Business Requirement for Key Recovery

Draft 2.1

September 4, 1997

"The primary focus of this paper, therefore, is to present the requirements of business users of encryption technology and products."

This document is in draft form and is subject to revision. It is being provided for review and comment only and should not be cited or quoted. This draft does not necessarily reflect the opinions of the Key Recovery Alliance or its members and should not be represented as such.

prepared by the
Business Scenarios Committee
of the
Key Recovery Alliance

Please provide comments to:
Bob Frith, Committee Chairman
at
bfrith@mot.com

Business Requirement for Key Recovery

Draft 2.1

1. Introduction

The Key Recovery Alliance (KRA) is an association with a global scope of over 60 suppliers and users of encryption-enabled products. There are member companies from Europe, Asia/Pacific and the U.S. These companies have come together to explore techniques that will enable the broad use of strong encryption for business purposes.

The basic market issues that have caused the formation of the KRA are:

- Businesses and commerce are multi-national and are increasingly operating on a global basis as the Internet continues to evolve
- Strong security mechanisms utilizing cryptography are essential to the safe use of the Internet for electronic business (business-business and business-consumer)
- Businesses can use encryption to protect the confidentiality of and access to internal information and shared sensitive information
- Companies will want to deploy any type of encryption they desire, commensurate with their business objectives
- Companies will need to have alternative access to their stored, encrypted information for a variety of reasons; e.g., lost or destroyed decryption keys or the unavailability of person possessing the decrypting keys
- Companies may need alternative access to real time communicated encrypted information to monitor information as it enters and leaves the company, to protect business assets, and to ensure compliance with company policy
- Customers will demand solutions that are manageable and interoperable across their business reach, multiple products from multiple suppliers and different countries of operations

The primary focus of this paper, therefore, is to present the requirements of business users of encryption technology and products.

Alternative access to encrypted information may be accomplished through a number of different methods, from “brute force” decryption methods to administratively constructing an “information recovery key”. With the wide range of business applications and user requirements there will not be a suitable universal mechanism for all encryption recovery situations. Therefore, an overall “framework” for the design and deployment of key recovery systems that will support the many various user requirements is crucial. Thus, the motivation for this paper is to:

- Define a basic set of scenarios, requirements and functions for key recovery, and
- Facilitate dialog with external communities on these requirements

Encryption can be used for many security purposes, including information confidentiality, digital signatures, licensing for intellectual property protection, access control, and authentication. The scope of this paper only covers keys used for confidentiality. *There is no business requirement for access to keys used for digital signatures, access control, authentication, and other non-confidentiality purposes. Mechanisms should not be provided for the recovery of keys used for these purposes that provide recovery by anyone other that the owner.* The user’s private key for digital signatures, for example, is only known to the user and if lost or compromised should be replaced, in the same manner that one would replace a lost or stolen credit card. Likewise, it is advisable to use separate keys for confidentiality purposes and authenticating purposes so that a key recovery process does not inadvertently expose the authentication key. The concept of “key usage” for the separation and identification of key types has been described in references such as ISO X.509v3, *To maintain user confidence in the use of encryption technologies and products, under no circumstances should the key recovery mechanism reduce the strength of the encryption process, either through exposing the decryption keys unnecessarily or using lower strength encryption for transporting keys than used initially to encrypt the information. Likewise, the use of key recovery must not compromise the capability for nonrepudiation.*

The intended audiences of this report are:

- Key Recovery Alliance Technical Committee - to explain business requirements so that they can develop technical recommendations, architectures, and protocols for interoperability of key recovery systems
- Key Recovery Alliance Deployment Requirements Committee - to define business scenarios so that deployment issues can be identified and addressed
- Key Recovery Alliance Policy Committee - to define business scenarios so that government policy issues can be identified and reflected in the technical requirements
- Key Recovery Alliance Outreach Committee - to provide resource materials for use in collateral to explain KRA purposes to potential members, media and interested parties (vendors, standards organizations and governments) and facilitate public discussion
- External audiences - to explain the business requirements and rationale for implementing key recovery and to facilitate dialog with external communities to refine requirements and scenarios e.g. users of encryption products with key recovery capabilities

While the focus of this paper is to describe the wide spectrum of business requirements, we also recognize the suppliers' need to conform with the laws of the countries in which their encryption-enabled products are manufactured, exported, imported, and/or used. Users will likewise need to be in compliance with the regulations of different countries governing their import, export and use of encryption-enabled products.

2. Scenarios

The scenarios that follow depict a wide range of instances in which information needs to be recovered from encrypted form and defines the relationship among the stakeholders and service providers. These scenarios will not be applicable to all users and will not share an equal ranking of need among users.

There are three parts to each scenario:

- Business Scenario: Illustrates a situation requiring key recovery, identifying the stakeholders, type of encrypted information, and operational considerations
- Key Recovery Requirements: Defines the attributes and objectives for key recovery mechanisms and service providers to ensure the controlled recovery of decryption keys
- Key Recovery Policy Considerations: Defines the policies that support the use of key recovery mechanisms

It should be recognized that scenarios that appear similar may lead to subtle, but significant, differences in the implications to key recovery design and implementation.

The scenarios are clustered into three broad categories:

- Those that relate to the usability considerations of key recovery
- Those that relate to the policy considerations of users and organizations
- Those that relate to operational aspects of Key Recovery Centers, both those internal to an organization and external to the organization

In the event that governments establish key recovery regulations and requirements for users of encryption products concerning export, import and use, a fourth category of scenarios has been included that describe how these requirements should be established and the policy considerations that would best meet user requirements.

Definitions

KRM: Key Recovery Mechanism (method by which encryption keys are made available for decryption operations)
KRC: Key Recovery Center (facility/capability to perform Key Recovery). A KRC may be either internal to an organization or operated a service organization.
KRA: Key Recovery Agent (an employee of a KRC authorized to process key recovery requests)
KRO: Key Recovery Officer (representative(s) of an organization who is/are authorized to recover key on behalf of the organization)
Organization: An enterprise, company, or non-profit operation with a centralized administration for defining encryption and key recovery policies
User: A person who, whether as a part of an organization or acting independently, utilizes encryption for confidentiality and may have authority to initiate a key recovery request for keys the user controls
Originator: the user who initiates the information encryption
TTP: Trusted Third Party
Stakeholder: A person who has a vested or legal interest in the content of encrypted information

A. Scenarios Affecting User Usability Considerations

Scenario 1 - Key Recovery for Stored Data

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
Data is stored in encrypted form in various locations throughout the organization in order to protect confidentiality. These locations include, but are not limited to, individual computing devices, file servers, and databases. Examples of situations requiring key recovery: 1. A user has encrypted a group of files, lost the decryption key(s), and needs immediate access to the files. 2. If a decryption key is not available because it has been lost or destroyed or the user is not present to provide the key, the organization cannot use the information. 3. A disaffected employee has destroyed the decryption key to prevent access to encrypted data. 4. An employee is using encryption to hide the use of a company computer for an unauthorized activity, such as operating a personal business. 5. Organizations may desire to manage the use of cryptography as with other business processes or “tools”. This management may extend to the general ability to recover encrypted information. 6. Organizations may store encrypted data at commercial off-site data storage facilities.	Key recovery mechanisms shall not reduce the effective strength of the encryption, including any exchange of the encryption keys with the KRC. The key recovery system may need to support multiple KRMs in order to satisfy all requirements KRMs and KRCs must support hierarchical levels of authority to request recovery of keys. E.g., levels of authority within an organization can recover lower levels of organizational keys as well as employee keys. Organizations should be allowed to recover their own organization’s keys within legal limits and based on company policy, but must not be able to recover any other organization’s keys. Note: requirements of KRCs operated as service organizations are described in Section C. Users should be allowed to recover their own personal keys, but must not be able to recover any other user’s key without authorization. The organization must be able to recover its encrypted data within legal limits and based on company policy without the cooperation or knowledge of the party that created the stored data.	Entities must be able to operate their own KRC, or register with one or more KRCs of their choice, to satisfy their business requirements. If government-approved KRCs are required to satisfy governmental regulations, entities must be able to operate their own approved KRC, or select an external approved KRC of their choice. Multinational organizations may be required to utilize multiple KRCs in order to comply with multiple localized policies. Keys shall only recoverable in accordance with the policy defined by the organization or user and controlling law. A user may require the ability to delegate permission to recover his keys to another user. Decryption of data stored at outsourcing sites must be under sole control of the data owner.

Scenario 2 - Key Recovery for Communicated Data

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
In network communications among users within and outside the organization, the information may be encrypted for confidentiality. This includes, but is not limited to; email (e.g., S/MIME), encrypted links (IPSEC) and sessions (SSL/TLS), and encrypted telephony/FAX. Outside of specific limited situations illustrated by these scenarios, key recovery for communicated data is not presently a broad-based business requirement. 1. An organization has a user who is utilizing encryption to hide the transmission of information to people within or outside the organization against policy; e.g., a stockbroker is violating insider-trading rules; an engineer is sending technical data to a competitor. 2. A user is using an organization's computer to download software over the Internet against organization policy. 3. An organization is being raided by a competitor and wants to be able to monitor incoming encrypted email; e.g., an engineer is being solicited to disclose technical information. 4. An organization may need to journal encrypted communications, e.g. a brokerage firm may need to record and retain communications with clients concerning transactions. 5. An employee is using encryption to hide the use of a company computer for an unauthorized activity, such as operating a personal business. Organizations may desire to manage the use of cryptography as with other business processes or "tools". This management may extend to the general ability to recover encrypted communications.	The organization must be able to monitor its communications, within legal limits and based on company policy, without the cooperation or knowledge of the communicating parties. Key recovery mechanisms shall not reduce the effective strength of the encryption, including any exchange of the encryption keys with the KRC. The key recovery system may need to support multiple KRMs in order to satisfy all requirements KRMs and KRCs must support hierarchical levels of authority to request recovery of keys. E.g., levels of authority within an organization can recover lower levels of organizational keys as well as employee keys. Organizations should be allowed to recover their own organization's keys, but must not be able to recover any other organization's keys. No requirement exists for users to recover their own individual keys for communicated or transient data. Audit capabilities must be provided to assure compliance with policies.	Organizations must be able to operate their own KRC, or register with one or more KRCs of their choice, to satisfy their business requirements. If government-approved KRCs are required to satisfy governmental regulations, organizations must be able to operate their own KRC, or select an external KRC of their choice. Multinational organizations may utilize multiple KRCs in order to facilitate operations. Keys shall only be recoverable in accordance with the policy defined by the organization and controlling law.

Scenario 3 - Compliance with Corporate Policy

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An organization has departments with different policies governing the use of encryption ranging from very strict to none at all. For example, the Corporate Office in the U.S. uses 168-bit triple DES, Human Resources in Japan uses 128-bit IDEA, engineering company-wide uses 56-bit DES and sales uses 80-bit RC5. Nonetheless, the organization has a duty to protect its assets that may include the recovery of encrypted information.	Interoperable key recovery mechanisms must be supported at all locations independent of algorithm types and key lengths. The KRMs must allow entities to set their own policies. For policies that are different, they need only be enforced by the communicating entities requiring them, unless otherwise specified by regulation. This may require multiple KRMs. With respect to the originator of encrypted communications, a multinational or corporate entity may require that a specific (global) KRC be used for all outgoing communications. Likewise, a subordinate/divisional entity may require that a specific regional or local KRC be used for all outgoing communications within that domain. Further, either the multinational or subordinate entity may require that all incoming encrypted communications use one or more specified KRCs in order to communicate using encryption. The setting of entity policy requirements shall be configurable. Only the authorized administrator can set the configuration of a crypto implementation. The localized requirements must be determinable and enforceable by the key recovery implementation. The key recovery implementation shall not be subvertable. The key recovery policy mechanisms shall not be subvertable. An implementation may support the policy either with a rules-base embedded in the implementation itself, or from dynamic information.	Entities may specify their own policies regarding KRMs and KRCs for encrypted information under their control. These policies may be more or less stringent than the policies imposed by government regulations, if any. If an entity uses a KRM/KRC to communicate with another entity that uses a compatible and entity-approved KRM/KRC then the communication is permitted. If an entity uses a KRM/KRC to communicate with another entity which uses an incompatible KRM/KRC or a KRM/KRC not approved by the entity, then the communication may be either permitted or denied. When a KRM is utilized by an entity, other communicating entities should be notified of such use. If communication is permitted between one **user o**r entity which uses a KRM and another user or entity which doesn’t use a compatible KRM or does not use a KRM at all, the entity that doesn’t should ideally assist in satisfying the rules set by the other. At a minimum, the use of incompatible KRMs, or no use of a KRM, should not preclude the KRM from performing properly while providing backward compatibility. Entities may impose control over the key recovery policy selection of crypto devices used by their employees, and support configuration from a system administrator function.

Scenario 4 - Portability

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An organization has individuals who carry computers between company facilities and/or across operational boundaries. These individuals need to encrypt and decrypt data and communicate securely with entities in other facilities without violating organization policies. For example, auditors may need to conform to encryption policies of local organizations that may differ from other locations.	Flexibility to comply with changing or multiple entity and/or operational requirements. Note: this needs to be coordinated with the requirement of non-subvertability.	Allow organization administrators to set and modify policies governing key recovery to accommodate the regulations in effect in the locations the user will be visiting. Facilitate selection of the appropriate policy for the local jurisdiction or entity.

Scenario 5 - Selection of Delegates

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An individual or organization selects the person, role, and/or delegate to perform key recovery on their behalf and specifies the policy governing the scope of the delegate's authority and the recovery procedures. The individual or organization may choose to use multiple delegates, each with differing authorities and policies.	Entities have the ability to specify who recovers encryption keys. Entities should be able to choose from a number of alternative KRCs, e.g. themselves, peer entities, outside legal counsel, banks, accounting and auditing firms, specialized key recovery firms (TTPs). The entity should be able to designate specific individuals or roles within the entity's KRC in conformance with applicable regulations. The entity should be able to designate different KRMs based upon the type of information to be recovered. For example, the recovery delegate may be a network security manager enforcing a policy on transmission of encrypted data destined for outside the organization. They may be allowed to recover keys for communicated data but not for data stored on a computer. Retrieval of keys must be under the control of the designated delegates and must be auditable.	Entity must be able to select the KRC. A KRC can only recover keys for users or organizations for which it has been designated. An encryption system must not allow substitution of KRCs without approval of the entity. Entities must be assured that the policy governing their relationship with the key recovery agent will remain consistent unless specifically changed by the entity. The KRC must not allow the substitution of another KRC or delegate without the approval of the user or organization.

Scenario 6 - Non-connected Operation

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An individual encrypts a file without being connected to a key recovery center. A requester obtains a decryption key without being connected to the key recovery center; e.g. user needs to decrypt a file while traveling and does not have the decryption key.	On-line, real-time interaction with the KRC must not be a requirement in this environment.	Allow interaction with the KRC to be accomplished out-of-band and/or ahead of time.

Scenario 7 - Efficient Operation

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An organization needs to recover information in individual database fields encrypted with different keys. Communications systems may have bandwidth or protocol restrictions. Devices may have memory or computational restrictions. Encryption may involve one-to-many communications, e.g. multicast, broadcast, or list-based email.	Minimize overhead in the implementation of the KRM.	Methods chosen should not levy an unacceptable burden on the environments described in the scenarios.

Scenario 8 - KRC Identification

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An individual or organization is in possession of information they cannot decrypt because they do not know which KRC can produce the decryption key.	An organization or individual should be able to determine the identity the associated recovery center from the user's information that has been encrypted, e.g. identify the key recovery information associated with the encrypted information.	Maintain ability to recover encrypted information. The identification of the KRC may be observable to anyone; however, organization or user policy will dictate the only conditions under which the key can be recovered.

Scenario 9 - Non-subvertability

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
A corrupt employee may attempt to defeat the key recovery mechanism. For example, an employee who is falsifying records will attempt to circumvent key recovery to avoid detection.	An organization needs assurances that the recovery method cannot be easily defeated or circumvented, either accidentally or intentionally, by either the person encrypting the information or by the person recovering it.	An entity must satisfy its obligation to protect its critical information.

Scenario 10 - Interoperability

Business Scenario	Key Recovery Requirement	Key Recovery Policy Considerations
An organization with systems that have key recovery implemented wishes to have them interoperate with systems that do not. An organization with key recovery implemented wishes to exchange information with other organizations with different or no key recovery mechanisms. An organization, which operates in multiple key recovery policy domains, wants to have them interoperate with each other. For example, an organization with offices in New York uses an US-based KRC while its Paris office uses a France-based KRC.	If communication is permitted between one entity that uses a KRM and another entity that doesn't use a KRM, the entity that uses a KRM should not prohibit the other entity from accessing the communications. If communication is permitted between entities that use different KRCs, the KRMs should allow interoperability. The use of interoperable KRMs may be the condition for this permission.	An organization may have policies covering different applications within the organization; for example, human resource and engineering department programs An organization may have policies covering communications with business partners or correspondents; for example, email attachments between a manufacturer and its suppliers using different recovery methods. If an entity uses a KRM/KRC to communicate with another entity that uses a compatible and entity-approved KRM/KRC then the communication is permitted. If an entity uses a KRM/KRC to communicate with another entity which uses an incompatible KRM/KRC or a KRM/KRC not approved by the entity, then the communication may be permitted.

B. Scenarios affecting User Policy Considerations

Scenario 11 - Key Recovery Policies

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An organization will have multiple key recovery policies governing the who, what, where, and how of key recovery in the following situations: • self-recovery by an end user, • organizational recovery of information, and • responding to legal requests (e.g., civil discovery) For example, • originators are allowed to recover their own data while others must have additional approvals Recovery in response to a legal request requires organization counsel approval.	KRM design should facilitate recovery by authorized entity while reducing the risk of abuse. The satisfying of key recovery requests shall be compliant with entity policy. In addition, satisfaction of requests shall be compliant with government regulations if the KRC is government approved. Support efficient key recovery by the owner of the data; e.g. batch requests for keys should be accommodated if it improves the performance of key recovery.	Appropriate to the recovery requirement, a policy should specify procedures, e.g. K-out-of-N or hierarchical authority, to prevent abuses such as improper disclosure of keys.

Scenario 12 - Disclaimer

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
Individuals or organizations might be liable for the security of the information sent to them in confidence if they fail to disclose the fact they are employing key recovery mechanisms. For example, a user sends an encrypted proprietary email message to someone not knowing that all incoming encrypted messages are subject to monitoring, thereby breaching the original confidentiality.	Users must receive a disclaimer or other notification if the device on which he or she is working or the communications in which he or she is engaged invokes an information recovery mechanism. This applies to individuals operating both within and outside of an organization with a defined recovery policy. The disclaimer must be displayed in such a fashion that it allows the users to abort or terminate the operation. For example, the sender should have the choice not to send a message after viewing the disclaimer and the receiver should have the choice to abort the receipt after the notice. Disclaimers must be displayed to all parties in a communications.	The user of a KRM wants to preempt and manage exposure to liability.

C. Scenarios Affecting Operational Requirements of KRCs

Scenario 13 - Key Recovery Center Performance

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An organization has established a relationship with a KRC and defined appropriate key recovery policy. 1. A user loses the decryption key for a specific item and requests that it be restored. The KRC validates the user's rights and returns only the requested key following the defined policy. 2. An authorized requester within an organization requests the decryption key(s) for some specific information and/or user(s). The KRC validates the requester's authority with respect to the policy and returns only the applicable keys. 3. An attorney representing a civil litigant subpoenas all records, including records that were encrypted with a key no longer available, pertaining to a specific incident or user. If the organization's legal counsel approves the request, the KRC validates the request with respect to the policy and returns only the applicable keys. An organization may choose or be required to establish a relationship with multiple KRCs serving different locations and will require the KRCs to operate independently. For example, an organization has branch offices located in countries A, B and C. The organization will not want encrypted communications between A to B to be recoverable by a KRC in country C unless permitted by organization policy.	Prevent third party intervention, abuse, or denial of service. Breach of a KRC's operations through its relationship with one organization or user does not compromise all organizations or users associated with that KRC. A request for a recovered key provides only the requested key for the specified time frame or encrypted item. Key recovery, requested through statutory right, for one entity does not provide access to another entity's keys. It may be necessary to label keys for information with different sensitivities; e.g. doctor's business records versus doctor's patient records must be separable. The provision of the decryption key to the requester shall not reduce the effective strength of the original encryption. When a key is recovered in response to a legitimate request, the requester may not inadvertently get keys other than those requested (e.g., for other users), nor shall someone other than the requester receive the key. Legitimate recovery events should not afford access to separately encrypted information. Breaches in confidentiality, should they occur, should be limited to the minimum practical amount. Unless policy dictates otherwise (e.g., for back up purposes), one KRC should not be able to produce keys maintained by another KRC A KRC sanctioned in one country should not have access to keys used to encrypt information neither originating from nor destined to that country.	Enable controls that prevent administration of the KRA from being easily compromised or having control passed undetected or without proper authorizations. Enable controls that prevent the KRC from providing key recovery results not specifically requested by an authorized requester. Provide audit procedures for use and management of the KRC. Provide controls that will enforce a policy requiring that a KRC notify parties in a communications of key recovery access activity.

Scenario 14 - Key Destruction

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
Individuals or organizations destroy, or schedule for destruction, decryption keys for the following business practices: 1. In order to prevent access to archived documents that have been authorized or scheduled for destruction. Destruction of the key will make a document inaccessible even if back up copies exist. This destruction may be to conform to government regulation regarding employee privacy, etc. This may also be required to comply with company policy regarding document retention practices. 2. An individual or organization may decide to replace decrypting keys. This could be done for a number of reasons: • the key is compromised • migration to stronger keys and algorithms • periodic replacement of keys to reduce communications risks • keys assigned to time-based functions (for example, the time frame for an outside consultant to access strategic business information has expired), etc. For these reasons, the individual or organization should also be able to define corresponding time frames for the keys stored. After the key has been replaced, the keys should no longer be accessible.	Support aging of key(s) in KRC. Support entity requested destruction of keys. Key recovery system must support different parameters for different data types and sensitivities, e.g. casual email vs. patent records, contracts, employee records, and health records.	The user of a KRC, whether self-operated or operated by another, should be able to specify policies for aging and the subsequent destruction of keys. Policies should also be supported for user-requested destruction of keys. Activities must be auditable for the destruction of keys and KRC may be required to provide authenticated evidence of destruction.

Scenario 15 - Timeliness

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An organization needs to decrypt an archived document within a policy-defined period of time. An organization needs to decrypt a communication stream immediately. An individual needs to decrypt a file by the end of the day.	Support specified procedures and specific time requirements (maximum & minimum) to perform recovery function. Ability to select urgency and priority on key recovery requests.	The KRC should be able to respond within certain guarantees for priorities. The ability to report and potentially bill based on timeliness of response may be desirable. Audit records indicating the responsiveness may be required.

Scenario 16 - Auditing

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An organization needs to evaluate the performance, reliability, and cost of its key recovery center. An organization needs to review key recovery services to protect against abuse.	An organization or individual needs to have a comprehensive record of the occasions upon and circumstances under which information has been recovered. The exact contents of the record are determined by the organization's policy with its recovery agent, subject to regulatory requirement.	An entity must satisfy its obligation to protect its critical information.

D. Scenarios affecting Governmental Regulatory Considerations

Governing law may require that all parties utilize compatible/approved KRMs and/or KRCs in order to encrypt information or communications. However, the same Key Recovery Requirements and Key Recovery Policy Considerations described in B and C above apply to governmental-imposed requirements. Governmental requirements should not impose additional requirements beyond the following Scenario.

Scenario 17 – Global, Commercial Products

Business Scenario	Key Recovery Requirements	Key Recovery Policy Considerations
An organization wants to use a commercial, off-the-shelf encryption product that can be configured to suit its individual security policy requirements. In some cases, the organization's options may be constrained by local government policy, precluding the use of some features and dictating the use of others. For example, the human resources offices of a multinational organization in different countries purchase the same application to encrypt personnel files. The users in one country may not be required by law to implement key recovery (but may by organization policy) while those in the other country must implement key recovery for both organizational and governmental reasons. An organization has individuals who carry computers across governmental or jurisdictional boundaries. These individuals need to encrypt and decrypt data and communicate securely with entities in other locations without violating jurisdictional policies. For example, auditors may need to conform to encryption policies of local governments that may differ from policies of other governments in which they also work.	With respect to the originator of encrypted communications, the government of Country A (the country of product origin) may require that a KRC approved by Country A is used for all outgoing communications. Likewise, the government in Country B (the country of use) may require that a KRC approved by Country B is used for all outgoing communications. Further, either or both of countries A and B may require that all incoming encrypted communications use a KRM/KRC approved by Country A and/or B in order to communicate. Govt. requested key recovery for one entity does not provide access to the keys of another, provide access to encrypted information beyond the time period specified nor access to communications which does not occur in that country. Flexibility to comply with changing or multiple jurisdictional requirements. Note: this needs to be coordinated with the requirement of non-subvertability.	Governing law may dictate that all parties utilize compatible/approved KRMs in order to successfully communicate To be in compliance with governmental regulations, entities may be required to utilize an external, government-approved KRC. If government-approved KRCs are required to satisfy governmental regulations over cryptography, entities must be able to operate their own approved KRC, or select an external approved KRC of their choice. Keys shall only be recoverable in accordance with the policy defined by controlling law. Apply administrative management facilities to enable appropriate KRM functions. Facilitate selection of the appropriate policy for the local jurisdiction.

4. Conclusions

The commercial marketplace is increasing its demand for stronger encryption technology to protect the confidentiality of information and communications. Encryption will be used more frequently in the normal conduct of business within an organization, between organizations, between an organization and it's customers and between an organization and various governmental agencies (e.g. taxing and reporting authorities). While strong encryption is critical for protecting confidentiality of information, there are business risks associated with using encryption. To prevent the loss of legitimate access to encrypted information, due to the unavailability of the encrypting or decrypting keys, various key recovery mechanisms will be used. For each customer situation, the technical and policy requirements must be identified and understood. The objective of this paper, "Business Requirements for Key Recovery", is to describe the relationships between customer needs, technical requirements and operational policies. In so doing, this will establish "baseline" objectives for key recovery mechanisms and their associated management systems.

For organizations to take full advantage of key recovery, there are a number of issues concerning the deployment of solutions that must be resolved. Certainly usability and performance considerations are critical, in terms of user impact and organizational support, especially for multinational organizations. Additionally, there are considerations concerning confidentiality of business information and various governmental regulations that must be addressed.

While the purpose of this paper is not to resolve all of the issues and concerns, it should have defined the framework in which key recovery must conform. If an outcome of this paper is to help create useful solutions for the global business environment it will have served its purpose well.

Note: Special acknowledgment is given to the European Security Forum for permitting us to adapt the structure of their paper, "The Business need for Cryptography", published September, 1996, to this paper.