CYLINK

CyKey™: Cylink's Key Recovery Solution

March 13, 1997

Introduction

With the increased use of encryption in business, encryption-key recovery has emerged as a critical issue to users. As encryption is deployed to protect files and network communications, users must include safeguards that prevent the inadvertent loss of data and use of the network for malicious intent. This paper explains what key recovery is, the motivation for key recovery, and how Cylink's CyKey works.

What is Key Recovery?

A key recovery scheme allows the owner of encrypted data or an authorized third party to *recover* a lost or otherwise unavailable key. The most popular schemes are trusted third parties (TTPs), key escrow, and key recovery.

In the **trusted third party** schemes, the TTP generates and owns the key. The TTP makes a copy of the key available to the user, who uses it to encrypt data. If the user loses the key, the TTP still has the original key.

The **key escrow** scheme achieved notoriety during the U.S. Government's Clipper initiative. In this scheme only government-controlled law enforcement agencies could recover keys.

Both trusted third party and key escrow schemes have received a lukewarm (and occasionally even hostile) reception from standards bodies and the business community.

The **key recovery** scheme is the most recent technique for recovering encryption keys. Key recovery involves the use of a key recovery field and a key recovery agent, the only entity with the authority and capability to recover the key. The agent keeps information needed to recover the key, but is never actually in possession of the key until recovering it.

Key recovery schemes are administered according to strict policies that ensure key recovery is triggered only legitimately. These policies governing who and under what conditions the key can be recovered are published by the agent and agreed to by the community that the agent services.

How Key Recovery Works

A generic key recovery scenario for encrypted files is illustrated in Figure 1.

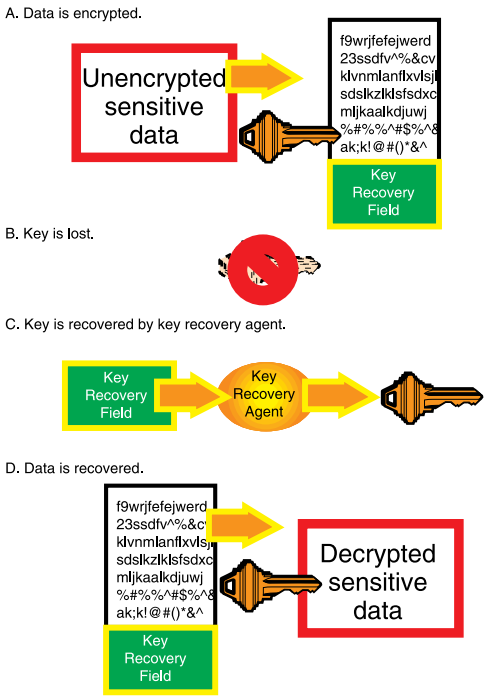

Figure 1
Basic Key Recovery
A key recovery field is appended to the encrypted data. The key recovery field contains the key used to encrypt the data. This key is itself encrypted, and can be decrypted only by the specified key recovery agent.

When the data is encrypted, a *key recovery field* (KRF) is generated, as shown in Figure 1-A. The key recovery field identifies a specific key recovery agent and contains, in an encrypted form only the agent can decrypt, the key used to encrypt the data.

In Figure 1-B, the key is lost or otherwise becomes unavailable, so the file cannot be read.

In Figure 1-C, the user presents the key recovery field to the key recovery agent. The agent decodes the key recovery field to extract the key, and gives it to the authorized user.

Once the key is obtained, as shown in Figure 1- D, the user can use it to decrypt the data.

This model works to recover keys lost by the individual who initially encrypted the data and for a third party who has a legitimate reason to access the encrypted data. In this case,

the user-agent agreement defines the terms and conditions under which the key may be recovered and who may receive it.

Examples of Key Recovery Use

This section describes the three typical business situations in which key recovery support is needed.

Case 1: To Recover Important File Data

Business people carry sensitive information on lap tops or other unprotected computers. For example, an executive might have customer lists, contracts in negotiation, and business plans on a single lap top. A business can be destroyed in the event that this kind of information falls into the "wrong hands".

It is prudent to encrypt sensitive files. But what happens if the key is lost? Without a backup of the key or a method of recovering the key, the data is lost forever. Copying the key or otherwise backing it up weakens the security. Therefore, a key recovery scheme is an attractive alternative.

In the event the user losses the key, the user can take the key recovery field (typically appended right to the file) to the responsible key recovery agent. After the agent determines that the user owns the encrypted data, the agent will recover the key and give it to the user. The user privately decrypts the data. Similarly a co-worker can recover the key by presenting affidavits to the key recovery agent that prove that the co-worker has legitimate access to the data. The agent can recover the key and make it available to the co-worker.

Case 2: To Monitor Communications

More and more, organizations are using strong encryption to protect communication among computers on its own network or with its trading partners. Now consider, an employee who is using the company computers for industrial espionage, running his/her own business, or distributing pornography. The company has a fiduciary, legal, and moral obligation to prevent such uses of its assets and facilities; but without a way to convert the cyphertext to clear text, the company cannot detect when a misuse has occurred.

Key recovery provides corporate security with the means to monitor encrypted network traffic. When circumstances warrant it, the network traffic (first the key exchange handshake and then the subsequent communications) is captured, the key recovery field is extracted and copied to the key recovery agent, the session key is then extracted by the agent, and finally, the message content is decrypted.

Case 3: To Export Encryption

U.S corporations run into U.S. Government policy governing the export of encryption when they want export products that perform strong encryption. U.S. Government policy, while perhaps controversial, currently includes the right to monitor citizens targeted by criminal or national security investigations. Many other governments around the world are adopting a similar stance. Key recovery, to be accepted by governments and still be effective, must protect the communicating

parties against the abuse of power while providing legitimate authorities access to file and message contents.

Key recovery schemes satisfy both requirements because the government does not have direct access to the encryption key. Although a government agency may capture the encrypted data, it cannot decrypt it without the key. Only the key recovery agent, an independent agency whose actions are governed by its agreements with its users and the laws of the land, can produce the key. Privacy is protected because the government must present sufficient evidence to warrant key recovery to the key recovery agent before anything is decrypted.

Key Recovery System Requirements

Key recovery systems should satisfy the following requirements:

- Key recovery must support the user's need to recover the key should it be lost or otherwise become unavailable.
- An organization must be able to choose its own key recovery agents. If desired, the organization can become its own agent if it meets the requirements of the relevant government.
- Key recovery should add negligible overhead to encryption and network operation.
- The key recovery system should be simple to use and manage, needing minimum infrastructure.
- Any reduction on the strength of the crypto system must be negligible.
- Key recovery must involve the key only; the data cannot be exposed.
- The system must conform to the relevant government regulations concerning the export and import of cryptographic products.

How CyKey Works

CyKey is based on the key recovery scheme. It has been approved by the U.S. Department of Commerce, qualifying Cylink for a License Exception KMI. Today, Cylink is exporting encryption devices that use strong encryption.

With CyKey, the user protects his data from key loss **with negligible reduction to encryption strength**. Only the user's designated key recovery agent can recover the lost key. The keys are strongly protected in the key recovery field. No unauthorized third party (including any government) can recover the key without going through the key recovery agent.

CyKey, which supports key recovery for stored encrypted files as well as for encrypted communications, is based on a trusted relationship among the user or owner of the encryption device, the key recovery agent, and the key recovery authority.

Establishing Trusted Relationships

A trusted relationship must be established between an encryptor (either a device or software that converts cleartext to cyphertext), the key recovery agent and a key recovery authority (a sanctioning body for key recovery agents). Figure 2 illustrates how the authentication process proceeds from the key recovery agent, to the key recovery authority, back to the agent, and finally to the encryptor to establish the trusted relationship.

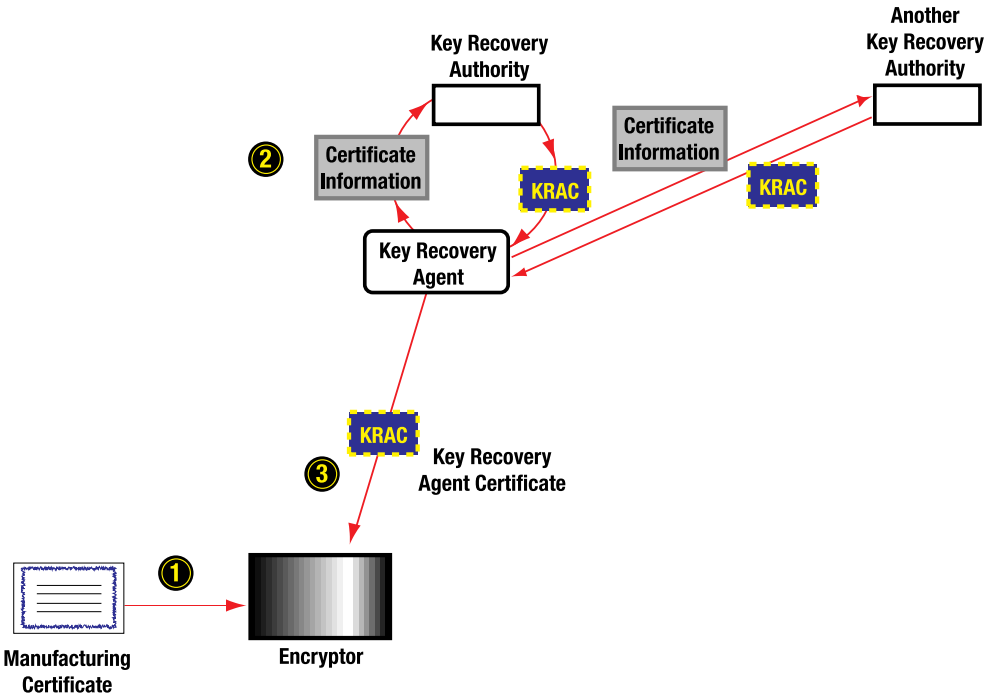

Figure 2

CyKey Authentication and Certification

1. The manufacturing certificate installed in the factory defines the key recovery authority that can sanction the encryptor's key recovery agents. The certificate contains the key recovery authority's public key.

2. The key recovery agent submits its certificate information (public key, ID, etc.) to the key recovery authority. The key recovery authority signs and returns it to the key recovery agent in the form of a key recovery agent certificate (KRAC).

3. The user registers with the key recovery agent and receives the KRAC. Before the encryptor accepts it, however, it checks the digital signature to verify it was issued by the designated authority.

Note that the key recovery agent can be certified by more than one authority.

Each encryptor has:

- a unique serial number or other ID
- a manufacturer's certificate assigned to that ID which defines the encryptor's key recovery authority and other configuration information
- a key recovery agent certificate, which identifies the key recovery agent.

The manufacturer's configuration information is set to one of the following key recovery states:

- key recovery not allowed
- key recovery optional
- key recovery required.

When key recovery is required, the manufacturing certificate specifies the public number (key) of the key recovery authority and other configuration information.

The authority defines the sanctioning policy and process to ensure that the key recovery agent has established the necessary safeguards against (1) unauthorized access to its systems and (2) unauthorized encryption key disclosure. Once the key recovery agent has satisfied the key recovery authority requirements, it presents its ID and its public key to the authority. From this, the authority produces for the agent a digitally signed key recovery agent certificate (KRAC). The KRAC contains the agent's public number and the authorities public key along with other information.

After an encryptor requiring key recovery has been installed, the user must register it with a key recovery agent sanctioned by the key recovery authority identified in the encryptor's manufacturing certificate, if key recovery is required. The encryptor will not recover a key until a valid KRAC has been presented. (It requires the agent's public key to encrypt the session key in the key recovery field.) Because an encryptor is configured for a specific key recovery authority, it will refuse a KRAC signed by any other authority. The manufacturer can therefore restrict use of a particular encryptor to a group of agents.

CyKey's simple key recovery infrastructure allows the encryptor vendor to ship it to a region—Europe, for example—without specifying a particular agent. This permits the customer to use a hierarchy of sanctioning authorities (including a government agency or government-appointed organization) and certified key recovery agents.

With CyKey, an encryptor can receive a new KRAC from the same or a different key recovery agent. (The KRAC must always be signed, however, by the key recovery authority specified in the encryptor's manufacturing certificate.) After accepting a new certificate, the encryptor uses the new public number of the key recovery agent, thereby renewing the cryptographic strength of the key recovery system. If the new certificate is from a new agent, the old agent cannot recover the new keys.

How CyKey Works with Encrypted Files

After the user has registered with a key recovery agent, key recovery is simply a matter of recording the key recovery field along with the file. When the file is encrypted, the encryption key itself is encrypted. The file's encryption key can be decrypted only with the key recovery agent's private key.

If the encryption key is lost or another party legitimately seeks access to the encrypted data, the key recovery field is copied from the file and sent to the key recovery agent for decryption. This is the first and only time the key recovery agent is involved in the key recovery process. The agent, after establishing the legitimacy of the request, decrypts the key recovery field and returns the decrypted key to the requesting party. The

customer-agent agreement defines the terms and conditions under which the key may be recovered and returned.

How CyKey Works with Encrypted Communications

Figure 3 illustrates how the trusted relationship for secure communications is implemented by CyKey.

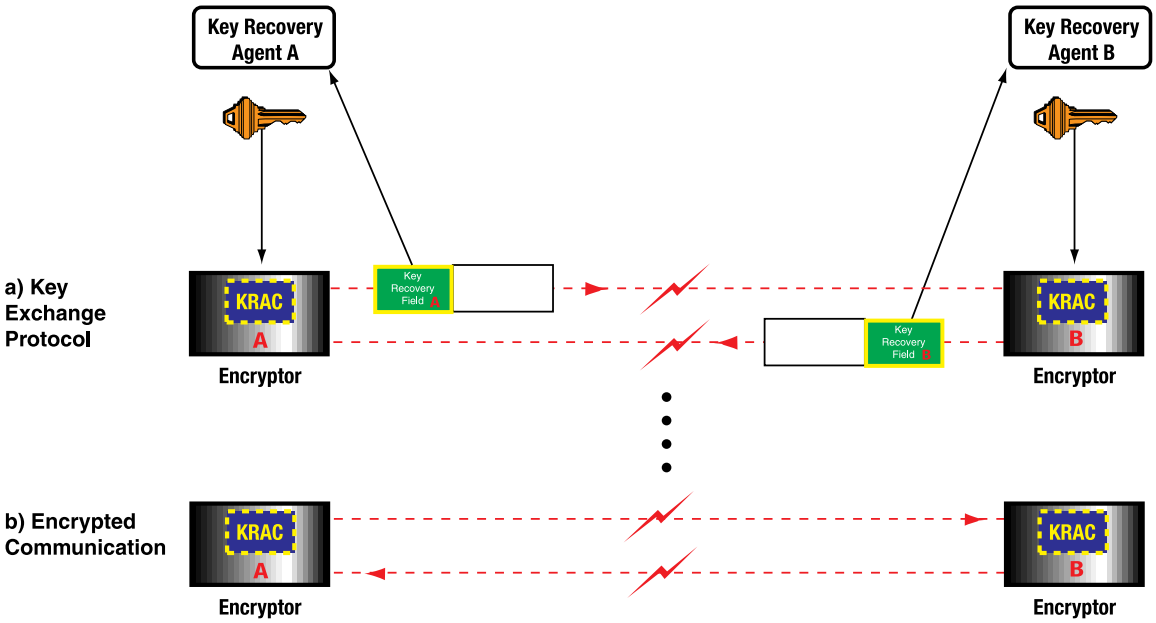

Figure 3
CyKey for Communications
Two components of the communications must be captured to recovery the encryption key and decrypt the message: (a) the key exchange protocol messages, into which the key recovery field has been incorporated, and (b) the encrypted conversation, which may occur some time later. To decrypt the data, the key recovery field is extracted from the key exchange messages and sent to the key recovery agent who, after ensuring the legitimacy of the request, returns the encryption key.

Unlike file encryption, the key used in encrypted communications is not stored along with the encrypted data. When encryptors are configured either to require key recovery or support it optionally, they begin generating key recovery fields based on the agent's public key in the KRAC. The key exchange protocol is extended to include the key recovery field during the handshake. This key remains in effect for all subsequent encrypted communications between the same two parties until another key exchange is performed.

Figure 3 illustrates the process between two such devices. Notice that the key recovery field is appended twice, once for Agent A, and the other time for Agent B. During the key exchange, encryptors A and B ignore the key recovery field. It is not needed for encryption or to establish the link; the key recovery field is necessary only to the person recording the session for subsequent review. Because the key recovery field is ignored

by the encryption devices, CyKey supports encrypted communications between systems with different agents and between systems in which one requires a key recovery scheme but the other does not—a valuable feature for companies that need to communicate among geographically dispersed offices and trading partners.

CyKey Components

CyKey consists of encryptor software, a key recovery agent, and certificate management software.

Encryptor Software

The software runs in the encryptor, performing the following functions:

- accepts and validates the key recovery agent certificate
- disables the encryptor if key recovery is required and no valid key recovery agent certificate is accepted
- generates a key recovery field and appends it to each encrypted file or as part of the key exchange protocol.

Key Recovery Agent

The CyKey key recovery agent application runs on a standard desktop system that:

- generates key recovery private and public keys
- presents the key recovery agent information to key recovery authorities to obtain a digitally signed key recovery agent certificates
- distributes key recovery agent certificates to encryptors
- manages the database of certificates and logs key recovery events
- recovers keys—returns keys and algorithms when presented with a key recovery field and the proper credentials.

Certificate Management

An encryptor must be part of a system with key recovery management. The key management program must have the capability to manage the installation of the key recovery agent certificates. The manager receives key recovery agent certificates from one or more agents. Before accepting the certificates, the encryptor must validate them against the list of designated authorities. Because there can be more than one designated authority, encryptors in the same network can interoperate with those having different key recovery agents. After validating the certificates, the manager downloads the certificates to designated encryptors.

In Cylink encryptors, for example, the key recovery agent certificate and manufacturer's certificate will be installed using SecureManager™. (Other vendors can use their own techniques.) If the key recovery authority is not known at the time the unit is shipped from the factory, an encryptor can be shipped without a specified authority. Since Cylink uses the manufacturing certificate to carry this configuration information, Cylink can update the unit in the field. In this case, the unit would be shipped without a manufacturing certificate. Once the configuration information has been determined, Cylink produces the manufacturing certificate for

that encryptor. This certificate is then loaded (using SecureManager) into the encryptor in the field.

Summary

Although strong encryption provides security, the potential loss of keys and the data encrypted with them presents a new danger. CyKey is a simple, efficient, inexpensive, and most importantly, cryptographically strong solution to this problem. The CyKey architecture supports a wide range of key recovery applications, including those managed by private providers, those within organizations, those requiring multiple key recovery agents on one network, and those that are government mandated.