IBM®

SecureWay

©1996 IBM Corporation

# IBM SecureWay Cryptographic Infrastructure

To enhance competitiveness in the global economy, modern businesses exploit computing technologies such as computers, networks and the necessary infrastructure to support reliable, secure business applications. This paper describes IBM's SecureWay cryptographic infrastructure, which helps applications insulate themselves from the underlying complexities of cryptography and allows application developers to exploit cryptographic functions within the larger programming environment in a consistent way.

## Introduction

Modern business exploits computing technologies to enhance competitiveness in the global economy. These technologies include computers, networks, and the necessary infrastructure to support reliable, secure business applications. In particular, business cannot function without security.

In this paper, the IBM SecureWay cryptographic infrastructure will be described. This infrastructure is part of the IBM SecureWay family of security offerings. SecureWay provides a common brand for IBM's broad portfolio of security hardware, software, consulting and services to help users secure their information technology.

The IBM SecureWay cryptographic infrastructure will help insulate the using applications from the underlying cryptographic complexities in a modular and extensible manner. Application developers will be able to exploit cryptographic functions within the larger programming environment, in a consistent way.

New commercial and business applications using network computing have dramatically emphasized the need for security in business transactions. In fact, the requirements go well beyond the encoding and decoding of business transactions, to functions such as user identification and authorization, access control to resources and services, confidentiality, data integrity, non-repudiation of transactions, and security management/audit. The science of cryptography provides the technologies to support these functions. IBM's support of these cryptographic functions is referred to as IBM’s cryptographic infrastructure.

The use of cryptographic services in I/T systems can occur at various levels, from the applications down to the cryptographic engines, depending on the degree of cryptographic "awareness" of the application - that is, the level of cryptographic functionality the application must know in order to meet its objectives. This suggests a layering of cryptographic functions, with the option for application access at whatever layer is appropriate.

Layering reduces the level of cryptographic awareness needed and increases the portability of applications through the use of standardized APIs. Cryptographic algorithms can be embedded into applications through the use of common libraries and toolkits. A layered approach helps identify and manage the infrastructure of supporting functions.

The identification and description of these layers, their implementation, use and management is necessary to fully communicate IBM's extensive support for cryptographic functions that help secure business applications.

Any layering approach will inevitably represent an oversimplification of the relative positioning and use of the various functions. However, a layered approach does communicate IBM's strategy to support additional functions in the layers and to include selected components into solutions. The complexity of using cryptographic functions is reduced while increasing flexibility in the choice of APIs and cryptographic engines.

## The IBM SecureWay cryptographic infrastructure

The IBM SecureWay cryptographic infrastructure is arranged into four conceptual layers, as shown.

Applications
..........................................................
Supporting Services and Sub-systems
..........................................................
APIs and Toolkits
..........................................................
Cryptographic engines

“Layers” are used to describe functions within a layer that are both complementary and related. Functions in one layer may exploit functions in any other layer. The layering is not rigid or insulated; functions may exploit other functions within the same layer. These functions are selectable and extensible, defining an open infrastructure with content driven by industry standards, where appropriate.

Functions, products, and services based on this infrastructure already exist and IBM will continue to extend its portfolio.

## The Layers - Introduction

The Application layer can use the Supporting Services or API layer directly, depending upon the level of cryptographic awareness required by the application. An example is electronic commerce applications over the Internet.

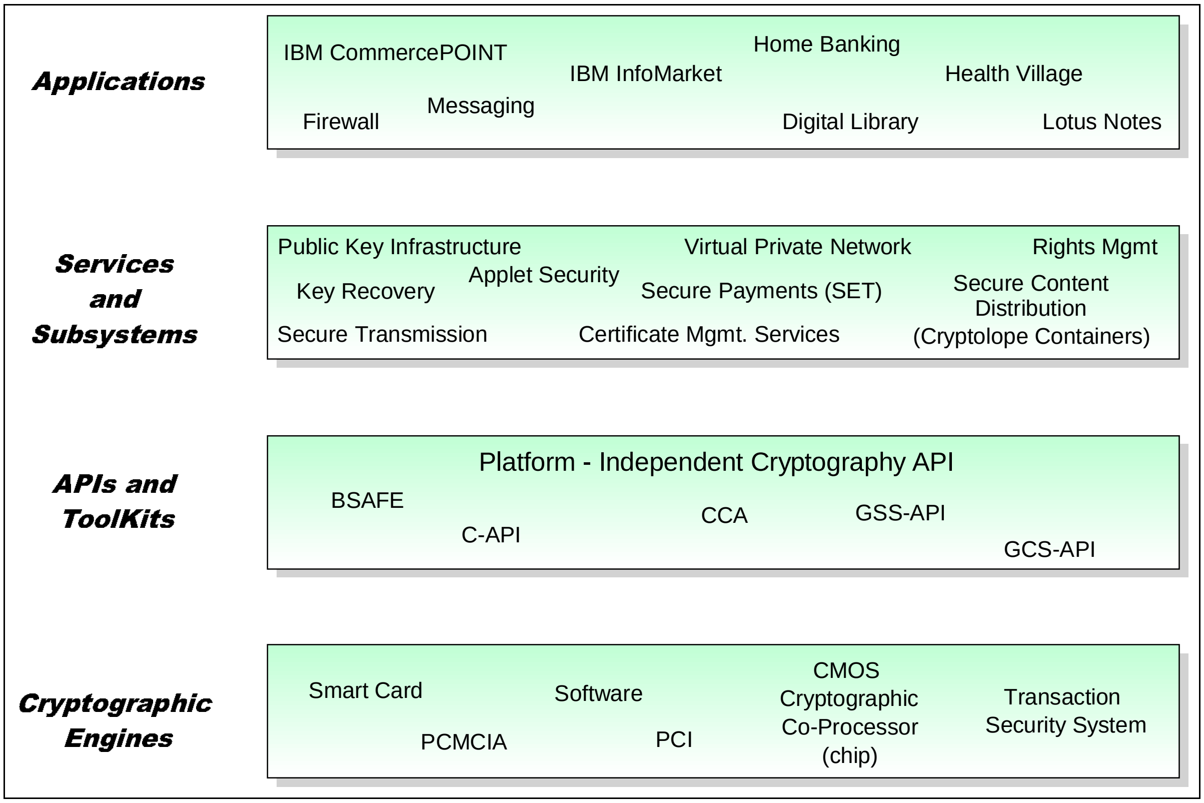
The Supporting Services and Sub-systems layer consists of an extensible set of services that invoke and exploit the APIs according to the level of cryptographic knowledge required by the service. These services facilitate the use of cryptographic functions by applications. An example is certificate management for public key infrastructures, consisting of a set of services used to generate, store, distribute, revoke, and renew certificates for other related applications.

The APIs and Toolkits layer consists of the industry-standard sets of calls to the underlying cryptographic engines or sets of linkable library routines that incorporate cryptographic algorithms into applications or supporting services. Regardless of the API set or cryptographic engine used for a given function, the functional results obtained will be the same, thus validating the modular mix/match suggested by the layered infrastructure.

The Cryptographic Engines layer is a common set of cryptographic functions, implemented across a variety of platforms. This set of functions is available in hardware or software. Hardware implementations have the advantage of superior speed of execution and resistance to tampering.

Some examples of this layer are integrated cryptographic co-processors, cryptographic adapters (add-on to any platform) and software routines.

## The Layers - Detail



## Applications

Networked business applications have exploited cryptographic capabilities to enhance security for years. Businesses are extending these applications to the Internet at a rapid rate.

The broad set of business applications that exploit the Internet are often referred to as e-commerce. Examples include Internet shopping, Internet banking, Internet information services and Internet-health related services. An overview of these e-commerce applications serves to illustrate how encryption services, APIs and cryptographic engines are all used by the application.

o *Internet Shopping Mall*

After browsing merchandise offered through the Web pages of a merchant at any convenient time and place, a user would select items to purchase. The user may select a credit card as the method of payment for the goods or services and the application invokes a secure payment cryptographic service using the industry-defined Secure Electronic Transaction (SET) protocols. The application would not have to be programmed at the cryptographic API level since that would be handled by the SET subsystem (see below under "Supporting Services and Sub-systems"). The cryptographic functions used would be invoked transparently between the communicating parties using the Protocol for Payment Negotiation (PPN). The added cryptographic value to the user is integrity and confidentiality of credit and payment information, plus verification of the merchant. The merchant can prove that the transaction occurred and that he will be paid.

o *Internet Banking*

Banking on the Internet is clearly an opportunity where proper security measures must be in place to protect the financial assets of the consumer and the corporate assets of the financial institution.

Consumers can be authorized to use these banking services through the use of certificate management services. These services provide the consumer and the browser application a certificate that would be used to authenticate the client, authorize the client to banking applications, and select the level of confidentiality and integrity appropriate to the application. Internet banking uses the Public Key Infrastructure services and the APIs and encryption algorithms below those services. All three levels of service will be transparent to the client application and the consumer.

o *IBM infoMarket Service*

IBM infoMarket Service addresses the need to control the distribution of information over the Internet and protect intellectual property rights. With the proliferation of search engines on the Internet, the challenge to users is to find those items of value and to pay for them, where appropriate. The challenge to publishers is to protect their intellectual property and to get paid for items ordered. IBM's infoMarket Service is an Internet-based content distribution utility for publishers who want to reach new customers, featuring security and copyright management, and allows for publisher control over content and pricing. Complete network and back-office support services are included. The IBM infoMarket Service provides compatibility with leading information storage and retrieval vendors. The use of encryption is transparent to the user.

o *Internet Health Care*

With an Internet-based health care system, patient records can be stored in a central location and accessed immediately by all properly authorized personnel required in the various processes. The information may be used by a primary care physician, by medical specialists, in the hospital and pharmacy and by the insurance company. Cryptographic functions, such as confidentiality, integrity, and authentication, are necessary and are invoked by the application, transparent to the users. Smart cards could also be incorporated, as a method of transporting patient medical records.

**Supporting Services and Sub-systems**

o *Key Recovery Services*

IBM is working on a solution to key recovery that will support all existing key distribution schemes and encryption algorithms. SecureWay key recovery technology will be a processwhich associates information with an encrypted message, perhaps as header information. Key recovery schemes could make use of underlying cryptographic functions and could extend already existing cryptographic APIs.

o *Secure Content Distribution (Cryptolope containers)*

The availability of the Internet has led to the proliferation of illegal copies of copyrighted, digital information. Software enforcement of copyright can be circumvented, posing the question of how to effectively protect the intellectual property of digital content owners. The IBM solution is to secure the content in a Cryptolope container. Cryptolope containers are advancing a new frontier in the world of electronic commerce.

Cryptolope containers feature advanced cryptographic enveloping technology, enabling businesses to penetrate new markets and launch themselves into the next century.

Cryptolope containers are based on a new packaging technology that enables and enhances electronic commerce on the Internet and communication within enterprises. A Cryptolope container is a sophisticated electronic package which holds an encrypted version of a text document or an electronic commodity, such as music, film, art, software, graphics and multi-media products.

Each container also has an abstract attached that describes its contents, their price (when applicable) and the terms and conditions for using the contents. While the contents are protected, the abstract is accessible. Cryptolope containers can only be opened using cryptographic keys which are provided to users who have purchased the contents.

Cryptolope containers protect copyrighted material on the Internet, directing the material to the authorized customer and providing a method for receiving payment for usage.

Cryptolope containers are digitally signed using RSA technology to identify the originator of the contents and to protect against alteration during transmission. DES is used for encryption, decryption, and key generation.

Cryptolope containers are deployed today in IBM's infoMarket Service. IBM is exploring the use of Cryptolope containers in multiple applications, including direct marketing, software distribution, electronic document delivery, and entertainment applications.

o *Virtual Private Network*

Businesses want to communicate with partners and suppliers over the Internet. This creates a concern for how to keep information confidential while flowing over a public network. The IBM firewall brings the capability of having a virtual private network, which can address this concern. Even though the traffic travels over the Internet you can still have confidential communications.

The firewall encrypts Internet Protocol (IP) packets, creating a private IP tunnel to transfer data. This process, called tunneling, provides data integrity, authentication, and confidentiality as the data flows across a public network between two firewalls that support the Internet Engineering Task Force IPsec specifications.

o *Applet Security*

The growing popularity of the Internet has led to a frenzy of development on the World Wide Web. Most noted of such developments has been the introduction by SUN Microsystems of the popular capability to download applications that run transparently inside the Web browser. The language used is Java and the downloaded applications are known as applets. The browser has no control over or knowledge of the applet contents. If the user is security-aware, he/she may be obliged to treat each applet as a potential virus, trojan horse, worm or simply a badly behaving program with respect to resource consumption. This realization has generated activity to address the pressing question of Java security, since Java’s popularity is widely expanding and is commonly used as the language for Web page executables and other e-commerce executables.

IBM has activities underway in the areas of: cryptographic services for Java applets, code signing combined with applet resource credentials, access control, and identification and authentication of applets. IBM intends to work openly with industry to share the results of these research activities.

o *Certificate management*

Distributed computing in a commercial context nearly always involves the exchange of information and execution of transactions that have value and need to be protected. Confidentiality, integrity and especially the authenticity of the unseen communication partners all

become important requirements. How is such electronic business conducted with the same degree of confidence as face-to-face business? The need to provide secure communications across public networks is a top priority for businesses in this environment.
The IBM Public Key Infrastructure will supply the technology to create, publish, maintain, revoke and renew digital certificates and to distribute them to various destinations, such as web browsers and smart cards. It supports authentication, encryption, digital signature and access control operations using the certificate contents. It also provides a communications transport that enables client and server applications to exploit protected communications over public or private networks. The certificate management services available with IBM's PKI shows how cryptographic functions and APIs can be applied without user knowledge of the details.

To further address this need, IBM is working with Nortel's Entrust technology to define and implement the infrastructure needed to ensure that digital identities can be created and used in electronic commerce applications.

Identities are issued by a trusted authority and are represented by a "certificate" that includes standard information such as a public key, a globally accessible name, expiration dates, and application-unique information such as a title, a degree earned, a license owned, and job responsibility. This certificate is digitally signed by the trusted authority, known as a certificate authority. The certificate authority validates information in the certificate and signs it thereby validating the authenticity of the information signed.

o *SET*

MasterCard International, Visa International and their technology partners have published a specification that details how bankcard transactions on the Internet and other open networks will be secured using encryption technology. The use of Secure Electronic Transactions (SET), is expected to accelerate development of electronic commerce and bolster consumer confidence in the security of cyberspace transactions.

SET provides a mechanism for automatically routing payment information among users, merchants, and their banks. SET provides a foundation for creating client and server applications that can transmit encrypted credit card information without the applications dealing with the underlying cryptographic APIs.

IBM was a key contributor to the design of SET and is supporting SET for consumer payment (using a browser like Netscape), in its Merchant Server (Net.Commerce Payment Manager), and in a new Payment Gateway, which connects the consumer/merchant to the financial institution for payment.

## APIs and Toolkits

### o *Platform-Independent Cryptography API (PICA)*

The Platform-Independent Cryptography API (PICA) builds on the Public Key Cryptography Standards (PKCS) process and technology submissions from several other companies. PICA's goal is to allow developers to introduce open, cross-platform security and cryptographic functions to applications regardless of the platform on which they reside. PICA should also make the task of developing differing domestic and exportable security requirements much easier.

### o *Common Cryptographic Architecture (CCA)*

The IBM Common Cryptographic Architecture (CCA) is a cryptographic API for secret key algorithms (DES) and public key algorithms (RSA). It provides services for data privacy, data integrity, key generation, distribution, and installation and Personal Identification Number (PIN) processing using the Data Encryption Standard (DES). It also supports digital signature generation and verification and distribution of Data Encryption Algorithm (DEA) key encrypting keys using the RSA algorithm. The architecture provides interoperability between products that are compliant, regardless of platform. CCA is designed for use within most standard programming languages.

CCA provides advanced key management through the use of control vector technology. Control vectors are non-secret quantities cryptographically bound to the key, providing key separation and limiting the valid uses of the key.
The CCA API provides a common set of services for cryptographically-aware applications to exploit without knowledge of the underlying cryptographic engines.

### o *BSAFE*

BSAFE is RSA's portable C programming toolkit that provides re-entrant, linkable code that supports a complete palette of the most popular cryptographic and hashing algorithms and a random number generator. BSAFE provides an API into encryption engines without the application programmer having to access the APIs. BSAFE supports many standards including the PKCS series - the Public Key interoperability specification - including PKCS #11, which is oriented to portable "tokens" (PC Cards or Smart Cards). BSAFE simplifies the integration into any C program state-of-the-art confidentiality and authentication features. BSAFE is licensed for use by a large number of vendors, including IBM. IBM and RSA announced plans for BSAFE to exploit the CCA API. IBM is ensuring that when its hardware cryptographic engines are present, they will be chosen by BSAFE over software implementations.

### o *Generic Security Services API (GSS-API)*

GSS-API is a session-oriented interface developed by the Internet Engineering Task Force (IETF) in conjunction with X/Open (now the Open Group) to facilitate the secure communication in a client/server environment. Its objective is to isolate the calling program from the security mechanisms being invoked.

The GSS-API includes support for mutual authentication and the establishment of appropriate levels of message confidentiality and integrity. IBM supports GSS-API through its various DCE deliverables. The advantage of using the GSS-API is the low level of security awareness required of the application program.

o *Generic Cryptographic Services (GCS-API)*

GCS-API is a generic, comprehensive, algorithm-independent, cryptographic API, produced by the Open Group's Security Working group (together with NIST and NSA) and is being designed to provide convergence on a single, multi-vendor standard.

o *Microsoft Crypto API (C-API)*

Microsoft’s C-API provides extensible, exportable, system-level access to common cryptographic functions such as encryption, hashing and digital signatures. Microsoft’s C-API requires a Cryptographic Service Provider (CSP) to implement cryptographic algorithms.

Cryptographic APIs/toolkits will be supported within the SecureWay cryptographic infrastructure as they appear in the industry and are required by customers.

## Cryptographic Engines

o *Smart Cards*

Smart cards will play an important role in cryptography because they are tamper resistant, cost effective, and a simple means by which a user can be authenticated across an insecure network.

Smart cards can enhance the Secure Electronic Transaction protocol (SET) by storing user certificates. This would mean that a SET-enabled smart card could be used in a secure browser equipped with an appropriate reader, increasing security and mobility by allowing SET transactions from a number of sources, in addition to the user's "home" workstation.

Smart cards can provide these services because they contain a microprocessor and a tamper-resistant enclosure that can securely store cryptographic keys, certificates, and other data. Operations can be performed on the data within the secure boundary. An example of such a smart card is IBM's MultiFunction Card (MFC). The MFC can separate and protect the data required by multiple applications on the same card and secure network transactions.

An example smart card application is for a single card to be used to access, reserve, and pay for travel and entertainment. This same card could store user preferences to be used by the application. Tickets and any loyalty schemes (e.g., frequent flyer miles) could be downloaded directly to the same smart card. This card would be presented at the airport during travel and would contain any necessary travel documents including the user's passport, credit, and debit cards.

IBM Smart Consumer Services leverage IBM experience in I/T to deliver end-to-end solutions. Smart Consumer Services are available from IBM now. The services consist of management consultancy, feasibility/business case analysis, design, development and card creation, management and administration, together with the prerequisite readers and modules. Applications have been delivered and others are under development for availability later.

o Workstation Interface Adapters

IBM is developing a PCI-based cryptographic co-processor. The co-processor has a general purpose PC-compatible subsystem, random number generator, and cryptographic functions, all inside a tamper-responding enclosure. The device will support high-speed cryptographic operations and will provide a protected environment for sensitive applications and data. IBM's plan is to include a rich set of data privacy and authentication functions in the initial PCI offering, including DES and CDMF encryption, ANSI message authentication, RSA digital signature generation and verification and key distribution. The hardware will be designed to meet the Federal Information Processing Standard 140-1 level 3. A PCMCIA (laptop) version is under consideration.

o *S/390 Integrated Cryptographic Co-processor Feature*

The IBM Integrated Cryptographic Co-processor Feature (packaged as a single CMOS chip), together with the Integrated Cryptographic Service Facility (ICSF), will provide the ability to support high-volume cryptographic transaction rates and bulk data security requirements. The programming interface to use the facilities conforms to the Common Cryptographic Architecture (CCA) and allows interoperability with other conforming systems. The cryptographic co-processor provides facilities for public and private key encryption (DES, CDMF, and RSA), hashing algorithms, digital signature, and key management.

o *Transaction Security System (TSS)*

The IBM Transaction Security System range of products and services provides comprehensive support for DES and RSA based cryptographic processing. The system uses the Common Cryptographic Architecture (CCA), described above, for interoperability across all the workstation and host environments.

The IBM 4755 Cryptographic adapter provides the DES and RSA based cryptographic processing for use with DOS, OS/2, AIX and OS/400 environments. The IBM 4754 Security Interface Unit, together with the IBM Personal Security card, supports strong authentication of users, optionally using a Signature Verification feature, and supports encryption on the smart card as an alternative encryption source. The IBM 4753 network security processor provides the cryptographic services for the MVS host environment.

## Conclusion

The IBM SecureWay cryptographic infrastructure provides a comprehensive set of cryptographic engines, Cryptographic APIs and toolkits, and cryptographic services and subsystems that facilitate the development of cryptographically enabled applications. IBM has developed and will continue to develop many applications which will exploit this infrastructure.

This infrastructure is open, supports industry and defacto standards, and provides a choice of APIs, toolkits, and services. It can be extended as new cryptographic engines, toolkits, and APIs evolve.

A total cryptographic function set is provided, supporting the many aspects of security across the IBM product line. Through the supporting services, the infrastructure can provide a cryptographic programming environment, which can be inserted into the broader business environment of object technologies and program development aids. The implied consistency helps with validation and scenario checking. The infrastructure provides a cryptographic product and services roadmap, allowing ISVs and end users alike to anticipate cryptographic extensions and enhancements.

By exploiting these four layers of cryptographic functions, APIs, services and applications across a variety of hardware and software platforms, businesses can build and extend applications. Businesses must be confident that they can fully and efficiently secure their applications in a consistent manner, independent of the platform used to provide the services and of the APIs most appropriate to those applications. In a larger security context, the IBM SecureWay cryptographic infrastructure provides the cryptographic services for the IBM SecureWay architecture.

This infrastructure enables consistency, choice, full function, high performance and simplicity to the high level of security required for today's business applications.

For more information on the cryptographic infrastructure, the SecureWay architecture, or any of IBM's SecureWay offerings, visit our homepage at http://www.ibm.com/security.

The following are trademarks or registered trademarks of International Business Machines Corporation: AIX, CommercePOINT, Cryptolope, HealthVillage, IBM, OS/2, OS/400, and SecureWay.

All other products or company names may be trademarks or registered trademarks of their respective companies.