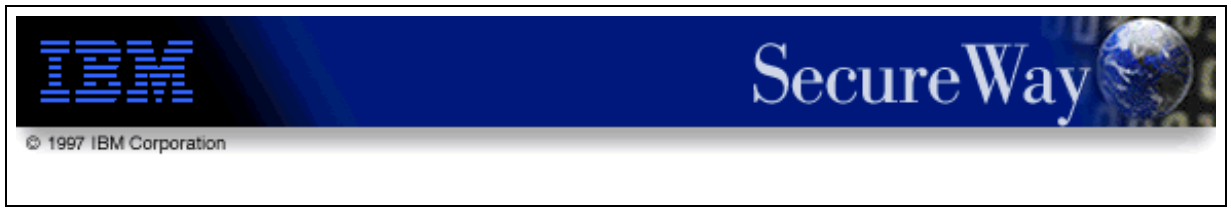

IBM SecureWay Key Recovery Technology

To compete in the rapidly emerging global economy, business and commerce require strong encryption schemes, available on an international basis, to protect the confidentiality and integrity of business transactions and electronic commerce. The IBM SecureWay key recovery technology operates in conjunction with the SecureWay Key Management Framework previously announced. IBM SecureWay key recovery technology is part of the broad IBM SecureWay portfolio of security hardware and software products, solutions, services, consulting and research activities. The SecureWay brand provides end-to-end security solutions for customers such as cryptographic facilities, single sign-on, distributed security administration, access control, firewalls, secure web servers and browsers, secure electronic commerce, smart cards, anti-virus and overall internet security.

Introduction

By taking advantage of the Global Information Infrastructure, businesses depend increasingly on networking technologies for communication with business partners and customers. Electronic communication enhances business competitiveness through more efficient, faster and cheaper business interactions. Businesses must safeguard sensitive information in transit to prevent loss of trade secrets, protect revenue, and maintain competitive advantage.
Information is a vital corporate asset. Cryptography has emerged as one of the most effective means of securing the transmission or storage of information. Cryptography, the science of 'secret writing', was once the exclusive domain of governments, protecting national security. Now, commercial cryptography applies not only to the encryption/decryption of business information, but to the other areas of information security, such as user authentication, data confidentiality, data integrity, and non-repudiation.

Cryptographic functions convert plaintext information into encrypted text, under the control of cryptographic **keys**. In most commercial cryptography, the algorithms are known and published, such as the Data Encryption Standard (DES). Anyone with the key can convert the encrypted text back into plaintext. For this reason, cryptographic keys must be secured and protected. On the other hand, the key must be readily available to authorized parties. Keys must be both secured and selectively available.

Information Recovery

Key management techniques exist to manage the lifecycle of cryptographic keys, such as creation, distribution, validation, update, storage, usage, and expiration. If keys are ever destroyed or rendered unavailable to authorized parties, then "information recovery" techniques are applied to reproduce the key and recover the encrypted information. Such techniques are an integral aspect of key management. (see the IBM Key Management Framework white paper at http://www.ibm.com/security).

Several techniques have been proposed to provide for information recovery.

Key escrow means that the key or key parts are distributed to key escrow agent(s) for storage. Information recovery using a key escrow system requires the key escrow agent(s) to provide the necessary key or key parts to recover the key. For example, the National Security Agency's Clipper microchip requires key escrow and two government key escrow agents. Authorized "eavesdroppers" to the encrypted communication would subpoena the
key parts from the government key escrow agents, recover the key, and intercept/decrypt the communication.

Trusted Third Party (TTP) means that a third party to the cryptographic application actually creates and provides the cryptographic keys to the participants, storing a copy for future key retrieval.

The **disadvantages** and limitations of both escrow and TTP schemes for information recovery include:

- o single point of vulnerability/compromise
- o poor scaleability
- o loss of control over key management
- o distrust
- o high entry cost

Scaleability is affected since communication with a third party is required for each session/archive key initiation. Distrust results from the fact that control of information recovery belongs to a single **jurisdiction** (government, country, company, etc).

Escrow and TTP schemes have already been implemented and both schemes are applicable in certain environments. The user simply needs to be aware of the inherent limitations of escrow and TTP schemes.

This paper introduces the IBM SecureWay key recovery technology that resolves these and other issues related to escrow and TTP information recovery schemes.

Cryptographic Schemes Supported

Cryptographic schemes in use today are either **symmetric** (sometimes called shared or secret) key or **public** (sometimes called asymmetric) key.

Symmetric-key cryptography uses the same, secret key for encryption (sender) as for decryption (receiver). Since the algorithm for the cryptographic function is known (at least for 'commercial' cryptography), security for symmetric-key cryptography depends on keeping the shared/private key secret. At present, symmetric-key schemes are more computationally efficient and are better suited for data confidentiality with bulk data and large volume traffic. Examples of symmetric-key schemes in use today include:

- o Data Encryption Standard (DES) and Triple DES
- o International Data Encryption Algorithm (IDEA)
- o Rivest Cipher (RC-4)

Public-key cryptography uses different keys for encryption and decryption. One key is kept private while the other, the public key, can be generally known and even published and circulated. The private key cannot be deduced from the public key, even though both are mathematically related. The elegance of public-key cryptography lies in the fact that no a priori secure

communication is needed to exchange a secret key. The respective public keys can be exchanged 'publicly' and secure communication can begin. Recipients of encrypted text simply apply their private keys to decrypt the message.

Public-key cryptography is best suited for authentication, symmetric (DES) key distribution, and for applications that require communications between many pairs of users . RSA (Rivest, Shamir, and Adleman) is the best-known and most widely-used public-key scheme. Diffie-Hellman (named for the inventors of the public-key concept) is another popular scheme that is used to create a common, shared secret between two or more parties.
For both symmetric- and public-key cryptography, the private/secret key information must be securely created, securely transmitted to all necessary parties, carefully managed and securely stored. The IBM SecureWay key recovery technology is independent of these other aspects of key management and of the particular cryptographic scheme employed, allowing for a smooth migration to a recovery-conscious environment.

The next sections describe the IBM SecureWay key recovery technology in more detail.

The Problem

Modern, cryptographic schemes are well-founded in concepts from the mathematical theory of computational complexity; that is, if the symmetric or private key is destroyed or unavailable, then no one, not even the original designer, can unravel the encrypted text. The information is lost. Key management techniques are an essential supplement to cryptographic schemes, because the key is the most sensitive piece of cryptographic data.

National security concerns demand that, in certain circumstances, encrypted messages flowing across international boundaries be intercepted, subject to the constraints of due process and the law. In this scenario, possessing the encrypted message but not the key is equivalent to the "destroyed key" scenario. In both cases, the fundamental problem is the **inaccessibility of encrypted information.**

There exists a commercial, national security, and law enforcement need for information recovery techniques.

Since World War II, the United States government has responded to the national security scenario by restricting the strength of cryptographic schemes that can be exported. The natural assumption is that weaker strength implies that the unknown key can be recovered or discovered through "brute force" and/or trial-and-error search techniques. Since one measure of cryptographic strength is "key length" in binary bits, the export restrictions limit key length.

In order to compete in the rapidly emerging global economy, business and commerce require strong encryption schemes, available on an international basis, to protect the confidentiality and integrity of business transactions and electronic commerce. In fact, since success of its international trade and commerce help define a country to the rest of the world, strong encryption

schemes will become a commercial element of “national defense”. The challenge is to harmonize international business competitiveness with the legitimate needs of law enforcement and national security.

A solution to the problem lies in extending key management functions to include “information recovery” techniques, without diminishing the original cryptographic strengths.

In fact, the U. S. government has recently announced potential relaxation in the export restrictions on strong cryptography, if “acceptable” information recovery techniques are implemented. IBM recently spearheaded the establishment of a Key Recovery Alliance of over 40 companies worldwide. The goal of the Alliance is to facilitate the legitimate recovery of encrypted information on a global basis.

Information Recovery Requirements

The discussion above suggests the following requirements for information recovery:

- low overhead
- self-contained/modular
- applicable to all cryptographic schemes
- scalable
- process integrity checks
- interoperable
- hardware or software implementation

Note that two distinct stages to information recovery exist:

- **preparation** of information needed to recover the key

- **recovery** of the key from this information, sometime in the indefinite future

Requirements can also be derived by viewing information recovery in the larger context of a security infrastructure on a global basis. In order to **scale** to the dimensions of the envisioned Global Information Infrastructure, information recovery must be optimized in performance and required overhead. The information recovery preparation stage will be invoked many more times than the recovery stage, so performance/overhead should be minimized during preparation. For example, the information recovery function should not require communication with an outside entity during setup or message encryption within the cryptographic application (adds overhead and inhibits scaleability). Other aspects of **modularity** require that information recovery must be **interoperable** with all cryptographic and key management schemes and with non recovery-conscious environments.

While the preparation stage addresses low overhead and modularity, the recovery stage must emphasize invincibility and immunity to cryptanalytic attack. For example, to promote confidence

and rapid acceptance, information recovery should be built from time-tested and off-the-shelf technologies; avoiding secret algorithms or unproven assumptions. Such standard techniques include cryptographic "dispersion" and "residual work factor".

Dispersion refers to the requirement that unanimous participation by multiple, designated entities be an essential step in information recovery. For this reason, the output of the information recovery preparation stage should be multiple pieces of information, each piece of information associated with an independent and trusted entity. Note that this information is 'associated' with the designated entities, but not physically passed to those entities, in order to preserve modularity and self-containment. Modularity allows the preparation stage to be added to existing cryptographic applications with minimal effort and self-containment reduces the infrastructure overhead required to support information recovery.

This (implicit) dispersion enhances the security of information recovery and thwarts collusion among the trusted entities. A stronger requirement is that information recovery be collusion resistant: participation by the dispersed entities is necessary for information recovery, but even their collusion is not sufficient ("dispersion without collusion"). Further, this recovery information should not be parts of the original key, but should include abstract parameters that are cryptographically derived from the key, using shuffling, hashing, padding and other well-known cryptographic techniques. In that way, no keys are exposed outside the cryptographic facility.

A **residual work factor** allows the communicating parties to retain a variable amount of information needed for information recovery, which must then be recovered through cooperation or trial-and-error techniques. A residual work factor option can be used to increase the overall work effort involved in recovery, to discourage 'casual' recovery requests and to keep part of the overall security of information recovery in the hands of the user. Use of the residual work factor is optional, depending on user or regulatory requirements.

Inherent **process integrity checks** should be built into the information recovery technology so that both users and observers can ascertain that the technology is being correctly invoked. The moment of information recovery is too late to learn that the information recovery technology has been improperly applied or bypassed. The process integrity checks guarantee that information recovery preparation has not been circumvented.

Since the communicating parties originally know the key, these parties can be **pre-authorized** to invoke information recovery, if necessary, to recover destroyed or mis-managed keys. This pre-authorization should be embedded in the preparation and recovery processes.

Information recovery should be possible in either hardware or software implementations, since all manner of inexpensive device will be employed for secure commmunications. Information recovery or security in general should not present a prohibitive cost factor.

Most importantly, information recovery should be adaptable to the regulations governing use of cryptography in a particular jurisdiction. Information recovery must be possible in each

jurisdiction involved in the cryptographic exchange, not just one of the jurisdictions. Any security infrastructure must span the globe, since business and trade are multi-national in scope.

IBM SecureWay Key Recovery Technology

In the following sections, several levels of detail behind the technology will be provided.

Technology Overview

The basic idea of the IBM SecureWay key recovery technology is that certain parameters **(recovery information)** are associated with the encrypted message or data file, either as header extensions or an appended file. Because this information remains with the encrypted message/file, no communication with an outside entity or agent is required. Later, this recovery information can be used to recover the key.

Key recovery service providers (trusted "dispersion points") are designated in each country or jurisdiction supporting the technology. These service providers can be private or governmental entities, or a combination of both, depending on the dictates of the jurisdiction. The number of service providers is independently selectable in each jurisdiction. Selection criteria, licensing, and approval for key recovery service providers can be jurisdiction-specific.

For each communication or archiving scenario eligible for key recovery, a subset of the key recovery service providers in a given jurisdiction is selected. Each key recovery service provider has a public-key key pair independently of each other and of the original cryptographic application. The key recovery service providers are responsible for securing the private key of their public-key key pair.

The IBM SecureWay key recovery technology uses the public keys of the selected key recovery service providers to encrypt part of the recovery information placed in the header or associated file. The recovery information also contains administrative and identifier information for the key recovery environment. The only contact with the service providers occurs when a key recovery operation is needed. The service provider is asked to apply its private key to decrypt the encrypted piece of recovery information associated with that service provider. After all the key recovery service providers have decrypted their respective piece of recovery information, the key recovery preparation process is then executed in reverse order to recover the original key.

All the selected key recovery service providers in a given jurisdiction are needed to recover the key. No "partial" recovery is possible if a subset of the key recovery service providers are compromised. More importantly, the information recovered by the service providers is necessary for key recovery, but not sufficient. IBM SecureWay key recovery technology is collusion resistant.

The **high-level flow** of the IBM SecureWay key recovery technology is as follows:

1) Select a subset of the key recovery service providers in each jurisdiction

2) **Phase 1**: Prepare recovery information using the public keys of the selected key recovery service providers

3) Select an encryption algorithm and a session/archive key (session: interactive or store/forward)

4) Select and encrypt a message/file

5) **Phase 2**: Prepare recovery information based on the selected session/archive key. Optionally, a piece of recovery information is withheld for either/both ends of the communication, thus creating a residual work factor for key recovery

6) Place the two-phase recovery information in the header or extended file of the encrypted message/file

7) Transmit

Note: Phase 1 is independent of the particular session/archive key.

The recovery information also contains administrative information that is useful if and when key recovery is necessary and authorized; for example:

- Sender/Receiver IDs (optional)
- Sender/Receiver Jurisdiction of Origin IDs
- Key recovery service provider IDs for both the sending and receiving jurisdictions
- ID of the message
- time period during which key is valid
- date and time of the message
- cryptographic algorithm used to encrypt the message

The key recovery process is an add-on to existing encryption schemes and can be invoked by any cryptographic application. Key recovery support could be either optional or mandatory, depending on the jurisdictional requirements.

IBM SecureWay key recovery technology is flexible and can support the regulations of the jurisdictions or corporations involved in the cryptographic communication. For example, the encrypted message may be transmitted between two different countries, each having different restrictions on the deployment of cryptography. However, appropriately authorized persons in either country have equivalent key recovery capability. A critical attribute of the IBM SecureWay key recovery technology is that recovery can be invoked in either the sending or receiving country

independently. Export/import and cryptographic usage restrictions in each country can be addressed.

Another valuable property of the IBM SecureWay key recovery technology is that either communicating party can optionally withhold a variable amount of recovery information. The recovery information is still calculated and associated with the encrypted message. However, any authorized attempt at key recovery would require an extra step using trial-and-error techniques (or cooperation) to complete the recovery. The withheld information is abstract and internal to the preparation stage (not just part of the original key), so that no pre-computation can be applied before the recovery request to reduce the trial-and-error search space. This option is selectable independently for the sending and receiving jurisdictions. The value of this option, if selected, is that even an authorized key recovery operation faces a "residual work factor".

For example, consider a country where the restriction on key length for exported cryptographic products is 40 bits. Consider using a stronger cryptographic algorithm (key length at least 56 bits), but setting the residual work factor to 40 bits. Any authorized key recovery requester can use the key recovery service provider information to reduce the effective key length to 40 bits. Only those authorized requesters with the computational ability to search through 40-bit key space using trial-and-error can complete the key recovery.

IBM SecureWay key recovery technology operates in concert with any existing, published encryption algorithms. Contact with an escrow agent or third party is not required. Any key creation and management approach can be used, along with existing mechanisms to distribute keys.
An authorized recovery request together with recovery information is presented to the key recovery service providers, who decrypt their associated pieces of information. The key recovery preparation process is reversed, which may require a trial-and-error search for the withheld piece of recovery information. The key is recovered.

Implementation Details

In order to minimize the preparation overhead, the recovery information is prepared in two phases: one phase is independent of the particular session/archive key being prepared; the second phase is dependent on the particular key and session parameters. The first phase, which uses public-key encryption, can be shared across multiple invocations of key recovery preparation, thus reducing overhead. The public-key encryptions can be stored for repeated use.

The public key encryptions are **not** applied to the original key or key parts. Rather, a **random** number (one random number per each selected key recovery service provider in each jurisdiction) is encrypted using the public-key of the respective service provider (Phase 1). These public-key encrypted values are independent of the session/archive key being prepared. These indexed random numbers, one per service provider, serve as starting points in a process that determines the remainder of the recovery information (Phase 2). Several methods for creating these indexed random numbers will be described below.

For Phase 2, any fast/convenient/strong symmetric encryption algorithm is selected. This could be the original encryption algorithm or an independent selection. The indexed random numbers from Phase 1 are used as input to a process that generates a secondary set of parameters. Using the selected, symmetric encryption algorithm, the secondary parameters are used as keys to encrypt the original session/archive key in nested order. All the secondary parameters/keys associated with the selected service providers per jurisdiction are used. The nested encryptions, one per jurisdiction, become part of the session-specific recovery information in Phase 2. Later, key recovery requires that the nested encryption in either jurisdiction be undone in reverse order to recover the session/archive key.

Therefore, the recovery information consists of two parts:

o Phase 1: the public-key encrypted random numbers associated/indexed with each selected service provider

o Phase 2: the nested, symmetric encryptions associated with each jurisdiction, using secondary parameters/keys derived from the indexed random numbers (plus administrative and identifying information).

For key recovery, **only** the public-key encrypted, indexed random numbers from Phase 1 are provided to the service providers in a given jurisdiction. Each service provider internally decrypts the random number, re-calculates the derived secondary parameter/key, and returns this key to the authorized requester. The indexed random number is not returned.

With the returned secondary keys, the authorized requester applies nested decryptions to the Phase 2 recovery information in the appropriate order to recover the original session/archive key.

Without the intercepted, nested encryption (which is **not** given to the service providers), *the service providers cannot recover the session/archive key.* The role of the service providers is essential to recovery, but is independent of the session/archive key. IBM SecureWay key recovery technology is collusion resistant.

At the same time that the two-part recovery information is being calculated, optional pre-authorization information can be calculated in a similar fashion and added to the recovery information. The original participants have exclusive knowledge of the pre-authorization information, in case the participants later require recovery of a destroyed key.

The duties of the key recovery service providers are two-fold:

o Select a public/private key pair and provide the public key, holding the private key in secret.

o When requested and authorized, apply the private-key decryption to the encrypted recovery information provided by the requesting authority. From the (indexed) random number decrypted, calculate the secondary parameter/key, which is then returned to the requesting authority.

Only one contingent of key recovery service providers (either jurisdiction, either end) is needed to recover the key. Key recovery can be invoked in either jurisdiction, abiding by the rules and regulations of that jurisdiction.

Jurisdiction Table

The IBM SecureWay key recovery technology allows for flexibility in the selection of the encryption and recovery variables. This information is stored in a table called the **jurisdiction table**. The table contains key recovery rules and restrictions for different jurisdictions and different algorithms. The information includes such things as:

- Specific cryptographic algorithm allowed (DES, RSA, etc.)
- Key length restrictions
- Public keys of the key recovery service providers
- Length of the user-withheld information (if allowed)

The relevant information in the jurisdiction table must be made available to the communicating parties, either through pre-configuration or access to a repository.

Process Integrity Check Variations

Given that the encrypted exchange originates from one end of the communication, the recovery information is calculated and installed as a header extension or file attachment by that end. In order for the other end to confirm that the recovery information has been correctly calculated, the same parameters used to calculate the two-part recovery information are needed; in particular, the indexed random numbers used to derive the sequence of secondary keys.

One variation has the two correspondents secretly exchange a random seed value that is then used to pseudorandomly derive the indexed random numbers. In this way, both correspondents have the same information and the recovery information can be validated by the receiving end.

In order to eliminate the secret exchange of a random seed value and to make the indexed random numbers “self-validating”, consider the following preferred variation.

Recall that the Diffie-Hellman scheme uses public-key cryptography to create a secret, shared parameter between two correspondents without resorting to a secret exchange. Use a three-way (sender/receiver/agent) Diffie-Hellman scheme to “exchange” the indexed random numbers needed in calculating the first part of the recovery information. Since the Diffie-Hellman scheme is a public-key scheme, its output also replaces the public-key encryptions required in Phase 1. The a priori secret exchange of a random seed is no longer needed.

By virtue of the Diffie-Hellman scheme, the receiving end is now able to decrypt the Phase 1 information and thus retrieve the indexed random numbers used in Phase 2. The indexed random numbers are “self-validating” because the Phase 1 calculations are covered by a Message

Authentication Code (MAC), which is a standard means of providing data integrity. The indexed random numbers need not be previously created at the receiving end, but instead are decrypted and self-validated directly from the Phase 1 information.

Under this preferred variation, the original session/archive key could also be "exchanged" using the Diffie-Hellman scheme.

Another advantage of this variation is that the Diffie-Hellman scheme is the basis for **elliptic curve** public-key cryptography. Simply put, elliptic curve schemes result from changing the algebraic structures being used; namely, from modular arithmetic to points on an elliptic curve. The advantage of elliptic curve schemes is that the computational overhead is significantly reduced without reducing the level of security provided.

In summary, the advantages of the preferred elliptic curve variation include:

o no a priori random number or random seed exchange

o indexed random numbers are self-validating

o performance boost in the public-key calculations

o option for Diffie-Hellman exchange of the session/archive key

Comparison to Alternatives

Three major approaches to 'information recovery' have been proposed thus far in an effort to satisfy the needs of the private and commercial sector for confidentiality, the needs of the government to protect national security, and the needs of legitimate law enforcement.

Key Escrow

Key escrow actually stores (escrows) the key directly with "escrow agents". The key can be split into two or more parts, with each part stored with a separate escrow agent. Law enforcement agencies solicit court orders to collect the key or key parts from escrow agents and combine them to recover the key. With the key, the message traffic can be decrypted.

Commercial concerns over key escrow schemes have been expressed in the professional literature and by trade organizations. The actual (split) key is escrowed, providing opportunity to compromise the key. There is overhead associated with sending all (session) encryption keys to key escrow agents. There are expense and administrative concerns associated with the storage of so many keys. Also, key escrow schemes are centered on a single jurisdiction and do not support multi-jurisdiction key retrieval without additional overhead.

Trusted Third Party

In a Trusted Third Party approach (TTP), both corporations and governments allow an impartial "trusted" party to issue keys. The “trusted” party also stores a copy of the key for recovery in the future. Information recovery consists of re-requesting the key from the TTP. For example, a postal service could provide encryption keys for secure e-mail applications. A charge card provider could provide encryption keys for electronic shopping applications. Concerns regarding TTP center on the high potential for compromise of the TTP, which represents a single point of attack. Also, an infrastructure is required that connects all users to the TTP in order to generate and distribute user keys. Key storage costs at the TTP are an additional concern.

IBM SecureWay Key Recovery Technology

The session/archive key is never stored or escrowed with an outside party. Instead, recovery information is associated with the encrypted message/file, supporting key recovery at a later time. Key recovery can also be used when encrypting data for archive purposes.

Key recovery is supported within and across multiple jurisdictions, subject to the restrictions and policies of each jurisdiction.

IBM SecureWay key recovery technology has no single point of attack as long as two or more key recovery service providers are designated in each jurisdiction.

Minimal overhead is incurred during normal operations.

IBM SecureWay Key Recovery Technology: Advantages

The IBM SecureWay key recovery technology provides for the recovery of forgotten, damaged, or destroyed cryptographic keys while allowing corporations to use generally-accepted strong encryption techniques. IBM SecureWay key recovery technology also offers a commercial solution to government and law enforcement needs for authorized access to encrypted data without resorting to key escrow or trusted third party schemes.

In summary, the ‘key’ benefits of the IBM SecureWay key recovery technology are:

o Scaleability for global use in network computing environments

o Low preparation overhead

o Flexibility to work with all encryption algorithms and key lengths

o Self-contained: no communication with an agent or third party

o Transparent operation to end users

o No single point of attack

o Key recovery within multiple jurisdictions

o Interoperability with jurisdictions not supporting key recovery

o No key parts exposed outside the cryptographic facility

o Collusion resistant

o Pre-authorization for communicating parties to perform key recovery

o Exploits elliptic curve public-key schemes (performance boost)

o Enables global exploitation of strong encryption (re: import/export/usage restrictions)

How to Get Started

The IBM SecureWay key recovery technology operates in conjunction with the SecureWay Key Management Framework previously announced. IBM SecureWay key recovery technology is part of the broad IBM SecureWay portfolio of security hardware and software products, solutions, services, consulting and research activities. The SecureWay brand provides end-to-end security solutions for customers such as cryptographic facilities, single sign-on, distributed security administration, access control, firewalls, secure web servers and browsers, secure electronic commerce, smart cards, anti-virus and overall internet security.

Customers should first consider their corporate security policy and the use of encryption services by their applications today, to get an understanding of where it would be appropriate to exploit the new IBM SecureWay key recovery technology.

IBM Security Consulting Services can help customers to establish appropriate security policies and recommend encryption capabilities for implementing secure communications and data practices. Contact your IBM representative for additional information regarding IBM Security Consulting Services.

For additional information, visit the IBM SecureWay home page at **http://www.ibm.com/security**.