SecureWay Technologies

Peter H. Callaway
Dept. MH6A, Theresa Doyle, I/T Security Marketing Programs

May 1998

1. Introduction . . . 3
2. Cryptography . . . 4
2.1. Introduction . . . 4
2.1.1. Secret or symmetric key encryption/decryption . . . 4
2.1.2. Public key encryption . . . 4
2.1.3. Hashing . . . 5
2.1.4. Digital signatures . . . 5
2.1.5. Key management . . . 5
2.1.6. Random number generation. . . . 6
2.2. Product Support . . . 6
2.2.1. Hardware Products . . . 6
2.2.2. Software Based cryptography . . . 7
2.3. Standards . . . 7
2.4. APIs . . . 7
3. Electronic Commerce - Public Key Infrastructure (PKI) . . . 8
3.1. Digital Certificate (X.509) Management . . . 8
3.1.1. Introduction . . . 8
3.1.2. Product Support . . . 9
3.1.3. Standards . . . 9
3.1.4. APIs . . . 9
3.2. Common Data Security Architecture (CDSA) . . . 9
3.2.1. Description . . . 9
3.2.2. Product Support . . . 10
3.2.3. Standards . . . 11
3.2.4. APIs . . . 11
3.3. Key Recovery . . . 11
3.3.1. Introduction . . . 11
3.3.2. Product Support . . . 12
3.3.2.1 The IBM Key Recovery Service Provider (KRSP) . . . 12
3.3.2.2 The IBM Key Recovery Server (KRS) . . . 13
3.3.3. Standards . . . 13
3.3.4. APIs and Protocols . . . 13
4. Electronic Commerce - Exploiters . . . 15
4.1. Vault Deposit Services . . . 15
4.1.1. Introduction . . . 15
4.1.2. Product Support . . . 15
4.2. Secure Electronic Transactions (SET) . . . 15

4.2.1. Introduction . . . 15
4.2.2. Product Support . . . 16
4.2.2.1 IBM Registry for SET . . . 16
4.2.2.2 IBM CommercePOINT . . . 16
4.2.3. Standards . . . 16
4.3. Cryptolope Containers . . . 17
4.3.1. Introduction . . . 17

5. Secure Networks . . . 18
5.1. Secure Sockets Layer Protocol . . . 18
5.1.1. Introduction . . . 18
5.1.2. Product Support . . . 18
5.1.3. Standards . . . 18
5.2. Virtual Private Networks and IPSEC . . . 19
5.2.1. Introduction to VPNs . . . 19
5.2.2. Introduction to IPSEC . . . 19
5.2.3. Product Support . . . 20
5.2.4. Standards . . . 20
5.2.5. APIs . . . 20
5.3. Firewalls . . . 20
5.3.1. Introduction . . . 20
5.3.2. Products Supported . . . 21
5.3.3. Standards . . . 21

6. Single Sign-On . . . 23
6.1. Introduction . . . 23
6.2. Product Support . . . 23
6.3. Standards . . . 24

7. DCE Security Services . . . 25
7.1. Introduction . . . 25
7.2. Product Support . . . 25
7.3. Standards Support . . . 26
7.4. APIs . . . 26

8. Smart cards . . . 27
8.1. Introduction . . . 27
8.2. Product Support . . . 27
8.3. Standards . . . 27
8.4. APIs . . . 28

9. Antivirus and Immune System Technology . . . 29
9.1. Introduction . . . 29
4.2. Product Support . . . 29

1. Introduction

IBM is a technology company backed by worldwide research and development resources. IBM's research laboratories have created industry-leading technologies over the last four decades. Noteworthy examples are DES, the Data Encryption Standard, used throughout the world; HMAC, an advanced message authentication hashing algorithm; technologies that support new antivirus immune systems, and Cryptolopes Technologies. IBM research also contributed significant technology to SET, the international standard for secure use of credit cards over the Internet.

IBM also participates in and contributes heavily to the work of standards consortia, alliances, and formal national and international standards organizations. Where appropriate, IBM will adopt consensus technologies in order to maintain openness, interoperability, and application portability. Examples are DCE (including GSS-API), CDSA, and the PAM component of IBM Global Sign-On.

2. Cryptography

2.1. Introduction

IBM has been a leader in Information Systems cryptography technology for several decades starting with the invention by IBM Research of the Data Encryption Standard (DES) in the 60's and its subsequent publication for worldwide use. Over subsequent years, IBM has continued to add a large suite of cryptographic algorithms to its product offerings. Today there is a comprehensive set of hardware and software products to support the ever expanding needs of public and secret (symmetric) key-based cryptography. These products are needed for applications used in the world of electronic commerce using public and private, untrusted and trusted networks such as extranets, intranets, and the Internet. Cryptographic algorithms provide a wide range of services essential to the conduct of secure business:

2.1.1. Secret or symmetric key encryption/decryption

This technology is used for the privacy/confidentiality of bulk stored or transmitted information and for a number of cryptography related functions.

The name derives from the fact that the same key is used to encrypt and decrypt the data. Therefore the privacy of the encrypted data can only be assured if the shared key is kept secret. This calls for careful key management when the algorithm is used for encrypting information in publicly accessible networks or systems.

In response to a 1970 request by the National Bureau of Standards for a standard cryptographic algorithm, IBM supplied an algorithm that eventually became known as the data Encryption Standard (DES).

The advantage of this algorithm is its relatively short keys and high speed. Consequently it is the algorithm of choice for bulk data encryption. The disadvantage is that the distribution of the secret keys to the communicants must be managed with absolute security..

Symmetric key algorithms are also used to provide secret key-based message authentication codes (MAC) that can validate that the message originated with the creator of the MAC and has not been altered. They are also used widely for PIN processing for financial applications, such as ATM transactions, and are used to distribute other symmetric keys.

2.1.2. Public key encryption

Public key encryption is used for encryption/decryption of communications with a common recipient whose certified encryption key is available from a public registry. Because of the algorithm's relatively large keys and slow speed, its use is generally limited to the encryption of small amounts of data such as symmetric keys for distribution and for digitial signature creation and verification (see next two subheadings).

This algorithm involves the use of a public/private pair of keys and it solves the problem associated with symmetric key key distribution. The algorithm is such that information can be encrypted by anyone with access to the publicly available key of the recipient, but the information can only be decrypted by the private key of the recipient. The private key is stored in a highly secure location known only to the recipient, for example his or her Smart Card. Thus if you possess a public/private key pair, you can publish your public key and anyone can use it to securely send you encrypted information that only you can decrypt. Conversely, if you encrypt information you transmit with your private key, it can only be decrypted by users who have gained access to your public key. Because of the way that public keys are stored and distributed, this proves that the information could only have come from you: in effect the encrypted data is electronically signed by you, and you cannot deny that you sent it. This facilitates the concept of electronic non-repudiation of transmissions.

RSA Data Security Inc. licenses the de facto standard public key algorithms most widely used today.

2.1.3. Hashing

Hashing, or the creation of message digests to ensure the integrity of information communication, is commonly used as a part of digital signature schemes.

Hashing algorithms take a message of any length and, using a one-way hash function (you cannot recreate the message from the result), compute a unique “message digest” of a constant length. This process will always yield the same result from identical data, but it is extremely unlikely that two different messages could produce the same result. The message digest can then be encrypted using the originator’s private key and sent with the message. The recipient can then compute the message digest of the received message using the identical hash function, decrypt the message digest sent with the message, using the originator’s public key, and compare the results. If one bit of information has been changed during transmission, the two digests will differ, and the recipient knows that the integrity of the message is suspect and should be discarded. Thus originally, the primary use of hashing was to ensure the integrity of transmitted information. However the encryption of the message digest using the originator’s private key amounts to a “digital signature,” because only the originator has that private key and only he/she could be the sender. This is stronger evidence of the authenticity of information than a hand-written signature that could be easily forged. See the next subheading for more details.

Several hashing algorithms are in widespread use, namely MD2 and MD5 from RSA Data Security Inc. and SHA-1 (the US National Standard) from the National Institute of Standards and Technology (NIST). More recently IBM has introduced higher levels of security in hashing by combining multiple passes of the hashing algorithm while appending secret text to the keys. This process is known as HMAC and it is being processed for standardization within the American National Standards Institute (ANSI).

2.1.4. Digital signatures

Digital signatures are used for mutual authentication of communicants and to make it impossible for the communicants to deny participation in completed transmissions. The latter is commonly known as non-repudiation).

As described under the previous subheading, the ability to create “digital signatures” is a direct consequence of the ability to create message digests. Thus a digital signature is a logical hash (mathematical summary) of information enciphered using an asymmetric key unique to the signer. A digital signature has properties that can help one accurately identify the creator of the hash and determine whether the original information or hash was tampered with. A digital signature cannot be copied from one message and applied to another because the summary, or "hash," would not match. Any alterations to the message after it is signed would also invalidate the signature. Thus with these properties, a digital signature can provide a greater level of security than a physical signature.

The three step process of decrypting the transmitted HASH (the signature) using the originator’s public key, comparing the result with a copy of the HASH that the recipient has computed on the transmitted message, and getting an exact match, is known as signature verification! Signature verification has obvious legal ramifications with regard to non-repudiation of message origin, transmisssion and receipt.

2.1.5. Key management

Since the success of secret key encryption depends upon the encryption keys being kept secure from all others besides the communicants, for such encryption to be usable and useful, support must be provided for the generation of unique keys, their storage, distribution, retirement, replacement, and secure retrieval. In particular, secure symmetric key management mandates a strong policy of hardware-enforced key separation. This is a high priority requirement for financial institutions doing financial transactions around the world.

For public key cryptography, the user's private key must be subject to the same considerations as secret keys, except that it does not have to be distributed. However the public key (of the private/public pair) must be stored in a publicly accessible repository and must be associated with a verifiable identity (a certificate) of the user. Such repositories may be known as registries and could be implemented in the form of an X.500 directory. This level of key management is not something that is provided by encryption algorithms; rather it lies in the domain of Public Key Infrastructures, which are discussed later in this paper.(LINK)

2.1.6. Random number generation.

The generation of encryption keys and hash function keys (see HMAC above, under subheading 2.1.3), involves the introduction of unpredictably random numbers. This makes the process of guessing keys that much more difficult. The service of random number generation is therefore considered to be an essential part of basic encryption technology.

See http://www.ibm.com/Security/html/cryptography.html for Feature Stories, White papers, and Position Papers on encryption.

2.2. Product Support

2.2.1. Hardware Products

A comprehensive set of cryptographic algorithms is supported on a number of hardware platforms and coprocessors. For a detailed list, consult the White Paper, IBM SecureWay Offerings Implement Open Security Standards, at http://www.ibm.com/Security/html/st_prodport.html

A summary list of the hardware facilities follows. For detailed information on each product, please consult the list at: http://www.ibm.com/Security/html/products.html, and follow the references for specific products.

- S/390 - The Integrated Cryptographic Feature (ICRF) is an optional feature of the ES/9000-9021 water cooled, bi-polar based family for use with ICSF/MVS. Together, ICRF with ICSF, implements and facilitates the use of the Common Cryptographic Architecture (CCA), a technology that is the foundation of IBM's primary cryptographic offerings. CCA implements all the functions described in the Introduction section for symmetric key cryptography, including key management, PIN generation, management and verification, message authentication and verification, and modification detection.

  CCA was developed to ensure consistent implementation of cryptographic services across IBM platforms and to provide guidance for vendors of similar products. It also facilitates enterprise-wide cryptographic solutions while allowing for compatibility with previous cryptographic services.

  The same cryptographic services are available via a channel-attached I/O unit, the IBM 4753 Network Security Processor. These facilities are exploited by the IBM Transaction Security System.

- S/390 - The Enterprise Server CMOS Cryptographic Coprocessor is an integrated feature of the S/390, CMOS based, Parallel Enterprise Servers - Generation 4 and an optional feature of Generation 3 servers, for use with OS/390 Version 2 . It provides all of the CCA based services previously supported by the optional ICRF, with additions for RSA public key cryptography that support digital signature generation and verification. The same cryptographic services are available via a channel-attached I/O unit, the IBM 4753 Network Security Processor.

- AS/400 Cryptographic Feature - the CCA-based set of cryptographic services are available via the AS/400 2620 and 2628 I/O processors (that use the 4755 card) for use with OS/400 via the CCA Services/400 PRPQ.

- RS/6000 and Intel-based PCs - the CCA based set of cryptographic services are available with the IBM 4755 Cryptographic Adapter via the Workstation Cryptographic Services for AIX and OS/2.

- RS/6000 and Intel-based PCs - a subset of the S/390 Enterprise Server CMOS Cryptographic Coprocessor services is available via the new IBM 4758 PCI Cryptographic Coprocessor for use with AIX 4.1 (and all subsequent releases), OS/2 Warp Version 3 and Windows NT release 4.0.

2.2.2. Software Based cryptography

A comprehensive set of software-based cryptographic services are available in numerous IBM products via the BSAFE Toolkit, a product of the RSA Corporation. Examples are all Internet Connection Secure Servers. Selected cryptographic services in this Toolkit are able to take advantage of the performance and security advantages of hardware cryptographic engines, when they are available, using the new BSAFE Hardware interface BHAPI. For details of products using BSAFE, see the White Paper, IBM SecureWay Offerings Implement Open Security Standards at http://www.ibm.com/Security/html/st_prodport.html

2.3. Standards

Standards-based algorithms form the core of functionality supported in the hardware and software products. The list is too long to repeat here. For a detailed list, consult the White Paper, IBM SecureWay Offerings Implement Open Security Standards, at http://www.ibm.com/Security/html/st_prodport.html

2.4. APIs

All hardware cryptographic coprocessors that comply with the IBM Common Cryptographic Architecture (CCA), for example those available with S/390, AS/400, and the IBM Transaction Security System, are invoked using the same API. On OS/390 this is facilitated by the Integrated Cryptographic Service Facility (ICSF). On AIX, OS/2 and Windows NT that are supported by the 4758 PCI Coprocessor, this is facilitated by the CCA Support Program.

CCA compliant cryptographic coprocessors may also be accessed by middle layer applications via the Common Security Services Manager (CSSM) API of the Intel Common Data Security Architecture (CDSA), supported by IBM KeyWorks toolkit. See The Open Group's specification on CDSA for details of the CSSM API at http://www.opengroup.org/security/cdsa/index.htm

The large collection of cryptographic algorithms provided by the RSA BSAFE toolkit may also be invoked via IBM KeyWorks. A selection of the BSAFE facilities (including MD5 and SHA1 digests, random number generation, DES CBC encryption/decryption and RSA signature genereration/verification) may take advantage of hardware implementations when available via the new BHAPI interface. See RSA's Home Page for BSAFE at http://www.rsa.com/rsa/products/bsafe/index.html

3. Electronic Commerce - Public Key Infrastructure (PKI)

3.1. Digital Certificate (X.509) Management

3.1.1. Introduction

This section provides an overview of:

- X.509 certificates
- Certificate authorities
- Registration authorities
- X.500 directories and registries
- The LDAP protocol

All are components of a public key infrastructure.

A **digital certificate** is an electronic credential issued and digitally signed by a **certification authority** (CA). The international standard upon which most commercial certificates are based is the **ISO X.509 certificate**. The digital certificate represents the **certification** of an individual, business, or organizational public key. It can also be used to show the **privileges and roles** for which the holder has been certified. Thus, digital certificates serve multiple purposes in electronic commerce systems. They are used to authenticate a server or Web site to a client so he can be sure he is dealing with a legitimate service; conversely they can be used to verify for the application or server that an authorized client is trying to invoke the service. Once a client is properly authenticated, privileges and roles can be extracted from his certificate, and authorization may be granted to access the service. In addition the certificate can provide the keys used for the algorithms of encryption, hashing and digital signature generation, thereby ensuring the **confidentiality and integrity** of the communications and providing a mechanism by which the occurrence of the transactions cannot be **repudiated**. The public key and secret key encryption mechanisms, introduced under heading 2 may be used in combination to accomplish these goals.

A **public key infrastructure** (PKI) is a networked system of certification authorities (CAs), **registration authorities** (RAs), **certificate management systems** (CMSs) and X.500 **directories.** It helps enable two parties unknown to each other to exchange sensitive information and monetary units over an unsecured network like the Internet.

Certificate Authorities manage a Public Key Infrastructure by issuing certificates and establishing PKI policies within its domain. Registration Authorities (RAs) act on behalf of CAs to register subscribers in the domain of a particular CA. A CA uses and controls a CMS to manage certificates life cycles. Typically ISO X.500 directories may be used as the **Registry** to store the public encryption keys associated with their certificates, together with other public information about certificate subscribers. Facilities must be provided to maintain valid certificates, revoke certificates when their validity has expired, certify those that are called upon for use, and make them available to legitimate users upon demand.

The ISO X.500 Directory standard is highly structured and generalized. It has been found that the prescribed protocol for communicating with such a directory is overly complex for the PKI Registry application. Consequently a simplified protocol has been developed that provides the necessary facilities in a simplified fashion with consequent performance improvements. This is known as the **Lightweight Directory Access Protocol** or LDAP and it is coming into widespread use in PKI implementations.

A PKI is also a network of **trust relationships**. Individual subscribers establish trust relationships with CAs. CAs may, in turn, establish trust relationships with other CAs to allow PKI secure communication between domains. In a transaction between two people who are unknown to each other, CAs act as **trusted third parties**. When the transaction involves two parties who are unknown to each other, an individual's certificate signed and verified by a trusted CA may be all that is needed to establish trust between the two parties.

A PKI with appropriate safeguards, management, and technology, can be used to enforce information policies, control information flow, compartmentalize information, and even assist in the productizing of information. It can be used to identify potential security threats and provide digital time stamping services. It can also be used to more securely store information.

These technologies and many others related to cryptography are described in full in a primer which answers many “what are, and why do I need them?” questions. The primer can be found at http://www.internet.ibm.com/commercepoint/registry/primer.html#d-pki.

3.1.2. Product Support

IBM Registry is a security-rich e-business platform that offers an integrated public key infrastructure (PKI) solution using X.509 digital certificates designed to address the number-one inhibitor to market growth over the Internet: security. IBM Registry gives you the authority to issue digital certificates, provide a more secure application environment, and help you determine your e-business security policy.

Thus, IBM Registry is a product that enables organizations to control access to their secure web server applications and other network computing services. In IBM Registry, organizations' authorized registrars, known as registration authorities (RAs), follow their organizations' policies and procedures when registering applicants to use the organizations' services. Once approved, applicants receive digital certificates from their Certificate authority (CA) that certify the keys they will use for access. Certificates are stored in an X.500 based directory and the Lightweight Directory Access Protocol (LDAP) is used for access.

For more details on all aspects of IBM Registry, please check out the IBM Registry Web site at http://www.ibm.com/Registry.

3.1.3. Standards

Public Key Infrastructure standards are the subject of intense work by The Open Group (TOG), The Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) and other organizations.

In the absence of international standards, de facto standards are emerging, supported by groups of vendors.

CDSA, mentioned above, provides the infrastructure for implementing the various components of a PKI, in a way that will allow interoperability and the use of a range of service providers for encryption, key and certificate management, and so on. IBM has implemented CDSA in the IBM KeyWorks family of products. See http://www.ibm.com/Security/html/prod_kw.html for a product overview and links to more detailed information.

3.1.4. APIs

Intel’s Common Data Security Architecture’s Common Security Services Manager API is the primary mid-layer application API for the provision of PKI services. IBM KeyWorks provides the tools to implement the required support for electronic commerce applications based on the use of a PKI. See The Open Group’s specification on CDSA for details of the CSSM API at http://www.opengroup.org/security/cdsa/index.htm

3.2. Common Data Security Architecture (CDSA)

3.2.1. Description

Intel’s Common Data Security Architecture is a framework or switch for supporting, via a single API, multiple security related service providers, such as encryption, certificate management, key recovery, trust policy and data storage. The framework accommodates multiple services and multiple service providers but is implemented to switch a connecting application to one service provider at a time.

Each of the security services supported can accommodate, via the framework architecture, multiple different mechanisms via Service Provider plug-ins. This allows security applications to use a single, functionally rich API to gain access to whatever back-end public key infrastructure-related security services they may wish to employ. This API, known as the Common Security Services Manager API (CSSM), invokes the services of the Service Providers in a way that is independent of the API of the Service Provider itself. This important feature can make the application independent of, for example, either the cryptographic services plug-in API or the certificate management plug-in API or the trust policy plug-in API. CSSM addresses the major problem confronting the electronic commerce industry today: the existence of diverse, competing implementations of basic PKI services. It makes the peculiarities of a particular Service provider transparent to the application.

CDSA, in addition to providing the framework for multiple PKI supporting services via a single API, also provides a set of services for each of the multiple Service Providers that can be plugged into it by:

- Identifying and registering the various service provider implementations
- Maintaining and storing information about the current state of the connection between applications and plug-in modules
- Verifying that the service provider implementations have not been tampered with.

3.2.2. Product Support

CDSA is supported by the IBM Secure Cryptography and Certificate Services (SCCS) Toolkit, part of the IBM KeyWorks family of products. It consists of a framework (SCCS Framework) and several service provider add-in modules. The following categories of service providers are supported:

- Cryptography - encryption/decryption, key generation, hash or message digest computation, etc.
- Key Recovery - the generation of Key Recovery blocks that can be used to recover original keys.
- Trust Policy - implement policies defined by authorities and institutions that issue digital certificates.
- Certificate Library - performs format specific, syntactic manipulation of certificates and certificate revocation lists.
- Storage Library - provides persistant data storage and manipulation operations for security objects, such as certificates.

See http://www.ibm.com/Security/html/prod_kw.html for a product summary and links to pages containing more details.

It is the intention that the SCCS Toolkit, together with the other KeyWorks products, shall facilitate the building of and provide the basic building blocks of the security facilities needed to enable e-business applications.

The IBM SCCS Toolkit Framework consists of software that provides a layer of isolation between applications on “top” (of the framework) and specific implementations of services or mechanisms on the “bottom”. Applications can access the desired service using a single, standard API. Service Provider implementations that support the service provider interface (SPI) can be plugged into the framework without any changes to the application. That is, an application using one Service Provider implementation today can decide to use a different provider’s implementation tomorrow without any changes. Thus, the primary benefit of the isolation “layer” provided by the framework is that software on one "side” of the framework can be modified, updated, or replaced without impacting the operation of software on the other side.

The IBM SCCS Toolkit Framework is based upon Intel’s Common Data Security Architecture (CDSA), which has been standardized by the Open Group. The API is the functionally rich CSSM API; IBM has extended the API with the addition of key recovery functions. Through the use of the IBM SCCS Toolkit, an application can perform cryptographic operations using a standard API.

The framework provides critical administrative functions that are essential for correct operation. These functions include:

- Add-In module management.
- Integrity services, for example ensuring the identity and integrity of plug in Service Providers by having them digitally signed.
- Support of different (national) trust policies.
- Protection of vital steps, for example making sure that the Key Recovery process is not bypassed.
- Maintenance of application to Service Provider status information.
- Transmission of application service requests to the appropriate Service Provider.
- Security context management for example when applications require multiple stages, between which secrets need to be securely stored.

The framework included in the IBM SCCS Toolkit is extensible; as additional functions are defined, the framework can be extended to include them. The framework also can accommodate multiple Service Provider implementations for each set of functions.

3.2.3. Standards

CDSA has been adopted by The Open Group as an industry-accepted specification for the development of secure applications that are extensible and offer cross-platform support. Security Dynamics, RSA and IBM recently announced agreements establishing the use of CDSA in open, multi-vendor environments for integrating and deploying enterprise security solutions for applications using the public key encryption method developed by RSA Data Security. This agreement will help ensure that the participating companies' products will work together and will allow vendors to create compatible security solutions.

3.2.4. APIs

The CSSM API is fully documented in the CDSA specification which is available from The Open Group Web sites at http://www.opengroup.org/security/cdsa/index.htm. CDSA has now completed its Fast Track into The Open Group, with the result that The Open Group is defining a commercial Product Standard, supported by testing, to enable suppliers to register branded products. The Open Group is also setting up a development partnership to enable companies who wish to reduce the costs, risks and time of development of CDSA through sharing with project partners.

3.3. Key Recovery

3.3.1. Introduction

The basic cryptographic functions are encryption and decryption, using a mathematical algorithm and a secret value known as a key in the "the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling [italics added]." This provides the ability to communicate between parties or store information in such a way that prevents other parties from accessing and understanding it.

In addition to reasons for hiding or encrypting information, there are legitimate reasons for recovering encrypted information such as :

- An individual has encrypted important information and has lost or forgotten the key
- A business needs access to employee-encrypted non-personal information and the employee is not available
- Law enforcement procures a court order giving them the right to access information (for example, a search warrant).

The cryptographic key is the critical item required to recover encrypted information. Therefore, the availability or accessibility of the key is a pivotal issue. A number of key recovery technologies exist to make the key available to recover encrypted information. There are two basic types of key recovery techniques:

- Those involving some form of escrow of the key or key parts with a trusted party and
- Those non-escrow techniques that involve creating key recovery fields, that are mathematically related to but not actually the key or parts of the key, and associating these fields with the message. Later the key recovery fields can be used to recover the key. Such techniques are called encapsulation.

The IBM key recovery technology, as implemented in the IBM Key Recovery Service Provider module plug-in to the KeyWorks framework, is based upon an encapsulation technique rather than an escrow technique. With IBM key recovery, no party actually holds either the cryptographic key or parts of the key. Information from which the cryptographic key can be reconstructed is associated with an encrypted message or file for potential later use. Information needed for the reconstruction process is distributed among multiple parties and they all have to get together to successfully execute the process. This means that a multi-party conspiracy is required to illegally execute the process. This greatly reduces the risk of illegal key recovery.

Thus with IBM key recovery technology:

- No one has a copy of the key or any part(s) of the key
- There is no single point of vulnerability or compromise
- No communication with a third party (escrow agent) is required for each session/key initiation, leading to excellent scaleability
- There is no loss of control over key management to a third party
- There is no need for a key storage infrastructure

For a more detailed discussion of this technology, please refer to the White Paper “Cryptography and Key Recovery” at http://www.ibm.com/Security/html/wp_keymgt3.html

3.3.2. Product Support

There are two basic functions associated with the key recovery process. First there is the transparent generation of the key recovery block of data fields on behalf of applications that need to send strongly encrypted information to a recipient. This function is provided by the IBM Key Recovery Service Provider. It plugs into the CDSA framework. Second there is the independent recovery of the encryption keys by the appropriate authorities, when the keys are either lost or need to be regenerated for some other reason. This function is provided by the IBM Key Recovery Server. Both products are part of the IBM Keyworks set of products.

An introduction to IBM Keyworks can be found at http://www.ibm.com/Security/html/prod_kw.html, where links to more detailed information may be found.

3.3.2.1 The IBM Key Recovery Service Provider (KRSP)

This product is part of the IBM KeyWorks family of products. The Key Recovery Service Provider is a plug-in to the Key Management framework component of the Common Data Security Architecture (CDSA). Key Recovery Service Providers (KRSPs) are modules that provide key recovery enablement functions.

The cryptographic functions provided may include:

- Key recovery field generation
- Key recovery field processing.

KRSPs generate and process Key Recovery Fields (KRFs) which can be used to retrieve the original session key if it is lost, or if an authorized party requires access to the decryption key.

Key Recovery Profiles.

The KRSPs require certain pieces of information related to the parties involved in a cryptographic association in order to generate and process KRFs. These pieces of information (such as the public key certificates of the KRAs) are contained in key recovery profiles. A key recovery profile contains all of the per-user parameters for KRF generation and processing for a specific KRSP. In other words, each user has a distinct profile for each KRSP.

For more details, including protocol flows, on the use of the IBM KRSP in conjunction with the IBM Keyworks SCCS Toolkit Framework, see the White Paper at http://www.ibm.com/Security/html/wp_keymgt4.html

3.3.2.2 The IBM Key Recovery Server (KRS)

Built to work with KeyWorks, the IBM Key Recovery Server (KRS) is a new stand-alone application that is designed to recover cryptographic keys. With proper authorization and participation by one or more local or remote independent agents, KRS uses Key Recovery Fields (KRFs) generated by the IBM KRSP to recover the keys that can be used to decrypt the ciphertext. Upon authorized request, the KRS can recover encrypted information when keys are unavailable, lost, or damaged. The KRS is intended to be used by enterprise employees and security personnel, law enforcement personnel, and KRSF personnel.

Some of the security features that are part of the KRS include:

- Supports multiple standards of encryption
- Verifies that requests come from authorized users
- Does not expose the recovered key to anyone but the authorized requester

Additional benefits for business include:

- Allows for the recovery of cryptographic keys for business use without escrow or trusted third party
- Provides a recovery operation that is transparent to end users

For more information on the key recovery operation using the IBM KRS, see the White Paper at http://www.ibm.com/Security/html/wp_keymgt5.html

3.3.3. Standards

Plug-in service provider modules support open standards including PKCS#11, RSA’s cryptographic functions, X.509V3 certificates, the trust policies of Entrust and Verisign, as well as the Lightweight Directory Access Protocol (LDAP). These plug-ins make it possible for the key recovery plug-in functions to be used with different cryptographic suppliers, standard certificates from various Certificate Authorities (CAs), trust policies from Verisign and Entrust, and any directory that can be accessed via LDAP.

3.3.4. APIs and Protocols

API’s employed are:

- CDSA’s CSSM API for PKI services, at http://www.opengroup.org/security/cdsa/index.htm
- IBM’s CCA API for cryptographic algorithms
- RSA’s BSAFE APIs for software cryptographic algorithms, that includes a hardware interface, BHAPI, for use when hardware accelerators are available, at http://www.rsa.com/rsa/products/bsafe/index.html

Protocols employed are:

- LDAP, a protocol for simplified communications with X.500 registries, see http://www.ietf.org/html.charters/ldapext-charter.html for current IETF work in progress on extensions to LDAP Version 3.
- SSL, used with and without IBM Key Recovery. SSL is a commonly used protocol that provides privacy and reliability between communicating applications.
- S/MIME , used for the creating and distribution of encrypted objects using PKCS#7

4. Electronic Commerce - Exploiters

4.1. Vault Deposit Services

4.1.1. Introduction

Vault deposit services are needed to provide "personal vaults" for users, Registration Authorities, and Certification Authorities. A personal vault provides a secure environment within Web servers for executing programs and services on behalf of a user. Personal vaults, and their contents, are accessible from SSL-enabled web browsers that contain the corresponding vault certificates. Access to personal vaults does not require knowledge of a vault password and keys. Access to personal vaults requires a vault certificate and key.

Information stored in personal vaults is protected against disclosure to unauthorized persons (e.g., system administrators and other vault owners) by encryption, against tampering by digital signing, and against untrusted communications with unknown parties by using digital certificates. Information can also be transmitted securely to other vaults using encryption, signing and certificates. Organizations need such a high level of security because their registration forms usually require customers to provide very sensitive information.

4.1.2. Product Support

Vault deposit services are provided via the Vault Deposit Server, a component of IBM Registry. For more details on all aspects of IBM Registry, please go to the IBM Registry Web site at http://www.ibm.com/Registry.

In addition to the Vault Deposit Server, IBM Registry provides a Vault Agent which is an optional lightweight vault process designed to run remotely at a customer's location. It incorporates a small subset of the Vault Deposit Server functionality. This subset enables the Vault Agent to exchange secure messages, with minimal changes to the existing application, with vault processes running under the control of the Vault Deposit Server. Organization applications may use the Vault Agent to request and receive certificates for customers and employees when it is used with the automated Registration Authority vault process.

4.2. Secure Electronic Transactions (SET)

4.2.1. Introduction

The SET protocol is used to facilitates secure electronic bank card payments, typically between client browsers, through the merchant Web server to the merchant's acquiring bank. The acquiring bank will then use existing processes and facilities to clear the payment through the client's bank that issued the credit card. This scenario is shown in the figure below.

The SET protocol enables secure credit card payment by hiding the card number from the merchants, ensuring the strong authentication of the participants in the transactions and providing privacy and message integrity for the transaction. In doing so, SET sustains existing relationships between cardholders and their banks and allows existing banking systems and networks to be used, it provides interoperability between systems using different but SET compliant credit cards and it provides one more important choice of payments for the end user.

Certification is a major reason why SET is such a strong standard for online payments. It helps identify each participant as having a legitimate role in the transaction. Certification of the cardholder is the job of the Issuing Bank. This, of course, is in addition to the other services, such as authorization, customer service, etc., that an Issuing Bank provides to its cardholders. It's another way to build more solid customer relationships. And helps keep disintermediation at bay.

4.2.2. Product Support

4.2.2.1 IBM Registry for SET

IBM Registry for SET is a software product that is intended to fulfill the need for a certificate authority to facilitate secure use of credit and other payment cards over the Internet. IBM Registry for SET provides the technology to issue and manage the encrypted digital certificates that underlie all SET transactions, enabling a buyer to verify that a merchant is bona fide and enabling the merchant to verify that the credit card is being used by the legitimate user.

IBM Registry for SET provides the Issuing Bank with the software needed to issue and manage certificates within SET.

For more information on this product, please refer to the following pages:
http://www.internet.ibm.com/commercepoint/payment/context.html

4.2.2.2 IBM CommercePOINT

For introductory information on IBM CommercePOINT products, please consult:
http://www.internet.ibm.com/commercepoint/

CommercePOINT Payment offers advanced features for more security and identification of transaction participants' roles, making online purchasing more comfortable for consumers and merchants. The CommercePOINT Payment suite of products integrates SET 1.0 into the phases of an electronic commerce transaction, and uses digital certificate technology for the consumer, the merchant and the acquiring bank's processor, resulting in a complete, more reliable electronic commerce solution.

The IBM CommercePOINT eTill is the merchant's electronic equivalent to a cash register for the Internet, passing necessary credit card information over the Internet to the financial institution for approval. IBM CommercePOINT Wallet delivers the consumer's credit card information in an encrypted form--all the way to the acquiring bank. IBM CommercePOINT Gateway is the acquiring institution's link to the Internet, routing, approving and managing SET transactions for acquiring institutions that process credit cards by seamlessly connecting those institutions' financial systems with the Internet.

CommercePOINT product components include:

- The SET protocol to facilitate secure electronic bank card payments.
  For more information on the use of SET for CommercePOINT payments, consult Web site:
  http://www.internet.ibm.com/commercepoint/payment/context.html
- Public key infrastructure technologies are used in the IBM Registry for SET product.
- The Merchant Server is a new technology for e-commerce
- The Payment Gateway is another new technology for e-commerce.
  For more information on the Merchant Server and Payment Gateway, please consult Web site:
  http://www.internet.ibm.com/commercepoint/net.commerce/

4.2.3. Standards

Secure Electronic Transactions (SET). Mastercard and VISA have cooperatively developed the Secure Electronic Transactions. SET was designed by IBM, MasterCard, Microsoft, Netscape, SAIC, Erisa Systems, Verisign and Visa.

SET is as an open, vendor-neutral, nonproprietary, license-free specification for securing on-line transactions. For more information on SET, please consult Web site http://www.mastercard.com/set/set.html

4.3. Cryptolope Containers

4.3.1. Introduction

Cryptolope container technology addresses the challenges faced by information management professionals today. Examples include:

- The need to leverage intellectual assets in order to help employees work more effectively.
- The desire to control the distribution of assets over external networks with vendors, suppliers and partners to ensure that the right information gets into the right hands.
- The need to extend distribution, commerce, and fulfillment services for sensitive content to the Internet.

Cryptolope containers are based on a technology designed to secure, manage, deliver, track, sell and fulfill digital content in Java environments across intranets, extranets and the Internet. The technology transcends “content access” to address the management of content access; namely how information is distributed, protected, accessed and used. The technology offers new opportunities for more flexible applications by allowing business rules to be implemented using a scripting language and Java extensions.

The Cryptolope technology is based on information object technology which binds code and data together in a single persistent object. The advantage of this information object model is that Cryptolope objects can be programmed to govern how enclosed information is used, thus offering a wide assortment of business applications.

The original Cryptolope container was an envelope or package that used cryptography to protect its content from unauthorized access or alteration. Today’s technology is more than simply a container; it is an information object.

The following functions are needed to meet the design objectives:

- A Cryptolope builder that is used to build dynamic, extensible, optionally encrypted “objects” which contain digital content and the business rules for the use of that content.
- A Cryptolope clearing center to provide back end processing, manage the exchange of encryption keys, provide an interface to a Cryptolope cashier and provide event logging.
- A Cryptolope player to provide a runtime system to run Cryptolope objects, preferably implemented as a Java applet for embedding within a Web page or as a separate application which may be downloaded and installed on a user’s desktop. It would require extensions for Cryptolope objects, including an HTML trusted viewer, a transaction envelope, and a clearing center interface.
- A Cryptolope cashier to provide the framework for integrating payment and tax calculation programs for real time credit card transaction processing.

5. Secure Networks

5.1. Secure Sockets Layer Protocol

5.1.1. Introduction

The primary goal of the SSL Protocol (a specification from the Netscape Communications Corporation) is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (for example., TCP), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently.

The SSL V3 protocol provides connection security that has three basic properties:

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

For the complete specification, please refer to the Netscape Web site at
http://home.netscape.com/eng/ssl3/3-SPEC.HTM#2

Note that this specification has been submitted to the IETF as an Internet-draft

5.1.2. Product Support

Many products support SSL as follows:

- All secure client browsers
- Secure software Web servers (for example, Lotus Go Web Server, Lotus Domino Server, all Internet Connection Secure Servers).
- IBM Telstra Directory Server in conjunction with LDAP
- DFSWeb Secure Gateway
- IBM Registry
- IBM Registry for SET
- CommercePOINT Payment
- IBM eNetwork Firewall

5.1.3. Standards

SSL has been submitted by Netscape Communications Corporation to IETF as an Internet-Draft for consideration as a formal standard. Due to the widespread use of SSL, it can already be considered a “de facto” standard.

5.2. Virtual Private Networks and IPSEC

5.2.1. Introduction to VPNs

A virtual private network (VPN) is an extension of an enterprise's private intranet across a public network such as the Internet, creating a secure private connection, essentially through a private "tunnel." VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners/suppliers into an extended corporate network. Companies need to communicate among their geographically dispersed locations; manufacturers and their suppliers need access to shared databases; and remote users need to reach applications and servers in their corporate intranet.

Internet service providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive leased lines, long-distance calls, and toll-free telephone numbers. A 1997 VPN Research Report, by Infonetics Research, Inc., estimates savings from 20% to 47% of wide area network (WAN) costs by replacing leased lines to remote sites with VPNs. And, for remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs. Additionally, Internet access is available worldwide where other connectivity alternatives may not be available.

For more information on VPNs, please read the IBM eNetwork Software White Paper: eNetwork VPNs - IBM's Virtual Private Network Solutions at http://www.networking.ibm.com/ene/vpn.html

5.2.2. Introduction to IPSEC

The Internet Protocol (IP) is the layer that hides the underlying physical network by creating a virtual network view. It is a best-effort connectionless packet delivery protocol. Rapid advances in communication technology have accentuated the need for security in the Internet. Thus the Internet Engineering Task Force (IETF) has commissioned the The IP Security Protocol Working Group (IPSEC) to develop mechanisms to protect IP datagrams. A security protocol in the network layer has been developed to provide cryptographic security services that flexibly support combinations of authentication, integrity, access control, and confidentiality.

The goals of the IPSEC group were to pursue host-to-host security followed by subnet-to-subnet and host-to-subnet topologies.

Protocol and cryptographic techniques have also been developed to support the key management requirements of the network layer security. The Internet Key Exchange protocol (IKE) is being specified as an application layer protocol that is independent of the lower layer security protocol. The protocol is based on the ISAKMP/Oakley work.

The work was based on five basic specification (RFCs) that were initially approved as the standard, these in turn have been progressed by committee work to more advanced Internet-drafts which are in the final stages of approval. Implementations of these I-Ds greatly facilitate the security of Virtual Private Network implementations. The relevant I-Ds that IBM VPN products are aiming to support are:

- draft-ietf-ipsec-esp-v2-04.txt , IP Encapsulating Security Payload
- draft-ietf-ipsec-ipsec-doi-08.txt, The Internet IP Security Domain of Interpretation for ISAKMP
- draft-ietf-ipsec-ciph-null-00.txt, The NULL Encryption Algorithm and Its Use with IPSEC
- draft-ietf-ipsec-isakmp-oakley-07.txt, The Internet Key Exchange (IKE) [new name for old ISAKMP/Oakley}
- draft-ietf-ipsec-auth-header-05.txt, IP Authentication Header
- draft-ietf-ipsec-arch-sec-04.txt, Security Architecture for the Internet Protocol
- draft-ietf-ipsec-isakmp-09.txt, Internet Security Association and Key Management Protocol (ISAKMP)

Details of these specifications may be found on the IETF Web site at:
http://www.ietf.org/html.charters/ipsec-charter.html

In addition, please read the IBM eNetwork Software White Paper “Using IPSec to Construct Virtual Private Networks” at URL http://www.software.ibm.com/eNetwork/library/whitepapers/vpn/

5.2.3. Product Support

IBM was one of the earliest providers of VPN offerings, delivering VPN capability in our AIX® Firewall in 1995. The AIX Firewall VPN capabilities were enhanced in 1996 to include IPSec, an IETF industry security standard Today, IBM eNetwork VPN solutions encompass a wide range of products consisting of the VPN-enabled Firewall (AIX), Clients (Win/95, AIX, OS/2 Clients), and Servers with added Firewall Functionality (AIX, OS/390), as well as ISP, consulting, installation, implementation and maintenance services. Throughout 1998 and into early 1999, IBM will extend its VPN offerings to include low-end (2210) and high-end (2216) routers - both with embedded firewall functions, Win/98 and Win/NT Client Support, AS/400 Servers with added Firewall support, and AIX and NT Firewalls with packaged load balancing, availability and caching proxy capabilities. In addition, IBM will incorporate VPN management capabilities -- such as policy, certificate, IP address, and key management -- into its solutions, and will "future-proof" offerings by adding critical functionality such as IPv6 to all products.

For more information on the AIX Firewall and its VPN capabilities, please read the ICSA certification announcement at http://www.software.ibm.com/enetwork/firewall/newsvpn.htm

For more information on the OS/390 Firewall Technology, see http://www.s390.ibm.com/marketing/g2214102.html

5.2.4. Standards

The technology to implement virtual private networks is just becoming standardized. Some networking vendors today are offering non-standards-based VPN solutions that make it difficult for a company to incorporate all its employees and/or business partners/suppliers into an extended corporate network. However, VPN solutions based on Internet Engineering Task Force (IETF) standards will provide support for the full range of VPN scenarios with more interoperability and expansion capabilities.

IPSec provides cryptography-based protection of all data at the IP layer of the communications stack. It provides secure communications transparently, with no changes required to existing applications. IPSec is the IETF chosen industry standard network security framework for use in both the IPv4 and IPv6 environments. It is also currently the technology-of-choice for more than a dozen networking vendors, such as Sun, Attachmate, and Bay Networks.

For more information about the IETF’s IP Security Protocol Working group, its charter, status and list of Internet Drafts (IDs) and Requests for Comments (RFCs), please consult Web site http://www.ietf.org/html.charters/ipsec-charter.html

5.2.5. APIs

The IETF RFCs for IPSEC define a set of protocols, not an API.

5.3. Firewalls

5.3.1. Introduction

Firewalls shield an organization's network from exposure when connecting to the Internet or any other external, "untrusted" network, and they prevent hackers and others from gaining authorized access to internal data, and computing resources. Firewalls provide software and hardware tools that precisely define, control, and limit access to computers on internal networks from the outside.

Firewalls typically control external access to enterprise resources through the authentication of requests from the users of common inter-enterprise communications applications such as FTP and TELNET. They also selectively restrict access to the enterprise by knowing the source of access requests. Firewalls can also facilitate secure communication with selected partners by setting up Virtual Private Networks (VPNs).

5.3.2. Products Supported

IBM supports all the above firewall requirements and more via IBM Firewall V3.1 for AIX. These requirements are also supported in OS/390 Version 2, Release 5 via the optional feature Security Server and eNetwork Communications Server and their integrated Firewall Technologies and are supported in Firewall for AS/400.

IBM eNetwork Firewall V3.2 for AIX and Windows NT with additional capabilities, became generally available in 4/98.

See the Web site at URL http://www.software.ibm.com/enetwork/firewall/ for highlights, news, links to related topics such as Virtual Private Networks and to download Beta versions of eNetwork Firewall3.2 for AIX and/or Windows NT.

See also Web site http://www.s390.ibm.com/marketing/g2214102.html for more information on the OS/390 Security Server and eNetwork Communications Server and their integrated Firewall Technologies.

IBM eNetwork Firewall 3.2 for AIX and/or Windows NT supports the following technologies:

- Expert filters to block access, for example spoofing attacks, for UDP, ICMP, and TCP protocols.
- Application gateway proxies to limit access from the untrusted network to selected target nodes and services, using strong authentication. FTP, Telnet, HTTP, DNS and real Audio are supported.
- Socks Circuit Gateway to limit access from the intranet to the Internet to specified trusted users, using socksified applications such as HTTP and FTP.
- Network Address Translation (NAT) that allows trusted (non-Socks) applications to connect to untrusted servers with non-registered addresses.(AIX only,NT NAT support is targetted for 6/98)
- Virtual Private Networks (VPN) that allow selected nodes to make secure connections, across the Internet (AIX only, VPN support for NT is planned for a future release).
- Split Domain Name Service that separates the internal DNS of the secure company network from the external DNS of the untrusted public network.
- Mail Forwarding or SafeMail. Users on the Internet are allowed only to exchange mail directly with specified “public” hosts.
- Remote administration based on an object oriented Java GUI, using administration levels and groups for separation of roles.
- The Security Dynamics ACE/Server software and two SecurID TM tokens, at no additional charge, to provides strong, two-factor user authentication.
- National Language support, available in 5/98, includes eight translated languages, including French, Japanese, Korean, Traditional Chinese and Simplified Chinese, providing easier administration and lower support costs for customers worldwide.

5.3.3. Standards

The IBM eNetwork Firewall for AIX is Firewall Certified by the International Computer Security Association (ICSA) and the IBM eNetwork Firewall for Windows NT has been submitted for ICSA Firewall certification. Also the IBM Firewall VPN feature for the IBM Firewall for AIX was Certified by the ICSA on December 16, 1997. The ISCA completed a set of rigorous tests to verify that the IBM Firewall met ISCA security standards for VPN function. IBM eNetwork VPNs provide cryptographically strong end-to-end encrypted tunnel connections across unsafe public networks such as the Internet, allowing businesses to securely take advantage of flexible, available, and low cost Internet access.

The IBM Firewall uses the “de facto” standards SSL for secure communications; for the Netscape specification of SSL V3, please refer to the Web site at http://home.netscape.com/eng/ssl3/3-SPEC.HTM#2

IBM Firewall also uses BSAFE for cryptographic support. See RSA's Home Page for BSAFE at URL http://www.rsa.com/rsa/products/bsafe/index.html

6. Single Sign-On

6.1. Introduction

In a distributed system environment connected by networks, users must access many services such as database systems, network systems, operating systems and mainframe applications. In order to use these services, the user must issue a separate sign-on command for each specific system or application. Each of these sign-ons may, in turn, have a different pair of user ids and passwords. This places the user under a significant burden to remember and maintain this information, which in turn may lead to security risks.

Technologies are required that enable users to sign-on once with a single ID and password to access all their business applications, services and data. The design goals are ease of use, secure primary authentication of users, integration with Operating System logons and capable of leveraging existing security infrastructures, consistent look and feel across Operating Systems, secure, transparent logon coordination to multiple applications and based on open standards.

The design goals call for an initial strong authentication of the user as part of the initial sign-on. Once this has been accomplished, sign-on to all the other applications and resources in the distributed configuration, using their particular sign-on protocols, should be automated and transparent to the user. The logon information required for the remote applications must be encrypted and stored securely. Similarly the transmission of the logon information to the remote applications must also be highly secure.

For the strong authentication portion of the initial sign-on to be portable to any environment, it must be independent of the underlying authentication protocols and encryption mechanisms. This calls for a technology that supports the "snapping in" of different authentication mechanisms using an authentication framework modeled after the Pluggable Authentication Module (PAM), documented in OSF RFC 86.0, now owned by The Open Group. Thus platform independence is achieved through the use of PAM’s high-level API. The framework architecture allows new authentication mechanisms to be added and therefore new environments to be supported without major redesign.

6.2. Product Support

The IBM Global Sign-On product meets all of the goals of the single sign-on requirements.

IBM's Global Sign-On solution consists of the following major components:

- GSO Authentication - Authenticates the user to the GSO system. On systems with local operating system security, this authentication mechanism is integrated with the local OS authentication. This component is specifically designed to handle the "snapping in" of different primary authentication mechanisms (for example, Kerberos, Sesame, Biometric systems).
- Configuration Information Manager (CIM) - Contains information on the various different processes needed for a given client to transparently logon to the (remote) applications listed that he is authorized to access. This component provides the ability to add new logon methods as the client expands the list of applications and subsystems that he needs to use.
- Personal Key Manager (PKM) - Contains secret information about a client, the keys needed for primary authentication, the applications to be accessed and passwords needed to logon to those systems. GSO is designed to support storing these in multiple places , such as smart cards, encrypted flat files, remote servers, etc. Since this information is centralized, users can access their resources with one sign-on from any workstation and manage their passwords from this one repository. Authentication to the data storage mechanism can be accommodated in a number of ways: secret key authentication, public key, PINS for smart cards, etc.
- Logo Coordinator (LC) - Retrieves the user's passwords from PKM and uses them in conjunction with the target specific logon code (listed in the CIM) to log users onto all their systems without any additional user intervention.

For more details on the architecture, design rationale and componentry of IBM's GSO product, please consult the White Paper at http://www.networking.ibm.com/gso/ssowpaper.html

6.3. Standards

Single Sign-On and the associated PAM technology are being worked on by The Open Group's Security Program Group. Details of their activities and the specification entitled "X/Open Single Sign-On Service (XSSO) - Pluggable Authentication Modules", may be found at http://www.opengroup.org/security/sso/index.htm

7. DCE Security Services

7.1. Introduction

DCE Security Services provide trustworthy identification and authentication of principals (users, clients, servers, and systems), offering a high level integrity and privacy of communications, and enabling controlled access to resources. It controls the interaction between clients and servers and objects managed by servers.

Today, most non-DCE systems provide one-way authentication, where the client proves its identity to the server. Server identity is rarely verified. In a distributed environment, this trust of servers may be lessened, leading to a requirement for mutual authentication.

DCE Security Services, acting as a third party trusted by both clients and servers, can identify and authenticate principals and provide information on the privileges associated with each principal and hence support fully authenticated access control of users to application services.

7.2. Product Support

DCE is designed to scale across your enterprise network, as well as be portable across most of the systems within your network. The family of IBM of products, into which DCE is integrated is growing fast, spanning the desktops and servers of all of its major platforms and systems. Sub-systems supported include DB2, MQSeries, Component Broker and Global Sign-On (GSO). Future plans include DCE integration with IBM resource managers such as APPN, and CICS. For more details on IBM implementations of DCE services and for links to a wide range of DCE related information, please check out the DCE Home Page at http://www.networking.ibm.com/dce/dcehome.html

Support for DCE is provided on the following platforms:

- AIX/6000
- Solaris
- OS/390
- OS/400
- OS/2 Warp
- OpenEdition VM
- Windows NT 1.1 and 2.0
- Windows 95

As an example of product support we will consider how the DCE Security Services have been utilized by, and integrated with, OS/390 and the OS/390 Security Server.

OS/390 Security Server DCE Services provides a fully functional OSF DCE 1.1 level security server that runs on OS/390. Availability of this critical DCE technology component on OS/390 can provide the following benefits:

- You can help keep servers and data on your OS/390 systems safe from accidental or malicious loss, and secure from outside attack (disclosure or corruption).
- S/390 is scalable. You can build DCE cells that are able to handle large numbers of accounts.
- OS/390 has higher availability than many other platforms that offer DCE. Therefore, a security server on OS/390 can be one of the most reliable and available DCE system, giving you the ability you need to run mission-critical applications in a DCE environment.

OS/390 Security Server provides security registry, privileges and authentication services for both DCE 1.1 and Kerberos V5 applications.

The OS/390 Security Server DCE 1.1 and Kerberos V5 Registry can be optionally implemented using DB2 as the underlying database. This is an option to using OS/390 UNIX file to hold the registry. This provides commit and backout of updates to the registry, transaction logging and log recovery. DCE Registry on DB2 provides performance, availability, and scalability to support large mission-critical DCE applications.

OS/390 Security Server provides interoperability between the RACF and DCE security functions. This interoperability allows:

- Appropriately authorized DCE servers to acquire corresponding OS/390 security credentials for the DCE client and to use the DCE clients corresponding OS/390 user ID for access to RACF-secured resources.
- An OS/390 user to be transparently logged into DCE when necessary, with-out prompting for a DCE user ID or password. With this single authentication feature, an authenticated OS/390 user can start a DCE application without explicitly reauthenticating to DCE.

The OS/390 Security Server also provides administration utilities that implement this interoperability by associating DCE principals with RACF user IDs.

For the latest information on the OS/390 Security Server and how it has been integrated with DCE Security Service, please check out http://www.s390.ibm.com/marketing/g2214102.html

7.3. Standards Support

DCE is the Open Group’s recommended standard for implementing, open distributed, heterogeneous, client-server environments. The following statement is taken from The Open Group’s Web site: “The Open Group's Distributed Computing Environment is the world's foremost technology that supports highly-secure distributed application processing, the secure implementation and integration of both critical client-server business and desktop platforms.

For more information on The Open Group’s DCE program and how it has evolved to the I/T DialTone Initiative, please check out http://www.camb.opengroup.org/tech/dce/

7.4. APIs

DCE is an environment for developing client-server applications in a way that the client can be anywhere in the network and the server likewise. The purpose of the standard is to have applications be implementable on and portable to any vendor’s platform that supports the DCE set of APIs. Consequently DCE may be looked upon from an application point of view as one huge API of which the security services are but a small piece.

Links to documentation on the complete DCE specification, including the security services APIs, may be found at http://www.camb.opengroup.org/tech/dce/info/docptrs.htm

8. Smart cards

8.1. Introduction

A smart card is a credit card-sized device that can be used to store a wide variety of applications because it contains an integrated circuit with secure memory and hardware support for security functions. The chip can be fed with data and a variety of application programs that can be updated whenever necessary. A high level of security protects the card issuer as well as the card holder from unauthorized access.

Typical applications are bank cards, travel cards and campus cards, used for electronic purses, personal identification, building access and prepayments.

8.2. Product Support

The IBM MultiFunction Card is an innovative smart card solution that opens up new horizons for the usage of smart cards. The IBM MFC Operating System is incorporated in sophisticated smart card chips, based on microprocessors with large memory and hardware support for security functions. The IBM MultiFunction Card with Public Key provides digital signatures and enables secure electronic commerce.

Combinations of different applications modules are built on these smart cards in response to the needs of the different industries. Many security services are included in these modules. Included are smart card holder verification through passwords; cryptographic authentication of the external world; card authentication to the external world based on symmetric and asymmetric algorithms; data integrity; data confidentiality and digital signatures.

Detailed information on IBM smart cards may be found at Web site: http://www.chipcard.ibm.com/

Security technology supported on IBM smart cards may be found in detail at Web site:
http://www.chipcard.ibm.com/overview/sc_2.htm#Security

8.3. Standards

The IBM MultiFunction Card complies with base standard ISO 7816 parts 1-9 and IBM continues to work with ISO on refinements to this base. The base standard deals with physical dimensions, interfaces and the Operating Systems. The standard allows for a range of functionality and method, thereby providing for industry freedom for applications.

Because of the freedom allowed by 7816, interoperability and portability of applications has become a concern and initiatives have been taken by a number of consortia in which IBM is active:

- Smart Card Forum, the primary vehicle for communication among the industry leaders in smart card research, development and use.
  Objective: to accelerate the widespread acceptance of multiple application smart card technology by bringing together, in open forum, the leading users and technologists from the public and private sectors. See http://www.smartcardforum.org/
- PC/SC Workgroup, lead by MicroSoft.
  Objective: standardize model for interfacing smart card readers and cards with PCs running Windows 95 /98 or NT (device independent drivers). See http://www.smartcardsys.com/
- Network Computer Reference Platform (NCRP), OpenCard Framework (OCF), lead by IBM.
  Objective: interoperability among major smart card companies, independent of smart card operating system, card data layout, or card reader terminal. Also to provide an OpenCard Framework for Java environments on NCs. See http://www.opencard.org/

- JavaCard Forum
  Objective: to influence the Sun JavaCard API which is a Worldwide standard for developing smart card based Java applications, enabling smart cards from one manufacturer to communicate with readers from another's. See http://java.sun.com:80/products/javacard/index.html

8.4. APIs

The consortia, listed above, are working on APIs. IBM is contributing to the work with the objective of compliance for application portability across different manufacturer smart cards and readers.

9. Antivirus and Immune System Technology

9.1. Introduction

Since their inception in the 1980's, computer viruses have grown into a persistent, worldwide threat. Today, there are more virus incidents than ever before, and new viruses are created at a record pace. With the rise of the Internet, viruses are likely to emerge and spread around the world more quickly than ever.

Viruses and software errors are among the leading causes of business disruptions and inadequate protection against them can bring a business to a standstill. Consider the following:

- On the average, six new viruses are created each day.
- Viruses are rarely isolated to a single PC as they spread through networks and diskette distribution.
- Instances of businesses infecting one another are on the rise.

Antivirus technology is expected to provide:

- Instant and automatic virus protection for all well known as well as unknown viruses.
- Fast reaction time to provide protection (real time immunity) for new viruses.
- Automatic checking of diskettes for "boot sector" viruses.
- Detection and disinfection of viruses with the touch of a button.
- Detection of viruses virtually free of false positives.
- Logging of all virus incidents for tracking and control.

4.2. Product Support

IBM AntiVirus is a comprehensive anti-virus product for all popular PC operating systems. It is designed to detect and remove viruses from your computer simply and reliably. It is the software that IBM uses to protect its own computers.

For companies dealing with completely **new** viruses for the first time, it may be critically important to respond quickly and effectively to prevent spread of the virus and possible shutdown of business. IBM has developed a solution to this problem, namely the new “Immune System for Cyberspace”. It is a worldwide distributed system that operates continuously, in real time, finding and curing new viruses faster than they can spread. Now in prototype, it is scheduled to become available to customers later in 1998.

For the first time, IBM can now detect previously unknown viruses on your PC, send them off safely over the Internet to the laboratory, where they are analyzed automatically and a cure crafted. When a new computer virus enters your organization, the immune system automatically captures it, removes it, and passes information about that virus to other copies of IBM AntiVirus so that it can be detected before being allowed to run elsewhere, all within minutes. The whole system is automatic, safe, and very fast.

Like the "innate" immune system, the computer immune system can combine self-knowledge (embodied for example in change detection and change analysis) with generic knowledge of broad classes of potential pathogens (embodied for example in static analysis based on viral machine-code features). These and other heuristics, some based on dynamic, behavior-based analysis, can be incorporated in a very natural way into an existing anti-virus product running on user's PCs.

For information on the features of IBM Antivirus, see http://www.av.ibm.com/IBMAntiVirus/Products/

For an introduction to the new immune system and for new release summaries, please look at http://www.av.ibm.com/current/FrontPage/

For a feature article on the new immune system, refer to http://www.av.ibm.com/current/CoverStory/

For a more in-depth discussion of the IBM Immune system, refer to the paper titled “Blueprint for a Computer Immune System” at
http://www.av.ibm.com/InsideTheLab/Bookshelf/ScientificPapers/Kephart/VB97/