NISTIR 5468

Report of the NIST Workshop on Key Escrow Encryption

Arthur E. Oldehoeft
Department of Computer Science
Iowa State University

Edited by

Dennis K. Branstad
Computer Systems Laboratory

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

NIST

NISTIR 5468

Report of the NIST Workshop on Key Escrow Encryption

Arthur E. Oldehoeft
Department of Computer Science
Iowa State University

Edited by

Dennis K. Branstad
Computer Systems Laboratory

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

June 1994

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arati Prabhakar, Director

Contents

1 Introduction

1.1 Background

As the U.S. builds its National Information Infrastructure (NII), wide-spread use of encryption will be needed to protect sensitive information. However, wide-spread use of unconstrained encryption makes lawfully-authorized electronic surveillance difficult, if not impossible.

In attempting to balance the need for privacy and the need for lawful surveillance, a Key Escrow Encryption (KEE) technology was developed by the National Security Agency (NSA). The Escrowed Encryption Standard (EES) based on the KEE was issued by the National Institute of Standards and Technology (NIST). Approved by the Secretary of Commerce[1], this voluntary standard seeks to satisfy the need for privacy while preserving the ability to perform lawfully authorized wiretaps. This escrowed encryption technology is embodied in an electronic chip containing the SKIPJACK algorithm for encryption of information and the technology for creating a Law Enforcement Access Field (LEAF) for use in many telecommunication applications. Both the SKIPJACK algorithm and the LEAF creation method are classified. The standard is intended to facilitate the acquisition of devices that implement KEE technologies by Federal government agencies. Its use is not mandated for Federal agencies, the private sector, or other levels of government.

In using the Escrowed Encryption Standard, communications are encrypted by the SKIPJACK algorithm using a session key agreed upon by the participating entities. The appended LEAF field, which contains among other things the session key (encrypted using the device unique key), is itself encrypted with an 80-bit family key. The only known way of recovering the session key is to first recover the two 80-bit components of the device unique key. Each of these components is "escrowed" (i.e., filed) in encrypted form with one of two escrow agents. The two escrow agents act under strict procedures that will ensure security of the key components and govern their release. Surveillance requires acquisition of both escrowed key components, through a predefined process.

Based on the desire to use existing expertise in the private sector and motivated partially by requirements of non-government entities, NIST has invited interested industry and academic partners to join a cooperative research consortium for developing the next generation of encryption technology that contains integrated cryptographic key escrowing techniques. In addition, an informal industry/government working group was established to explore the possibilities of software implementation of key escrowing. Finally, representatives from key U.S. industries were invited to participate in this workshop in order to initiate a dialogue on the issues of escrowing encryption keys. This partnership with the private sector is necessary to arrive at a mutually acceptable solution that will balance the need for privacy, the need for lawful electronic surveillance, and the needs of industry, both as users and vendors.

[1] The following three quotations are from a February 4, 1994 a statement released by the White House Secretary:

"Advanced encryption technology offers individuals and businesses an inexpensive and easy way to encode data and telephone conversations. Unfortunately, the same encryption technology that can help Americans protect business secrets and personal privacy can also be used by terrorists, drug dealers, and other criminals."

"... the Administration is announcing its intent to work with industry to develop other key escrow products that might better meet the needs of individuals and industry, particularly the American computer and telecommunications industry."

"The Administration is expanding its efforts to work with industry to improve on the Key Escrow chip, to develop key-escrow software, and to examine alternatives to the Key Escrow chip."

1.2 Participants

INDUSTRY ATTENDEES

Allied Signal	J.P. Niehus
AT&T	William Franklin
	Phil Servidea
Compaq	Michael Angelo
Computer Associates	Lynn Grant
	Ken Farber
DEC	Roger French
EDS	Bill Poulos
Fischer International	Addison Fischer
Hewlett Packard	Jim Schindler
	Keith Klemba
IBM	William Whitehurst
Iris Associates	Alan Eldridge
Motorola	Larry Puhl
Novell, Inc.	Roger Schell
Oracle	Linda Vetter
	Laure Mann
Racal-Guardata	Don Cole
Semaphore	William Ferguson
Software Publishers Association	Doug Miller
SPYRUS	Russ Housley
Sun Microsystems	Whitfield Diffie
Tandem/Atalla	Dale Hopkins
TECSEC	Jon Roberts
	Edward Scheidt
Trusted Information Systems	Stephen Walker
	Dave Balenson
	Steven Lipner
WordPerfect	Cameron Mashayekhi
UNISYS	Steve Semen
Uptronics	Jimmy Upton

GOVERNMENT/ACADEMIA ATTENDEES

Executive Office of the President	Skip Johns (OSTP)
	Rich Wilhelm (NSC)
	Ed Springer (OMB)
	Tina Westby (OMB)
Department of Justice	Geoff Greiveldinger
	Kent Walker
NIST	Ray Kammer
	James Burrows
	Lynn McNulty
	Dennis Branstad
	Miles Smid
	James Dray
	Arthur Oldehoeft
	Ed Roback
	Anne Enright-Shepherd
NSA	William Crowell
	Ed Hart
	Rick Proto
	Jan Manning
	Jim Arney
	Don Lewis
OTA	Tom Hausken
SPAWAR	Francis Deckleman
Georgetown University	Dorothy Denning
MIT	Silvio Micali

1.3 Agenda

NIST Lecture Room B, Friday, June 10, 1994

Opening Session

8:45 Registration (Outside Lecture Room B)
9:00 Welcome: Raymond G. Kammer, Deputy Director, NIST
9:05 Workshop Overview and Participant Introductions: F. Lynn McNulty, CSL, NIST
9:15 Objectives of Key Escrow Encryption: Lionel S. "Skip" Johns, OSTP
9:40 NSA Perspectives: William P. Crowell, Deputy Director, NSA
and Edward A. Hart, Deputy Director for Information Systems Security, NSA

Current Key Escrow Encryption Method

10:00 Current "CLIPPER" Key Escrowing Method: Miles Smid, NIST
10:25 Industry Perspectives: (Position Papers, Participants)

Key Escrow Encryption Alternative #1

11:00 Coordinator: Don Cole, Racal-Guardata, Inc.
Software Key Escrowing Proposal: Stephen Walker and
David Balenson, Trusted Information Systems
11:30 Lunch

Key Escrow Encryption Alternative #2

12:30 Coordinator: Jimmy Upton, Uptronics
Multi-Purpose Key Escrowing Methods: Silvio Micali, MIT
Private Escrow Key Management: Jon Roberts, TECSEC
Industry Responses, Suggestions: Participants
2:00 Break

System Integrity Requiremennts

2:30 Coordinator: James Dray, NIST
Criteria for High Integrity Software: Jim Arney, NSA
System Requirements for Software Integrity:
Stephen Walker, Trusted Information Systems
Industry Suggestions: Participants

International Aspects of Key Escrowing

3:45 International Aspects of Key Escrowing:
Dorothy Denning, Georgetown University
Industry Suggestions: Participants

Summary and Future Directions

4:15 Summary/Future Directions: F. Lynn McNulty (Discussion)
4:45 Adjourn

2 Session Summaries

2.1 Session 1: Opening Session

Senior government officials discussed the objectives of the workshop in light of the key escrow encryption initiative announced in April, 1993. This initiative seeks to provide good encryption-based security to a number of information processing environments while preserving the lawful interests of law enforcement and national security. The Escrowed Encryption Standard (EES), announced as Federal Information Processing Standard 185 on February 4, 1994, resulted from this initiative. In addition, the "CLIPPER" escrowed encryption device was designed and built under this initiative. Finally, a Key Escrow System is being designed and implemented to store the escrowed keys securely and make them available to authorized entities for legally authorized electronic surveillance.

Raymond G. Kammer, Deputy Director of NIST, and F. Lynn McNulty, Associate Director for Computer Security at NIST, provided the welcoming and introductory remarks. (Mr. McNulty also served as moderator for the workshop.) Mssrs. Kammer and McNulty stated that the objective of the workshop was to engage the private sector in dialogue on the issues of key escrow encryption.

Lionel "Skip" Johns, Associate Director of Technology, Office of Science and Technology Policy, Executive Office of the President, stated that the National Security Council has the responsibility of coordinating security policy in the Executive Branch of the U.S. Government. Intelligence remains a critical activity of national interest and the U.S. must be able to detect and act in a timely manner on real threats of terrorism, crime, and danger to the national security. OSTP seeks to engage in dialogue with U.S. industry so that effective intelligence collection can be conducted with a minimal threat to privacy. He stated that acceptable solutions may be hard to find and, unfortunately, a final solution may be suboptimal.

William Crowell, Deputy Director of the National Security Agency, pointed out the need to ensure that a balance is achieved among four equities: privacy, public safety, ability to market new products, and national security. Three options, when implementing cryptography, are possible: flawed cryptography, strong cryptography with contents unreadable by all, and key escrowing. The latter seemed to have the most viability for achieving balance among the four equities. CLIPPER is a first (interim) solution – there is a need to look at more software intensive solutions. Edward Hart, Deputy Director for Information Systems Security, NSA, reiterated NSA's desire for openness, collegiality, and desire to work with U.S. industry in seeking mutually acceptable solutions.

Industry participants, in an open discussion, raised the following issues/questions/concerns:

1. Currently the delay in obtaining licenses to export products prevents U.S. industry from being internationally competitive.

2. The uncertainty over whether a license will be granted discourages even applying for a license. There needs to be more information as to what applications have been made and their disposition. A counter-point is the need for nondisclosure of export license applications that might compromise the economic interests of the applicants or compromise the interests of national security.

3. Given the four equities, how are we planning for change? It is important that we not be constrained in meeting future needs.

4. If the CLIPPER Chip is only an interim solution, why not wait for a final solution? The response was that key escrowing is an integral part of current cryptography policy and will be so through all stages of evolution.

5. Foreign countries have proprietary encryption algorithms that they want to put into chips. What restrictions apply on manufacturing the chips in the U.S.? Is an open dialogue with NSA possible on this? NSA stated that they supported the capitalistic free enterprise system and invited dialogue with industry on the issues as how the current regulating processes might be changed.

6. It was noted that security of information is an international issue and is not a new issue.

7. There is a need for NSA to have a dialogue with industry and academia to define new processes to meet the requirements of global information security. The primary concern for industry is satisfying the security needs of their commercial customers. The response was that a process has to be developed, amenable to all interests.

8. Concern was expressed for the feeling that, when industry raises an export problem with NSA, industry representatives have their integrity questioned. NSA needs to be more responsive and less critical of intent.

9. Concern was expressed that there may not be a satisfactory solution to balance the four equities.

10. With regard to the import/export of cryptography, individuals in foreign countries want to use their own algorithms – they do not trust ours. At present, we are unable to export the technology they want. The response was for industry to provide the technology to NSA for their approval for export.

    It was further noted that foreign countries sell DES products to the U.S. but the U.S. cannot sell U.S. products containing DES to them. For example, DES can be purchased in such places as Moscow, Singapore, and Stockholm. Kerberos, with any encryption technique, is available outside the U.S. but U.S. industry is not allowed to export it. U.S. companies are unable to compete for the global market for cryptographic devices and, from the standpoint of technology and economics, are falling behind (or losing ground to) other nations.

11. Concern was expressed for the the fact that U.S. processes dealing with import/export are too far behind to be effective – DES was cited again as an example. For international competitiveness, the U.S. needs to not only speed up the process, they must be able to be ahead of the curve in determining what new processes will be needed.

12. NSA was encouraged to form a task force on the exportation of cryptography to technology in order react quickly to the market demands for solutions – there is a need to establish this task force this fiscal year. NSA must meet industry somewhere within the 60%-40% compromise lines.

13. With regard to the four equities, it was noted that not everyone understands them in the same way. There is a need for more solid information about what the problems are and what is required to solve them.

2.2 Session 2: Current Key Escrow Encryption Method

This session summarized the current key escrowing system designed to work with EES devices such as CLIPPER. Industry representatives were given the opportunity to present their positions.

2.2.1 Current "CLIPPER Chip Key Escrowing System", Miles Smid, Key Escrow System Program Manager, NIST

Intensive work on the key escrowing system began with the April 16, 1993 announcement of the KEE Initiative. NIST appointed a program manager in August. In addition to NIST, other participating agencies are the Department of Justice, the FBI, the Department of Treasury, and the NSA.

View graphs were shown describing how the KEE system is designed to work: manufacturing of the chip, programming of the the chip, key escrowing with two independent government agents (NIST, Department of Treasury), obtaining court authorization for a wire tap and the corresponding release of keys, and decryption of communications.

Four phases of key escrowing have been defined. The first phase, consisting of developing a prototype system, has been completed. The first programming of a chip took place in October, 1993 and by March, 1994, the keys for 17,000 CLIPPER chips had been escrowed. At present, no key components have been released. Phases 2-4 are designed to move from the prototype system to a target production system. The target system will include automated procedures for handling and storing escrow components, a decryption processor, a simple key component extraction system, an escrow agent workstation, and a transition to life cycle support. A number of evaluations are planned during phases 2-4. Recent efforts have included preparing for key escrowing for CAPSTONE. Also, the Vice-President has asked for a review of other possible escrow agents.

In discussion, several questions were raised:

Q1. How does a foreign law enforcement agency get the ability to lawfully decrypt?

Discussions on this issue are currently underway.

Q2. Will KEE technology be exportable to foreign countries for their use or will it be restricted to Americans for individual use overseas?

Encryption devices can be carried out of the U.S. temporarily for personal use without a license. KEE devices may be exported to most end users after an initial review and will qualify for special licensing[2].

Q3. For decryption, does one have to know in advance what the chip ID is?

No, the chip ID is in the LEAF.

Q4. Will the escrow agencies need a presence at the programming facility during phase 4?

At this point, we do not know if sufficient assurance will allow for a non-presence.

Q5. What are the consequences of a non-accredited key escrow system?

Key components will not be released until accredited.

[2] See February 4, 1994 statement by Dr. Martha Harris, U.S. Department of State, on "Encryption – Export Control Reform".

Q6. In production lots of 10,000, present cost estimates are $15 for a CLIPPER Chip and $90 for the CAPSTONE. These costs may be prohibitive. Will they be reduced?

Efforts are underway to reduce costs.

2.2.2 Industry Perspectives

The written position statement of several industries and the technical papers of some presenters appear in Appendix A. The following are brief position statements verbally offered by various industry representatives.

1. AT&T

   We are currently selling equipment with an optional built-in CLIPPER chip. It is important to move forward with reasonable solutions. Our current sales are mostly to the government and to a lesser extent to commercial customers. The prices of both CLIPPER and CAPSTONE are of great importance.

2. Compaq:

   We need to compete with competitors in the foreign marketplaces. Economic espionage is a major concern. We would like to use CLIPPER, but we need to know the import/export restrictions. The preliminary cost figures are too high. We have no position at the moment on key escrowing issues.

3. Computer Associates

   We are a large software vendor with a large foreign and domestic customer base. We deal with multiple platforms which causes some problems. We do not want to depend on hardware manufacturers for encryption; we are more interested in software encryption. Encryption standards are needed, but they must be wanted by the customers. We need to be able to export our products.

4. DEC

   What we sell depends on what the customers want and what the government will allow. We are apprehensive about key escrowing.

5. Fisher International

   We have been doing software key escrowing for a decade for use on portable computers and PCs. We developed the system, including sharing of keys, because customers have a fear of encryption and losing their encryption key.

6. Hewlett-Packard

   A slide was shown depicting sales world-wide – government vs. commercial and foreign vs. domestic. The commercial sector tends to be leery of government solutions. (Some of HP's work was described during the time allotted in Session 5 for industry participants.)

7. IBM

   U.S. manufacturers enjoy significant foreign sales. The National Information Infrastructure will "not" be national; it will be global. It needs to be secured and therefore security is a global issue. In government/industry dialogue, it is necessary to talk about industry requirements and objectives, not just get industry perspectives.

8. Tandem/Atalla

   The commercial banking industry will not accept government control of key escrowing. Commercial needs have to be evaluated and solutions must work across multiple platforms. Implementations on various platforms requires hybrid hardware/software solutions.

9. WordPerfect

   We are a software company and need a software implementation. If current system becomes a standard, the software will have to interface with the hardware. If the algorithms are a closely guarded secret, software implementation becomes a problem.

10. Uptronics

    We are a service organization. We need a healthy growing business in cryptography. The issues need to be resolved.

11. Motorola

    Cellular phone conversations are clear at the switch and therefore do not need key escrow to allow for law enforcement. Most customers expect security at no additional cost. Encryption algorithms should be available to all manufacturers worldwide. Manufacturers need to be able to implement the encryption algorithms in their own processes; the method for doing the key escrow needs to be simplified; standards have to be defined. The current direction in using smart cards for authentication do not match concepts for key escrowing.

12. Novell

    We are a software vendor with an international market across a lot of different platforms. An algorithm in hardware requires a software interface. Business has to be built on widespread international adoption; one cannot afford to uniquely tailor a product for a specific environment. Export is of significant concern; controls have an increasingly adverse impact on competitiveness. In the key escrow process, who will be the alternate key escrow agents (government only, U.S. only)? How will the integrity of the programming process be ensured? Why should the customer trust it? Is there publicly available information on the certification process?

13. Oracle

    We are a large software vendor on hundreds of platforms in heterogeneous environments. Software solutions are important for interoperability; it would help such things as installability and cost. Standards are needed for exportability. The four equities listed by NSA are too narrow; they must take into account the international aspects of things. We would like DES plus a key exchange standard.

14. SPYRUS

    We are a small security products company. Our customer base is divided into groups of "do not care", "no way", and "yes, we want escrow". There are three applications: message (e.g., email), streams or circuit encryption, and packet encryption. In the latter, there is concern that the overhead of the LEAF is larger than the packet. There is a need to design cryptography systems with "holes" to allow teaming with other entities who can fill the "holes" with appropriate encryption algorithms.

15. Sun Microsystems

    More than half of our business is outside the U.S. We are mostly concerned with software solutions, albeit we build hardware. There is concern about government controlled encryption, there is worry about customer acceptance.

16. Semaphore

    We are on record as being in favor of key escrow as a technology. We need a corporate entity to be a key escrow agent – large banks want this. A range of vendors is needed to build chip solutions – to allow integration of SKIPJACK. Internationalization has other twists with impact on global economies. Consider a U.S.-based company with U.S. equipment which is purchased by a foreign-based company. If the equipment is not exportable, does it have to be returned?

17. TECSEC

    See the presentation in Section 2.4.

18. TIS

    Key escrowing like wire-tapping can encroach on personal privacy. Americans will not accept the concepts unless Congress passes the necessary laws. See the presentations in Section 2.3 and 2.5 for other comments.

2.3 Session 3: Key Escrow Encryption Alternative #1

Session Coordinator: Don Cole, Chief Scientist, Racal-Guardata, Inc.

NIST has published announcements seeking Cooperative Research and Development Agreements (CRADAs) with organizations having the capability and interest in developing alternative key escrow encryption methods, especially in software but also in hardware. As a result, several organizations are participating in a Key Escrow Encryption Working Group seeking to specify requirements and acceptability criteria for key escrow encryption systems and then to design and/or evaluate candidate systems.

2.3.1 A Software Key Escrow Approach, Stephen T. Walker (Member of Working Group) and David M. Balenson, Trusted Information Systems, Inc.

A working group consisting of four non-government individuals (Cole, Denning, Upton, Walker) and two government agency individuals (Arney, Branstad) have been exploring ways to perform key escrow encryption in software. The motivation is to develop a broadly acceptable, low-cost system that achieves the objectives of law enforcement. It does not solve problems that CLIPPER/CAPSTONE do not solve as both can be defeated by a determined software hacker.

Many aspects of the design and usage are similar to the specifications in the EES. Rather than secret key cryptography, the proposed model uses public key cryptography and will work with any public key algorithm although software implementations cannot keep the algorithm secret. It will work with PCM cards. Components of a private key are escrowed with two independent escrow agents. Each instance of the software is a shrink-wrapped package, with a unique ID assigned to it either at the time of creation or the time of first invocation, and with embedded cryptographic checksums to guard against code modification. This ID is provided in a LEAF which is created by the software when invoked. The method of escrowing keys and their authorized retrieval by law enforcement agencies was outlined.

TIS is currently building a working prototype. They are also looking at some alternatives that do not parallel the aspects of CLIPPER/CAPSTONE.

2.4 Session 4: Key Escrow Encryption Alternatives #2

Session Coordinator: Jimmy Upton, President, Uptronics

Individuals may desire key escrowing as a backup procedure in case the normal key management system malfunctions or their valuable information cannot be decrypted because the key is lost. Corporations may desire key escrowing to prevent employees from holding encrypted information "hostage". Representatives from academia and industry presented approaches to key escrowing for corporate purposes and for multiple purposes.

2.4.1 Multi-Purpose Key Escrowing Methods, Silvio Micali, Massachusetts Institute of Technology

Key escrowing is fundamentally a good idea, but something more is required. The need for key escrowing may arise in multiple contexts: state vs. company (may need keys escrowed inside), communications vs. stored data (will be retrieved later), simple private call (friend) vs. recorded private call (stock broker), national vs. international context, etc. What is needed is multi-purpose key escrowing.

The proposal is for "Fair Public Key Cryptography (PKC)" as an alternative to the CLIPPER Chip. Fair PKC is distributed, flexible, open, economical, and complete, whereas the CLIPPER Chip is centralized, rigid, hidden, expensive, and partial. Private key cryptosystems have limited use because of the need for key management; on the other hand, in public key cryptosystems, through the use of public directories, it is easy to talk to someone you have never met. In the CLIPPER chip, the focus of attention has been on the issues of escrowing, but communicating entities still need to establish a session key.

From a law enforcement perspective, the idea of combining public key cryptosystems with private key cryptosystems is not a good one. Individuals can use the public system to exchange the private key K and then can use a standard method (e.g., DES) to encrypt. The key is not available to law enforcement for an authorized wiretap. Furthermore, the encryption can be made reasonably strong, e.g., $E_{K_1}(D_{K_2}(E_{K_1}(message)))$.

Fair PKC works in the following way. First, determine a public key PK, secret key SK pair. The secret key is divided into two components SK_1 and SK_2, the first of which is escrowed with trustee T_1 and the second escrowed with T_2. Each of T_1 and T_2 can certify that they have a legitimate component of SK without actually knowing the other component. The public key is filed with a center and approved (i.e., made available for distribution). Law enforcement requires acquisition of the secret key components from the trustees.

Here is an analogy of how Fair PKC might work. Suppose the public key is X and the private key is $\sqrt{X}$, where the square root is performed modulo some number n. The difficulty of finding the secret key is based on the difficulty of finding the square root (which is as hard as factoring). The user selects two numbers which are defined to be $\sqrt{a}$ and $\sqrt{b}$ and serve as SK_1 and SK_2. The user forms a = $(\sqrt{a})^2$ and b = $(\sqrt{b})^2$,the public key $X = a*b$, and the secret key $\sqrt{X} = \sqrt{a}*\sqrt{b}$. Trustee T_1 is given $(X, a, b, \sqrt{a})$ and T_2 is given $(X, a, b, \sqrt{b})$ where a is less b. T_1 can check $X = a*b$ and $(\sqrt{a})^2 = a$ and similarly T_2 can certify that it has a component of a legitimate secret key. But each is unable to determine the component held by the other trustee. A law enforcement agency, if authorized, can obtain the components from the trustees and form the private key $\sqrt{X}$.

An important fact is that there is more than one (modulo n) factorization of $X = a*b$, so the key can be escrowed in different ways with different trustees.

In comparing the CLIPPER chip approach to Fair PKC, one finds:

- Control: With CLIPPER, the user does not choose the encryption algorithm. With Fair PKC, the user chooses both the algorithm and the keys.
- Cost: CLIPPER requires secure hardware. Fair PKC allows either hardware or software.
- Prior Exchanges: In using the CLIPPER chip, a prior exchange of the session key is necessary. In Fair PKC, no prior exchanges are required.
- Compatibility: Using CLIPPER, there are only two trustees. In Fair PKC, many independent sets of trustees are possible.
- International Isolation: With CLIPPER, yes – with Fair PKC, no.
- Ambiguity: With CLIPPER, yes – with Fair PKC, no.
- Reliability: In CLIPPER, if a single trustee goes down, the court-authorized wire-tapping is not possible. In Fair PKC, "n of m" trustees is enough, e.g. 3 of 5.
- Duration of Tap: With CLIPPER, a tap can be forever. With Fair PKC, a tap is only for a court-authorized period of time.

The right key escrow system should be flexible, interoperable, economical, simple, and multi-purpose.

2.4.2 Private Escrow Key Management, Jon L. Roberts, President, TECSEC, Inc.

The espoused encryption model would maintain privacy at the "file level". It is then no longer necessary to secure the channel in order to maintain privacy of communicated information. Individuals would be in charge of encrypting their own files and would maintain their own own keys in a manner regulated by legislation. In the event of a suspected crime or a suspected threat to national security, the government can obtain a court order and subpoena the keys. The theory is that individuals who, to avoid prosecution, destroy their keys would also destroy their access to the information. To operate in the international arena, there would be a suite of multiple independent software algorithms that would satisfy the international community and the U.S. government. TECSEC has an application program VEIL that supports these ideas.

2.4.3 Industry Comments

C1. A lot of corporate America is afraid of encryption – afraid that keys may be lost or forgotten, information may be held "hostage", or information may be used against them. This indicates a need for the corporation to manage the keys. These keys could be encrypted with a public key so they could always be retrieved.

C2. There is concern that with software one cannot protect against a sophisticated, dedicated hacker. The concern is that we have the necessary structure in the software that could fix a problem when it occurs, i.e., the software should not have a fundamental weakness. The response was that we should not try to make things impossible because in an escrow system, the trustees must be compromised in order to enable a hacker.

C3. We now have seen several alternatives. Are any of these attractive to the various stake-holders? The response was that key escrowing is fundamentally good from the corporate viewpoint, as well as from the viewpoints of law enforcement and national security, because it provides the ability to recover a key in the event that it becomes necessary to do so. So, cooperation is in the best interests of all the stake-holders.

C4. I am a supplier for the government. Often times, the government waives the requirements of a FIPS because some products do not comply and it would be too expensive to make them comply.

C5. The premise of the discussion is that people will want to have their public keys registered in a directory. But what about the individual who does not care and avoids escrowing keys? The response was that one cannot protect against this kind of individual without passing laws of compliance and society has a legal system to deal with noncompliance.

2.5 Session 5: System Integrity Requirements

Session Coordinator: James F. Dray, Advanced Authentication Initiative Leader, NIST

Use of a key escrowed encryption device in a security application requires a high level of system integrity to assure that all security relevant events are performed correctly. Utilization of a key escrowed encryption device (e.g. CAPSTONE) in a more complex information processing application such as distributed electronic commerce requires many functions of the computer system to have high integrity, both to assure that the data is properly protected and also that the the LEAF field is transmitted and received properly. Integrity requirements for software encryption and operating system controlled execution were the subject of this session.

Jim Dray presented a model for an escrowed encryption device. Important points to be noted are the need for an interface between the cryptographic device and the general purpose system and the need to communicate through untrusted layers of software. The threat scenarios include all communication pairs: rogue system/rogue system, rogue system/legitimate system, legitimate system/legitimate system. The high-level implications are that one needs to prevent use of an EES device that circumvents the LEAF; it would be ideal to design cryptographic modules to withstand attacks in an untrusted environment; and the LEAF imposes additional requirements.

2.5.1 Criteria for High Integrity Software Encryption, James W. Arney, Chief, Developmental Systems Security Evaluation Office, NSA

A system security paradigm was outlined for evaluating KEE alternatives. It is important to remind oneself about the user/customer needs for integrity, confidentiality, and availability. Design requirements are needed to approach the problem. The development of a solution is evolutionary because initial perspectives may be short-sighted and because threats may change. Evaluation/verification is required. The design requirements need to consider both the higher algorithm/protocol level and also the implementation level in hardware and software. Good software engineering is a starting point to the effective protection of embedded software cryptography.

2.5.2 System Requirements for Software Integrity, Stephen W. Walker, President, Trusted Information Systems, Inc.

Software integrity is needed unless the entire computing system is packaged in a box that is highly resistant to reverse engineering. Two years ago, TIS was asked by ARPA to develop technical means for controlling high-performance workstations so that the government might be willing to allow their export to such countries as China and Russia for use in "approved" applications. In this project (called the ARPA Safeguards Project), a technology base was identified for controlling the execution of the operating system so that it would only run on a given machine; its modification would be resisted by storing it on some kind of read-only medium; and it would be packaged in a tamper-resistant box (which included methods of tamper detection and audit reporting to the U.S.).

The insight gained in developing these controlled execution procedures is directly applicable to any software system where the integrity of the software must be preserved. It can be used for controlled execution of an operating system. The programs are stored on ROM and require a digital signature as authorization to effect an update (therefore also resistant to viruses).

The analysis performed in this project has shown that these same techniques can be used in software-only deployments of encryption and key escrow. The approach will not allow the use of classified algorithms in software since there is no way to protect them from disclosure.

2.5.3 Industry Suggestions, Participants

Jim Schindler and Keith Klemba described the work of Hewlett-Packard Company. HP had looked at its domestic/foreign customer base to determine what was needed. The sentiments were that security functions were needed in both hardware and software; there was a need to stabilize the manner in which the crypto technology interfaces with applications; and a common cryptographic policy framework was needed for various governments.

HP has designed a "national flag" card (NFC), about the size of a postage stamp, that would enforce the cryptographic policy of a nation. The NFC would fit into a drawer in a cryptographic unit (CU) which is designed to provide cryptographic services (under the strict control of the NFC). The NFC is removable, interchangeable, and expirable. The CU would be designed for performance and protection with customization for a given host system. The initial discussions for the CU have centered around a PCMCIA hardware format. The CU features protection of the keys and algorithms and would likely have to be certified.

The host system is some hardware component that delivers information technology service to the user (e.g., personal computer or laptop, workstation, network server, mainframe, network printer, personal digital assistant). Gateways would be required to allow for two nationality systems to interconnect. There would be free export of the host system, and national security fears would be eased because governments can play a role.

The key points are

1. HP wants to sell equipment everywhere and needs the cryptography issue problem to be solved.
2. The PCM card with interchangeable national flag unit is a possible solution. HP is planning a controlled experiment to demonstrate its feasibility.
3. What is proposed here is of general interest – not just HP's interest.

2.6 Session 6: International Key Escrow Encryption - Proposed Objectives: Dorothy Denning, Georgetown University

Dorothy Denning talked about her personal research on international aspects of key escrowing. Four general requirements were identified for an international key escrow system: encryption products that provide secure communications, a key escrow system for authorized government access, international communications, and use of encryption products outside of the country that holds the key.

The general properties of escrowed encryption are: strong security, authorized government access, hardware or software implementations, classified or unclassified algorithms, multiple standards and gateways, and private sector key escrow - separate or integrated.

National control is needed over the import/export/use of products and over who holds the keys. International and bilateral agreements are needed to assist in criminal investigations, sharing of technologies, and constraints on the sale and use of products. Several national policy options for export and for internal use of products were presented. Law enforcement scenarios were enumerated, e.g., country A wishes to investigate subject X from country B and country C holds the encryption key.

Industry Questions/Comments

Q1. How do the presented requirements and solutions correspond with actual international law enforcement requirements and solutions? Professor Denning stated that there had been no official law enforcement review of the ideas presented. However, informal comments that had been received showed a large correspondence between the requirements stated and those presently identified within the law enforcement community.

Q2. Concern was expressed that it may not look good to be studying these issues now, more than a year after the initial announcement.

3 Actions

3.1 Government Proposed Post-Meeting Action Plan

At the final session of the workshop, Lynn McNulty presented a government proposal for post-meeting actions. Industry participants were asked to review the proposal and decide whether they would agree to participate in a task force.

3.1.1 Assumptions

- All parties are in agreement that public cryptography is a serious public policy issue that requires the cooperation of government and industry.
- The ultimate objective of collaborative activities on the part of industry and government is to find a solution to the fundamental policy objectives that underlie the government's key escrowing encryption initiative:
  - provide effective cryptographic security needed to assure the personal privacy of individual American citizens;
  - protect sensitive information held by U.S. corporations and unclassified government entities, domestically and overseas;
  - do not harm the ability of U.S. law enforcement and national security components to accomplish legally authorized electronic surveillance and intelligence operations; and
  - preserve the competitive posture of U.S. computer and telecommunications manufacturers in the global market place.
- The process employed to examine commercially viable alternatives to existing government developed microelectronic devices should assure private sector and government participation.
- The results of deliberations and discussions between the government and private sector should be publicly disclosed, consistent with the national security interests of this country.
- Possible requirements for corporate/organization key escrowing will be considered in the development of future key escrow systems.
- The need to ultimately achieve an internationally acceptable solution will be considered in the development of national policies and technical implementation.
- An acceptable solution should be widely exportable.

3.1.2 Government Proposed Action Plan

1. Participants should consider today's discussions and prepare corporate positions on working with the government to seek other approaches to key escrow encryption.

   The position papers should be submitted to NIST[3] by July 1, 1994.

2. Form a joint industry/government working group.

   - Establish a Joint Industry/Government Working Group(s) under the leadership of NIST to critically examine all known key escrowing proposals.
   - These will be examined and evaluated under criteria jointly developed by government and industry. Such criteria shall include an assessment of the costs to manufacturers and users, as well as the operation of the supporting key escrow system.
   - A public seminar/workshop will be held to discuss and document the results of alternatives analysis.
   - Prepare a final report that summarizes the results of the alternative analysis and public seminar workshop. This document will be used as the basis of subsequent discussions between senior government officials and members of the private sector.

3. Other Activities

   - The government and industry shall examine existing vehicles for collaborative research and development and determine if these are adequate or if new venues need to be created.
   - Identify suitable algorithms for use in conjunction with key escrow. Develop criteria for acceptability of selected algorithm(s).
   - Identify and address intellectual property issues inherent with any proposed solution with a goal toward widespread public availability on a royalty-free basis. (This includes the algorithm, key escrow methodology, supporting infrastructure, etc.)
   - Government to create a key escrowing task force, run by NIST under policy guidance of the NSC/OSTP-led Interagency Working Group to manage and expedite the search for key escrow alternatives.

3.2 Closing Comments from Industry Participants

Q1. Other approaches to key escrowing have been presented. Does the charter for the industry/government working group allow for discussion of alternatives that might be more internationally acceptable?

That would be allowed – re-analysis is acceptable.

Q2. The general concerns are as follows. The government started with the CLIPPER chip technology as the solution. Industry got it restricted for use only in voice, FAX, and low-speed

[3] Lynn McNulty, Associate Director for Computer Security, NIST, Technology Building, Room B-154, Gaithersburg, MD 20899 (Tel: 301-975-3240, Fax: 301-948-1784, email: mcnulty@ecf.ncsl.nist.gov).

data communications. But it is being pushed by the government into higher bandwidth communications. All of this is happening without addressing such things as software solutions and international problems.

The administration will feel that key escrowing is desirable for the development of the NII. The current solutions may not be final, but the government feels that the key escrowing technology is definitely the way to go.

Q3. In Tessera, there are a number of unstated issues for the IRS, law enforcement, etc. The goal is simply to expand. Industry does not in general disagree – they would like to "sell" it.

Q4. Who is actually making the decision to push the technologies of Tessera and key escrow?

No decision has been made on the applicability of Tessera. The use of the key escrow is voluntary.

Q5. How about the secrecy of SKIPJACK?

It has been reviewed by NSA and the policy is to maintain its secrecy.

Q6. If this is true, why form an industry/government group to try to find commonly acceptable solutions?

It may be possible to use other encryption algorithms.

Q7. If the infrastructure in Tessera is already established and cannot be undone, then we may be wasting our time. Can we get more representation in the working industry/government working group from those who make the decisions?

That can be arranged, perhaps not full time, but definitely for interim briefings.

A Contributed Position Papers and Technical Papers

A.1 AT&T: Interests in Commercial Encryption

AT&T

Secure Communications Systems

Guilford Center
P. O. Box 20046
Greensboro, NC 27420
800-203-5563 (Voice)
910-279-5746 (Fax)

June 9, 1994

Subject: **AT&T Interests in Commercial Encryption, NIST Conference, June 10, 1994**

AT&T Contacts:

William A. Franklin, Secure Products Manager, AT&T Secure Communications Systems, 910-279-6987, fax: 910-279-5746
David P. Maher, Chief Scientist, AT&T Secure Communications Systems and member of Bell Laboratories, 813-530-8716, fax: 813-530-5436
Philip D. Servidea, Director, AT&T Federal Government Affairs, 202-457-3855, fax: 202-466-2746

AT&T serves the voice, data and fax commercial security markets on a broad front with a variety of hardware and software products. AT&T was the first firm to implement the Government EES system in a commercial system, in its Surity (TM) Model 3600 Telephone Security Device.

AT&T supports the government's encryption policy objectives of balancing the public's expectations of privacy in communications and its expectations for the protection provided by law-enforcement agencies. AT&T believes the current government policy, manifested in the voluntary Escrowed Encryption Standard (EES) strikes an appropriate balance. AT&T will offer EES in specific proposals for software based EES solutions once the ground rules for such are made clear.

An important reason for AT&T's support is that EES is the first standard put forward for voice encryption. It is the only standard in an area that has been seriously hampered by a lack of standards. The lack of standards in secure communications has prevented the kind of interoperability among secure telephones that we take for granted when using conventional telephones, fax machines or virtually any other type of communications equipment.

AT&T supports standards in all areas of telecommunications. In view of the historic lack of standards in secure communications, we feel we should bring this standard to the market for its consideration, with the understanding that we will continue to offer our customers what they want, to include alternative forms of encryption.

We are concerned about several issues:

- The Government will greatly facilitate the ability of US firms to offer a full range of encryption solutions, and not just EES, from the ITAR list, by making them generally exportable, as outlined in the Cantwell Amendment to the Export Administration Act. Such an action is fully within the purview of the Executive Branch. The ability of customers to communicate freely, and securely, across national boundaries is essential in the growth of international business. Solutions which limit those capabilities on a broad scale, as do US export regulations for encryption, hamper this critical commerce. Continuing to use export as leverage for wide spread implementation of EES on an international scale only serves to delay the ability of US firms to respond quickly, efficiently and securely to international business and work with global partners to compete in all markets.
- There is a need to establish international standards in encryption and key management through the use of existing technical standards bodies, with minimum Government impedance (all governments). EES based systems are obvious candidates for these standards, along with other technologies and offerings. In announcing the EES FIPS on February 4, 1994, the Administration established an interagency Working Group on Encryption and Telecommunications. This group was to work with industry to refine encryption policies. The purely "U.S. flavor" of the EES has been a major industry concern since the inception of the policy review in April, 1993. Industry has suggested submission of the EES to an international standards body for world -wide consideration. Industry remains concerned that no action has been taken on this issue.
- Corporate equity continues to be of concern. The ability of a firm or enterprise to control the use of its information, which may be subject to strong encryption through Government provided EES, is currently in question. AT&T will provide offerings, most likely in the file system and E-mail areas which will allow our corporate customers to control their own information while using strong encryption with EES.

AT&T will work with the other corporate entities, standards bodies and the Government to develop security alternatives and standards which will facilitate international commerce.

A.2 Compaq Computer Corporation: Proposed NIST Draft

COMPAQ Computer Corporation
Proposed NIST Draft

Over the past few years both the computer consumer and business markets have become increasingly aware of the need to protect data. This awareness has evolved to a level where customers are no longer concerned with simply creating backup schemes, but are trying to define methodologies to protect data from criminal destruction and competitive theft. Awareness has been increased by a multitude of articles detailing Hackers, Crackers, Viruses, Worms and Trojans. Finally, the government is currently publicizing the importance of protecting electronic information in the global marketplace. This awareness, in Compaq's customers, has forced us to start examining the issues involving the protection of data.

The easiest and most efficient method of protecting data is encryption. The main stumbling block in Compaq's encryption development effort has been the restrictions imposed upon us by the Government of the United States. Their restrictive position has severely hindered our competitive advantage in this area. We find ourselves under the constraint of not being able to export a superior product while our foreign competitors may import freely into the U.S.

Compaq's short term cryptography strategy is:

- Implementation of a mechanism to provide for secure content delivery and or metering.
- Encryption of data on a machine.
- Creation of secure communication channels.

Compaq's long term strategy is to:

- Explore research into the creation of Unique identity keys for each machine. This will allow us to:
    1. Authenticate software.
    2. Protect flash technology with secure update channels.

- Create more secure communication channels for use by:
    1. Servers for secure remote machine administration
    2. Point to Point transfer of information - i.e. fax, data, voice

- SetTop Box (NII) - i.e.. Electronic Cash, Anonymity

Clipper Questions:

1.. Cost:
   - How much will a board cost?
   - What is the encumbrance fee?
2. What is the performance impact if we:
   - Use it in the disk I/O subsystem?
   - Use it in the communication subsystem (modem / fax / network)?
   - Use it in the loader?
3. If we use Clipper,?
   - Can it inter-operate with non-Clipper units?
   - Can a user disable clipper, if they don't want it?
4. How does Skipjack work (i.e. What is the Algorithm)?
   - Has it been exposed to the same scrutiny that other algorithms have?
   - Is it importable to France, and other foreign countries?
5. What prevents a user from pre-encrypting with DES and then sending the packets out through the Clipper board?
6. What prevents a user from modifying the FEAL?
7. The agencies that will be escrowing the keys:
   - Who are they?
   - How will they be funded?
   - What is there encumbrance on the product?
   - How many points of presence will exist?
   - How will they generate the keys? i.e. block generation..
   - Will they keep track of which keys are sent to which manufacturer?
8. Key Escrow:
   - Will manufacturers have both sets of keys at any given instance?
   - How do they get the keys?
9. What is the mechanism whereby a law officer can obtain keys?

A.3 Addison Fischer: Software Key Escrow – Corporate Implementation

Software Key Escrow -- Corporate Implementation

Kep Escrow Encryption Workshop

June 9, 1994
Gaitherburg, Md

Addison Fischer
Fischer International
Naples, Fl 33942

Fischer International has supplied government and industry with escrow-based encryption systems for over 10 years.

With WatchDog, we pioneered the use of transparent data encryption for information residing on distributed systems. We also pioneered the use of flexible public-key based escrow systems with WatchDog KeyMaster to prevent the use of such encryption against an organization by any of its information's custodians (employees).

In the late 1980's, as a research project, Fischer International developed prototype key escrowing systems "KISS" (Key Integrity with Split Stewarding) and "KEMS" (Key Escrow Management System), which were designed as software-only, cryptographically secure systems embodying a number of sophisticated concepts including weighted M of N split secret sharing, public key distribution of the split parts to "Key Stewards", and automatic recovery of the original key given mutual concurrence of any appropriate subset of the Stewards.

With the recent arousal of interest in escrow systems, Fischer International has been exploring exhanced escrow systems incorporating the latest cryptographic advances, as well as techniques and designs using secure hardware tokens, such as, especially, the SmartDisk.

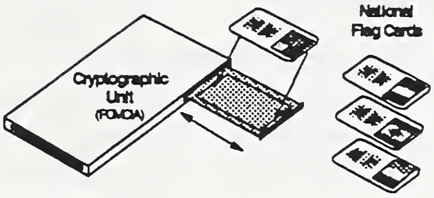
A.4 Hewlett-Packard: International Cryptography Framework

HEWLETT PACKARD

International Cryptography Framework

Concept Discussion

June 8, 1994



Keith Klemba, Security Program Coordinator
Computer Systems Organization, Hewlett-Packard

Disclaimer: This document is designed to stimulate discussion regarding International Cryptography and the issues impacting progress in this area. It does not pretend to present a fully fleshed out proposal but rather some fresh points of view. It does not presume to represent expert testimony on the fine points of International law or cryptographic science.

Abstract: A cryptographic framework is presented that consists of four basic service elements. Hypothesis - that national policies governing cryptography can be independently developed and maintained using a such a framework. Furthermore, that these common service elements provide the necessary focus for progressing technologies and policies towards interoperability.

BACKGROUND

Customers of large computer systems are typically multinational corporations wanting to purchase enterprise wide computer based solutions. The distributed nature of such organizations requires them to use public international communication services to transport data throughout their organization. Naturally, they are concerned about the security of their communications and seek to use modern end-to-end cryptographic facilities for privacy and integrity. The use of cryptography in communication is governed by national policy and unfortunately, national policies differ with respect to the use of cryptography.

Each national policy is developed independently generally with a more national emphasis rather than international considerations. Some standards groups talk about developing a common cryptographic algorithm suitable for international cryptography. However, this is not a technical problem. It is a political issue that has national sovereignty at its heart. As such, it is not realistic to expect the different national cryptography policies to come into alignment by a technical standardization process.

Nations have reasons for adopting policies that govern cryptography. Often these reasons have to do with law enforcement and national security issues. Within each country there can be debates between the government and the people as to the "rightness" and "acceptability" of these policies. Nevertheless, it is not the purpose of this paper to engage in these debates nor to forecast their outcome. Rather, the paper accepts the sovereign right of each nation to establish an independent policy governing cryptography in communication.

Policies governing national cryptography not only express the will of the people and government but also embrace certain technologies that facilitate cryptography. Technology choice is certainly one area where standardization can play a role. However, as indicated earlier this is not solely a technical problem, so selection of common cryptographic technologies alone will not resolve the national policy differences. Consequently, the thrust of this discussion moves towards a common cryptography framework. A framework wherein independent technology and policy choices can be made in a way that still enables international cryptographic communications as allowed by these policies.

This paper presents a four part technology framework for supporting international cryptography. It asserts this framework will support the design, implementation, and operation of any and all national policies. The paper seeks to expose this concept for serious discussion and consideration of an international demonstration project.

PROBLEM STATEMENT

How to provide global information technology products featuring security, while respecting the independent development of national cryptography policies.

HP INTEREST

Before moving on it would be appropriate to declare how this issue is of interest to the Hewlett-Packard Corporation. Hewlett-Packard manufactures open-standards-based Information Technology (IT) products for a worldwide market. Our customers want these IT products to be secure. More and more of our customers are themselves multinational and look to HP to help them resolve the international cryptography issues inhibiting their worldwide IT development. The persistence of unresolved differences and export restrictions in national cryptography policies has an adverse impact on HP's international market growth for secure open computing products.

As a worldwide corporation HP has a responsibility to provide business input to all governments. HP also encourages its employees to recognize their national citizenship and to participate in government affairs.

DISCUSSION HYPOTHESIS

What if there was a framework that unified the design, development, and operation of independent national security policies? The nature of such a framework would be to give standard form to the service elements of national security policies. Service element definitions would include such things as hardware form factors, communication protocols, on-line and off-line data definitions.

PROPOSED FRAMEWORK

The technology framework being proposed here has 4 service elements (Fig 1) each offering different types of services. Three of the four service elements have a fundamentally hierarchical relationship. The National Flag Card is installed into the Cryptographic Unit which in turn is installed into a Host System. Cryptographic functions on the Host System cannot be executed without a Cryptographic Unit which itself requires the presence of a "valid" National Flag Card before it's services are available. The fourth service element, a Network Security Server, can provide a range of different security services including verification of the other 3 service elements.

Messages encrypted using the proposed framework would carry an electronic "Stamp" identifying the National Cryptography Policy under which the message was encrypted. The Network Security Server would also provide "Stamp" verification services for message handling systems.

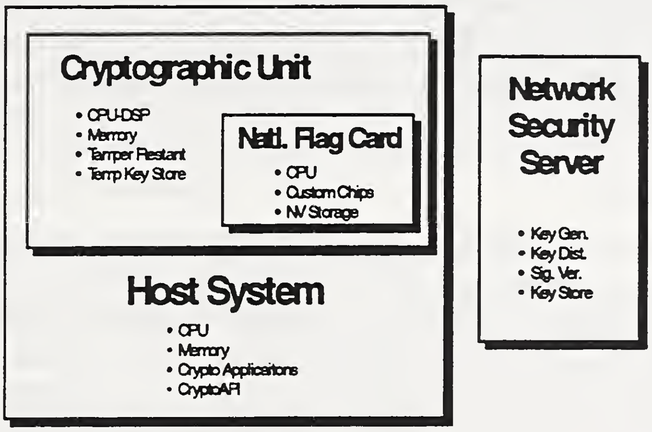


Figure 1. Security Framework

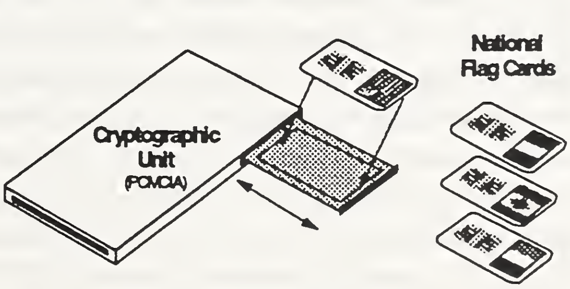
In the following sections each service element will be discussed further followed by a section of scenarios to illustrate possible interworking of the 4 service elements.

NATIONAL FLAG CARD (NFC)

The NFC is a small stamp sized (25 x 15mm) form of an ISO 7816 smart card that would be independently produced and distributed exclusively by National agencies. The Post Office would be a natural distribution channel for NFCs. The function of the NFC service element is to enforce a Nation's cryptography policy. An NFC is a complete computer that can be constructed as a multi-chip architecture to include custom ICs. It also would include all tamper resistance features of Fips 140. All services of the NFC are provided via standard ISO 7816 message exchange protocol between the NFC and other service elements. This format is identical to the smart card used in Europe to support GSM in cellular voice services.

CRYPTOGRAPHIC UNIT (CU)

The CU is a hardware component designed to provide protected cryptographic services under the strict control of a NFC. CUs would be produced competitively by system vendors and third parties and be free of import and export restrictions. Since the CU features protection of algorithms and keys, it is likely that it would be certified (e.g., NIST, NCSC, or ITSEC Certified) for customer assurance. This component would be designed for performance and protection with customization for a given Host Systems. Initial discussions of this component have centered around a PCMCIA hardware format but other formats are equally valid. One PCMCIA format would be GEMPLUS's "Smart PC Card", which includes a small drawer to support the stamp sized NFC.



The CU itself could contain popular cryptographic algorithms such as DES and RSA. However, these algorithms would not be functional without the presence of a valid NFC. This is a variation of the "cryptography with a hole" concept with a very controlled methodology and framework for filling the hole. NFC validity and the NFC verification protocols are not discussed in detail in this paper. Nevertheless, these are very well bounded problems and there are more than a couple solution methodologies available. Since there are likely to be other verification issues surrounding each service element it will be better to consider all these issues in the design of verification methods.

HOST SYSTEM (HS)

The HS is identifiable as the hardware component that delivers secure IT services directly to the user. HSs are typically a general purpose IT device and would be produced competitively in a wide open market. Examples include Personal Digital Assistants, Personal Computers, Workstations, Laptops, Plamtops, Networked Servers, Main Frames, Network Printers, or Video Display Units. The function of the HS service element (in this framework) is to provide an Application Programming Interface (API) for accessing the CU service element. Most likely CU support would be an option available on the HS.

The HS represents a very large and diverse class of IT equipment. Initially, it seems O.K. to group all these systems uniformly into this class. However, in time, it might become valuable to break this class down into specialized subclasses. Similarly, this framework allows for different types of NFCs to be used, perhaps to identify these different HS subclasses.

NETWORK SECURITY SERVER (NSS)

The NSS is a network node designed and designated to provide trusted third party security services. In the context of national security, NSSs would probably be developed, owned, and operated by government agencies. Some of the functions provided by the NSS service element include service element authentication, message "Stamp" authentication, national policy enforcement, and cryptographic key distribution.

Importance of the NSS can rise sharply in environments where a strong degree of verification is prerequisite to cryptographic use. The NSS will also play a significant role in the interoperability of differing National cryptographic policies.

OPERATING SCENARIO - USERS PERSPECTIVE

Tom is a buyer in the U.S. working for Slam International Inc. He has purchased a palmtop (HS device) from Hewlett-Packard which he intends to use to send bid and delivery information directly to manufacturing sites worldwide. He will also be able to access backlog information directly from regional sales centers while negotiating. Tom's business is very competitive and all this information is considered very sensitive. Tom purchased cryptographic option (CU device) with his palmtop so he can encrypt and decrypt his messages. However, to activate this capability he has to go to a U.S. Post office and purchase a United States "Class 5 Smart Stamp" (NFC device) and install it into the CU in his plamtop. Tom's HS/CU/NFC combination is now verified by a FCC operated Network Server (NSS device) in Denver via a local GTE cellular service. Tom uses CC-Mail on his plamtop to send and receive his messages. CC-Mail will encrypt Tom's messages prior to transmission and decrypt messages after receipt. After 30 days the Class 5

Smart Stamp in Tom's palmtop will expire and so to will Tom's ability to encrypt and decrypt messages until he purchases a new Smart Stamp.

Every now and then Tom has to leave the U.S. to visit the manufacturing facilities around the world. Tom is freely able to take is palmtop in and out of the U.S. with the validated HS/CU/NFC intact. Use of the U.S. policy in non-U.S. countries would depend on the political relationship between that country and the U.S. Public carriers transporting messages have the option to accept or deny traffic encrypted using another country's cryptographic policy. The electronic stamp provided by the NFC insures that message carriers will be able to identify the national policy used to encrypt the message.

OPERATING SCENARIO - GOVERNMENT PERSPECTIVE

Bill is a government agent investigating trafficing of contraband, and Tom (from User Perspective above) has come under suspicion. After considerable investigation Bill suspects that Tom is using his palmtop for more than legitimate business and seeks a court order to investigate further. Subsequently, Tom's messages are recorded off of public carrier facilities. The messages carry an electronic "Stamp" identifying the cryptographic policy used to encrypt the message. Consequently, since they have been encrypted in accordance with a U.S. NFC, the government, after due process, is able to decrypt Tom's messages for analysis. One additional element of evidence also exists that links Tom's plamtop to the source of the messages. Since each NFC and its electronic stamp is unique, the HS/CU/NFC combination verified by the government run NSS ties Tom's messages to that uniquely verified combination .

DISCUSSIONS

National cryptography policy often varies by industry segment, political climate, and/or message function. This makes it difficult to assign one uniform policy across all industries for all time, consequently, the flexibility of NFCs is very attractive.

RECOMMENDATIONS

The purpose of this paper is to stimulate discussion about resolving problems surrounding international cryptography. It presents a framework along with a hypothesis that this framework can be used to support the design and development of any national policy regarding cryptography.

The point of discussing this perspective is to stimulate the creation of a multinational demonstrator project where experts could come together to develop various aspects of this proposal. Already, with just a brief exposure of these ideas several industry experts and governments have shown significant interest in participating in just such a demonstrator project. The project should have a series of milestones to report progress and issues associated with this methodology. After 12 months the demonstrator project should be concluded with a final report made available to governments and citizens for consideration of a pilot phase development.

A.5 Iris Associates: Key Escrow for Lotus Notes

Key Escrow for Lotus Notes

Lotus has been using cryptography for the security of its Lotus Notes product since its first release in 1989. Notes uses RC2 to encrypt stored data; RC4 to encrypt network traffic; and RSA for key management, for network authentication, and for electronically signing documents. Notes also uses RSA for signing public key certificates.

Some sort of key escrow mechanism would be a welcome enhancement to Notes if it solved the following two problems. First, it would need to provide a key backup facility so that a user's lost keys could be recovered. Second, it would need to provide management with the ability to recover a key in order to read documents encrypted by a former employee.

Typically, all bulk data is encrypted with a randomly generated bulk data key. The bulk data key is then encrypted with either an RSA private key or an RC2 "document encryption key" and stored along with the bulk data it encrypted. Note that the term "document encryption key" is somewhat misleading because the key is used to encrypt the bulk data key rather than the actual bulk data. There are names associated with both the RSA and the document encryption keys, and these keys are therefore visible objects within Notes: human interaction is required to manage them and they are stored in known locations. These characteristics make them convenient choices for key escrow. Fortunately, because these are also the only top level keys used within the product (all other keys are stored encrypted by one of these keys), they are also the only keys that need to be escrowed.

If it were possible, software only escrow solutions would be preferred over solutions requiring special hardware. This is partially because Notes runs on quite a few operating systems, and the development cost of providing special hardware support for each of those platforms would be significant. But it is also because not all Notes users who want the benefits of key escrow would be willing to pay for the additional hardware.

Any implementation of key escrow for Notes might be expected to support, as an option, federally recommend (or required) standards such as Clipper. However, it is not reasonable to expect that any U.S. standard would be acceptable overseas. Therefore, because roughly 50% of all Lotus' sales have traditionally been to foreign customers, one goal of any key escrow solution for Notes would be that it is flexible enough to allow its customers to choose which escrow technology to use.

Alan Eldridge
Designer/Programmer
Iris Associates, Inc.
One Technology Park
Westford, MA 01886

A.6 Novell: Encryption Alternatives

NOVELL

June 8, 1994

NIST Workshop: Encryption Alternatives

This paper is an input to the NIST-sponsored key escrow encryption workshop to discuss industry and government perspectives. Novell, Inc., is an international leader as an information system software company, developer of network services, specialized and general purpose operating system products, and application programming tools. This input and Novell's participation in this NIST-sponsored workshop is provided in the hope that it will contribute to encryption alternatives that are compatible with the business interests of Novell as a U. S. company with a significant international customer base.

Novell has a major and growing interest in commercial cryptography. We are committed to providing commercial products that meet the growing needs of our customers for information security, and cryptography is an important component of the technology we apply to meet these needs. We have for several years included encryption to support the advanced security capabilities in our standard products. Cryptography is an integral part of several key security services in wide-spread use by our customers today; these include user authentication, communications integrity and network directory services. Products currently under development are designed to enhance security with not only compliance with the Trusted Computer System Evaluation Criteria (TCSEC) at Class C2 for NetWare and Class B2 for UnixWare but also extended cryptographic support for capabilities such as encrypted audit files. It is emphasized that Novell products, including those for security, are directed at the broad international commercial market, not just specialized or niche markets.

A significant limitation to the international competitiveness of Novell products is U. S. export restrictions on the security capabilities of our products -- especially restrictions on cryptography. The path we expect to follow for future products includes security enhancements to protect our commercial customers against deliberate, malicious external attack. We believe this path not only needs to include support for multilevel security, as reflected in higher TCSEC evaluation classes, but also high assurance trusted systems technology selectively coupled with high-quality cryptography. We are especially interested in cryptography alternatives that will permit our commercial products to include widely-used, high quality cryptography. A key property of our current products that allows them to meet commercial needs is that the identical, mass-produced products can be sold to domestic and export customers. Attractive future trusted system and cryptographic alternatives should be consistent with this property of our commercial products.

The Novell products are particularly capable of utilizing various hardware or software cryptographic alternatives, including those that support key escrowing. A distinctive property of Novell products is their ability to operate on a growing set of diverse hardware platforms. Novell commercial products include modular software support for various widely-used hardware, so customers can choose the particular software modules consistent with their particular hardware. This modular approach does not preclude encryption chips or other cryptographic hardware interfaces as essentially specialized hardware co-processors with their corresponding software modules selected at the time of installation. Similarly, since software modules are selectively linked into the running products at the time of installation, software alternatives for cryptography are not precluded with Novell's modular approach.

Although Novell clearly has the potential to utilize a wide range of feasible alternatives, the attractiveness of various candidate technologies for inclusion in our commercial products will be determined primarily by business considerations. The importance of a common, mass-produced product base for both domestic and export customers has already been identified. Also, it is generally cost-effective to include support for hardware and/or software alternatives that are actually available in the commodity platforms of a significant number of our current and potential customers -- both domestic and export. Further important considerations are the compatibility of the selected cryptographic alternatives with a standard generic security service application program interface and the use of high assurance technology to provide our customers confidence in the integrity of any key escrow implementation. Finally, a decisive factor that could effectively preclude consideration of such cryptographic alternatives will be export restrictions on customer selection and installation of cryptographic support.

In summary, Novell has had in the past, and expects to have in the future, a major interest in commercial cryptography. The Novell technology is particularly adaptable to alternative hardware and/or software cryptographic implementations. Actually realizing this potential in our commercial products will depend on a positive business case, and significantly depends on actions by the U. S. and other governments that dictate export restrictions, determine the assurance of the integrity of any key escrow, and affect the wide-spread adoption of specific cryptographic implementations as commodity items for our customer base which is international in nature.

A.7 Semaphore: Letter from Bill Ferguson

SEMAPHORE
ecure Network Communications

June 7, 1994

Mr. Lynn McNulty
Associate Director for Computer Security
National Institute of Standards and Technology
Gaithersburg, MD 20999-0001

Dear Lynn,

Thank you for the invitation to participate in the conference for Cooperative Research and Development. This marks a positive step for industry government cooperation for advancing the use of key escrow cryptography for the benefit of all parties. As we have discussed many times, Semaphore has no cryptographic bias, and is committed to implementing system using encryption and key management technology tha are accepted and demanded by global users.

Semaphore Communications has an interest in participation for the benefit of developing standards that can be applied to its advanced systems for high-performance global computer and communications security applications. Semaphore is already acclaimed as having system architecture and encryption processors that lead the industry, today. As the uses of cryptographic technology proliferates to meet the needs of global computer and communications users, Semaphore intends to continue to be an active participant in bringing solutions to the market. In line with this intent, next week, Semaphore will introduce new technology that could be adapted to any new encryption standards.

Semaphore is already on record with the National Security Agency as being an advocate for the use of key escrow technology. Presently industry and the NSA have different opinions on how to achieve global acceptance for escrow systems. The matter of assigning escrow agents also needs to be resolved for the benefit of all potential global users. As an advocate, Semaphore firmly believes that the standards must evolve from the cooperative efforts of the scientific, business, and government communities. Foreign participation is necessary for true standards to evolve.

With the global use of cryptography growing at a rapid pace, there is a need to strive for progress over process. If industry is arriving at the conference in a cooperative mood, and we hope the same is reflected by the government participants.

There is an opportunity to have this conference kick-off a direction that can result in US government and industry taking the global leadership role in the encryption technology market segment. There is a vibrant global market, and it is looking to the USA for leadership. We can capture that leadership role by cooperating to show a new face to global users. If we don't start the process now, others will.

## more ##

The first step in the global leadership process is to demonstrate business leadership by permitting US vendors to compete for any and all market opportunities that are now open for bidding in the USA's global trading-partners' markets. If our experience at Semaphore is any indication of the opportunities, there are chances to evolve the secure hardware and software industries into significant contributors to foreign trade. Every day, Semaphore receives correspondence from some of the world's largest corporations and foreign governments seeking advanced encryption systems technology. There is a vibrant global market, and it is looking to the USA for leadership.

It is extremely difficult for a US supplier of security systems to explain the current export restrictions to a potential foreign user that is excluded by the current export rules. When those potential users are friendly foreign governments, the explanation is even more cumbersome. We seek the US Government's cooperation in permitting innovative market leaders, like Semaphore, the freedom to pursue global market opportunities by encouraging the passage of the revisions to the Export Administration Act now in the House Select Committee on Intelligence.

The cooperation that industry can provide is in taking the leadership role in working with global standards groups to advance the acceptance and standardization on key escrow as an alternative methodology. Frankly, it is about time for security technologies to move forward. In the past 15 years, computer technology has gone through as many as two advances per year. Security technology has not made significant advances since DES was introduced. If government and industry can work together, there is an opportunity to advance security technology to the advantage of both.

Semaphore is ready to cooperate within its capabilities to advance these issues, and looks forward to an open and vibrant conference.

Sincerely,

Bill Ferguson

Bill Ferguson
Vice President, Marketing

A.8 TECSEC: Private Escrow Key Management

TECSEC Incorporated
1953 Gallows Road, Suite 220, Vienna, Virginia 22182
703-506-9069, (Fax) 703-506-1484

Private Escrow Key Management

Prepared by
Edward M. Scheidt, CEO
and
Jon L. Roberts, President

June 5, 1994

Private Escrow Key Management:

A Method of Meeting the Needs of National Security, Law Enforcement, and the Rights of the Individual to Privacy

By

Edward M. Scheidt, CEO

and

Jon L. Roberts, President

TECSEC Incorporated

The Problem

There exists today a significant conflict between the rights of the individual to privacy in communications and information and the Government's need to access information for national security and law enforcement purposes. At the heart of this debate is the difficulty in arriving at a position whereby a robust implementation of an encryption process can be accomplished that protects sensitive data yet insures that the government can have access to information if that information is part of a criminal conspiracy or enterprise, or other action hostile to the Untied States.

The Government has tendered a solution based on communication encryption technology. Communication encryption technology focuses on the need to protect the channel by which the communication is effected. Using communication encryption technology, the Government would like to mandate an encryption process for which it maintains the key used for decryption of traffic moving over any given communications path. This key would be split between two Government agencies . The split key would have to be combined if the government were to use the key to decrypt and monitor criminal or any activity. A court order would be required in order for the key combining to occur. This key management scheme is known as the Clipper Escrow Key Management plan.

A second and equally important objective of the split key encryption process represented by the Clipper Escrow Key Management program (recently published in FIPS Pub. 185 as the Escrow Encryption Standard) is to safeguard computerized records, files, and telephone conversations from illicit eavesdropping or piracy of the data contained in such files. This objective is to be accomplished through the use of a new robust encryption algorithm. The Government asserts that the Clipper encryption scheme is one such algorithm which represents improvements over existing standard encryption schemes such as the Data Encryption Standard or DES.

Thus use of the Clipper technology will allow the government to listen to communications as they occur. As will be seen, this is not the only issue at hand.

The Government hopes to "convince" industry to adopt the Clipper process (both the encryption and key management) as a standard by requiring that the Clipper chip be the mandatory encryption used when dealing with the Government or when encrypting Government data and information.

Opponents of the Clipper Chip have argued that the Clipper process infringes on the rights of the individual to privacy. It is further argued that US. industries that manufacture security equipment will be placed at a competitive disadvantage when trying to sell equipment that relies upon the Clipper process since it is doubtful that any foreign entity will purchase Clipper-based equipment when it knows that the US Government has access to the keys and hence the unencrypted data.

At the same time as the debate on the use of Clipper technology for communications encryption, there is emerging a new trend in protecting data. This trend involves the protection of the data at the file level and not simply during the communication of that data. Advances in technology have set the stage for this new basis for protecting data. Traditionally, communications technology is concerned with the protection of the flow of information and not on protecting the information itself. Thus the government and industry has traditionally been concerned with protecting the channels of communication. File protection, on the other hand offers promise of a new way of protecting data, differing from the communication paradigm.

The Solution

Industry has developed a key management architecture that offers an alternative to the Clipper process. This architecture address both the national security issue and that of privacy of the individual. In lieu of the communication architecture approach to encryption, advances in microprocessor technology have allowed a shift toward a new definition of protection based upon file encryption, that is, instead of protecting the **means** of communication of information, one protects the **information** that is being communicated. This technology is based on file management and intelligent data separation.

A wide variety of capable and flexible information managers exist as commercial off the shelf products. It is these information manager products that form the basis of protecting information and applying privacy concerns. If individual files can be protected or encrypted, the information or communications path becomes irrelevant. Information that is intercepted is protected through the encryption process.

Using file management techniques combined with appropriate encryption, files are protected. As part of the file encryption process an independent selection of an algorithm can be the basis for acceptance of this new process in the international community. Instead of the government maintaining the key to decrypt data on a communications path, the individual maintains the key to decryption of files that are stored by the individual. Keys must be maintained by the individual in order to decrypt needed data. This fact allows a user to have a high degree of comfort that his files are private and safe from unauthorized viewing. However, in much the same manner that the Government can obtain records from the individual with an appropriate court order and after appropriate due process, the Government can also obtain the keys maintained by the individual which can then be used to decrypt data stored in an encrypted form in a computer system.

The natural question to ask is what assurances does the Government have that its combined needs to protect national security and meet the requirements of law enforcement can be met? The answer is simple. If a person keeps information in an encrypted form to protect the data, that person will need the keys to decrypt the data for the person's own use. If the person destroys the key before the Government can access the data, that person also destroys his own access to the data, since his own access is dependent upon access to those same keys. An additional element to this protection of governmental interests is that users of encryption processes can be required through legislation to keep and protect keys for a period of time.

Law Enforcement Equities

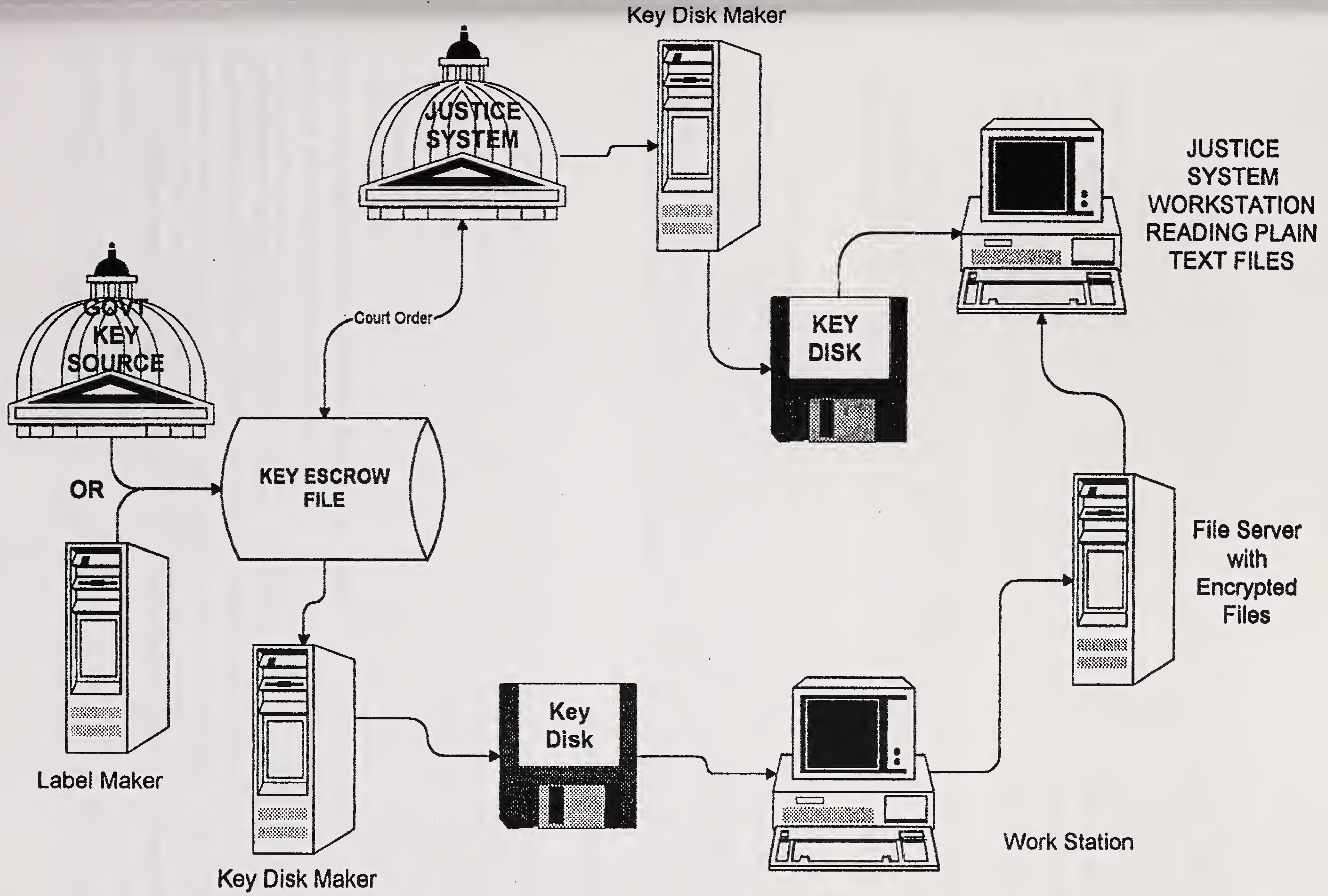
A key concern of the government is the ability to enforce laws against illegal activity. While much focus is made of organized crime activity, there are many other illegal activities that the government polices for the well-being of the citizens. For example, government fraud carries both civil and criminal sanctions. While a person has a right against self incrimination, a wrong-doer's company cannot resist a subpoena for documentation to back up the government's case against fraudulent activity. Thus encrypted files are subject to examination by the government after appropriate judicial hurdles have been overcome.

The government is charged with policing environmental crimes. Again, such crimes carry civil penalties. Companies and individuals cannot resist a subpoena for records involving civil penalties only. As a result, the government can in fact retrieve encrypted files by making appropriately framed demands for the encryption keys and the files themselves.

Other types of civil actions and criminal statutes can be equally enforced by subpoenas upon the record of parties not a part of the action. Banks, stock brokerage firms and industrial organizations are but a few examples of those who must turn over records to the government if appropriately requested to do so. Appropriate procedures now exist for the government to obtain records that can be used to enforce SEC regulations, to obtain organized crime business records held by unwitting third parties, and to obtain records that can be used by the to prosecute government and business fraud actions of all types. Appropriate requirements and regulations to maintain keys to encrypted files protects the vested interest of the government to obtain such records and therefore enforce laws to protect citizens from illegal activity.

Summary

It is suggested in this paper that file encryption, rather than a communications encryption approach, can do a much better job at protecting sensitive data while still giving individuals and businesses the comfort of knowing that the keys to the sensitive data are not being held by the government. The user controls not only the encryption process but the means to decrypt the data. This approach combined with a private escrow key management scheme offers the user the needed privacy and control over encrypted information, yet still gives the government access to encrypted information should it be necessary to enforce laws via traditional methods of due process associated with access to stored documents and data.



KEY ESCROW SYSTEM USING VEIL KEY MANAGEMENT

A.9 TIS: A Possible Bases for Software Key Escrow Encryption

A Possible Basis for Software Key Escrow Encryption

Stephen T. Walker
President
Trusted Information Systems, Inc.

February 7, 1994

Summary

In August 1993, NIST announced a cooperative program with industry to explore the possibilities of performing key escrow cryptography using software-only techniques. The purpose of this effort is to determine if there are alternatives to the hardware implementations and secret encryption algorithm requirements of the US government's Clipper Initiative.

There are several software-only key escrow techniques that have been described in the literature. The major problem with them is that they can be bypassed or subverted relatively easily and thus cannot by themselves be relied upon to perform the law enforcement key escrow function envisioned by the Clipper Initiative.

This paper explores the issues surrounding:

- hardware vs. software key escrow,
- the role of classified encryption algorithms in selecting a hardware vs software approach and
- a technique for ensuring the integrity of software functions such as key escrow that may have significant additional benefits for a variety of important applications such as the Defense Message System (DMS).

Background

The April 16, 1993, Presidential announcement of the "Clipper" Initiative called for a hardware implementation of an algorithm that is "significantly stronger than those currently available to the public" and also containing a capability for the government to recover the keys used for encryption, a capability referred to as key escrow. Since this announcement, there has been considerable discussion of alternatives to these hardware implementation requirements that may work as well or better in at least some applications. In August 1993, NIST announced a cooperative program with industry to explore possible approaches to software key escrow.

There are a number of issues (hardware implementation, classified encryption algorithms, how much trust one must put in the user) that intertwine in any discussion of this topic. It is important to unravel these factors and to focus on finding a means to achieve a key escrow capability similar to that provided by Clipper initiative without the need for any special purpose hardware devices or interfaces.

Why a hardware implementation?

There are many factors that support the decision to require the use of separate hardware in the Skipjack Clipper/Capstone design:

- Separate hardware implementations (such as in a PCMCIA card) provide a degree of protection for the encryption process difficult to obtain in integrated software systems. In particular, if a classified encryption algorithm is used, separate hardware may be essential to protect the design and functioning of the algorithm.

- Key storage can be achieved relatively easily on such devices with a high degree of protection since unencrypted keys never appear outside the PCMCIA card.

- A separate device that is implemented using a common interface (e.g., PCMCIA) can be readily ported to a wide variety of workstation architectures.

- Widespread proliferation of an encryption capability is perceived to be easier to control with hardware than with software approaches.

- A hardware device can provide a means for individual identification across networks of computers, though there are other simpler devices that can achieve this same function.

Why a classified encryption algorithm?

The Clipper initiative called for use of a classified algorithm that is claimed to be much stronger than existing publicly available algorithms such as DES. Having a strong algorithm is a valuable selling point for an initiative involving key escrow concepts. But protecting a classified algorithm requires, at least at this stage of technology, a hardware implementation with special measures to resist reverse engineering of the hardware chip. Such a design, in turn, requires some form of hardware such as a PCMCIA card.

Classified encryption algorithms are generally considered much stronger than those in the public domain since they are typically used to protect military classified information. But since they are not available for public review, their use to protect unclassified information is suspect due to the possible existence of unknown trapdoors or faults. The principal strength of DES is that even after fifteen years of public scrutiny, no inherent fault has been found.

Key escrow techniques do not require classified algorithms and can just as easily be used with publicly available algorithms such as DES. If a publicly available algorithm were used, it would not be necessary to have a hardware implementation to protect the encryption algorithm from disclosure.

This interdependence between hardware implementations and classified encryption algorithms causes considerable confusion in examining the feasibility of software key escrow approaches. If one has a hardware encryption implementation, one can consider the use of either a publicly available or a classified encryption algorithm. If one requires a classified algorithm, one must use hardware to protect the algorithm.

Until the introduction of Clipper, publicly available algorithms had been prescribed for the protection of unclassified information. If key escrow techniques can be shown to work in software solutions, then there is no need to resort to classified algorithms.

Why would one want software key escrow?

The principal disadvantage of using hardware for key escrow and therefore the primary advantage of integrated software implementations is cost. The effort needed to distribute specially developed hardware capabilities (such as PCMCIA cards) using hardware implementations of encryption algorithms is generally viewed as considerably greater than that of pure software versions of the same capability.

To at least some, a second disadvantage of hardware implementations is the opportunity this offers to require the use of a classified encryption algorithm. As discussed above, key escrow does not require a classified algorithm.

A major advantage of software implementations is simplicity of operation. Software solutions can be readily integrated into a wide variety of applications. Generally, the mass market software industry seeks to implement everything it can in software so as to reduce its dependencies on hardware variations.

Problems with software key escrow techniques

The inherent problems with software-only solutions include:

- Difficulty in ensuring that the software will work correctly and not be modified once in place to allow bypass or corruption of the encryption process. (This issue remains a problem even in hardware solutions with the software that controls the flow of information to and from the hardware encryption device.)

- Difficulty in handling keys in a way that does not expose them to compromise.

If, however, a technique could be found to achieve a high degree of integrity for essential software performing any critical functions (such as encryption or key escrow), the result could have importance well beyond the realm of security.

And how much do we have to trust the user?

Hardware solutions such as Clipper make it difficult for users to corrupt the actual hardware-based encryption or key escrow processes. But these systems remain subject to corruption of the software that controls the flow of information before or after it is encrypted.
It will be relatively easy, for example, to encrypt the text of a message using some form of publicly available encryption prior to sending it to a Tessera PCMCIA card. If two or more cooperating users were to employ such a technique, their use would appear entirely proper until a key escrow-based decryption was attempted and the underlying encryption was discovered.

Similarly, the software that handles the encrypted text after passing through a hardware encryption device could modify the law enforcement access field (LEAF) in the message and thus render the law enforcement decryption process invalid. Techniques such as these are recognized to be beyond the scope of protection of the Clipper/Capstone process, and therefore the user must be trusted not to employ them.

Understanding just what the user must be trusted to do or not to do is an essential aspect of assessing the risks with software or hardware key escrow implementations. The major drawback of software solutions is the perception that software modifications by the user or system software handlers could render the software solution invalid. But as just discussed, even with hardware encryption, there is a substantial vulnerability to software modifications.

It would appear that for either hardware or software solutions to work properly, some significant means of assuring the integrity of the software surrounding the cryptography must be in place.

Even with such measures, the user of the workstation must be trusted not to interfere with either the hardware or software of the workstation. The Clipper/Capstone hardware solution is apparently based on the premise that these risks are acceptable. If this is so, it would seem that such assumptions should also be applicable to software key escrow techniques.

What is needed to ensure the integrity of a software solution?

Two years ago, TIS was tasked by ARPA to develop technical means for raising the level of high performance computer workstations that the US government might be willing to export to third world countries for "approved" applications. The premise of this program was that the US government might be willing to sell high performance computers to the Ukraine for use in organizing the transportation of farm products if it could have a reasonable degree of assurance that those computers were not being diverted for military purposes. It was recognized that once a system was shipped, its potential diversion could not be prevented in any absolute sense. But if the purchasing country believed that a diversion could be detected, the threat of loss of future sales of similar or improved computers might be enough to deter any widespread diversion.

One of the principal techniques that emerged from this effort was a software integrity approach that we term "controlled execution." The operating system and all applications approved for export loaded on a read-only medium, such as a read-only partition of a hard disk, a CDROM, or other form of read-only memory. The operating system is modified so that it will execute software only from that read-only memory.

In this system the only programs that can execute are those preloaded on the read-only memory. And, short of tampering with the read-only medium, the integrity of these programs is very high. Techniques for adding additional approved applications are included using digital signature procedures so that the system could remain up-to-date but not be easily changed in an unapproved manner.

The insight we gained in developing these controlled execution procedures is directly applicable to any software system where the integrity of the software must be preserved.

For example, the normal read-write hard disk storage of a controlled execution system can be infected with a computer virus during normal operation just as any other system. However, since there is no way the virus can be loaded onto the read-only medium. there is no way the virus can execute, thus preventing it from doing any damage or propagating itself to any other systems. These characteristics make controlled execution techniques likely candidates for controlling essential software functions such as key escrow.

In the next few years, these techniques may see extensive use in protecting ordinary workstations against virus invasions. Any system that does not require frequent updates to its executable software can use these techniques to protect the integrity of the system.

Software Key Escrow Techniques

There have been several software key escrow techniques that have been proposed, including those of Silvia Micali. The problem with all such approaches as proposed is that without some form of integrity protection, they are essentially voluntary systems, subject to the whim of the user.

If such techniques were to be implemented in a system employing controlled execution techniques, they would no longer be "voluntary." Enforcement of their proper functioning could be ensured by these techniques.

A Case Study: The Defense Message System

The ARPA Safeguards project demonstrated the application of controlled execution techniques to enforce software integrity in various environments. The initially envisioned application, sale of a system to a potentially hostile user, involved tamper detection and audit techniques in addition to controlled execution.

If applied in a less hostile environment in which the user can be trusted not to maliciously modify his or her workstation hardware configuration, controlled execution techniques can provide a very significant improvement in software integrity.

The DMS, which is the initial customer for the MOSAIC Tessera system, represents such a constrained environment where controlled execution-based systems might allow use of software key escrow techniques. The following case study illustrates one way that such a system might work.

This approach is based on the premise that users of the DMS will be required to register with the DMS Program Office and utilize DMS-approved software packages in order to ensure that vital functions such as key escrow are properly employed. A major advantage of such an approach would be that workstations used for DMS communications could only run "DMS-approved" applications, protected by a controlled execution mechanism. Such systems would be invulnerable to most common computer virus attacks.

It is important to note that use of a controlled execution approach might be highly advantageous even if hardware key escrow is used, since it could assure proper functioning of the software that supports the Tessera PCMCIA card as well as provide substantial virus protection.

When the user installed his or her DMS software package, the installation process would automatically reformat the workstation hard disk and create a read-only partition on to which it would load all executable software. The remainder of the hard disk would be available in a read-write mode for the storage of user data. As part of the installation process, the user would be required to register with the DMS central facility. At this point the user would be issued a personal identification number (PIN).

Whenever the user sends a DMS message, regardless of which software key escrow technique was used, this unique identifier combined with the date and time of the message and the identity of the workstation would ensure the uniqueness of the message encryption and key escrow transactions.

The digital signature-based upgrade process of controlled execution could ensure that the user can easily upgrade new software applications as they become available. Periodically, the DMS Program Office would distribute the digitally signed hash values for new application programs that have been approved for use on DMS workstations. The user would insert the off-the-shelf "shrink-wrapped" disk in the floppy reader and run a special install program that would first check to see if the signature of the application was on the DMS-approved list. If it was, the new application would be added to the "read-only" medium and be available for execution at any time.

With such a controlled execution system, all DMS workstations could operate with a high degree of software integrity and in particular could perform message encryption and software key escrow techniques without requiring the use of special hardware devices.

Conclusions

This paper has explored:

- The variety of factors that influence the choice of hardware or software based mechanisms for encryption and key escrow,

- Software integrity techniques based on a controlled execution process that evolved in the ARPA Safeguards Project, and,

- The application of such techniques to a software-only version of encryption and key escrow for the DMS.

This analysis has shown that software-based key escrow techniques can be employed with results similar to those of hardware key escrow. This approach will not allow the use of classified algorithms since it provides no way to protect the algorithm from disclosure.

B View Graphs of Presenters

B.1 James W. Arney: Criteria for High Integrity Software Encryption

Key Escrow Encryption Workshop

Criteria for High Integrity - Introduction

- GOAL: Provide a framework to judge escrowed encryption
- ROLE: I am advisor to Dr. Branstad; experienced with similar jobs
- This is NOT: Policy talk; Defense of EES talk
- OUTLINE:
  - System Security Engineering paradigm - applied to escrow
    - user/customer needs
    - ** design requirements **
    - development
    - evaluation/verification
  - Design Requirements
    - algorithm / protocol level
    - hardware
    - software

p1, Jim Arney, Arney@dockmaster.ncsc.mil, NSA, 301-688-6058, 10 June '94

System Security Engineering paradigm

applied to escrow

- User / Customer Needs
  Dynamic - must feedback, educate, listen
  Who?: information owner; intended recipient; authorized escrow
  What?: integrity
  confidentiality
  availability / access
  What adversary / threat?: mistake or accident
  hacker/corporate/university
- Design Requirements (details on next chart)
  Intimately tied to user needs (which change)
- Development
  Evolutionary - can't always meet all needs initially
- Evaluation / Verification
  Assesses residual risk; met and unmet user needs

p2, Jim Arney, Arney@dockmaster.ncsc.mil, NSA, 301-688-6058, 10 June '94

Design Requirements

applied to escrow

- Algorithm / Protocol
  prevent "single rogue user" from avoiding escrow while communicating securely (e-mail scenario)

- Hardware
  controlled execution ??
  protected supervisory states
  "swap to server" limitations
  interrupt handling

- Software (details on next chart)
  protecting the software - circumvention, modification
  protecting variables
  good software engineering
  other software concerns

p3, Jim Arney, Arney@dockmaster.ncsc.mil, NSA, 301-688-6058, 10 June '94

Protecting Embedded Software Cryptography

applied to escrow

- Thanks to Steve LaFountain, NSA, former TPEP Chief Evaluator

- Protecting the software - modification, circumvention
  ROM
  Access Control / memory protection
  Crypto-sealing (detect, not prevent, modification)
  Process isolation
  Application trust
  Interrupts and context switching

- Protecting variables - in addition to above
  Zeroization

- Good software engineering - modularity, layering, least privilege, covert channels

- Other software concerns - operating system, hardware trust

p4, Jim Arney, Arney@dockmaster.ncsc.mil, NSA, 301-688-6058, 10 June '94

B.2 Dorothy E. Denning: International Dey Escrow Encryption - Proposed Objectives

International Key Escrow Encryption: Proposed Objectives

Dorothy E. Denning

Georgetown University

International Key Escrow System

Encryption products that provide secure communications

Key escrow system for authorized government access

International communications

Use of encryption product outside the country holding the key

General Areas of Objectives

1. General properties of escrowed encryption
2. Escrow agents and escrowing of keys
3. National controls and international and bilateral agreements

General Properties of Escrowed Encryption

1. Strong security

    a. Strong cryptographic security

    b. Strong assurance against abuse/misuse of keys

2. Authorized government access

    a. Escrowed key unique to a product

    b. Law Enforcement Access Field (LEAF)

Initial access within 2 hours; real-time thereafter

Access to communications originating from all parties using the key of one

General Properties of Escrowed Encryption (continued)

3. Hardware or software
4. Classified or unclassified algorithms
5. Multiple standards and gateways
6. Corporate (private sector) key escrow - separate or integrated

Key Escrow Agents and Escrowing of Keys

1. One or more escrow agents

   Optional "k out of n" system

2. Single nation escrow

3. Keys escrowed before first use

   a. Time of manufacture

   b. Time of first use

National Controls and International and Bilateral Agreements

1. National control

    a. Import/export/use

    b. Who holds keys for products used within jurisdiction and for products exported and imported

2. International and bilateral agreements

    a. Assisting with criminal investigations

    b. Sharing encryption technology or manufacturing facilities

    c. Permitting sale and use of products

Law Enforcement Decryption Assistance

1. Receive encrypted communications, decrypt them, and return plaintext

2. Send government officials with decrypt device loaded with the key

3. Give out the key

National Policy Options

Export Options

E1 Products treated like unescrowed encryption products
E2 Products generally exportable as long as keys held by N
E3 Products generally exportable if keys held by N or by a nation with a mutual assistance agreement with N
E4 Products exportable without constraint

Internal Use Options

U1 Products treated like unescrowed encryption products
U2 Products can be used only if N holds the keys
U3 Products can be used if keys are held by N or by a nation with a mutual assistance agreement with N
U4 Products can be used without constraint

Possible Scenarios for the Export of EES Technology

1. U.S. holds the keys

2. Foreign country escrows keys of chips manufactured in the U.S.

   The foreign country uses a U.S. chip programming facility to acquire the keys to chips programmed under its supervision.

3. Foreign country manufactures its own chips and escrows its own keys.

Law Enforcement Scenarios When Country A Investigates Subject X

Scenario	Location of Subject X	Source of Product	Holder of Key	Country A's Objectives	Country B's Objectives
1	A	A	A		
2	A	A	B	KA from B	
3	A	B	A		
4	A	B	B	KA from B	
5	A	B	C	KA from C	
6	B	A	A	IA from B	KA from A
7	B	A	B	IA from B	
8	B	A	C	IA from B	KA from C
9	B	B	A	IA from B	KA from A
10	B	B	B	IA from B	
11	B	B	C	IA from B	KA from C
12	B	C	A	IA from B	KA from A
13	B	C	B	IA from B	
14	B	C	C	IA from B	KA from C

Notation: IA = investigative and intercept assistance, KA = key assistance

Summary

Strong security for international communications

Authorized government access

Hardware or software, classified or unclassified technology

Multiple technologies and standards, gateways

Single nation escrow with one or more escrow agents

Keys escrowed before first use

National control over export/import/use and who holds keys

International and bilateral agreements

B.3 Silvio Micali: Multipurpose Key Escrowing Methods

View graphs are available from the author.

B.4 Jon Roberts: Private Escrow Key Management

Private Escrow Key Management

A Solution for
National Security/Law Enforcement/
Privacy of the Individual

TECSEC

Clipper Escrow Key Management

Voice vs. Computerized Records

TECSEC

New Definition of Information Protection

Protection of the <u>Information</u>

vs.

Protecting the <u>Means of Communicating</u> the Information

File Encryption for Computerized Record Protection

TECSEC

An Expanded Encryption Model

Communications Encryption

&

File Encryption

File Encryption Process

Keys must be maintained by individual
for later retrieval

Government access through court order
to private files

TECSEC

Law Enforcement Needs

Documents from third parties

Support for civil and criminal actions to enforce laws

- SEC
- Environmental
- Government Contract
- Banking

A Solution for the International Community

Multiple Algorithms

&

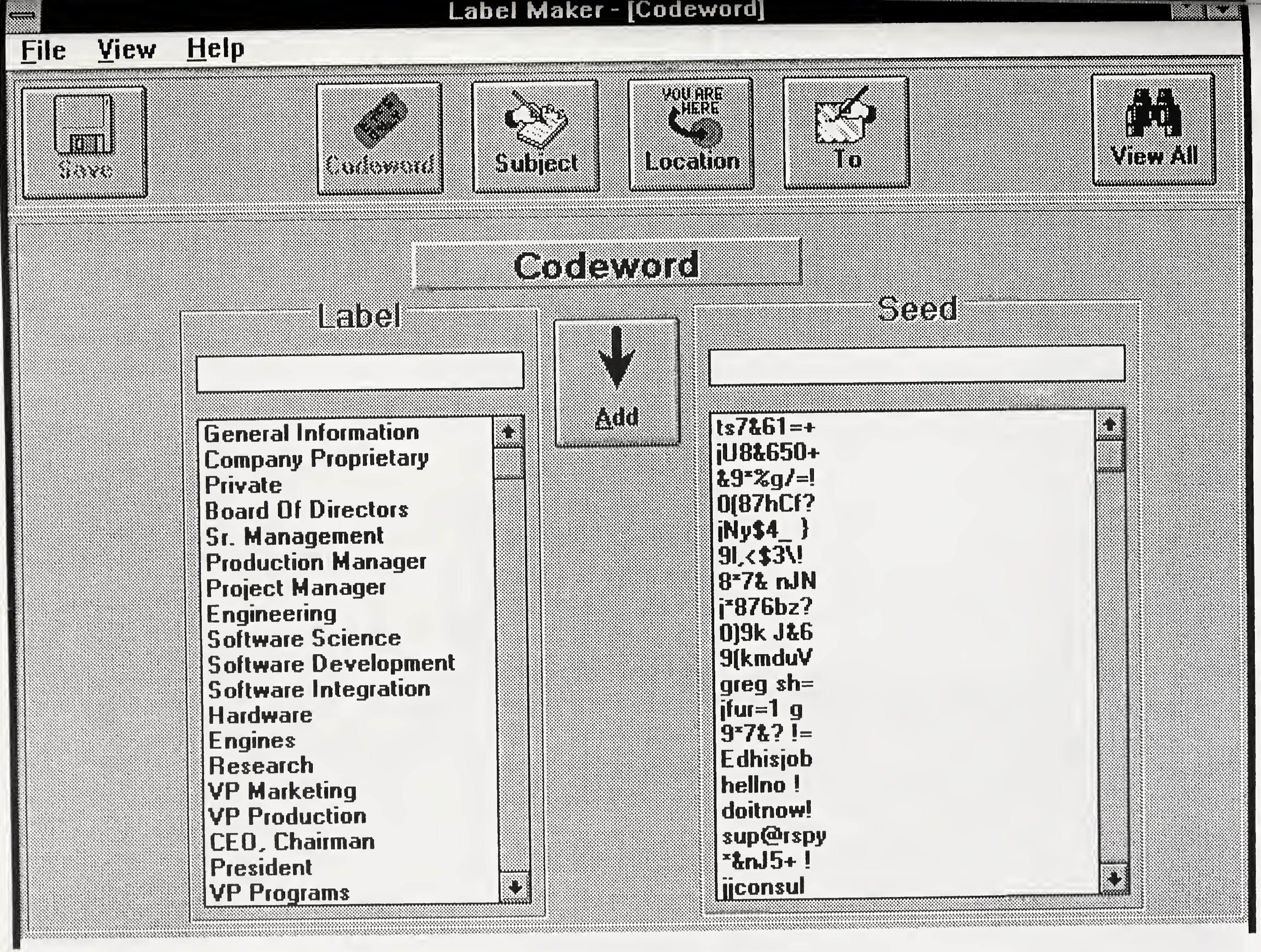
Algorithmic Independence

TECSEC

An Example of a Commercial Private Escrow Key Management Program

VEIL

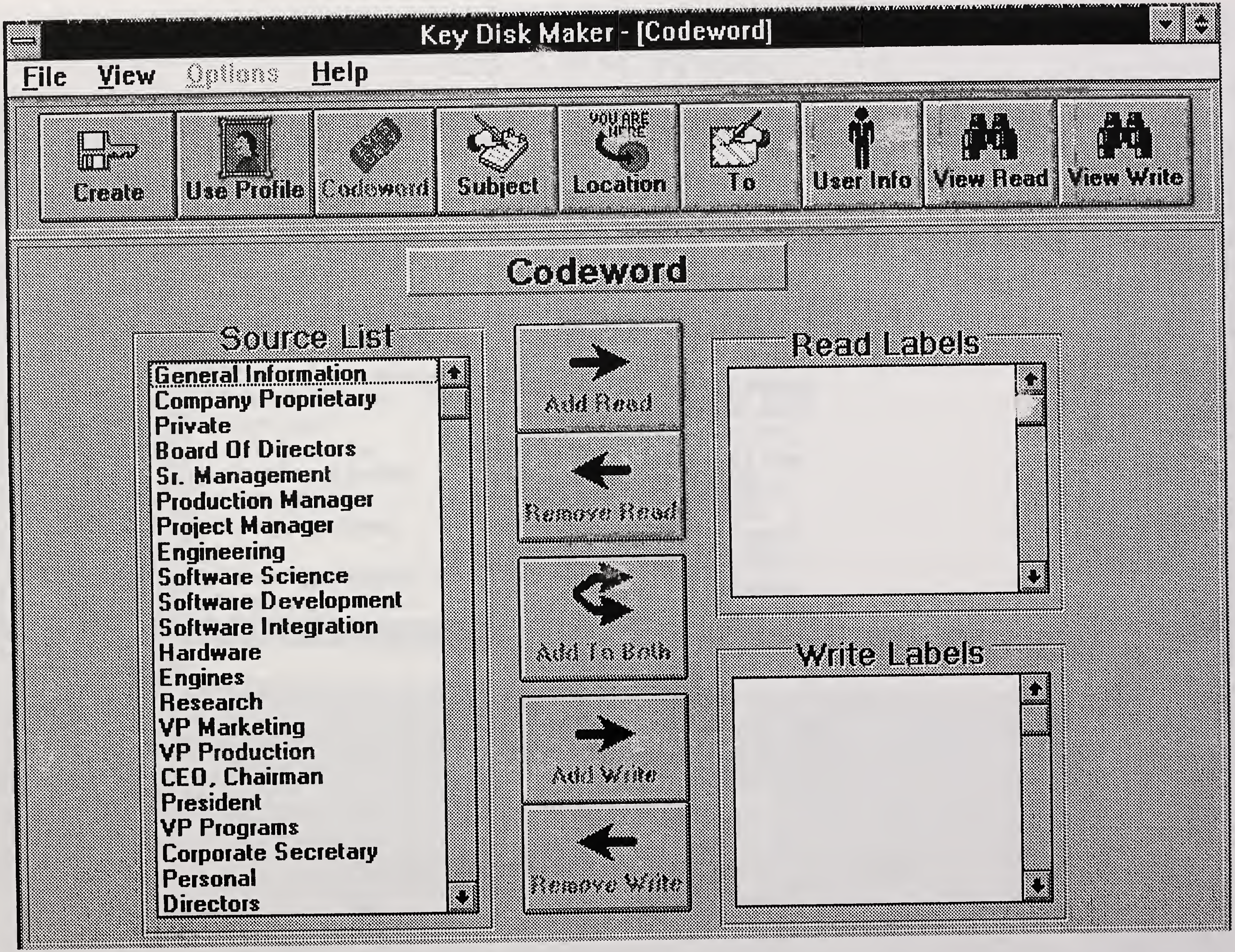
TECSEC



General Information
Company Proprietary
Private
Board Of Directors
Sr. Management
Production Manager
Project Manager
Engineering
Software Science
Software Development
Software Integration
Hardware
Engines
Research
VP Marketing
VP Production
CEO, Chairman
President
VP Programs

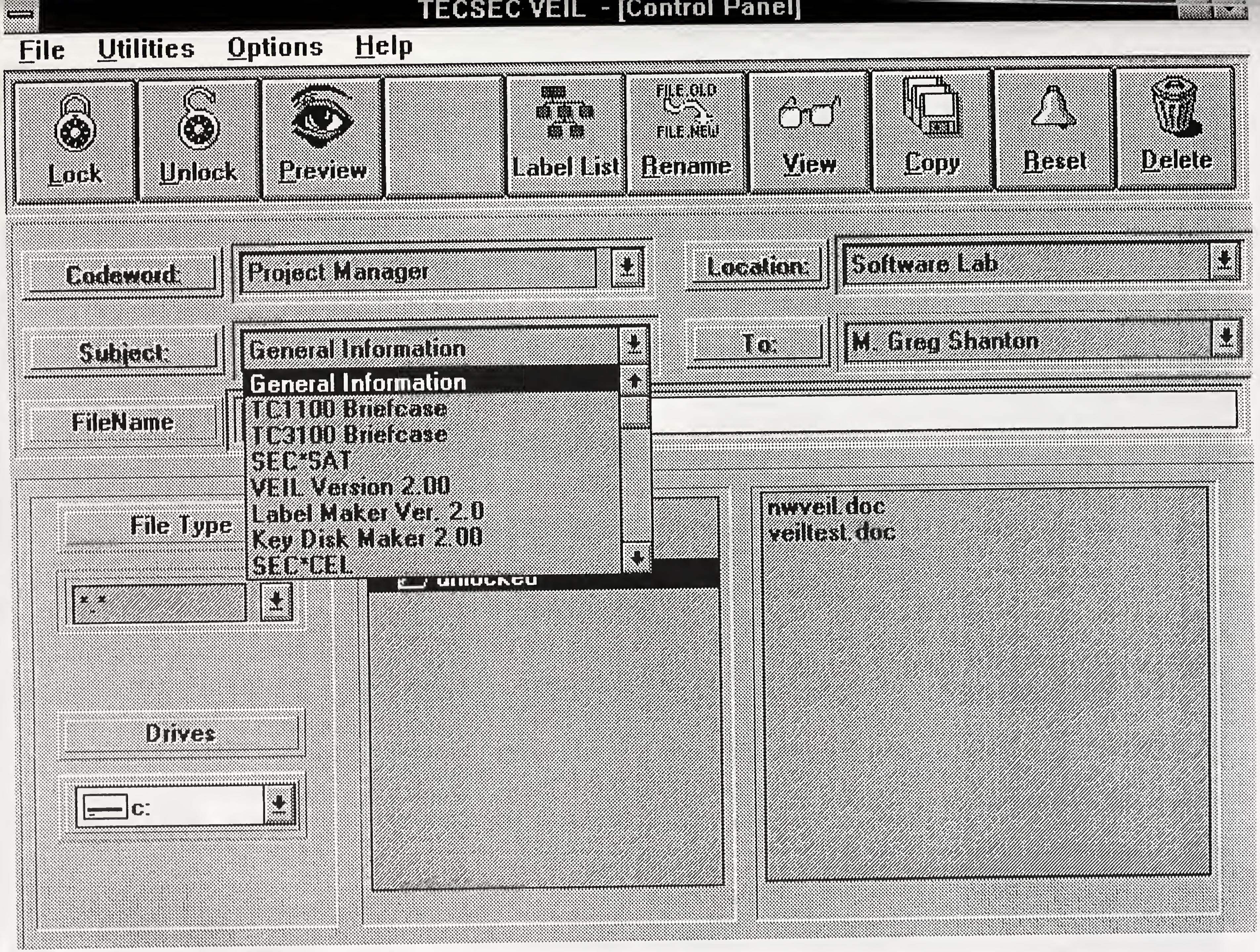
```
ts7&61=+
jU8&650+
&9*%g/=!
0(87hCf?
jNy$4_ }
9l,<$3\!
8*7& nJN
j*876bz?
0)9k J&6
9(kmduV
greg sh=
jfur=1 g
9*7&? !=
Edhisjob
hellno !
doitnow!
sup@rspy
*&nJ5+ !
jjconsul
```

VEIL Label Maker



General Information
Company Proprietary
Private
Board Of Directors
Sr. Management
Production Manager
Project Manager
Engineering
Software Science
Software Development
Software Integration
Hardware
Engines
Research
VP Marketing
VP Production
CEO, Chairman
President
VP Programs
Corporate Secretary
Personal
Directors

VEIL Key Disk Maker



TECSEC VEIL - [Control Panel]

Codeword: Project Manager

Location: Software Lab

Subject: General Information

To: M. Greg Shanton

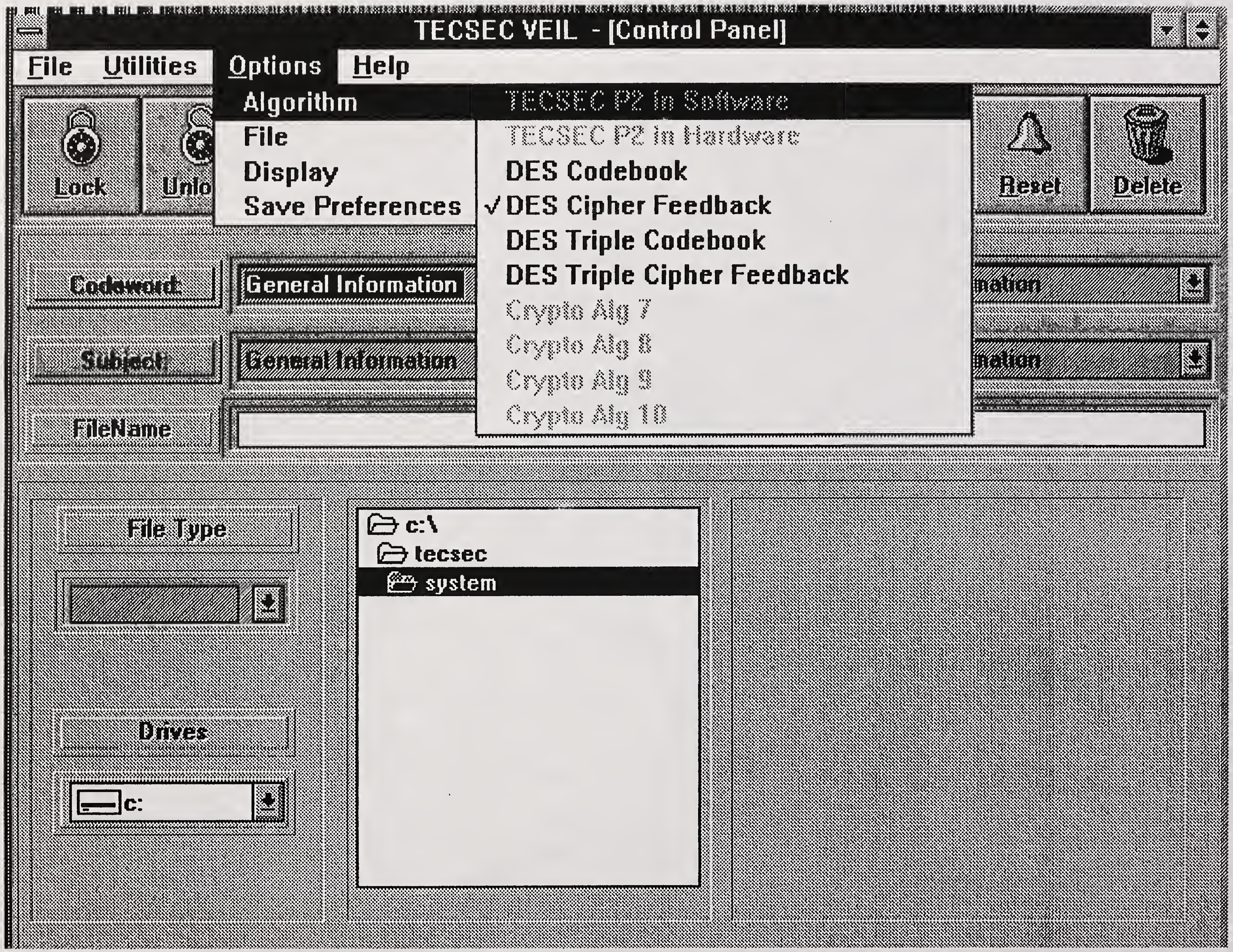
FileName

File Type: *.*

Drives: c:

nwveil.doc
veiltest.doc

VEIL Main Screen



✓DES Cipher Feedback

Codeword: General Information

Subject: General Information

c:

VEIL Main Screen - Choosing Algorithm

B.5 Miles Smid: The U.S. Government Key Escrow System

The U. S. Government Key Escrow System

Miles E. Smid
NIST

Presidential Directives
April 15, 1993

- Announced “Clipper Chip” and “Key-escrow” system
- Directed Government agencies to develop a policy on encryption
- Review to consider broader export options for key-escrow products
- Examine feasibility of software key-escrow
- Examine impact of technology on law enforcement

Goals of Escrowed Encryption

- ✦ To provide cryptographic protection to unclassified, sensitive telecommunications data
- ✦ To allow for the decryption of encrypted telecommunications when lawfully authorized

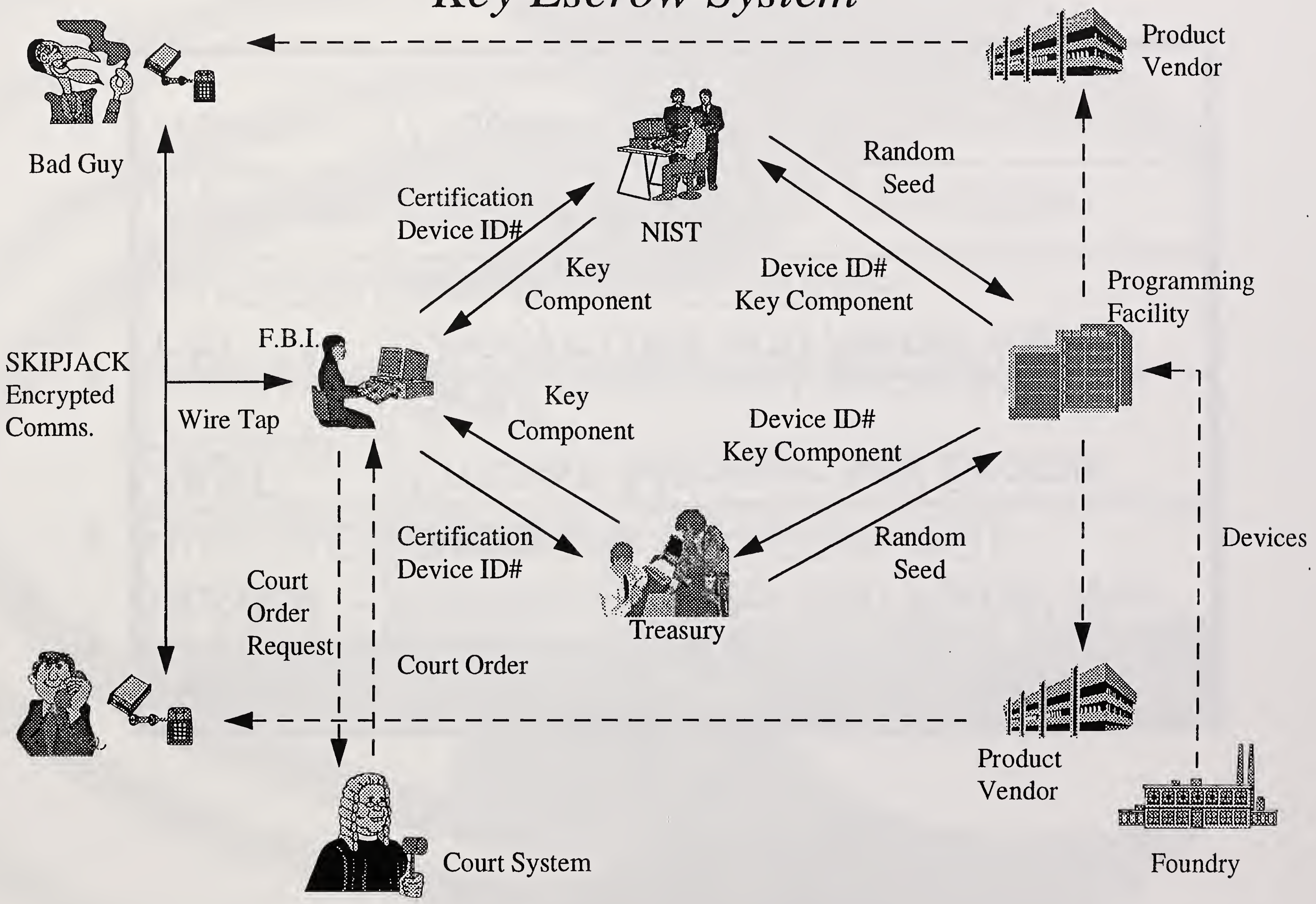
Status

- *NIST Appointed Program Manager*
- *Development of Procedures*
- *Two Months to Establish Working System*
- *First Programming (October 93)*
- *17,000 Clipper Chips Escrowed (March 94)*

Participating Agencies

Agency	Role
Justice	System Sponsor and Family Key Agent
NIST	Program Manager and Escrow Agent
FBI	Decrypt User and Family Key Agent
Treasury	Escrow Agent
NSA	Program Developer

Key Escrow System



Key Escrow Functions

- *Production of Chips*
- *Generation of Random Seeds and Initial Keys*
- *Generation of Key Components and Chip Programming*
- *Key Component Transportation and Storage*
- *Controlled Release of Key Components*
- *Decryption of Communications*

Today's System

- Prototype Components
- R&D Software
- Manual Operations

The Target System

- ✦ Upgrades Chip Programming Facility
- ✦ Employs Cryptographic Functions to Automate Key Transportation
- ✦ Develops Trusted Escrow Agent Workstation
- ✦ Completes Trusted Decryption Processor

Four Phases of Development

- *Phase 1 (Sep. 93 - March 94)*
  - *Prototype Programming Facility*
  - *Manual Procedures for Handling and Storage of Escrow Components*
  - *No Decryption Processor*
- *Phase 2 (April 94 -   )*
  - *Prototype Decryption Processor*
  - *Simple Key Component Extraction Prog.*
  - *Manual Key Component Release Procedures*

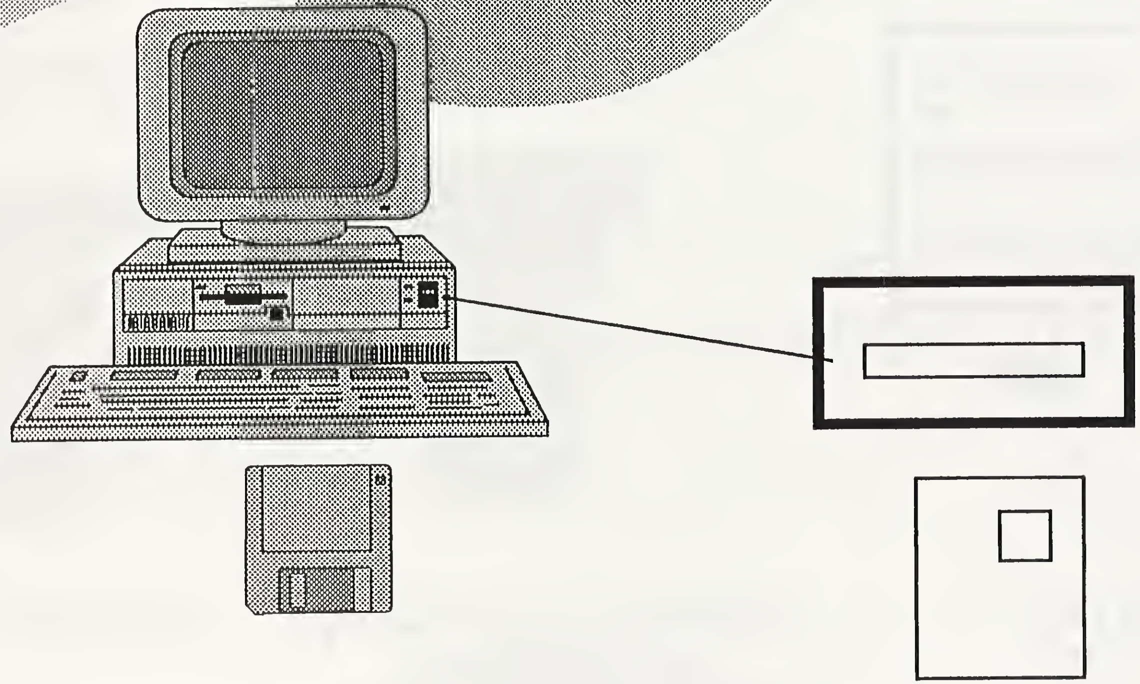
Four Phases of Development (Continued)

- Phase 3
  - 1st Release of Target Programming Facility
  - 1st Release of Escrow Agent Workstation
- Phase 4
  - Deployment of Final Operating Capability for all Subsystems
  - Transition to Life Cycle Support

Escrow Agent Functions

- *Random Seed Generation*
- *Chip Programming*
- *Key Component Transportation and Storage*
- *Key Component Release*

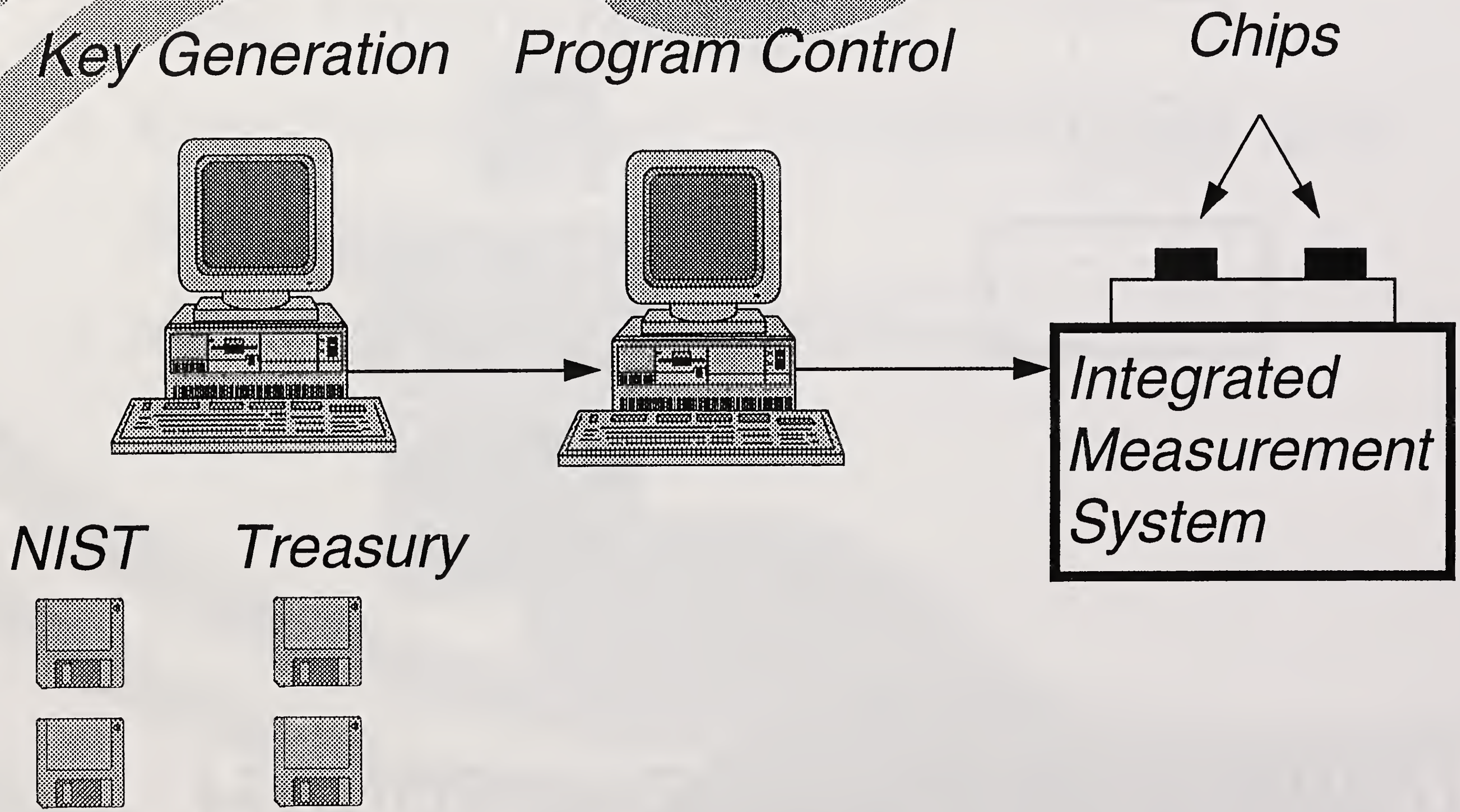
Random Seed Generation



f(ai, dt, time, SHA) -> PRNG

SHA FIPS 180
PRNG ANSI X9.17

Chip Programming



Key Generation

Program Control

Chips

Integrated Measurement System

NIST

Treasury

Key Transport and Storage

- Dual Control / Two Person Integrity
- Split Knowledge
- Redundancy
- Key Component Generation and Storage Logs

Physical Security

- Memory Wipe
- Shrink-wrapped Software
- Double Safes
- Site Security
- Clearances
- Packaging
- Logs

Evaluations

- *Reviews*
- *Audits*
- *Independent Verification and Validation*
- *Certification*
- *Accreditation*

Key Escrow Review Group

- Membership: Dr. Ernie Brickell, Dr. Dorothy Denning, Dr. Steve Kent, Dr. Dave Maher
- Meet on March 24-25 at NIST
- Recommendations to be Factored into Target Key Escrow System Design

Certification and Accreditation

- ✦ *Based on DOD Certification and Accreditation Process Handbook*
- ✦ *Certification by Key Escrow Certification Working Group*
- ✦ *Independent Verification and Validation*
- ✦ *Accreditation by Department of Justice*

Recent Efforts

- Preparation for CAPSTONE Programming
- SHA modification to SHA-1
- Search for Possible New Escrow Agent
- Target System Requirements Review

B.6 Stephen Walker and David Balenson: A Software Key Escrow Approach

A Software Key Escrow Approach

Trusted Information Systems, Inc.

Stephen T. Walker
David M. Balenson

June 10, 1994

9406-009.wp

- OVERVIEW
  - Background
  - Motivation
  - Assumptions
  - Protection Model
  - Softwarc Key Escrow Approach
  - Strengths of this Approach

- BACKGROUND

  - August '93

    - NIST Software Key Escrow CRADA

  - Group of 4 + NIST + NSA met

    - December '93, February '94, April '94

    - Ground rules for key escrow alternatives

- MOTIVATION

  - To develop a broadly acceptable, low cost software key escrow system that achieves the objectives of law enforcement.

- **ASSUMPTIONS**

  - Software key escrow must work as well as the key escrow in Clipper/Capstone:

    1. Escrow process must ensure with a reasonable degree of certainty that law enforcement, when authorized, will be able to decrypt communications.

    2. Software escrow process need not solve problems that Clipper/Capstone escrow does not solve,

       e.g., super-encryption prior to submission to key escrow.

    3. In general, neither system can solve the problems of a determined software hacker.

- PROTECTION MODEL

    - Software key escrow system cannot protect secret information in generally available commercial products .

        - Neither algorithms or secret keys.

        - Our approach is based on public key cryptography:

            - Private keys held by escrow agents.
            - Public keys held in commercial product.

        - Our approach will work with any available cryptographic algorithm:

            - But it cannot protect a secret algorithm.

- PROTECTION MODEL (CONTINUED)

  - Key escrow systems depend upon unique identification of device/program:

    - Clipper/Capstone based on device unique identifier.

    - Our approach provides unique program identification either during manufacture or at program initialization by user.

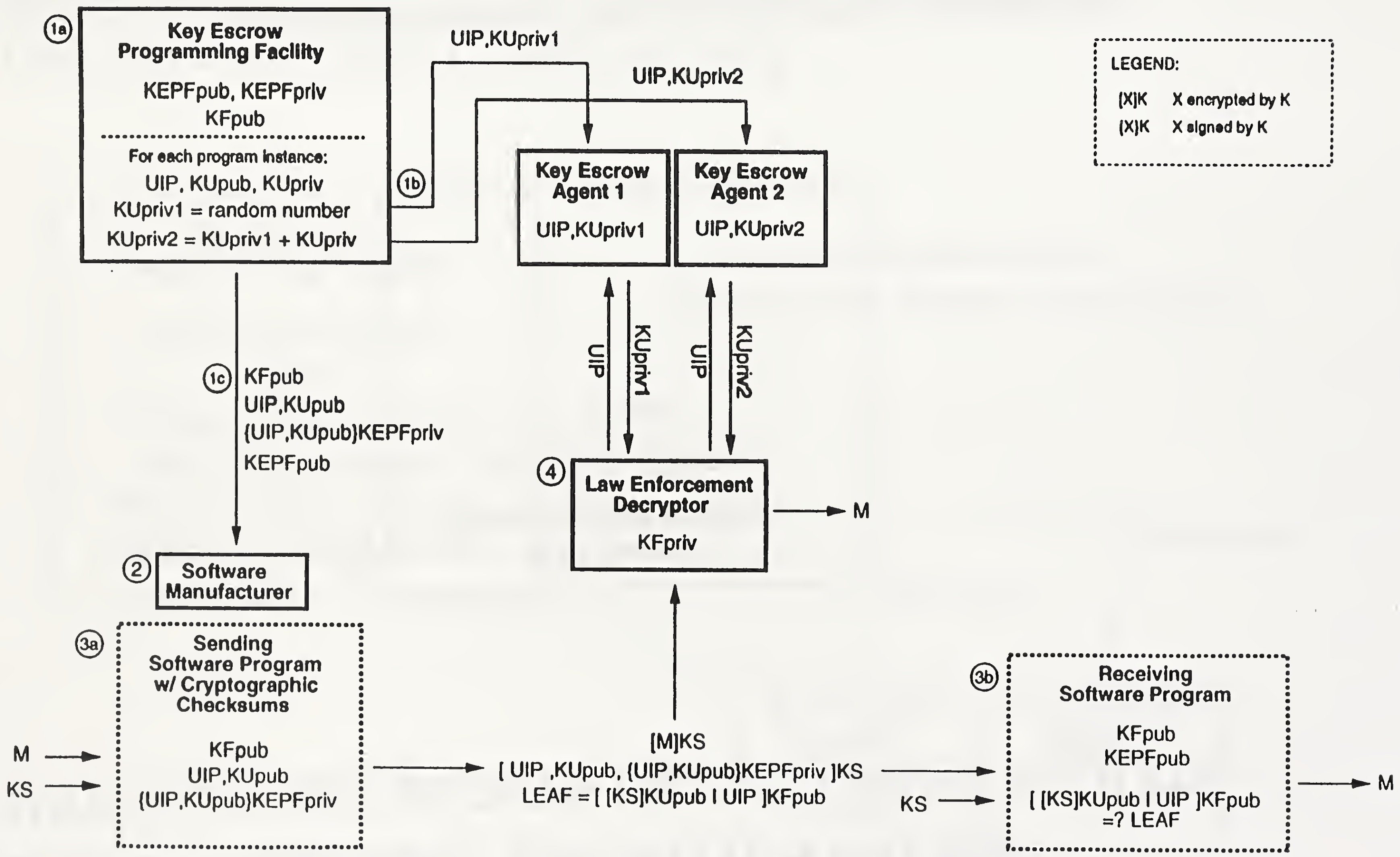
- PROTECTION MODEL (CONTINUED)

  - The software key escrow system will be embedded in a "shrink wrap" software application.

  - Cryptographic checksums will be embedded at multiple points in the application to check for code modification -- similar to software piracy checks.

  - Combination provides commercial quality integrity protection equivalent to Tessera with the software that drives it.

COMPLETE SOFTWARE KEY ESCROW SYSTEM



1a
Key Escrow Programming Facility

KEPFpub, KEPFpriv
KFpub

For each program instance:
UIP, KUpub, KUpriv
KUpriv1 = random number
KUpriv2 = KUpriv1 + KUpriv

1b
UIP,KUpriv1
UIP,KUpriv2

Key Escrow Agent 1
UIP,KUpriv1

Key Escrow Agent 2
UIP,KUpriv2

LEGEND:

[X]K	X encrypted by K
{X}K	X signed by K

1c
KFpub
UIP,KUpub
{UIP,KUpub}KEPFpriv
KEPFpub

UIP
KUpriv1
UIP
KUpriv2

4
Law Enforcement Decryptor
KFpriv

M

2
Software Manufacturer

3a
Sending Software Program w/ Cryptographic Checksums

KFpub
UIP,KUpub
{UIP,KUpub}KEPFpriv

M
KS

[M]KS
[UIP ,KUpub, {UIP,KUpub}KEPFpriv]KS
LEAF = [[KS]KUpub I UIP]KFpub

KS

3b
Receiving Software Program

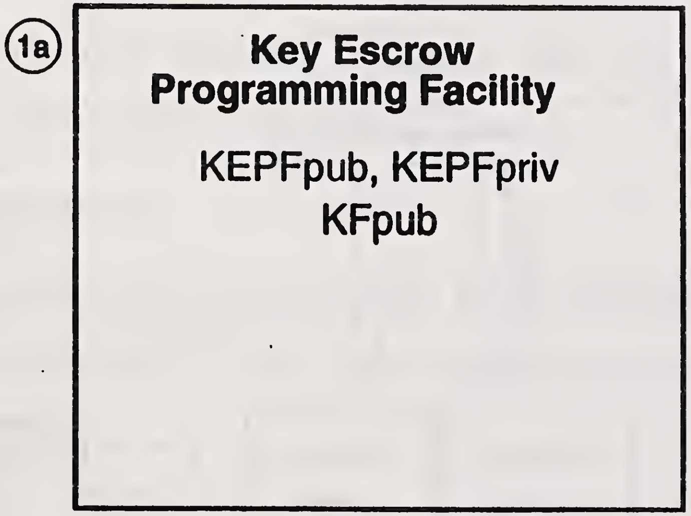
KFpub
KEPFpub

[[KS]KUpub I UIP]KFpub
=? LEAF

M

SOFTWARE KEY ESCROW SYSTEM:

INITIALIZE KEY ESCROW PROGRAMMING FACILITY



1a

Key Escrow Programming Facility

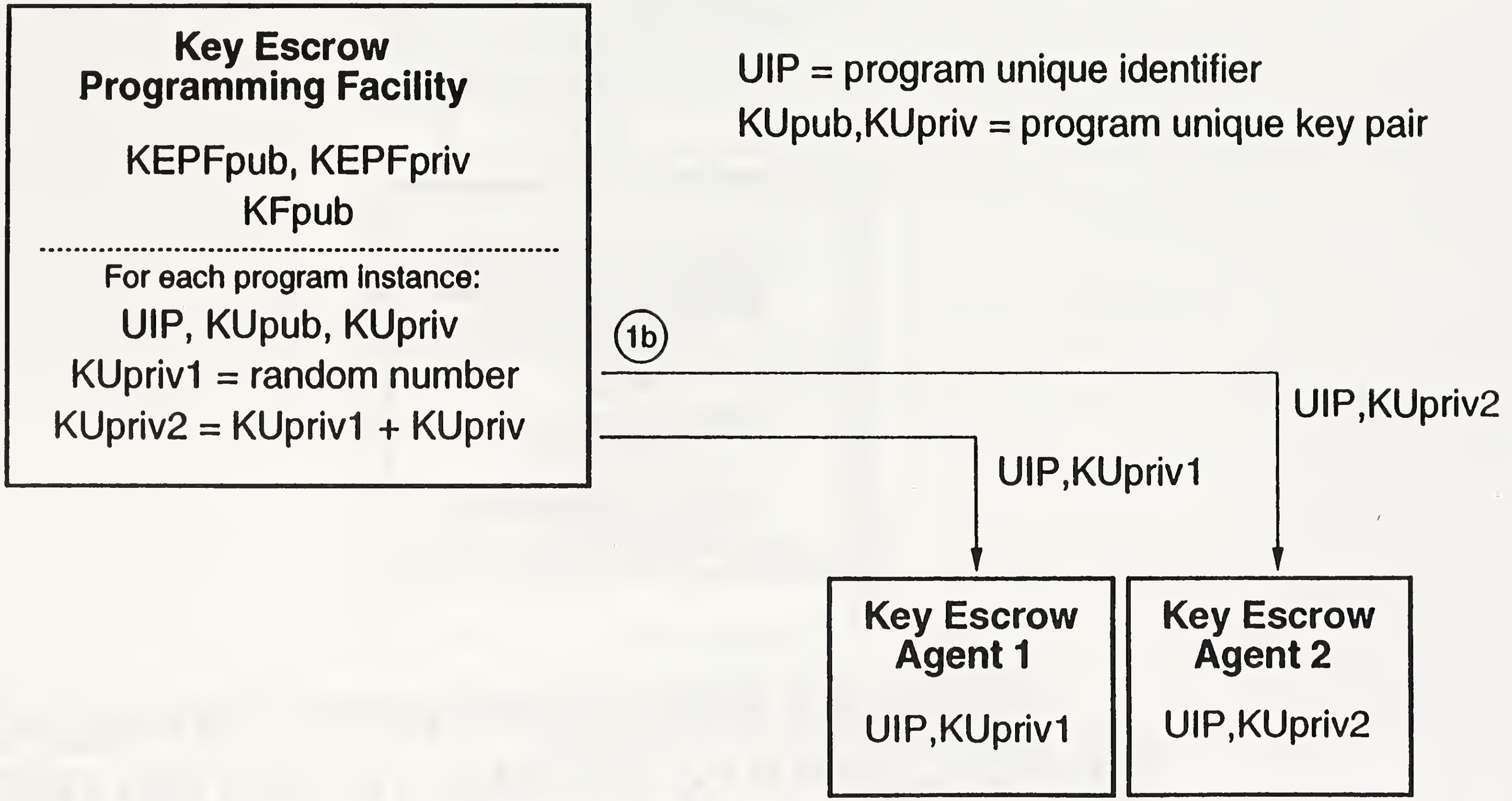
KEPFpub, KEPFpriv
KFpub

KEPFpub,KEPFpriv = key escrow programming facility key pair
KFpub = family key (public component)

Trusted Information Systems, Inc., June 10, 1994

SOFTWARE KEY ESCROW SYSTEM:

FOR EACH PROGRAM INSTANCE, GENERATE PROGRAM UNIQUE PARAMETERS AND ESCROW THE PRIVATE KEY COMPONENTS



Key Escrow Programming Facility

KEPFpub, KEPFpriv
KFpub

For each program instance:
UIP, KUpub, KUpriv
KUpriv1 = random number
KUpriv2 = KUpriv1 + KUpriv

UIP = program unique identifier

KUpub,KUpriv = program unique key pair

Key Escrow Agent 1

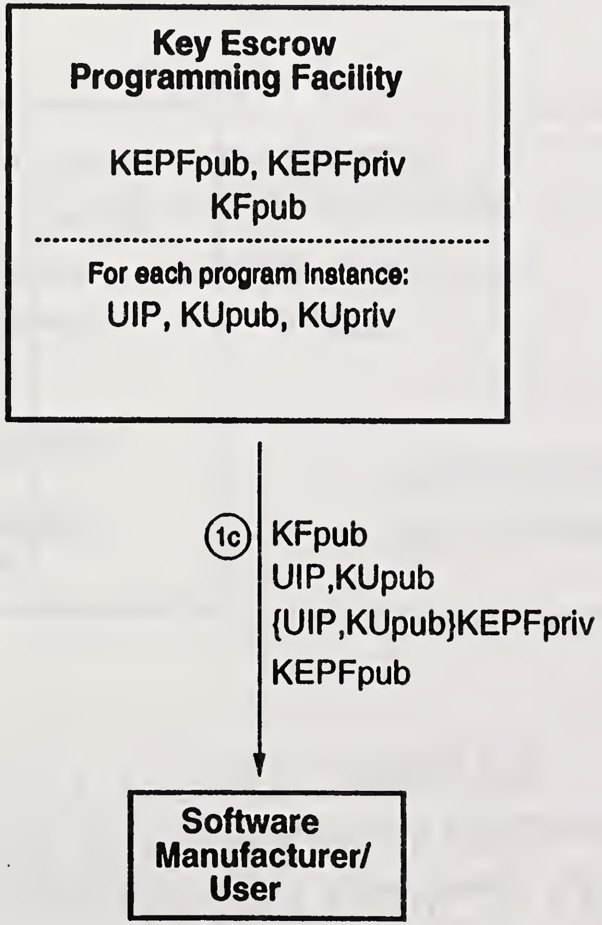
UIP,KUpriv1

Key Escrow Agent 2

UIP,KUpriv2

SOFTWARE KEY ESCROW SYSTEM:

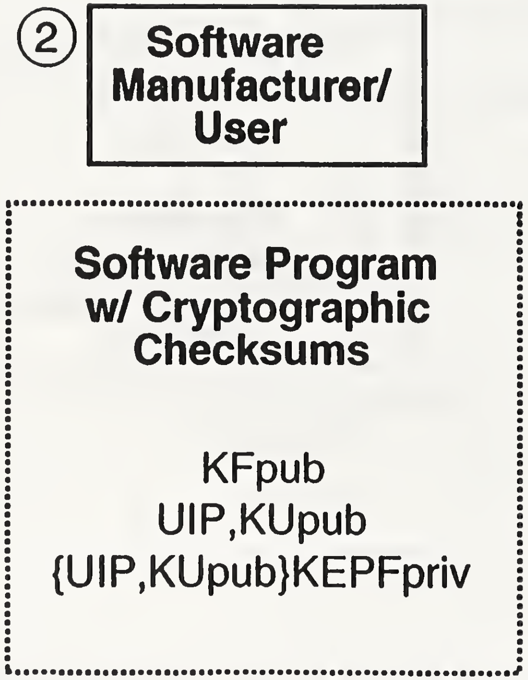
SEND PROGRAM UNIQUE PARAMETERS TO SOFTWARE MANUFACTURER OR USER



Trusted Information Systems, Inc., June 10, 1994

SOFTWARE KEY ESCROW SYSTEM:

EMBED PROGRAM UNIQUE PARAMETERS IN SOFTWARE PROGRAM



② Software Manufacturer/ User

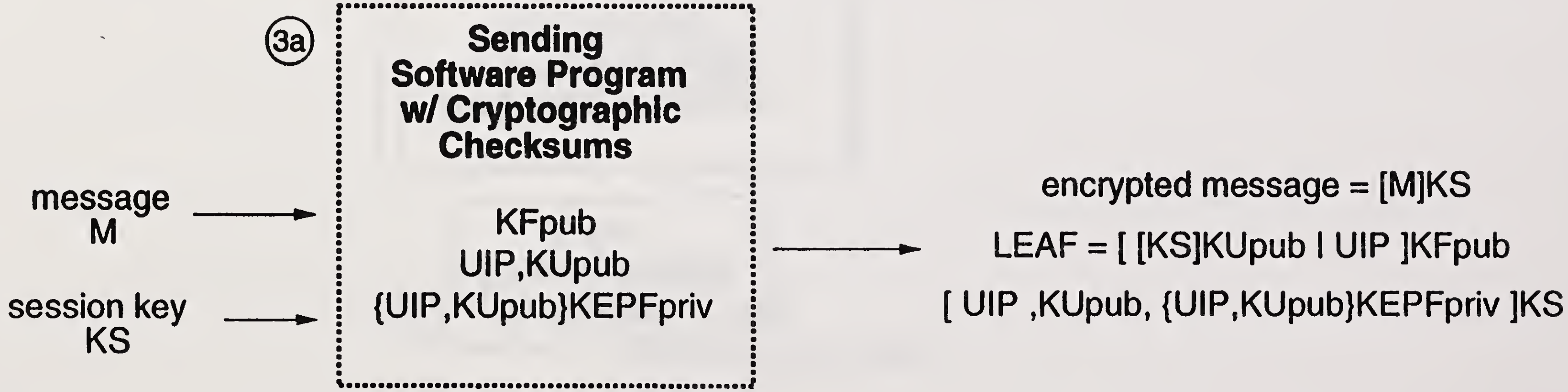
Software Program w/ Cryptographic Checksums

KFpub
UIP,KUpub
{UIP,KUpub}KEPFpriv

Trusted Information Systems, Inc., June 10, 1994

SOFTWARE KEY ESCROW SYSTEM:

SENDING SOFTWARE PROGRAM TRANSMITS ENCRYPTED MESSAGE AND LEAF



3a

message
M

session key
KS

Sending Software Program w/ Cryptographic Checksums

KFpub
UIP,KUpub
{UIP,KUpub}KEPFpriv

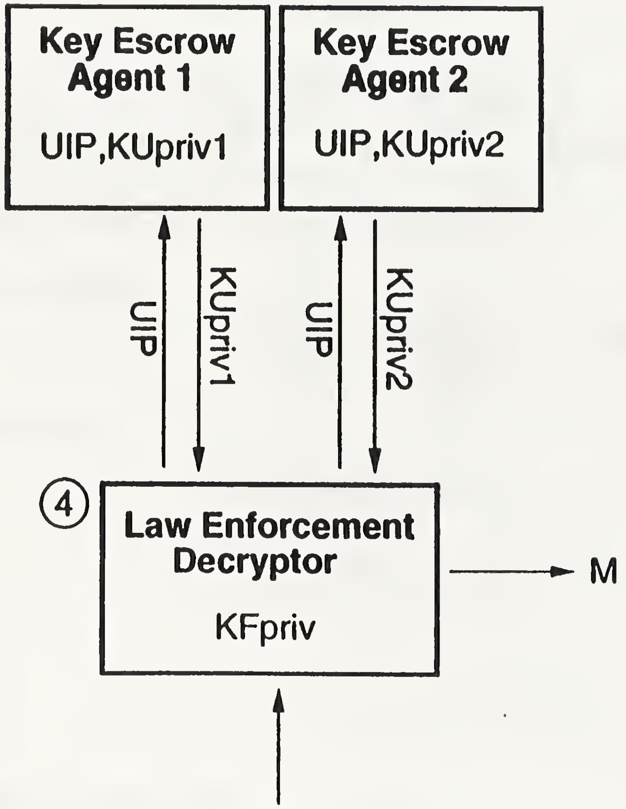
encrypted message = [M]KS

LEAF = [[KS]KUpub I UIP]KFpub

[UIP ,KUpub, {UIP,KUpub}KEPFpriv]KS

SOFTWARE KEY ESCROW SYSTEM:

LAW ENFORCEMENT DECRYPTOR OBTAINS PROGRAM UNIQUE PRIVATE KEY AND DECRYPTS MESSAGE



Key Escrow Agent 1

UIP,KUpriv1

Key Escrow Agent 2

UIP,KUpriv2

UIP

KUpriv1

UIP

KUpriv2

4

Law Enforcement Decryptor

KFpriv

M

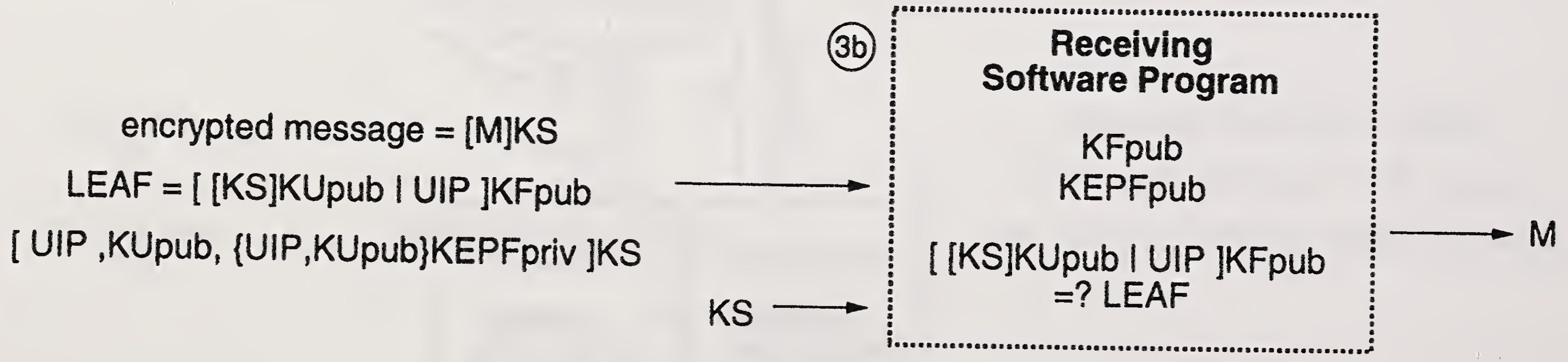
encrypted message = [M]KS

LEAF = [[KS]KUpub I UIP]KFpub

[UIP ,KUpub, {UIP,KUpub}KEPFpriv]KS

SOFTWARE KEY ESCROW SYSTEM:

RECEIVING SOFTWARE PROGRAM AUTHENTICATES LEAF AND DECRYPTS MESSAGE



encrypted message = [M]KS

LEAF = [[KS]KUpub | UIP]KFpub

[UIP ,KUpub, {UIP,KUpub}KEPFpriv]KS

KS

(3b)

Receiving Software Program

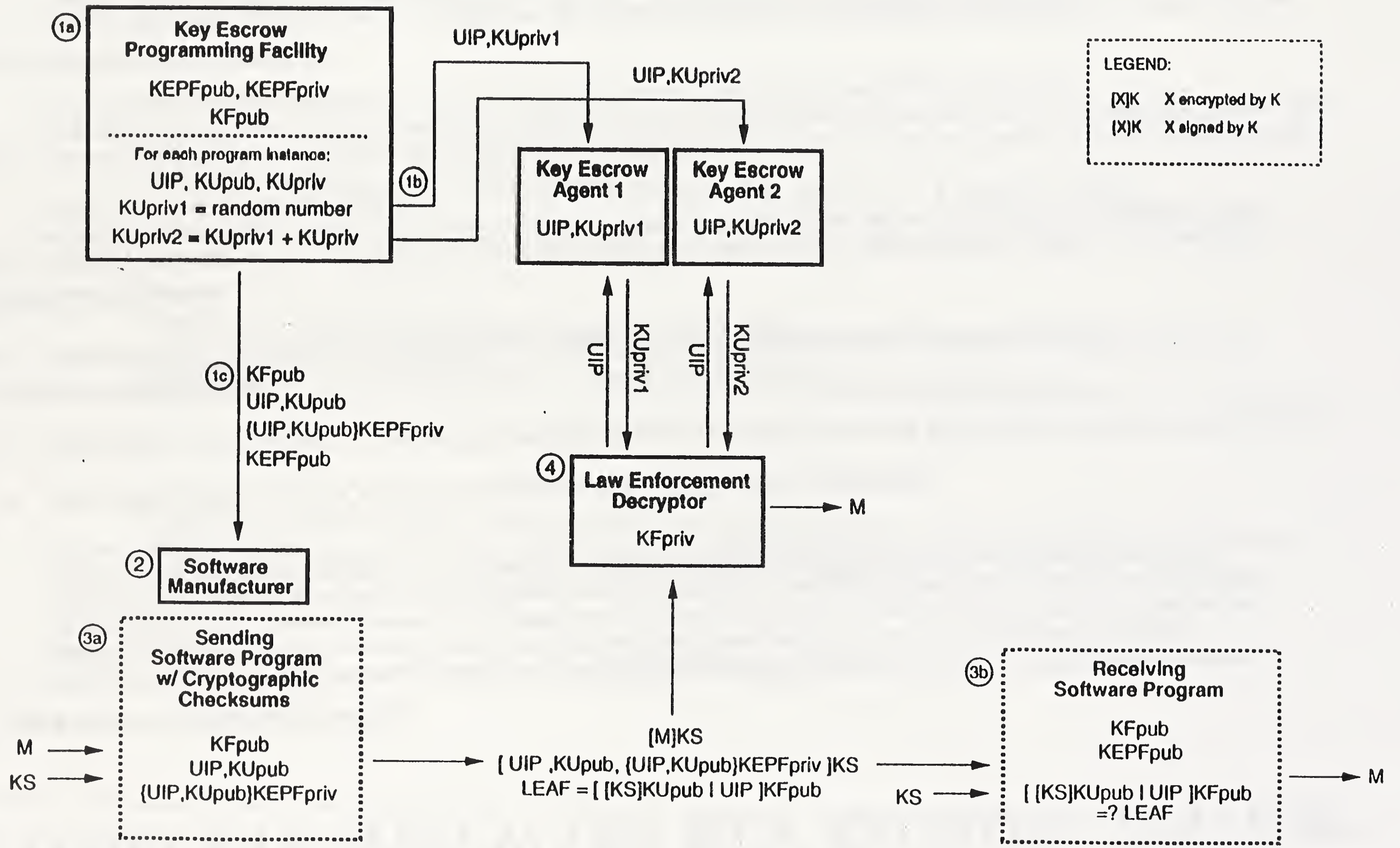
KFpub
KEPFpub

[[KS]KUpub | UIP]KFpub
=? LEAF

M

Trusted Information Systems, Inc., June 10, 1994

COMPLETE SOFTWARE KEY ESCROW SYSTEM



1a

Key Escrow Programming Facility

KEPFpub, KEPFpriv
KFpub

For each program instance:
UIP, KUpub, KUpriv
KUpriv1 = random number
KUpriv2 = KUpriv1 + KUpriv

1b

UIP,KUpriv1

UIP,KUpriv2

Key Escrow Agent 1

UIP,KUpriv1

Key Escrow Agent 2

UIP,KUpriv2

LEGEND:

[X]K	X encrypted by K
{X}K	X signed by K

1c

KFpub
UIP,KUpub
{UIP,KUpub}KEPFpriv
KEPFpub

UIP

KUpriv1

UIP

KUpriv2

4

Law Enforcement Decryptor

KFpriv

→ M

2

Software Manufacturer

3a

Sending Software Program w/ Cryptographic Checksums

KFpub
UIP,KUpub
{UIP,KUpub}KEPFpriv

M →
KS →

[M]KS
[UIP ,KUpub, {UIP,KUpub}KEPFpriv]KS
LEAF = [[KS]KUpub I UIP]KFpub

3b

Receiving Software Program

KFpub
KEPFpub

[[KS]KUpub I UIP]KFpub
=? LEAF

KS →

→ M

COMPLETE SOFTWARE KEY ESCROW SYSTEM

Key Escrow Programming Facility

1a. Receive key escrow programming facility key pair (public key KEPFpub and private key KEPFpriv); receive family public key KFpub (corresponding family private key is embedded in law enforcement decryptor); for each program instance, generate program unique identifier (UIP) and program unique key pair (public key KUpub and private key KUpriv); split program unique private key into components by setting first component KUpriv1 to a random number, and computing the second component KUpriv2 as the difference between KUpriv and KUpriv1.

1b. Send UIP,KUpriv1 and UIP,KUpriv2 to key escrow agents 1 and 2, respectively.

1c. Send KFpub, UIP, KUpub, a copy of UIP and KUpub signed by KEPFpriv, and KEPFpub to software manufacturer.

Software Manufacturer

2. Embed KFpub, UIP, KUpub, and the signed copy of UIP and KUpub into the software programs.

Software Programs

3a. Sending software program encrypts a message M with a session key KS, generates the LEAF, and sends the encrypted message, a copy of UIP and KUpub along with their signature, all encrypted with KS, and the LEAF to the receiving software program.

3b. The receiving software program uses KEPFpub to verify the signed copy of UIP and KUpub, recomputes the LEAF by encrypting KS with KUpub, combining it with UIP and encrypting the result with KFpub, authenticates the received LEAF by comparing it against the recomputed LEAF, and decrypts the message M using KS.

Law Enforcement Decryptor

4. Decrypt the LEAF using KFpriv; send UIP to key escrow agents; receive KUpriv1 and KUpriv2 from key escrow agents; combine KUpriv1 and KUpriv2 to form KUpriv; use KUpriv to decrypt KS; and use KS to decrypt M.

- STRENGTHS (RELATIVE TO TESSERA)
  - Achieves law enforcement goals as well as Tessera does.
  - Software solution less costly and thus much more attractive to computer marketplace -- and to telephone marketplace.
  - Can be used with commodity cryptographic algorithms -- such as DES and RSA -- but not with secret algorithms.

- STRENGTHS

  - Software cryptography (with or without key escrow) may be viewed as weaker than hardware cryptography.

  - But... this key escrow approach can be used with any hardware crypto boards or smartcard/PCMCIA crypto without modification.

B.7 Stephen Walker: A System for Software Integrity

System Requirements for Software Integrity

Trusted Information Systems, Inc.

Stephen T. Walker

June 10, 1994

9406-001.wp

- Background
  - Software Key Escrow CRADA discussions.
  - "A Possible Basis for Software Key Escrow":
    - Hardware vs. software implementations.
    - How much must we trust the user?
    - Controlled Execution DMS case study.

- How much must we trust the user?

  - Hardware is "harder" to corrupt than software.

  - But all hardware is controlled by software, which is corruptible:

    - Super encryption, Blaze checksums.

  - For either hardware or software, some form of software integrity mechanism is needed.

- ARPA Safeguards Project
  - Allow export of high-performance computer workstations to China and Russia for approved applications.
  - Three critical ingredients:
    - Controlled Execution Operating System,
    - Tamper Detection,
    - Audit.

- Controlled Execution Operating System

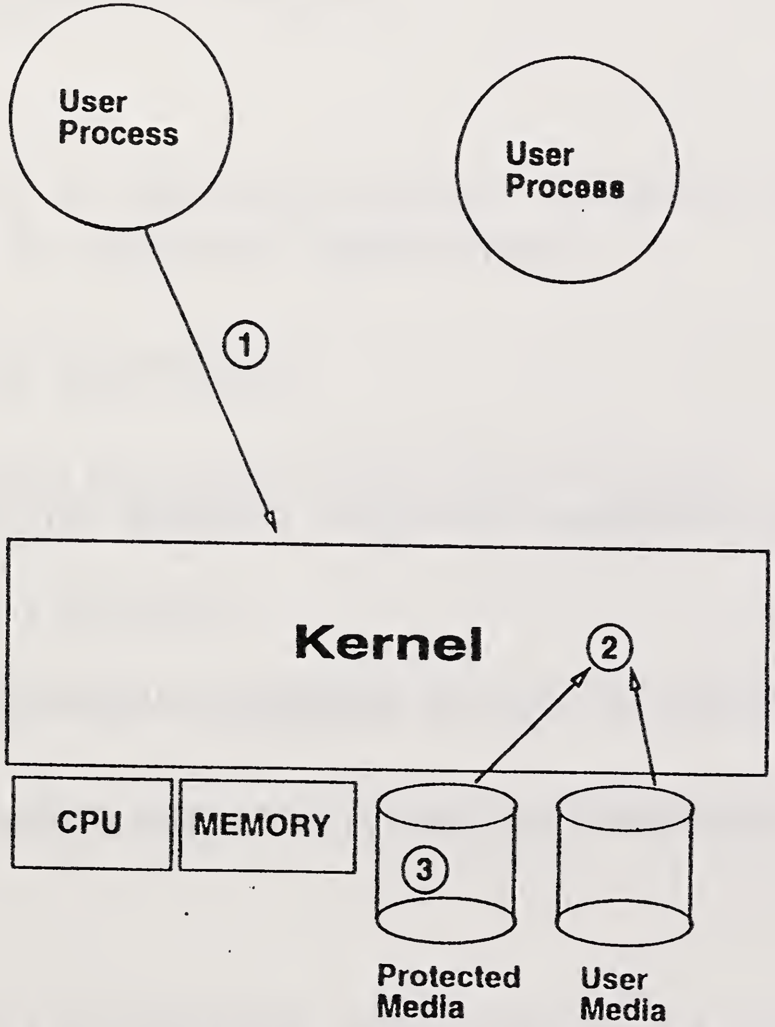
  - All executable software loaded on read-only medium.

  - Operating system modified to execute software only from read-only medium.

  - Provisions for periodic software additions using digitally signed updates.

Safeguards Software System Architecture

Controlled Execution Unix

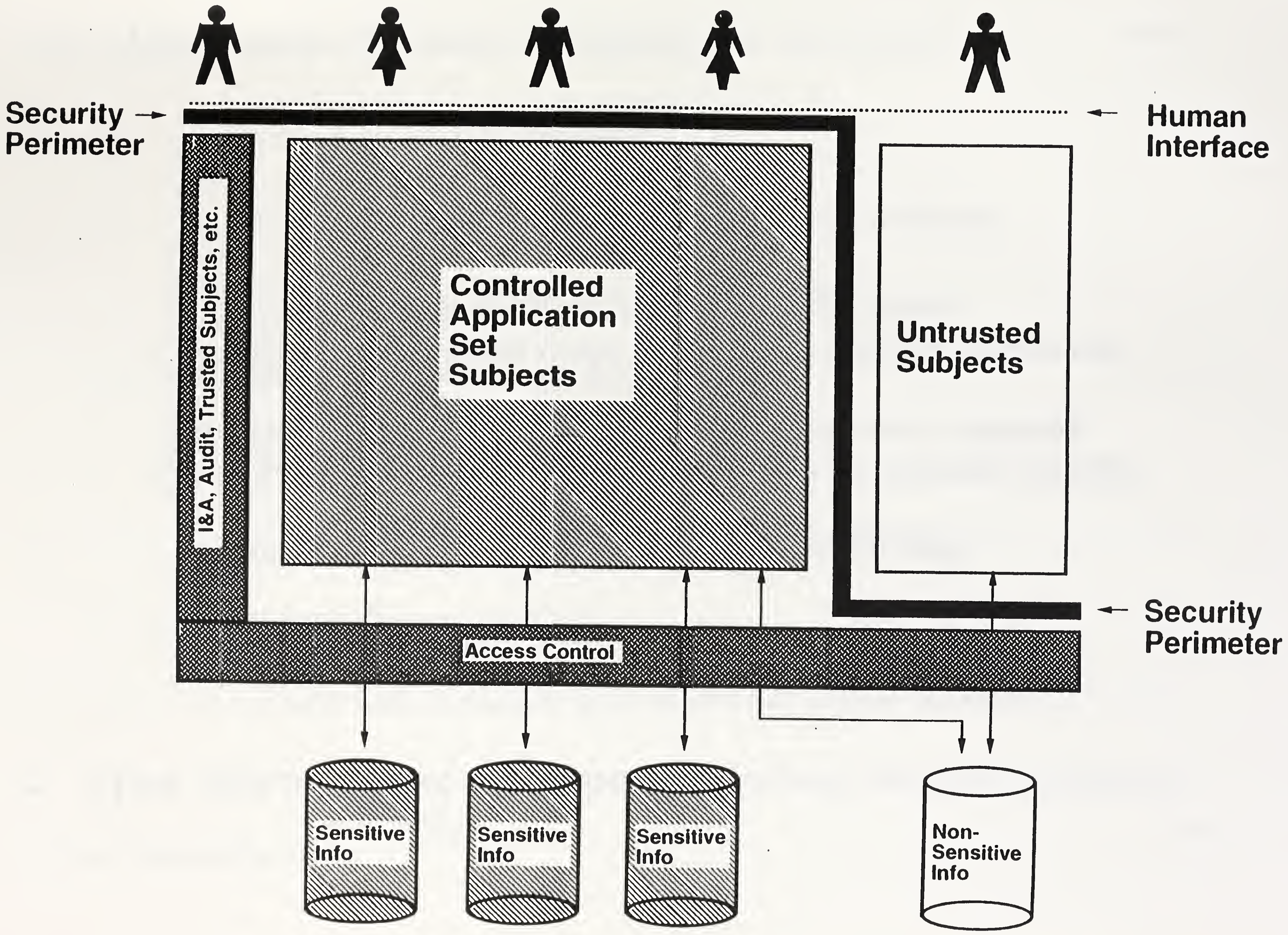


1. User process make a program execution request

2. Kernel determines if requested program resides on Protected Media or on User Media

3. If program resides on Protected Media, execution is permitted

Controlled Application Set (CAS) Architecture and Security Perimeter



- How much can we trust the user?

  - For safeguards: not very much.

    - Need controlled execution, tamper detection, audit.

  - For U.S. Government applications, e.g., Defense Message System: user unlikely to tamper with workstation hardware or software.

    - Controlled execution could be useful for ensuring authorized software execution and protection against viruses.

- How much Software Integrity do we need?
  - Software Key Escrow Proposal:
    - Checksums embedded in shrink-wrapped software.
      - Assumes user won't hack software.
  - Controlled Execution Operating System:
    - Rigid control of executable software.
      - Assumes user won't modify the hardware.
  - Safeguards Protection Suite:
    - Controlled execution plus audit and tamper detection.
      - Assumes user may modify hardware but audit mechanisms will detect.

- To be absolutely certain that hardware or software key escrow will work:
  - Need full safeguard protection.
- To have high confidence (for applications like Defense Message System):
  - May need controlled execution mechanisms.
- To have reasonable confidence (for commercial applications):
  - Checksums in shrink-wrapped software may be enough.