The following paper was originally published in the
Proceedings of the First USENIX Workshop on Electronic Commerce
New York, New York, July 1995.

Developing and Deploying Corporate Cryptographic Systems

Diane E. Coe and Judith A. Furlong
The MITRE Corporation
Bedford, Massachusetts

For more information about USENIX Association contact:
1. Phone: 510 528-8649
2. FAX: 510 548-5738
3. Email: office@usenix.org
4. WWW URL: http://www.usenix.org

Developing and Deploying Corporate Cryptographic Systems

Diane E. Coe (dec@mitre.org)
Judith A. Furlong (jfurlong@mitre.org)

The MITRE Corporation
202 Burlington Road
Bedford, Massachusetts 01730-1420

The MITRE Corporation has developed a number of cryptographic systems that provide security-related capabilities for its growing electronic information environment. These cryptographic systems were developed using commercial off-the shelf products and widely accepted standards. Standards were adhered to in order to assure interoperability with emerging products such as those used to conduct electronic commerce on the Internet. However, there are many shortcomings within the marketplace and the Internet community that are limiting the extent to which interoperability can be achieved. Products are not as “open” as we need them to be, infrastructures are not in place, and standards are still evolving. This paper presents many of the issues with which we are faced and, in some cases, provides solutions. MITRE's needs are not unique. They are the needs of any enterprise wishing to provide an integrated security solution for the access and exchange of valuable electronic information.

This paper first introduces The MITRE Corporation and describes its corporate cryptographic systems and information infrastructure. The paper then discusses issues associated with integrating MITRE's cryptographic systems with emerging electronic commerce products both for use within the corporation and for conducting electronic commerce externally. The paper concludes with recommendations and lends some insight into where The MITRE Corporation is headed in terms of its corporate cryptographic systems and electronic commerce.

The MITRE Corporation

The MITRE Corporation is a multifaceted engineering organization providing technical and strategic guidance in communications, information, and environmental systems. MITRE's expertise encompasses a broad range of disciplines including computer science, electrical engineering, mathematics, management, and administration. Serving military, government and civilian needs worldwide, MITRE supports a diverse set of national and international clients.

In order to provide for more efficient operations, MITRE is transitioning many of its paper-based business applications to an electronic environment. With this transition comes changes in business practices. Practices which were applied in a paper based environment may no longer be applicable or implementable in an electronic environment. Existing business practices must be examined to determine which practices are still needed in an electronic environment and to identify which practices need to be modified to work in an electronic environment.

One business practice that is needed in both a paper and an electronic environment is an approval capability. In the paper world, approval is usually given through a handwritten signature applied to a document, form, etc. An analogous approval capability is needed in the electronic world. Such an approval capability may be implemented using a cryptographic mechanism called digital signatures.

Digital signatures provide not only an approval capability but also the security services of authentication, integrity, and nonrepudiation. Thus, digital signatures offer more capabilities than its handwritten counterpart, which cannot ensure the integrity of information after it is signed.

A second change that is occurring at MITRE is in the architecture of its information systems. In the past, a few mainframes were used to support all of MITRE's corporate applications. However, new applications are client-server based and, while the mainframes are being phased out, the number of servers in use by the corporation has increased dramatically. Users of these systems, who had a small number of account names and passwords to keep track of in the past, now have more than they can possibly remember. In addition, with more and more valuable information and assets being managed and stored electronically, the need to protect authentication information has taken utmost priority. These changes have caused a revisitation of the authentication mechanisms in use at MITRE.

The following sections describe the digital signature capability that has been developed at MITRE, the key management system that will support the digital signature capability, and the authentication system that is being deployed throughout the corporation.

MITRE's Digital Signature Environment

Digital signatures are being implemented at MITRE to decrease both the amount of time and the amount of money spent on processing and archiving paper forms. The first corporate application that will provide a digital signature capability is an application known as Data Capture. The Data Capture initiative comprises a set of electronic forms called transactions, a digital signature capability, and a work flow system. With Data Capture, forms are generated, signed, and routed for approval electronically. Information is captured in a central database when it is first created. Rekeying of data is eliminated and data is reusable, thus eliminating the need to type the same information over and over. Data Capture significantly reduces typographical errors, both by virtue of the fact that rekeying is eliminated and because validity checks are automatically performed on the electronic data.

Data Capture is a client-server application. It is written in C++ and accesses a relational (SQL-based) database. Data Capture clients run on both Macintosh and Windows 3.1 platforms and will run on additional platforms in the future. The server and database reside on a UNIX platform.

Using a commercially available toolkit from RSA Data Security Incorporated called BSAFE, MITRE developed two digital signature application programming interfaces (APIs) that are called by the Data Capture application. One API performs a signing function, and the other performs a signature verification function. These APIs are written in ANSI C and easily port from platform to platform. They can be called by Data Capture or by any forms package or development environment that provides a C interface.

Before an employee can digitally sign a Data Capture transaction, the employee must obtain a public-private key pair. With RSA public key cryptography, the keys in the pair are mathematically related in such a way that what is encrypted by one key can be decrypted by the other and vice versa. Yet, the private key cannot be easily derived from knowledge of the public key. Together, these two attributes are what allow the technology to be used for digitally signing information. When the user obtains his key pair, he keeps his private key private and uses it to encrypt information, thus applying his “signature" to it. He makes the public portion of the key pair publicly available so that anyone can retrieve it and decrypt the information he has encrypted. If the recipient of the signed information can successfully decrypt the information using the signer's public key, he is assured that the information was, in fact, signed (i.e., encrypted) with the signer's private key. If the signer has not divulged his private key to anyone, he is the only one who could have produced that signature. The key management system that supports MITRE's digital signature capability is described in the following section.

Once a user has a key pair, he is ready to sign. With the Data Capture application, all data appearing on a form is signed by the employee. This does not have to be the case and, in the future, will not be. In subsequent versions of Data Capture, only certain data fields appearing on the form will be signed by employees acting in particular roles. As an example, on a Purchase Requisition, an employee's manager may sign only fields that describe the items being purchased, thus signifying approval of the items, while someone in the budget office may sign the Project Number and Total Cost fields, thus signifying that the identified project can support a purchase of that amount.

Because encryption using public key technology is relatively slow, the data to be signed is first sent through a hashing function. This function reduces the data to a 128 bit "fingerprint" of the information, regardless of the amount of data to be signed. The hashing algorithm is strong enough to detect even a single bit change of the data—that is, if any bit of the data is changed, a different hash value will result. It is this 128 bit hash value that actually gets signed, or encrypted, using the employee's private key. The encrypted hash is the employee's signature on the data. The hashing of the data provides integrity (i.e., any change of the data will be detected) while the signature provides authenticity and nonrepudiation. The signature is stored in the database with the data with which it is associated.

MITRE's Key Management System (MKMS)

In order to support digital signatures, a key management system is needed. MITRE's key management system (MKMS) plays a pivotal role in the generation, distribution, and management of the cryptographic keys that each MITRE employee needs to utilize the digital signature capability. The MKMS also provides protection of these cryptographic keys. The confidentiality of the private keys is provided through encryption. Digital signatures on public key certificates, which bind users' identities with their public keys, assure that the integrity of the public key contained within the certificate is maintained.

At MITRE, employees obtain their key pairs from centrally-located Key Generator systems. There are multiple Key Generator systems to service all of MITRE's sites. The Key Generator systems are operated by Corporate Security representatives. Each employee presents himself to the representative who authenticates the employee and directs him or her to run a simple key generator program. This program first prompts the employee for his or her employee id. The employee id is used to obtain the employee's distinguished name from MITRE's X.500 directory. The distinguished name is later used in generating a certification request. Once the name is obtained and the employee confirms it is correct, the employee is then prompted for a password. The employee chosen password is used to encrypt the employee's private key before it is stored on a floppy disk. The floppy disk is readable by both the Windows and Macintosh versions of Data Capture. (An effort is underway to transition from a floppy disk medium to a multipurpose smart card. This effort is discussed in the following section.)

The key generator application then creates a certification request adhering to Public Key Cryptography Standard (PKCS) #10, Certification Request Syntax Standard The certification request is signed by the Corporate Security representative to attest to the employee's identity. The signed certification request is sent to MITRE's Certification Authority (CA) for processing via a server program. The key generator program does not maintain a copy of employees' passwords nor private keys.

There are several reasons why a centralized key generation scheme was implemented. While the key generator application could be made available to individual employees, each employee would still need to present themselves to Corporate Security before their public key certificate is generated. (Corporate Security is responsible for attesting to the employee's identity and ensuring that the certificate request contains that employee's distinguished name.) In addition, the logistics involved in maintaining a few instantiations of the key generator program and its external interfaces (e.g., an X.500 interface is required to retrieve employees' distinguished names) seemed much simpler than maintaining a corporate-wide disbursement of the program. In time, the software may be rearchitected and given to end users.

As stated previously, private keys are on floppy disks. Employees are advised to protect the disk as they would other important personal information and are discouraged from recording their password or storing their keys on unprotected Macintosh or PC machines. The disks are a distinctive color so they are easily distinguishable from other disks. Floppy disks are considered an interim solution that provide a low-cost, platform-independent capability. Employees can take their disks with them and can sign from their home computers or while traveling. Because the signatures being applied in the initial versions of Data Capture are not critical, in that they cannot obligate significant sums of money or provide access to highly sensitive data, this interim capability is considered acceptable. The transition from a floppy medium to a smartcard will provide enhanced protection for the private keys in the future.

Public keys are sent to MITRE's CA in PKCS #10 format to be put into signed certificates. Certificates bind an employee's identity with his public key. The certificate contains identifying information about the employee and his or her public key. The binding takes place when a trusted entity (i.e., the CA) signs the certificate. Just like any other information that has been signed, the signature on the certificate can be verified using the signer's (i.e., the CA's) public key. Every employee has a copy of the CA's public key. Use of signed certificates guards against masquerading.

Once a public key certificate is generated, there must be a mechanism for revoking the certificate should the affiliated private key be lost or compromised. For the initial implementation at MITRE, the CA operator is notified by a corporate security representative when a certificate needs to be revoked. The CA operator uses a function within the CA system to indicate that the certificate has been revoked.

A question that needed to be resolved was how will the certificates and the CRLs be made available to individuals and applications that need to access them? Initially, it was envisioned that all certificates and CRLs would be stored in the corporate X.500 directory server. X.500 provides an easily-accessible storage location for employee information. There are, however, drawbacks to using an X.500 directory in a corporate environment.

At MITRE, digital signatures applied to corporate information may need to be verified relatively soon after they have been applied or they may need to be verified days, months, or even years later. In the X.500 directory, certificates are stored in a "last in, first out" order within a user's X.500 entry and are not individually addressable. If a user has multiple certificates (e.g., a current certificate and some number of expired and/or revoked certificates), a query against that user's entry in the X.500 directory will return all of the user's certificates. The application would then need to parse through each of the certificates to find the certificate that was valid at the time the signature was applied. Once the appropriate certificate is found, a check needs to be made to ensure that the certificate was not revoked prior to the time the signature was applied. To do this, the application must first extract the serial number from the retrieved certificate. It then performs another query against the X.500 directory. This second query is against the certification authority's (CA's) entry in the directory and retrieves the certificate revocation list (CRL). If the CA's entry contains multiple revocation lists, the application must parse through the retrieved CRLs and find the first list that was produced after the signature in question was applied. The application then searches through the CRL to determine if it contains the serial number of the retrieved user's certificate. If it does, the date of revocation is checked; and if the revocation date is prior to the signature date, the signature is considered invalid. If the revocation date is later than the signature date or if the certificate is not on the CRL, the certificate is valid. This is quite a bit of processing to be performed every time a signature needs to be verified.

To reduce the amount of processing that has to be performed to verify a signature, a decision was made to store certificates in MITRE's data warehouse which is managed by a relational database management system (DBMS). The tables containing the certificate information can be read by corporate applications but updates to the tables are controlled by a secured maintenance account. When a certificate is created by the CA system, it is sent to a server program known as the KG/CA server. This server stores the certificate in the data warehouse, indexed by the employee's unique employee number. The validity dates of the certificate are stored as individual fields in the table, as well, so that queries can be performed against them. CRLs are also sent to the KG/CA server. The server parses the CRL and updates the records in the certificate table to indicate the date a certificate has been revoked. This simplifies the signature verification process significantly in that now a single query can be used to determine whether or not a valid certificate exists. Certificates and CRLs will continue to be stored in the X.500 directory, but only the user's current certificate and the current CRL will be stored. It is envisioned that the X.500 directory will be used in the future for sending and verifying secure messages and for communicating securely with external entities.

Distributed Authentication

MITRE's rearchitecting of its information systems has caused an increase in the number of corporate servers and, thus, the number of accounts each user has. Passwords are currently the common method of user authentication to MITRE's servers. Typically, a user must supply a login identifier and a password to gain authorized access to a particular computer system or host. In most cases, passwords are user selectable, although restrictions apply. User-selected passwords are often easy to remember which renders them easy to guess. In practice, assigned passwords are usually difficult to remember and are often written down, making these passwords vulnerable to unauthorized disclosure. To avoid having to remember multiple passwords for different systems, users often use the same password on every system to which they have authorized access. Thus, multiple systems are at risk under a single or common attack. The high volume of abuse regarding the selection of user passwords combined with the failure to administer user password protection successfully has resulted in the high demand for unitary authentication in MITRE's distributed computing environment.

MITRE has an effort underway to deploy a distributed authentication system based on Version 5 of Kerberos. Kerberos is a trusted third-party unified network authentication service. It is designed to operate in a client/server environment. In a "kerberized" environment, users are known as principals. A list of authorized users, or principals, is maintained in the Kerberos principal database. Once a user is known to the principal database, he or she can get what's known as a Ticket Granting Ticket (TGT) from the Kerberos Key Distribution Center (KDC). A TGT is a credential that will allow the user to obtain other credentials, or tickets, for kerberized services within the user's Kerberos environment. The user's environment is called his realm. A realm consists of all the users, services, and hosts listed in the Kerberos principal database.

To get a TGT, the user provides his user or principal name to the KDC. The KDC then sends the user a TGT, but portions of the TGT are encrypted in a password known only to the user and the KDC. The user enters his password and decrypts the TGT rendering it usable. This is the only time that the user must provide authentication information. All subsequent authentication within the Kerberos environment is performed by Kerberos on behalf of the user. This provides a unitary authentication capability. Note too, that because decryption of the TGT is performed at the user's workstation, his or her password never traverses the network.

Once a user has a TGT, he can present the TGT to the KDC and receive tickets for kerberized services. The product MITRE is investigating for widespread deployment provides a number of kerberized services, including a kerberized login, which allows users to remotely log in to UNIX hosts; rsh, which allows users to execute a command on a UNIX host; and rcp, which allows users to copy files to and from UNIX hosts. In a nonkerberized environment, each time a user wishes to access one of these services, he has to authenticate himself to the service or host. With Kerberos, tickets are used for authentication and are passed on behalf of the user to the service or host. No other authentication is required.

Some of the biggest proponents of distributed authentication are system and database administrators (DBAs). At MITRE, DBAs administer databases residing on as many as six different machines. In order to perform administration and testing, the DBAs often log into the systems in different roles, thereby obtaining different privilege sets. Given that there are approximately four roles that a DBA may assume on each of the six machines hosting database management systems, there is a potential twenty four account names and passwords that a DBA must remember. Kerberos reduces this number to one.

MITRE is currently evaluating Kerberos for potential deployment throughout the corporation with DBAs being the first set of users. The prototype environment currently consists of Macintosh, PC, and UNIX Kerberos clients and a KDC and principal database residing on a SunOS machine. Kerberized services are resident on SunOS, Solaris, and AIX machines and are currently being installed on a Sequent machine. This prototype environment mirrors the corporate environment and will be used as a testbed until the production system is deployed.

Integrated System

As described in the previous sections, MITRE is actively pursuing the integration of security services into MITRE applications. Capabilities presently being examined are digital signatures and distributed authentication. Future capabilities may include secure mail and data encryption. The implementations of these capabilities require that MITRE users possess certain credentials or information. In the case of authentication, MITRE users need authentication credentials such as Kerberos tickets; while in the case of digital signatures, users need public/private key pairs. Each of these security capabilities are being independently developed, and each require some amount of support information. The goal of the MITRE single token task is to consolidate the support information for all the security services on a single token. In some instances, the actual security service may be performed on the token. In other instances, the token will provide secure storage for the information. MITRE's single token will be an ISO smartcard.

A number of capabilities will ultimately be supported by the single token. The token will support MITRE's digital signature capability by providing a more secure storage media for private keys. Data will be sent to the card to be signed so the private key will never be vulnerable in the workstation. MITRE's digital signature APIs have already been modified to access the ISO smartcard, and a prototype smartcard-based signature capability has been developed.

The Kerberos-based distributed authentication capability is being incrementally integrated into the MITRE environment. The integration of the Kerberos authentication protocol at MITRE is the first step towards achieving a single sign-on capability. MITRE is working with its Kerberos vendor to develop a smartcard interface for the Kerberos product.

Kerberos is not a complete solution for achieving single sign-on. Kerberos currently provides single sign-on for only some UNIX servers. A full single sign-on capability cannot be achieved until a means for handling the passwords associated with nonUNIX systems is implemented. Toolkits for developing scripts are being investigated as a means for storing passwords on the smartcard, thus moving us closer to our goal of a truly single sign on capability. The token can support the single sign-on capability by storing various types of authentication credentials so the user will not be required to memorize and supply authentication information each time he wishes to connect to a MITRE system.

In a fully-automated corporate environment, restricted information must be electronically accessible by authorized users. In order to support this capability, MITRE must add encryption to its environment. With encryption, restricted information such as salary information or personnel information can be kept confidential while it is transferred to computers throughout the corporation. The token can support an encryption capability by providing secure storage for the keys used in the encryption process. It is also possible that the token could perform some of the necessary encryption functions.

MITRE presently uses a challenge-response mechanism to provide access across its firewall. It is hoped that the single token system can also replace this mechanism.

Another important use of the token will be for facility access. Currently, a badge is needed to allow MITRE employees access to MITRE facilities and restricted areas within such facilities. To reduce the number of tokens required by MITRE employees to conduct their daily business to one, the MITRE badges will be replaced by the ISO smartcard. Replacement of badges will also provide some assurance that employees won't leave their smartcards in unattended systems since they must have their badge on their person at all times.

MITRE Information Infrastructure

While the aforementioned systems are being developed by MITRE's Information Security Division, the Information Systems Division is developing MITRE's Information Infrastructure (MII). The MII is an electronic information system based on World Wide Web technology and will be the primary source of information at MITRE. At the present time, no restricted information is posted on the MII. All information residing on the internal Web servers is accessible to all MITRE employees, and all information residing on MITRE's external server is publicly releasable. In order to post information having dissemination restrictions on these systems, security in the form of access control and authentication is required. This security is necessary to protect the corporation's valuable information assets from unauthorized disclosure and to protect the privacy of employee-related data.

Integration of the MII with Corporate Cryptographic Systems

MITRE began investigating secure Web products in February of this year to determine whether or not they could provide the security MITRE needs. The ideal product would meet the MII's security requirements by using one of the cryptographic systems already in place or in development. Products were assessed to determine the extent to which the products could be integrated with MITRE's public key infrastructure or its Kerberos environment. Most of the products found were public key-based and implemented either the Secure HyperText Transfer Protocol (S-HTTP) or the Secure Socket Layer (SSL) protocol. One Kerberos-based product was also found. Given the number of security-enhanced products that existed, our assessment began on an optimistic note.

The optimism quickly faded. It turned out that although S-HTTP servers existed, the protocol was not supported in any of the commercially-available browsers. The SSL protocol had both browser and server implementations, but the products could not be integrated with our existing public key infrastructure. The public and private key pair of the SSL server must be generated by software embedded within the server. Key pairs generated by MITRE's Key Generator system could not be used, nor could a certificate signed by MITRE's certification authority because the products only recognize certificates issued by a small set of CAs and the certificates associated with those CAs are embedded in the client software. This means that although MITRE is purchasing thousands of certificates to support its digital signature capability, it could not use any of these certificates for its Web servers.

There were other limitations found in the investigated products that hampered integration with MITRE's public key infrastructure. Systems supporting public key technology had the private key of the server encrypted in software and stored on the server. There was no flexibility to store the private key on an external storage device such as an ISO smartcard or even a floppy disk as is done at MITRE.

Client authentication and access control in the Web products was also a problem in terms of providing a capability consistent with MITRE's goals. Because there were no products supporting public key-based authentication for clients (only for servers), authentication is performed using passwords. MITRE is trying hard to eliminate the number of passwords users have to remember. Implementation of password-based authentication in our Web server is contrary to our single sign-on goal.

The Kerberos product proved promising from an integration perspective, but it also had its shortcomings. On an optimistic note, we were delighted to find that the Web application, which implements Version 4 of Kerberos, could, in fact, obtain tickets from our Version 5 Kerberos server. However, the client we tested stored the retrieved tickets in a nonconfigurable location, thus we were not able to use the same credential cache for both applications. This necessitates logging on to our Kerberos server twice; once to get a Ticket Granting-Ticket (TGT) that can be used to obtain a ticket for our Web server, and once to get a TGT to get tickets for all our other applications. So the integration of the kerberized Web product with our Kerberos environment wasn't fully successful, but it came much closer than the public key-based products.

External Use of Corporate Cryptographic Systems

It has always been a goal within MITRE to develop cryptographic systems that are expandable to allow for secure external communications, as well as to provide security within the corporation. Our cryptographic systems are based on standard technologies and protocols. We have public key certificates that follow the X.509 standard; we are storing our certificates in an X.500 directory server; our digital signatures are created using the MD5 hashing function and the RSA algorithm; our distributed authentication system is a standard V5 Kerberos implementation; and our token is an ISO smartcard. We have followed all the guidelines, implemented all the standards, and developed open systems, all in an effort to ensure interoperability with the rest of the world; and with whom have we achieved interoperability with respect to our cryptographic systems? That remains to be seen.

Probably the biggest shortfall in the community today, the one area most hampering the widespread use of public key technology, is the lack of a ubiquitous public key infrastructure. Public key cryptography is less than two decades old. Infrastructures to manage public keys and certificates in large environments have only recently been developed and are just now being implemented. Not all the issues associated with public key and certificate management have been resolved. Competing approaches to public key management along with the need to support different public key algorithms have resulted in several different public key infrastructures being in existence today. The Internet (PEM) Key Infrastructure, the NIST Public Key Infrastructure, and the MISSI Infrastructure are three of these infrastructures. It is unclear whether a single public key infrastructure that services the needs of all communities will exist in the future. Because of this, organizations are developing their own custom hierarchies, and trust among hierarchies does not exist. Certificates generated within one environment cannot be authenticated by a recipient in another environment because the environments do not have a mutually trusted CA. Certificates generated by MITRE are not going to be accepted by Visa or Mastercard or by any of the many companies now conducting electronic commerce on the Internet. Each will either issue a certificate signed by its own CA or develop its own method for providing authentication and nonrepudiation services. One method currently being used is a call-back mechanism. Users placing orders are sent confirmation requests to their registered electronic address. Orders are not filled until the confirmation is received. This prevents anyone except those having access to the user's electronic mailbox from masquerading as the registered user. Ad hoc trading is not being supported. The only trading that is occurring is between parties having preestablished relationships.

Even in the world of EDI, bilateral trading agreements are negotiated out of band and in advance of any EDI orders being accepted. Currently, there is little security within EDI transactions. Rather than securing the transaction, threats are being dealt with by mutually-accepted policies established in trading partner agreements or by the systems processing the transactions. The threat of receiving orders from someone masquerading as an authorized trading partner is being mitigated by the implementation of rules at the receiving system that detect and flag anomalous orders. We have yet to find a company among the fifty thousand currently conducting business using EDI that uses digital signature in its EDI transactions. Products exist to support digital signatures in EDI, but is anyone using them? It does not seem possible with the ubiquitous hierarchy.

Systems supporting Kerberos are also emerging in the world of electronic commerce. Can we authenticate ourselves to these systems using our Kerberos credentials? No. Kerberos credentials are only recognized within the realm in which they were issued. Inter-realm authentication does not quite yet exist in the community.

Conclusion

In spite of it all, we are still pretty excited about the cryptographic efforts ongoing at The MITRE Corporation. We have learned a lot of valuable lessons and have gained insight and experience in many different areas. We have made great strides in working towards our goal of a paperless environment and are providing enhanced security in our electronic systems as well. In the end, we believe we will have a more efficient and more secure workplace and lower operational costs. However, we have some recommendations that will help, not only us, but also companies and agencies, both government and civilian, with similar goals and desires of which we believe there are many.

Products need to be more open. They should allow for the use of keys generated external to the product's environments. Flexibility should be provided to allow private keys, in particular, to be stored on an external storage device such as an ISO smartcard or even a floppy disk.

Certification authorities, key lengths, and algorithms should not be hardcoded into the products. RSA is not the only public key algorithm in existence today which may be used for digital signature and key exchange. Other digital signature and key exchange algorithms include the Digital Signature Algorithm (DSA) specified in FIPS 186 - Digital Signature Standard and the Key Exchange Algorithm (KEA) implemented on the FORTEZZA crypto card. In order to be used in a larger number of environments, the products should provide support for a wider range of public key algorithms, thus allowing users within specific environments to choose the algorithms that they will use. It should be noted that the RSA algorithm is unique in that it may be used for both digital signature and encryption/key exchange purposes. Other public key algorithms may only be used for one of these applications.

Strong client authentication needs to be supported. Current implementations of the SSL and S-HTTP protocols are focused on transmission security. Only servers have public-private key pairs and certificates. The impetus behind this seems to be a driving push to get credit cards across the Internet safely. This may be a worthy goal; however, it must be understood that if these products are to support all types of electronic commerce which includes the interchange of ideas, opinions, or sentiments as well as the buying/selling of commodities, support for client keys and certificates is needed. Given that the Internet has been used more for the former than it has for the latter, it seems that security solutions providing protection for ideas or information would be at least as sought after as those that provide security for the transmission of credit card numbers.

Products should include an interface to an X.500 Directory. In many public key management approaches, certificates are stored in an X.500 Directory, which is a publicly-accessible place for storing information. Directory servers play a pivotal role in any large scale public key infrastructure where key material must be disseminated to large numbers of people and applications operating in various geographic locations.

Certificate revocation needs to be supported. When client certificates are supported, servers will need to know that the clients to which they are speaking are genuine clients and not a masquerading client. Adding support for certificate revocation means that the products will need to support Certificate Revocation Lists (CRLs), be able to retrieve CRLs and/or receive CRLs, and to process the information contained within them. CRLs are often stored in an X.500 Directory, providing another motivation for adding an X.500 Directory interface to the products so that CRLs may be retrieved from the Directory.

And, of course, more work needs to be done in the community to solve the issues associated with public key and certificate management. Competing approaches to public key management along with the need to support different public key algorithms have resulted in several different public key infrastructures being in existence today. It is unclear whether a single public key infrastructure that services the needs of all communities will exist in the future. If not, interoperability issues between different infrastructures will need to be resolved in the future.

Where do we go from here?

MITRE plans to continue with its cryptographic endeavors and its quest to integrate electronic commerce products with its security infrastructures. We believe this is an achievable goal. In the last few months, we have seen much more emphasis in the community on providing the services we need. Services such as strong client authentication, support for CRLs, and interfaces to external systems are receiving much more attention of late.

MITRE participates as a member of many standards' bodies and is actively involved in the World Wide Web Consortium (W3C). We also actively participate in the W3C security workshops. In addition, MITRE is hosting a Public Key Infrastructure (PKI) Invitational Workshop along with The National Institute of Standards and Technology (NIST) and the NII Security Infrastructure Program Management Office (SI-PMO) in September 1995 to resolve PKI interoperability technical issues. We are working with both vendors and customers to ensure that our needs and theirs are well understood within the community. We hope that these efforts, as well as the efforts of the so many others that have similar goals and desires, will create a truly open and interoperable world for electronic commerce.

Bibliography

Berkovits, Dr. S., Dr. S. Chokhani, J. A. Furlong, J. A. Geiter, and J. C. Guild, April 1994, Public Key Infrastructure Study Final Report, MTR 94W0000180, The MITRE Corporation, McLean, VA.

CCITT, Geneva, 1989, Data Communication Networks: Directory, Recommendation X.500 - X.521, Blue Book, Volume VIII–Fascicle VIII.8.

Federal Information Processing Standards Publication, Digital Signature Standard (DSS), 19 May 1994, FIPS PUB 186, U. S. Department of Commerce/National Institute of Standards and Technology, Gaithersburg, MD.

Federal Information Processing Standards Publication, Secure Hash Standard (SHS), 31 May 1994, FIPS PUB 180-1, U. S. Department of Commerce/National Institute of Standards and Technology, Gaithersburg, MD.

Heckman, Donald, 18 August 1993, MOSAIC Key Management Concept, Revision 2.4, National Security Agency, Ft. Meade, MD.

Hickman, K., and T. ElGamal, June 1995, The SSL Protocol, Internet Draft, IAB.

Kaliski, B., 3 June 1993, An Overview of the PKCS Standards, RSA Data Security, Inc.

Kent, S., February 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate Based Key Management, RFC 1422, IAB IRTF PSRG, IETF PEM WG.

Kohl, J., The Kerberos Network Authentication Service (V5), September 1993, RFC 1510, IAB IETF Network Working Group.

Public Key Cryptographic Standard (PKCS) #10: Certification Request Syntax Standard, 1 November 1995, Version 1.0, RSA Laboratories.

Rescorla, E., and A. Schiffman, December 1994, The Secure HyperText Transfer Protocol, Internet Draft, IAB.

Rescorla, E., and A. Schiffman, July 1995, The Secure HyperText Transfer Protocol, Internet Draft, IAB IETF Web Transaction Security Working Group.

Rivest, R. L., A. Shamir, and L. Adleman, February 1978, "On Digital Signatures and Public Key Cryptosystems," Communication of the ACM, Vol. 21, No. 2, pp. 120-126.

Rivest, R., April 1992, The MD5 Message-Digest Algorithm, RFC 1321, IAB IETF Network Working Group.

Steiner, J., C. Neuman, and J. Schiller, 1988, Kerberos: An Authentication Service for Open Network Systems, Paper presented at USENIX, Dallas, Texas.