA_mp using CA_np

      An *authenticated* public key is a public key which was obtained from a certificate validated as described in Section 4.6, or a public key distributed as described in this Section 4.2.2.

[3] ANSI X9.9, OpCit.

b) If an entity does not have an authenticated copy of a currently valid public key of the CA, that entity may obtain a copy when applying for a certificate. The CA's public key (CA_np) should be transmitted using a machine readable media. The delivery of the media (when used) shall be authenticated.

c) If the CA's key is contained in a certificate in a path, the initial certificate in a path shall be validated via a public key which is not contained in a certificate. The validator shall ascertain that the public key is currently valid.

2. From a remote cache or directory service

If an entity has an authenticated copy of a currently valid public key of the CA, say CA_np:

a) the entity may request a new public key, CA_mp from a remote cache or directory service,

b) the message transmitting CA_mp shall be signed by the CA using CA_ns, and

c) on receipt, the entity shall authenticate the received public key, CA_mp using CA_np, or

c. Trusted Delivery of a CA's Public Key

The CA's public key may be embedding in a cryptographic module (module) in equipment prior to shipment.

1) If an entity has an authenticated copy of a currently valid public key of the CA, say CA_np:

a) A new public key, CA_mp shall be signed by the CA using CA_ns. The CA_mp and the signature shall be loaded in the module in a secure environment and under appropriate controls and procedures before the module or the equipment containing the module is distributed, and

b) on receipt, the entity shall authenticate the received public key, CA_mp using CA_np, or

2) If an entity does not have an authenticated copy of a currently valid public key of the CA, the distribution of the equipment or other medium shall be authenticated.

d. Extraction of a CA's Public Key From a Certification Path

A CA's key may be contained in a certification path, in which case it may be validated using the public key from the previous certificate in the path. The initial certificate in a path is validated by a public key which is not contained in a certificate, and may be distributed by one of the methods described above. The validator shall ascertain that this public key is currently valid.

Figure 3 Summarizes the above methods of distributing a CA's public key.

4.2.3. Security Requirements for a CA's Private Key

Since the certificate generated by a CA shall be used to provide proof of the identity and integrity of the entity's public key, the CA shall be implemented in a cryptographic module not controlled or accessed by any subscribing entity. Since the cryptographic module employs the private key of the CA which issues the certificate, this key shall be given a high level of protection since its possession would enable an intruder to masquerade as the CA and generate forged certificates. This private key shall be generated internally to the cryptographic module in which it shall be used. It shall never appear outside of that cryptographic module in any form (plain text or enciphered). The cryptographic module shall afford level 4 protection[4] to private keys.

4.3. The Trust Model

The Certification Authority is "trusted" by its subscribers. Such trust is based on the use of:

- cryptographic module designed to meet the requirements for financial institution use,
- sound management and control practices that are confirmed by an independent audit function (internal, external or both) which shall report audit results to the subscribers.

A C2[5] level of functionality is recommended.

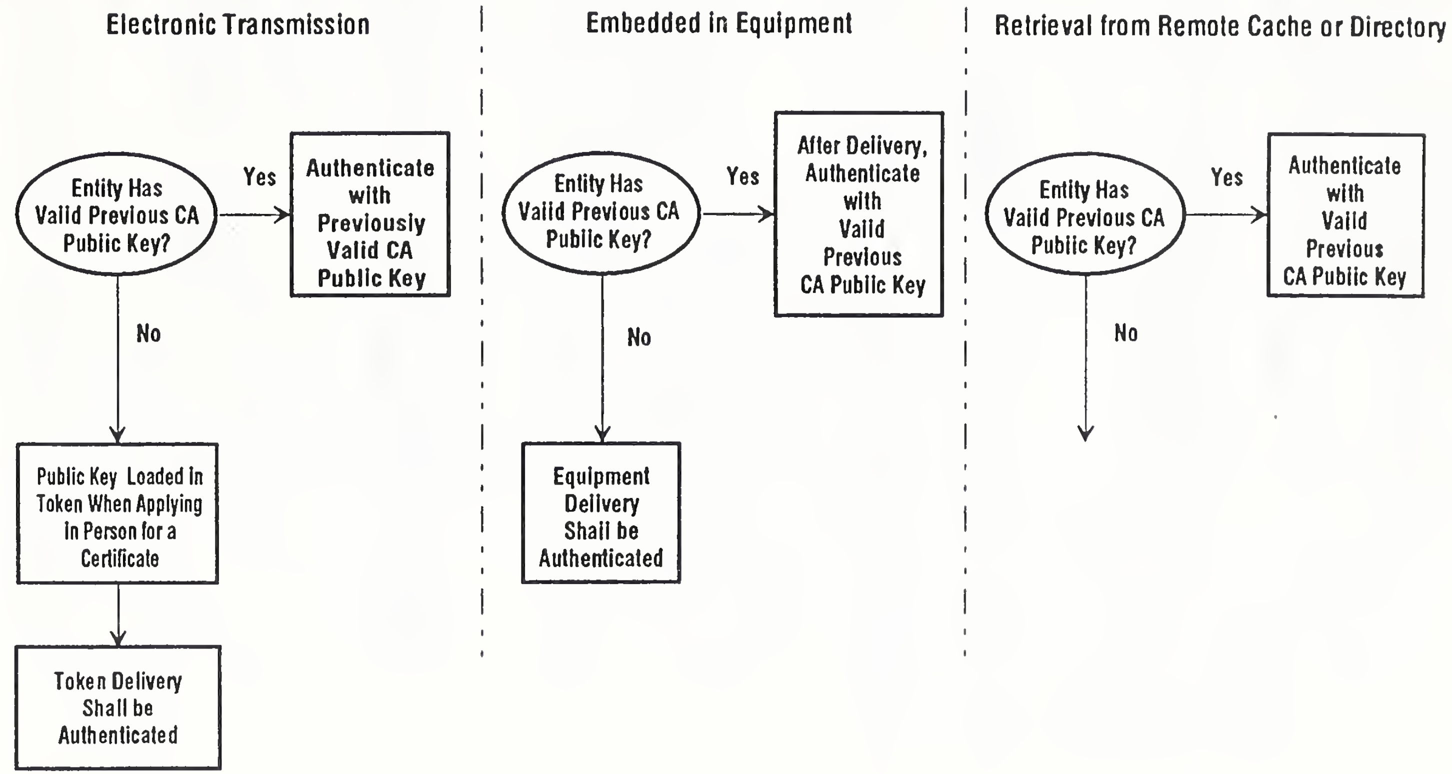
1. A subscriber trusts all certificates issued by its CA;
2. If a subscriber's CA issues a certificate whose subject is another CA, then the subscriber trusts all certificates issued by that other CA,
3. A CA is trusted:
   a) to certify its subscribers

[4] As defined in draft Federal Information Processing Standard 140-1.

[5] As defined in CSC-STD-001-83, *Department of Defense Trusted Computer System Evaluation Criteria*, August 15, 1983.

FIGURE 3

SUMMARY OF METHODS OF DISTRIBUTING A CA'S PUBLIC KEY


Electronic Transmission
Entity Has Valid Previous CA Public Key?
Yes
Authenticate with Previously Valid CA Public Key
No
Public Key Loaded in Token When Applying in Person for a Certificate
Token Delivery Shall be Authenticated
Embedded in Equipment
Entity Has Valid Previous CA Public Key?
Yes
After Delivery, Authenticate with Valid Previous CA Public Key
No
Equipment Delivery Shall be Authenticated
Retrieval from Remote Cache or Directory
Entity Has Valid Previous CA Public Key?
Yes
Authenticate with Valid Previous CA Public Key
No

b) in the case where the CA is in a hierarchy, to certify CAs, if any, immediately adjacent to it (either superior or subordinate) in the hierarchy,

c) optionally, to cross-certify other CAs

4. A CA may be trusted to cross-certify other CAs not adjacent to it in the hierarchy.

Requirements for cross certification may be more stringent than for normal certification.

Examples illustrating this model are contained in Section 5.10. Other trust models are discussed in Appendix B.

4.5. Certificate Generation

The certificate generation process shall take place prior to the signing and sending of financial transactions or other messages.

Generation of a certificate is a five-step process. The following is an overview of the process with references to pertinent sections in this Standard.

1. Preparing Certificate Request Data

   The Certificate Request Data shall be prepared by the entity requesting a certificate. The entity shall use a digital signature to allow the detection of errors in the certificate application process. The private key used for signing the Certificate Request Data shall be that corresponding to the public key in the Certificate Request Data. See Section 5.4, below.

2. Accepting Certificate Request Data

   Suggested requirements for accepting Certificate Request Data are contained in Appendix A. See also Section 5.4, below.

3. Checking Certificate Request Data for errors and changes

   The CA shall use the public key contained in Certificate Request Data to verify the signature on the Certificate Request Data submission.

4. Generating the certificate.

   The certificate contains the Certificate Request Data, information provided by the Certification Authority, and the signature. See Section 5.5.

   In high risk financial applications, two signatures from independent cryptographic facilities may be used to ameliorate the risk in the event that the private key of a CA is compromised. See Section 5.9.

5. Creating the Audit Journal entry.

   Actions of the CA in the certificate generation process shall be journalized See Section 6, below.

Figure 4 summarizes the certificate generation process.

4.6. Certificate Validation

To validate a certificate, the receiving entity:

1. obtains the certificate of the sending entity and any CA certificates in the certification path from the sender to the recipient from:
   - the sending entity,
   - a Directory Service or
   - a local cache.
2. checks the validity of the certificates (see Section 5.10),

   This implies loose synchronization and secure maintenance of the clocks of the sender, recipient and all CAs in the path.
3. checks the Certificate Revocation List, and
4. verifies the CA's signature on all certificates in the certification path (see Section 2.3).

4.7. Certificate Revocation List (CRL)

4.7.1. General Requirements

A certificate has a lifetime which is indicated by a validity period stated in the certificate or is otherwise defined by the CA's management (such as the expiration date of an IC card[6]). Certificates may only be revoked prior to their scheduled expiration by the CA that issues the certificate. This may occur for a number of reasons, including:

- compromise or suspected compromise of an entity's[7] private key,
- cessation of operations,
- change of affiliation of an entity (E.g., affiliation with a different CA_1), or

[6] An Integrated Circuit Card (IC card) is often referred to as a "Smart Card."
[7] The entity may be a CA.

APPENDIX K

CONTRIBUTION TO THE WORKSHOP ON ELECTRONIC SIGNATURES

George Papapavlou

Brussels, 1 December 1992

CONTRIBUTION TO THE WORKSHOP ON ELECTRONIC SIGNATURES, BRUSSELS, 1 DECEMBER 1992

George Papapavlou, Head of sector
"Legal aspects of new information technologies"
DG XIII-E1

The main purpose of this brief contribution is to argue in favour of the inclusion of criminal law considerations in the future work both on information security, in general, and electronic signatures, in particular. In the 10 minutes I have at my disposal this has to be done in a telegraphic way. Essentially I will give very brief answers to the following questions:

1) What is computer related crime?

2) What is the relevance with electronic signatures?

3) What is the relevance with information security?

4) What has been done sofar in the Member States and in the Community?

5) What can be done in the future?

1) What is computer related crime?

There is no single definition of this concept. I may use the OECD definition "computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data" or a senior expert's definition "any illegal action in which a computer is a tool or object of the crime". What is more important is to understand that the computer today offers some highly sophisticated opportunities for law-breaking.

A recent Council of Europe report distinguishes twelve different computer related illegal acts: computer related fraud; computer forgery; damage to computer data or programs; computer sabotage; unauthorized access; unauthorized interception; unauthorized reproduction of a protected computer program; unauthorized reproduction of a topography; alteration of computer data or computer programs; computer espionage; unauthorized use of a computer; unauthorized use of a protected computer program.

As there is a known difficulty with reporting such illegal acts to the police and going to court, estimates of losses suffered differ widely. There is no doubt, however, that we are talking of a problem with serious economic, social and strategic dimensions.

2) **What is the relevance with electronic signatures?**

Two of the illegal acts I mentioned, computer related fraud and computer forgery have a clear relationship. Any manipulation of an electronic signature of any form would fall under the one and/or the other of these acts. Computer related fraud is defined by the COE 1990 report as "the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing, thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person". Computer forgery is defined as "the input, alteration erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence".

3) **What is the relevance with information security?**

I think this is very clear. It is like the relationship between criminal law provisions on theft and a lock or alarm system to prevent theft. Technical security measures are necessary but not sufficient. Legal measures, in the form of criminal law, are also required to act both in a preventive and in a repressive way. It is clear that technical or organizational and other practical measures have to be taken to prevent the illegal acts I listed before. It has to be made clear, however, that these are illegal acts punishable by law. I don't think I need to argue this point any further.

4) **What has been done sofar internationally, in the Member States and in the Community?**

Efforts aiming at better protection of computer related economic values started not with criminal but civil law provisions in the context of topography and computer programs. Criminal law provisions were first introduced in the seond half of the 1980s.

I will, of course, refer to some important developments only. Internationally there have been two important initiatives, both of a non-legally binding nature. In September 1989 the Council of Europe Committee of Ministers adopted Recommendation N° R(89)9 by which it asked Member states to take into account when reviewing their legislation or initiating new legislation, the report on computer-related crime (that I referred to already) and to report to the S.G. of the C.O.E. during 1993 on any relevant developments in their legislation, judicial practice and experiences of international legal co-operation. The report concerned not only includes detailed description and analysis of the various illegal acts that should be included in national substantive penal laws but also has an analysis of the very important issue of procedural law and international cooperation which are necessary if substantive law provisions are to become effective.

In September 1992 the OECD - at the level of experts - finalized Guidelines for the Security of Information Systems and a relevant draft recommendation of its Council of Ministers. The guidelines include reference to the adoption of appropriate policies, laws, decrees, rules and international agreements, including provision for penal, administrative or other sanctions for misuse of information systems; jurisdictional competence of courts including rules on extraterritorial jurisdiction, and administrative competence of other bodies; mutual assistance, extradition and other international cooperation in penal matters; and means of obtaining evidence in information systems and the admissibility of such evidence in penal and non-penal legal and administrative proceedings.

At the level of national legislation most Community Member States have adapted their penal laws in some way in order to deal with computer-related criminal acts (examples: the Danish 1985 "penal code amendment act", the German 1986 "second law for the prevention of economic crimes", the French 1988 "loi sur la fraude informatique" and the UK 1990 "Computer Misuse Act)".

Due to obvious competence questions no specific penal law measures have sofar been taken by the Community. In the context of the various legal issues identified in relation with the IMPACT programme on the information services market, computer related crime has been studied in 1987 and discussed in 1988 with our group of legal experts called the LAB but no decisions on further action were taken because of the competence questions I mentioned but also because of other urgent priorities.

Moreover, in March 1990 the Commission organized a 2-day conference in Luxembourg, jointly with the Council of Europe , part of which was dedicated to the issue of cumputer related crime.

5) **What can be done in the future?**

Since 1987 when we first studied this problem, a number of things have happened which, in my view, justify its reexamination.

a) The two international initiatives, COE report and OECD Guidelines, that I have referred to already. In addition, since September, the COE has reopened this dossier by starting discussions on the issue of penal procedure and international cooperation;

b) the gradually increasing awareness of this problem by Community Member States most of which - if not all - have introduced relevant provisions in their penal laws;

c) two Council directives - insider trading and money laundering - which include - limited - penal provisions;

d) initiatives taken to combat fraud against the Community (DG XX);

e) the Maastricht Treaty in its article K1 provides for a number of issues on which legal cooperation among Member States will have to be increased. These include the combat of international - scale fraud, judicial cooperation in civil and penal matters and police cooperation for combatting (among other things) serious forms of international crime;

f) last but not least, the Information Security action plan (INFOSEC), adopted by Council last March, makes references to action also in the legal field.

All these developments indicate that there is now much more room for Community involvement in the field of computer related crime. Of course, the Community has no competence to propose specific penal sanctions. Moreover the debate following the Maastricht Treaty Danish and French experiences has led to more emphasis being given to the so-called subsidiarity principle. Be that as it may, I think a number of Community-level actions could still be considered.

I will give some ideas starting with the minimalist and ending with the maximalist approach.

First, computer related crime in its different aspects (substantive law, procedural law, training and awareness, etc.) should be included in the legal issues to be examined in the context of the information security action plan. One or more meetings with

Member States Ministry of Justice officials could be organized to have an exchange of views and precise information on the current situation in each Member State.

Second, once the Maastricht Treaty is ratified, and the modalities of closer judicial and police cooperation are established, it should be emphasized to the appropriate Commission services and to the Member States that such cooperation should also cover computer related crime, by nature often of an international nature and requiring particularly quick and effective cooperation procedures. It might be useful to establish a link with the relevant work currently undertaken in the Council of Europe. We will follow developments there but it might also be useful if SOGIS members take direct contact with their officials attending the COE meetings.

Third, information awareness and training initiatives may be undertaken, in parallel with similar initiatives concerning security. DG XIII has made a short study and could propose a number of such initiatives.

Fourth, it is certain that the Community does not have a competence to propose specific penal sanctions. What it could do, if it was considered necessary, is list a number of actions related to data processing that would not be allowed, and ask Member States to provide for effective sanctions. In addition establish a mechanism for effective investigation and copperation among Member States. This has been done in the context of the money laundering and insider trading directives. I am not proposing this at this tage. When we first studied the problem there did seem to be serious gaps in the laws of certain Member States. This seems to be less the case now with the recent adaptations of penal laws. First, we need precise up to date information in order to see if there is still a need for encouraging penal sanctions. Effective procedural and mutual cooperation measures, however, certainly need to be seriously considered.

APPENDIX L

VIEWGRAPHS PRESENTED AT NIST SYMPOSIUM ON APPLICATIONS OF THE DIGITAL SIGNATURE STANDARD

Stephen Kent

BBN Communications

ADDITIONAL INFORMATION

The following set of viewgraphs were prepared by Dr. Stephen Kent, BBN, and presented at a NIST Symposium of Applications of the Digital Signature Standard. This Symposium was held in February, 1993. Since the viewgraphs reflect some of the discussion of the workshop and the results of the workshop, they are included in the report of the workshop. However, they were prepared subsequent to the workshop and hence are not officially a part of the proceedings summary.

Dennis Branstad, Editor

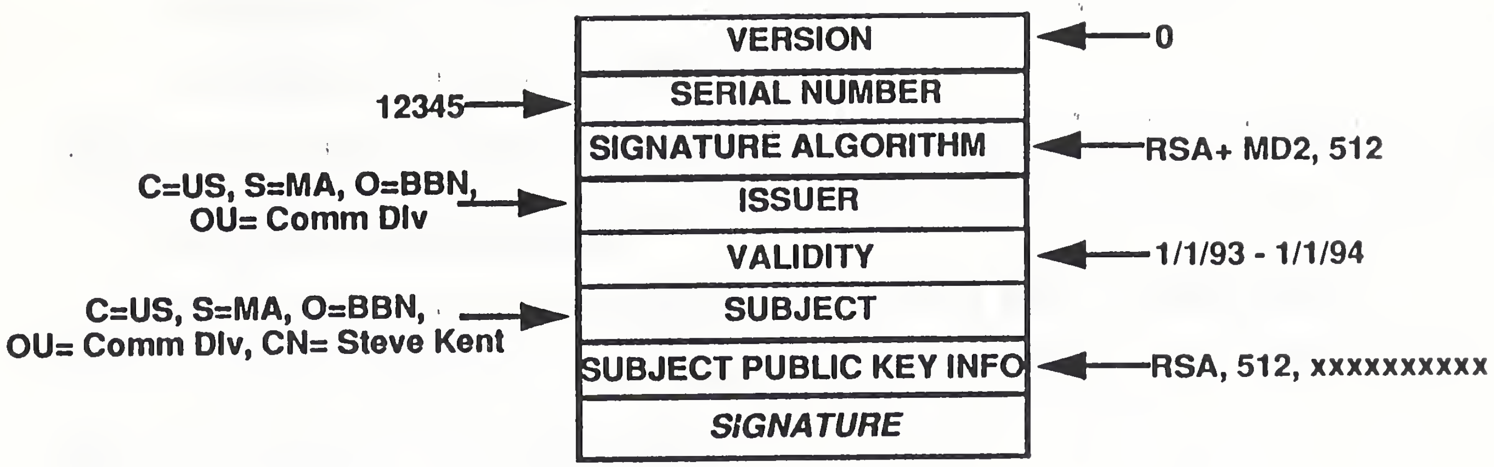
Certificate Management Architectures

Dr. Stephen Kent
Chief Scientist
BBN Communications

What is Public Key Certification?

- Public-key cryptosystems make use of "certificates" to bind public keys to attributes
- X.509 defines a syntax and semantics for certificates used for identification/authentication
- X.509 certificates can be used as a basis for a variety of access control policies, based on the identity of a user, organization, or a role
- Additional certificate formats are being developed for binding other attributes, e.g., fiduciary authorization, to identities

X.509 Certificate Example



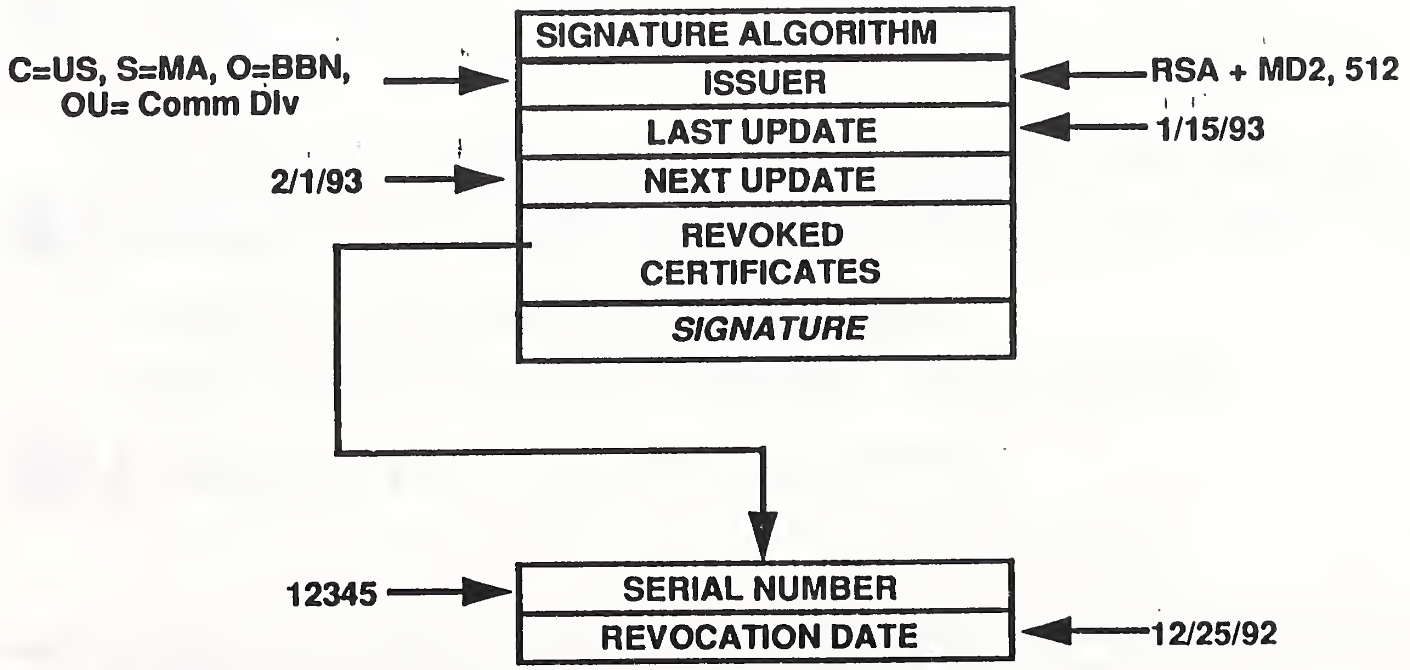
Generic Certification Issues

- Certification topology
  - —single root vs. multiple roots vs. mesh
  - —mapping between name structure and certification
  - —cross-certification
- Authentication vs. authorization
  - —certificates for identification
  - —certificates for authorization
- Trust
  - —trust in certification activity (identification)
  - —broader trust in certified entities (goodness)
  - —user-centric trust models, managing the models

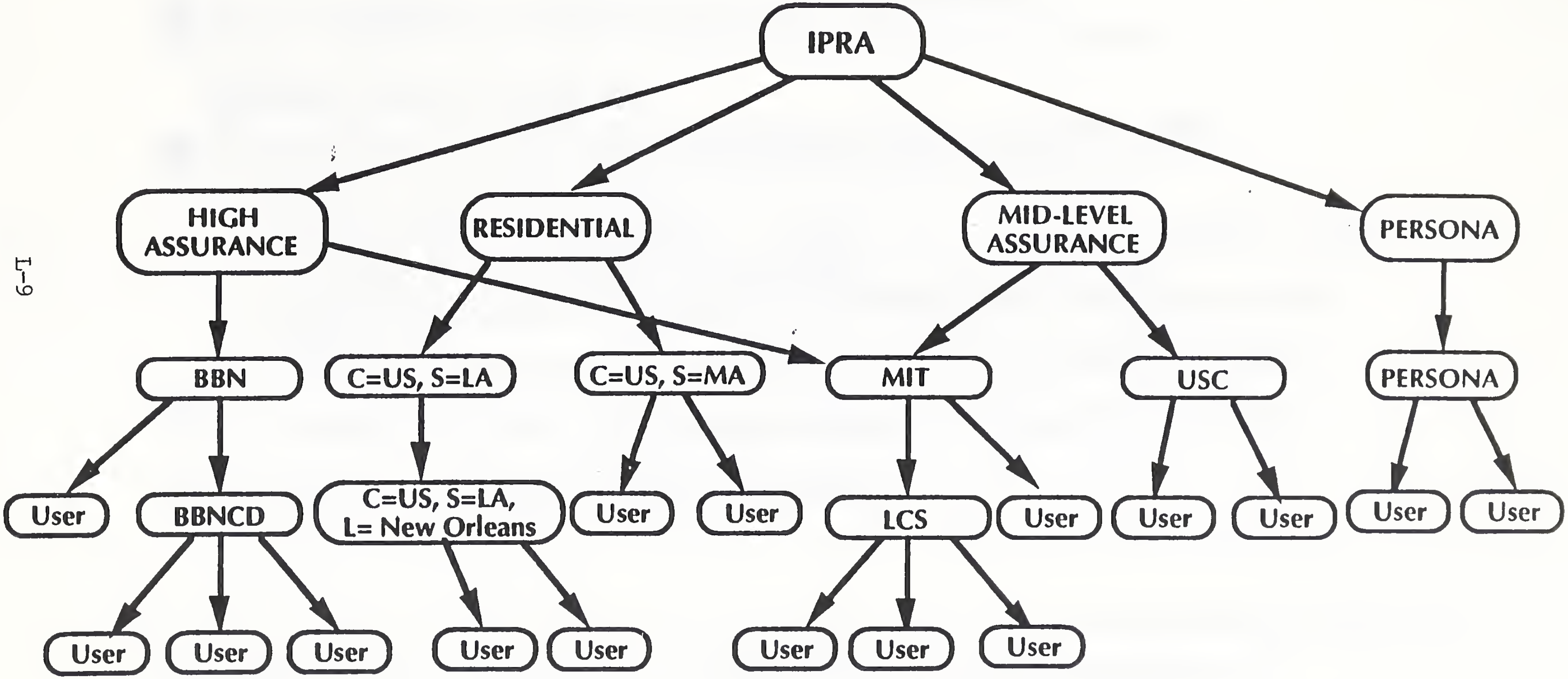
Certificate Revocation

- A certificate is revoked because:
  - —private component is believed compromised
  - —identity binding is no longer valid
- Revoking a certificate does <u>not</u> revoke a key or an identity; it invalidates the binding between the two
- Certificate Revocation Lists (CRLs) provide a means of distributing revoked certificate information via either "push" or "pull"
- Expired certificates need not be listed on CRLs
- Internet format adds "next update" field an simplifies CRL entry format

Internet CRL Format



Internet Certification Hierarchy



Internet Certification Features I

- Three or more level hierarchy
  - —Internet Policy Registration Authority (IPRA) is root
  - —Policy Registration Authorities (PCAs) form 2nd level
  - —Organizational and Residential CAs form 3rd level and may occupy lower levels too
  - —Users start at level 4
- Certification paths parallel name hierarchy starting at level 3
- PCAs define explicit trust semantics
- No cross certification, but a CA may be certified by multiple PCAs

Internet Certification Features II

- CAs (level 3) represent organizations or geographic regions
- Organizational CAs issue certificates to individuals "affiliated" with the organization, e.g., employees, students, professional society members, ...
- Residential CAs issue certificates to users based on geographic "affiliation" without any organizational affiliation, e.g., the postal address of a user's home

Internet Policy Registration Authority

- Single root makes possible provision of "full" certification paths, important for X.500 chained operations and for certificate validation in the absence of ubiquitous directory service
- The IPRA certifies PCAs, ensures that they agree to common certification policy, publishes PCA policies, maintains PCA CRL, ...
- The IPRA co-ordinates unique distinguished name registration across PCAs and co-ordinates access to global CRL database (interim measures)

Common Certification Policy

- PCAs must co-ordinate to avoid duplicate name certification
- Each PCA must publish its policies
- PCAs and CAs must issue CRLs
- CAs may certify entities only if they are name subordinated
- A CA certified by more than one PCA must utilize a different public key in the CA certificate signed by each PCA

Policy Certification Authorities

- The PCA concept accommodates a wide range of certification policies, but permits all users to unambiguously identify the policy under which any certificate is issued
- A PCA may serve users across national boundaries
- More than one PCA may offer the same certification policy, but with different rates, etc.
- Provide access path to global CRL database

PCA Policy Aspects

- Quality of authentication of would-be CAs
- CA security procedures, e.g., CA authentication of users, CA private key management
- Maximum lifetime of certificates issued by a CA
- Frequency of CRL issuance by PCA, CAs
- Archiving of CRLs
- Privacy of ancillary data provided by CAs in support of certification

Three Example PCAs

- High Assurance

  —legally binding organization registration

  —strong user identification practices

  —stringent CRL management

  —CAs use Certificate Signing Units

- Collegial Assurance

  —strong organization registration procedures

  —moderate user identification practices

  —"responsible" CRL management

- PERSONA

  —unique, unauthenticated names

  —focus is on user privac

Persona Certificates

- Persona certificates are issued to users who do not wish to disclose their identities in certificates, but who do want to exploit security technology such as PEM
- These certificates are issued by organizational CAs, consistent with the overall Internet certification hierarchy
- Names are not "authenticated" but are guaranteed to be globally unique
- The policy of a Persona PCA explicitly states the lack of authentication, thus protecting users from being "fooled" by a Persona certificate

Conclusions

- A pure mesh certification topology is inappropriate for large, distributed system
- Hierarchic certification matches common user trust models for identification
- A certification system serving a large community must accommodate a variety of certification policies, including "Persona" policies
- Local cashing of certificates can provide good performance for multi-layer certificate hierarchies
- The Internet certification system is a good model for a global certification system