Commercial Key Escrow:

Something for Everyone Now and for the Future

Stephen T. Walker
Steven B. Lipner
Carl M. Ellison
Dennis K. Branstad
David M. Balenson

Trusted Information Systems, Inc.

January 3, 1995

Summary

A tension has been growing for the past twenty years between the interests of the public to protect its sensitive information and the interests of governments to access the information of their adversaries. The Clipper Key Escrow program, introduced by the U.S. Government in 1993, was an attempt to overcome this tension by giving the public good cryptography while retaining for law enforcement the ability to decrypt communications when authorized. But Clipper has many problems that make it unattractive to the public.

The basic concepts of key escrow are very attractive to individuals and organizations who fear the consequences of losing their encryption keys. A key escrow system that satisfies the concerns of individuals and corporations and also meets governments' interests could help resolve this growing national tension.

This paper reviews the reasons for this tension and the evolution of software key escrow systems. It then examines the variety of alternative key escrow systems and describes why the government must take urgent steps to promote commercial key escrow before serious and permanent harm is done to government's law enforcement and national security interests.

A Fundamental Tension

Secret writing has existed since the beginning of recorded history. During this century, encryption has been largely the domain of governments. The history of World War II shows how important the secret wars over secret communications have been and still are to the conduct of modern government. During most of this time, the general public had little knowledge of or interest in encryption.

Twenty years ago, with the introduction by the U.S. Government of the Data Encryption Standard (DES), encryption was made easily accessible to the public for protecting sensitive, non government information. DES awakened public interest in encryption that led to, among other things, the development of public key cryptography by non-government scientists. The public's desire to be able to protect its sensitive information quickly led to a **fundamental tension** between governments and their people over the "right" of individuals to protect important information versus the "right" of governments to listen to the communications of their adversaries.

Governments have always used export controls[1] on cryptography to attempt to control its proliferation and use against their interests. Even though the use of encryption is not controlled in most countries, U.S. Government export controls have seriously impeded the use of encryption in commercially available software products and thus its use by individuals and organizations within as well as outside the U.S. This de facto internal use control has served to increase the **tension** between the public and its government.

With the explosion of personal computers and global information infrastructures, this **tension** has increased further, as more citizens have realized that their sensitive information is openly vulnerable, and, some argue, the national economic interest is at stake.

Congressional hearings [Brooks] warned of serious consequences of foreign and domestic industrial and government espionage. National Research Council reports [NRC] repeatedly called for a careful examination of these issues.

A National Cryptography Policy?

During this period, a proposal was put forth for a national cryptography policy, which was intended to forge an acceptable balance between both sides:

> Good Cryptography shall be available to the public without government restriction, where
>
> > "Good cryptography" is defined as DES (with 56-bit keys) and RSA with a modulus less than 1024 bits, and
> >
> > "without government restriction" means without export control or other mandatory government restriction.

It was noted that the present de facto national cryptography policy in effect defines "good cryptography" as symmetric key algorithms restricted to 40 bits and asymmetric keys limited to 512 bits.

---

[1] A few countries such as France and Singapore also use import or internal-use controls.

Twenty years ago, with the introduction by the U.S. Government of the Data Encryption Standard (DES), encryption was made easily accessible to the public for protecting sensitive, non government information. DES awakened public interest in encryption that led to, among other things, the development of public key cryptography by non-government scientists. The public's desire to be able to protect its sensitive information quickly led to a **fundamental tension** between governments and their people over the "right" of individuals to protect important information versus the "right" of governments to listen to the communications of their adversaries.

Governments have always used export controls[1] on cryptography to attempt to control its proliferation and use against their interests. Even though the use of encryption is not controlled in most countries, U.S. Government export controls have seriously impeded the use of encryption in commercially available software products and thus its use by individuals and organizations within as well as outside the U.S. This de facto internal use control has served to increase the **tension** between the public and its government.

With the explosion of personal computers and global information infrastructures, this **tension** has increased further, as more citizens have realized that their sensitive information is openly vulnerable, and, some argue, the national economic interest is at stake.

Congressional hearings [Brooks] warned of serious consequences of foreign and domestic industrial and government espionage. National Research Council reports [NRC] repeatedly called for a careful examination of these issues.

A National Cryptography Policy?

During this period, a proposal was put forth for a national cryptography policy, which was intended to forge an acceptable balance between both sides:

> Good Cryptography shall be available to the public without government restriction, where
>
> > "Good cryptography" is defined as DES (with 56-bit keys) and RSA with a modulus less than 1024 bits, and
> >
> > "without government restriction" means without export control or other mandatory government restriction.

It was noted that the present de facto national cryptography policy in effect defines "good cryptography" as symmetric key algorithms restricted to 40 bits and asymmetric keys limited to 512 bits.

---

[1] A few countries such as France and Singapore also use import or internal-use controls.

Even though this proposed policy highlighted that the gap between the public's and the government's interests may be only the difference between 56 bits and 40 bits, that gap appeared effectively insurmountable.

The tension rose to the point where those who spoke in favor of the national economic interests and of the reality of worldwide availability of cryptography, even in the face of government export controls, were accused of acting against the interests of national security. Clearly something was needed to relieve this fundamental tension.

Enter Clipper - a Tension Reliever?

In April 1993, the U.S. Government introduced Clipper,[2] and with it a new concept, key escrow, which was intended to relieve some of the tension. The idea was to give the public good encryption, better than was generally available before, but retain the ability for law enforcement, when authorized, to access encrypted communications or files. It was hoped that this would satisfy the interests of both sides and relieve the growing tension.

But Clipper has problems. In order to provide better-than-commonly-available encryption, a classified encryption algorithm is used that must be embedded in hardware to be protected from disclosure. Software vendors want a software solution. The classified algorithm stirs suspicion: Is it really as good as claimed, or does it have special trap doors? Despite the early years of controversy, much of the public has come to trust DES to an extent that any other algorithm that has not undergone many years of public scrutiny will not be acceptable.

And the Clipper form of key escrow, which we will henceforth refer to as government key escrow, has problems of its own. It requires extensive government-controlled data bases of escrowed keys. Once the key for a hardware chip is revealed, that chip could be compromised forever. The government established a wide variety of procedures to safeguard against abuse: two key escrow centers so neither had the whole key, controls on who could access the escrowed keys, and more, but concerns remained.

The biggest problem with government key escrow is that it does nothing for the user or his or her employer. While it ensures that the government can always have access to a key to decrypt communications or files, if a user loses his or her key, government key escrow will not help. Any Marketing 101 class will convince us that a product that does little or nothing for its purchaser will not fare well in the marketplace. Without a solid market incentive, Clipper will likely be restricted to a segment of the market driven mostly by mandatory government requirements.

Following Clipper's introduction last year, opposition by the software vendors, civil liberties

---

[2] The Clipper Initiative includes programs such as Clipper for telephone devices and Capstone for computer applications. Throughout this paper the term Clipper will be used to refer to all U.S. government programs using key escrow hardware such as Clipper or Capstone.

First Step: A Clipper Software Key Escrow Design

In the spring of 1994, we developed a software key escrow system that we believe provides law enforcement capabilities equivalent to those of Clipper [TIS]. Designed to parallel government key escrow as closely as possible, our Clipper Software Key Escrow design (see Figure 1) has several advantages over the hardware Clipper system.

It can be implemented entirely in software (firmware or hardware implementations are also possible but not necessary). It can use any encryption algorithm for the basic encryption functions. Our design could be used with classified algorithms such as Skipjack, but software-only solutions will not protect the secrecy of the algorithm.

Our design uses public key cryptography, with the government controlling the private keys of the public / private key pairs associated with each software product. All of the information in the user's software packages is publicly available. This gives our approach a unique advantage in detecting spoofing of the Law Enforcement Access Field (LEAF). The receiving or decrypting program has available to it all of the information to completely reconstruct the LEAF and compare it with the received LEAF. In this way, our design can detect even single bit errors in the session key used in constructing the LEAF. Our design is not subject to the attacks on the Clipper design proposed by Matt Blaze [Blaze].

We have implemented our design in a prototype demonstration that has been shown widely to the government and industry. This demonstration has led to extensive discussions within government and between government and industry concerning the government's interest in software key escrow systems, as expressed in the Vice President's letter to Congresswoman Cantwell [Gore].

A Word on Software Binding

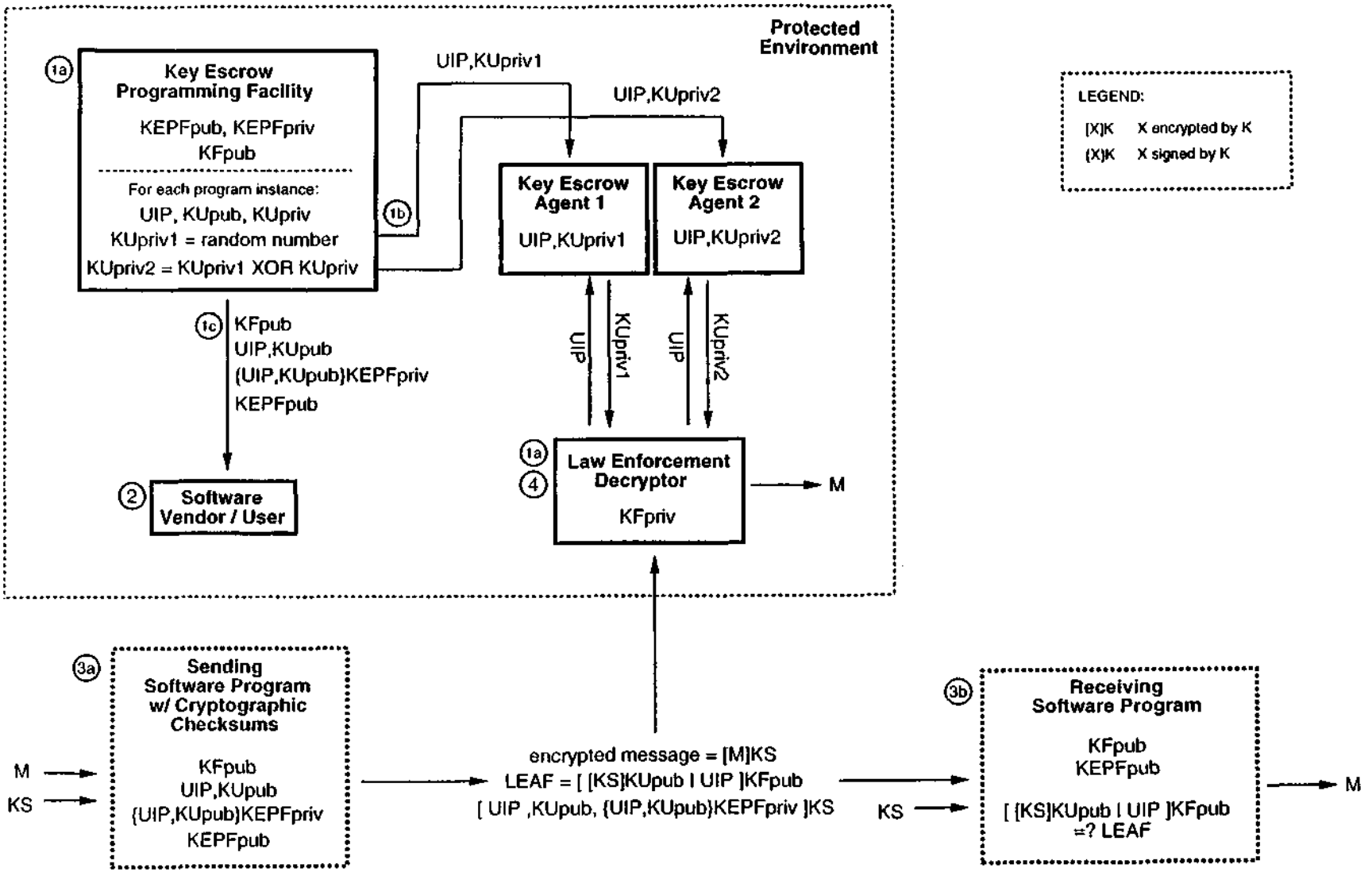
It is essential for any software key escrow system to be closely bound to the application that it is protecting.[4] Concerns for a user disabling the key escrow process or for pirated copies of an escrow-enabled software product being sold with the key escrow process disabled have been the major impediments to consideration of software solutions in the past.

In order to make progress, we must understand what we are trying to prevent with either a hardware or software solution. In either case, we cannot prevent someone from writing software that employs encryption without key escrow. We also cannot prevent a pair of sophisticated software hackers from modifying their own copies of a program that uses either hardware or

---

[4]One of the strengths of the Clipper design is that the government key escrow system is closely bound in hardware with the encryption process so that it is very difficult to disable the escrow process while allowing encryption and decryption to take place.

CLIPPER SOFTWARE KEY ESCROW



software key escrow since we know the dual-rogue issue cannot be stopped with either hardware or software.

The threat we must try to prevent in the case of software key escrow is the widespread deployment of a pirated copy of an escrow-enabled commercial product wherein the key escrow has been defeated. We believe that, against this type of threat, we can make software binding arbitrarily difficult and thus deter attempts to reverse engineer the original product. Such binding techniques will more likely force the pirate back to writing his or her own incompatible version from scratch. As with all such techniques, however, the more difficult one makes reverse engineering, the harder it may become to maintain the product. Such tradeoffs are part of the process we must all understand to build a system that satisfies all interested parties.

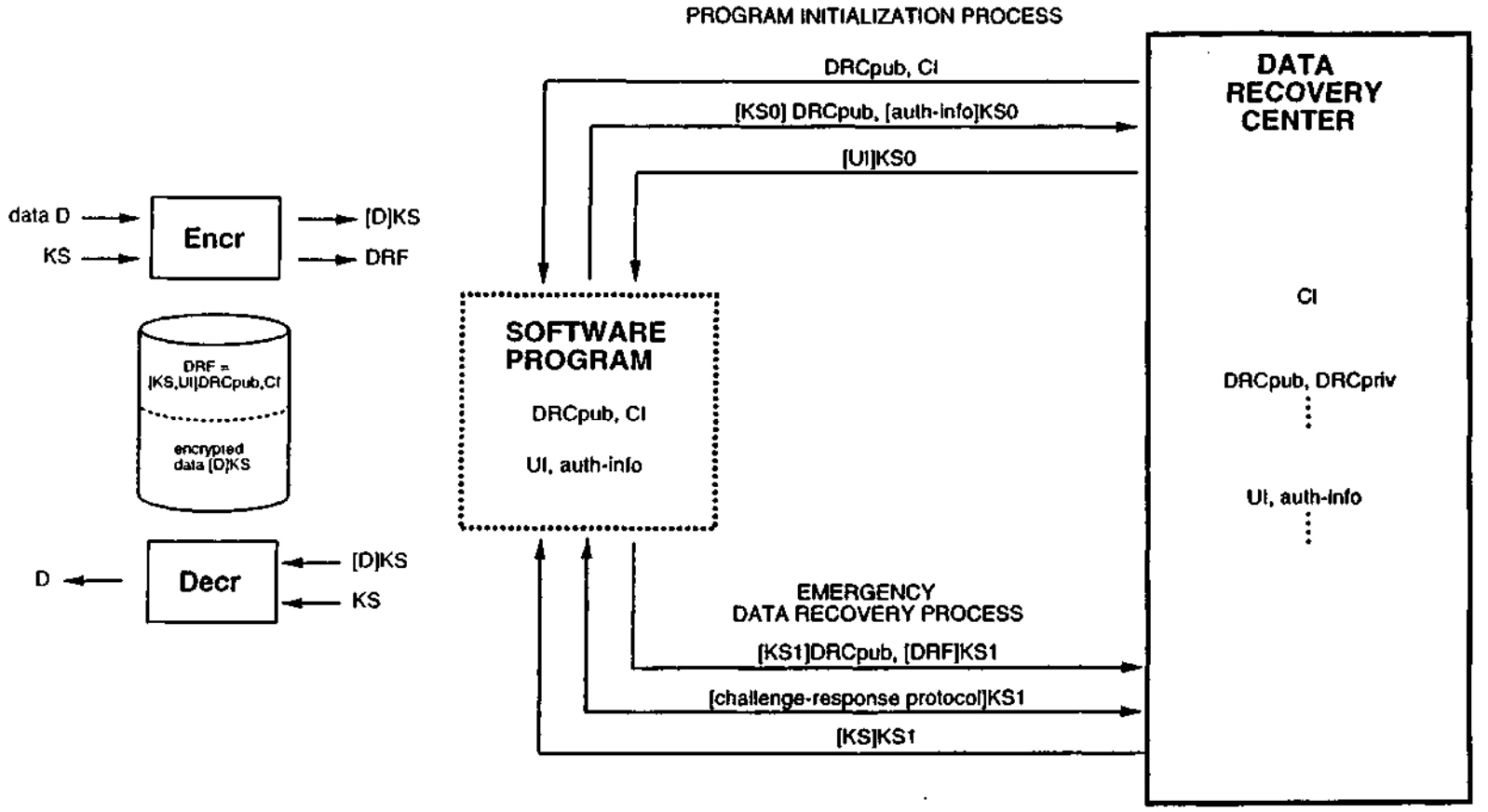
Second Step: A Commercial Key Escrow System

A software-based Clipper design is still a Clipper design, and we have already established that Clipper is not the tension reliever that we have been seeking. So in August 1994, we set about to devise a commercial key escrow system that would address the objections to Clipper without sacrificing the government's law enforcement interests.

Our commercial key escrow design (see figure 2) employs a Data Recovery Center (DRC) established by a commercial entity (a corporation might establish one for its own use or a bonded service organization might offer the service for the public at large). A corporate DRC will be a central point within the organization with which all corporate "escrow-enabled (EE)" software programs are registered. We envision the general process as follows:

> **Initialization:** Registration takes place when the user installs the EE program on his or her workstation or laptop. Registration consists of the user providing the DRC with the information needed to authenticate himself or herself if it should be necessary to recover a lost encryption key. During registration, the DRC will return to the user's program an identifier for the user, the DRC's public key (its private key is held in secret by the DRC), and the identity of the DRC itself.
>
> **Key Escrow:** Every time an EE program encrypts a file or message, it will add a Data Recovery Field (DRF) that contains the session key and user's identity encrypted in the DRC's public key and the DRC's public identifier. This information is stored within the file or message and is the only place that the encrypted session key is kept. There is no data base of escrowed keys at the DRC or any where else.
>
> **Recovery:** If the user ever finds he or she is unable to decrypt a message, the user need only send the DRF along with proper authentication to the DRC. The DRC will use its private key to decrypt the session key and return it to the user using a protected protocol exchange. If corporate management should ever need to decrypt a file or message from an employee who is unavailable, they can obtain the session key from the DRC by a similar means.

COMMERCIAL SOFTWARE KEY ESCROW SYSTEM



UI = user index
CI = [data recovery] center identifier
DRF = data recovery field = {KS,UI}DRCpub,CI
KS0 = session key for initialization process
KS1 = session key for emergency data recovery process
KS = session key for data encryption/decryption
(normal memory or exchange of KS not shown)

LEGEND:
[X]K X encrypted by K

Liability: The question of liability for loss of the information by improper disclosure is eliminated in the corporate case, since all of the information is already the property of the corporation. Liability in the case of a bonded public service DRC is no different from that faced by other bonded services.

Law Enforcement: If law enforcement authorities ever need to decrypt a file or message of an employee of a company, they need only approach management with appropriate legal authority, and they, too, can obtain the session key in question. The issue of law enforcement access is thus reduced to an already well-understood legal procedure. If law enforcement anticipates that it may encounter many such files or messages, it may be able to establish a means to obtain rapid access once initial authority has been obtained.

If an individual needs to encrypt information of a personal nature, he or she may decide to subscribe to one of many bonded commercial key escrow services that are expected to become available. In this case, only the user will normally be able to access the escrowed session key. But law enforcement, given the appropriate legal authorization, will again be able to access this information in a procedure similar to a normal search warrant process.

International law enforcement escrow key recovery also reduces to already well established procedures. If U.S. law enforcement authorities wish to recover encrypted files or messages from an American in the United Kingdom, they need only ask UK authorities for assistance in obtaining the session keys from the UK corporate or public DRC. The international nightmare of unilateral agreements to allow governments to share government escrowed keys is thus reduced to already- in-place international police agreements.

What Are The Alternatives?

To best understand why commercial key escrow may provide the best answer to the national and international tension between governments and their citizens, we must first understand who the players are in any such system and the consequences of choosing one approach over another.

Who Are The Players and What Do They Want?

First, the interests of the user, individual, and corporation, must be satisfied, for unless they are, no system will be of any value.

- The individual user wishes to protect his or her sensitive information using the best products and the best cryptography available while retaining the ability to recover encrypted information whenever an encryption key is lost.

– The corporation (or other organization) wishes to protect its sensitive information while retaining the ability to recover encrypted information whenever an individual user is unavailable for whatever reason.

Second, we must satisfy the interests of the software publishers, for without software the user will not have the products with which to achieve his or her goals.

– The software publisher wishes to provide the user, whether an individual or corporation, with the best possible product using the best possible encryption techniques available on a worldwide basis.

It is important to note that in general, neither the individual, the corporate user, nor the software publisher is in any way interested in doing any harm to the government's interests, either law enforcement or national security.

Third, the interests of the government, both for law enforcement and national security, must be met in any workable solution.

– Law enforcement must have the ability to decrypt communications of suspected illegal activities within its jurisdiction, when authorized.

– National security interests, including, when possible, the ability to decrypt the communications of terrorists and other adversaries, must be accommodated.

This set of what appear to be mutually conflicting requirements must all be balanced if we are to find the tension relaxer that we are seeking.

In the following section, we will examine a number of cases that represent the spectrum of key escrow alternatives. This analysis will be done in light of the particular interests of each of the players listed above.

How Many Ways Can We Escrow Keys?

Alternative 1: Do It Yourself

The first alternative is the simplest and most obvious one whereby each individual is responsible for safeguarding the encryption key of each message or file that the user encrypts. He or she does this by making an extra copy of the key and storing it on a floppy disk or other token that is stored in a safe place, like a safe deposit box, or with a trusted neighbor.

This simplest form of key escrow is one that everyone should be using, in the absence of a better alternative, and some people no doubt are, at least for especially sensitive encrypted files.

This approach is	GOOD	for the Individual, when it is used,
	BAD	for the Corporation,
	BAD	for the Software Publisher,
	BAD	for Law Enforcement,
	BAD	for National Security.

Since no one other than the individual knows how to recover the escrowed key, no one else can benefit from this alternative. Fortunately, this approach will never be used on a widespread basis and therefore represents one extreme in the overall key escrow spectrum.

Alternative 2: Product-by-Product Ad Hoc Solutions

The solution much more likely to become widely available is the one in which each vendor who produces a product that uses encryption creates a "backdoor" system administration function that can be used to recover encrypted data if the key is lost.

This is the nightmare situation for vendors. They do not want to advertise this capability since it represents a significant vulnerability for their product. But they cannot do without such a feature since their customer base will be very unhappy if they invest heavily in encrypting all their sensitive information only to find that it is all lost when they cannot remember the encryption key.

This approach serves an essential recovery function for the software publisher. It also is useful for the individual except that if each product he or she uses has its own "backdoor," the user will most likely be confused by the variety of ways to recover from lost keys. For the corporation, this is a very poor option since the confusion the individual encounters with multiple products is multiplied by the number of employees.

This alternative presents a disaster scenario for law enforcement and national security. If there is widespread proliferation of ad hoc product-by-product solutions, the interests of all governments in recovering encrypted information will be severely harmed now and for all the future.

This approach is	OK	for the Individual, but confusing,
	POOR	for the Corporation; too many options,
	OK	for the Software Publisher,
	POOR	for Law Enforcement,
	BAD	for National Security.

Alternative 3: Licensed Data Recovery Centers

This option is the principal topic of this paper. Companies and private organizations operate Data Recover Centers serving their own interests. This approach assumes that the DRCs are registered (or licensed) in the countries in which they operate so that law enforcement authorities can obtain access to them to recover file encryption keys when appropriately authorized.

This alternative is attractive to the individual and corporation because it provides a useful service, the recovery of encrypted data when the original encrypting key is not available, in a centralized and easily accessible manner. This approach is also attractive to the software publishers because it relieves them of the obligation to provide a system administrative function to recover keys when lost by the user.

Law enforcement will find this approach attractive since it provides a clear and convenient path to recovery of encrypted files. The identity of the DRC is contained within the file, and the file encryption key is readily obtained using normal search warrant or equivalent procedures. National security interests are better served by this approach than by the previous two since it is generally easier to deal with one common approach to escrowed keys than a multitude of ad hoc product-by-product solutions.

This approach is	GOOD	for the Individual,
	GOOD	for the Corporation,
	GOOD	for the Software Publisher,
	GOOD	for Law Enforcement,
	OK	for National Security.

Alternative 4: Government Key Escrow

This approach is exemplified by the Clipper system introduced by the U.S. Government in 1993. It serves the needs of law enforcement and presumably national security very well, to the extent that it is used by the public. But since it provides little incentive to the user, corporation, or software publisher, it is unlikely to see widespread commercial use and thus will fall short of its potential for satisfying the government's interests.

This approach is	POOR	for the Individual,
	POOR	for the Corporation,
	POOR	for the Software Publisher,
	VERY GOOD	for Law Enforcement, to the extent it is used,
	VERY GOOD	for National Security, to the extent it is used.

Looking at these four alternatives in the spectrum of key escrow solutions, alternative 3 looks the most attractive and the most likely to satisfy governments' interests if it became widely used.

The argument can be made that:

> If commercial key escrow such as outlined in alternative 3 above,
>
> > satisfies law enforcement's interests as well as Clipper and
> >
> > since Clipper-equipped devices are intended to be exportable (presumably to make them more attractive to a wider customer base),

then, it follows that alternative 3 appropriately bound with commonly available algorithms such as DES should also be exportable.

This leads to a fifth alternative:

Alternative 5: Licensed Data Recovery Centers with Exportable DES

In this approach, the software publishers can achieve their goal of worldwide availability for products with good quality cryptography. This would in turn lead to widespread use by individuals and corporations that would, in turn, lead to greatly expanded recovery of encrypted files by law enforcement, when authorized. Similarly, widespread use will make this approach much better for national security interests than the proliferation of ad hoc solutions described in alternative 2.

This approach is	VERY GOOD	for the Individual,
	VERY GOOD	for the Corporation,
	VERY GOOD	for the Software Publisher,
	VERY GOOD	for Law Enforcement,
	GOOD	for National Security.

But What If We Do Not Proceed With Alternative 5?

It is understandable that governments would prefer key escrow solutions such as Alternative 4 that provide them with full and complete control of databases of escrowed keys. But the last two years have shown that the issues associated with Clipper key escrow are sufficient that it will not achieve widespread use commercially.

While there is always a tendency in government to "stick with what we have," it is often necessary to look beyond one's own ideas and realize that by accepting an approach where the government has a little less direct control, all of the government's interests may be far better served.

The Commercial Key Escrow system described in Alternative 5 has the potential to become widely available throughout the computer and communications industry throughout the world because it provides a highly useful service to individuals and corporations / organizations worldwide. The exportability of a commonly available encryption algorithm such as DES, appropriately bound to the key escrow system, provides a powerful incentive to the software industry to make this approach widely available throughout all its products.

To the extent that CKE becomes widely used in the U.S. and around the world, **the government can ensure that law enforcement will have appropriate access** to encrypted files and communications, now and for the foreseeable future.

But if they should fail to promote CKE, with the export approved of appropriate encryption algorithms in a timely manner, the government will in effect be promoting the further development of ad hoc, product-by- product key escrow solutions, and, through the ensuing confusion, **ensuring that law enforcement and national security interests are seriously damaged,** now and for the future!

Unfortunately, there is little time left! While the government continues to "study the problem," more and more ad hoc solutions are being introduced in the marketplace! We predict that there is approximately a six-month window in which the government can exercise the only lever it has left, export control, to limit the expansion of incompatible product-by-product solutions and promote a solution that will help all parties involved.

A New National Cryptography Policy

If a Commercial Key Escrow system similar to Alternative 5 is adopted, we may soon all be able to relax our fundamental tension with a national cryptography policy such as:

> Good cryptography shall be available to the public without government restriction, where:
>
> > "Good cryptography" is defined as DES and RSA bound with commercial key escrow, and
> >
> > "Without government restriction" means without export control or any other mandatory restriction.

We believe that Commercial Key Escrow, properly bound with exportable DES, is the only way to reduce the ever-growing tension between the public and government interests in encryption. We hope that the U.S. and other governments around the world will take appropriate actions to enable this approach to succeed before its too late!

Status

Trusted Information Systems, Inc., is implementing its commercial key escrow system for use in all applications that offer encryption. TIS is working with software developers to include commercial key escrow user functions in their applications. An initial Data Recovery Center will be available for test use on the Internet early in 1995. Operational DRCs will be available for corporate and individual use later in 1995. Additional information can be obtained from: Trusted Information Systems, Inc., 3060 Washington Rd. (Rt. 97), Glenwood, MD 21794; Phone: (301) 854-6889 / FAX: (301) 854-5363 or via E-mail to: *tis@tis.com*

References

[Blaze] Protocol Failure in the Escrowed Encryption Standard, Matt Blaze, AT&T Bell Laboratories, Preliminary Draft, June 3, 1994.

[Brooks] Hearings before the Subcommittee on Economic and Commercial Law, Committee on the Judiciary, U.S. House of Representatives, Congressman Jack Brooks presiding, May 7, 1992.

[Cantwell] HR3627, 103rd Congress, 1st Session, November 1993.

[Gore] Vice President Al Gore, letter to Representative Marie Cantwell, July 20, 1994.

[NRC] Computers at Risk: Safe Computing in the Information Age, published by the National Academy Press, Washington, D.C., 1991.

Finding Common Ground: Export Controls in a Changed Global Environment, published by the National Academy Press, Washington, D.C., 1991.

Global Trends in Computer Technology and their Impact on Export Controls, published by the National Academy Press, Washington, D.C., 1988.

Balancing the National Interest: U.S. National Security Export Controls and Global Economic Competition, published by the National Academy Press, Washington, D.C., 1987.

[Time] Clipper-related articles appearing in TIME Magazine, March 14, 1994; NEWSWEEK, March 14, 1994; US NEWS AND WORLD REPORT, March 14, 1994; among others.

[TIS] A New Approach to Software Key Escrow, Trusted Information Systems, Inc., August 15, 1994.