Volume 41 | Issue 1 Article 6

1996

Key Escrow Encryption Policies and Technologies

Dorothy E. Denning

William E. Baugh Jr.

Recent Developments

KEY ESCROW ENCRYPTION POLICIES AND TECHNOLOGIES*

DOROTHY E. DENNING**
WILLIAM E. BAUGH, JR.***

I. INTRODUCTION

IN today's information age, encryption is considered essential to ensure the security of electronic data and transactions. At the same time, however, there is growing recognition that the spread of powerful encryption technology is not entirely beneficial. As encryption proliferates worldwide, it could seriously imperil the ability of law enforcement agencies to counter domestic and international organized crime and terrorism, because terrorists, drug dealers and others can use the technology to facilitate crimes and to operate with impunity. Furthermore, proliferation of encryption could eliminate valuable sources of foreign intelligence which have been vital to national security. Encryption additionally has potential drawbacks within individual businesses. For example, if encryption keys are lost or damaged, valuable data may become inaccessible. Similarly, employees can use encryption to cover up fraud, espionage and other crimes.

In response to these concerns, in April 1993, the Clinton administration announced an initiative to promote encryption in a way that would simultaneously satisfy the competing objectives of security and privacy on one side, and public safety and national security on the other.[1] This was to be accomplished primarily through the adoption of "key escrow" encryption standards and

---

* This Recent Development is available at the *Villanova Law Review* home page at http://vls.law.vill.edu/academic/jd/journals/law-review/Volume_41/. Additionally, an earlier version of this Recent Development, with the footnotes, appeared in *Information Systems Security*, Summer 1996.

** Professor of Computer Science, Georgetown University; B.A., 1967, M.A., 1969, University of Michigan; Ph.D., 1975, Purdue University. Dr. Denning's home page is available at http://www.cosc.georgetown.edu/~denning/.

*** Vice President, Information Technology and Systems Sector, Applications International Corporation, McLean, VA; former Assistant Director, Information Resources Division, Federal Bureau of Investigation; B.A., 1967, Louisiana Polytechnic University; J.D., 1969, Louisiana State University School of Law.

1. White House Press Release, *Statement of the Press Secretary*, Apr. 16, 1993, 1993 WL 357773; *also available at* http://library.whitehouse.gov.

products.[2] Key escrow encryption makes use of special data recovery keys which are held by a trusted fiduciary to enable backup decryption. Use of the backup decryption capability is restricted to users and to government officials who have been authorized to access the encrypted information.

By providing a mechanism for authorized government access, key escrow products would have another advantage: they would be exportable. Currently, United States law defines encryption products as munitions, which cannot be exported without a license.[3] Businesses have objected that export regulations have made it more difficult for them to obtain strong encryption to protect international communications. Similarly, U.S. manufacturers of computer products complain that the regulations put them at a competitive disadvantage in the global marketplace. The Administration's 1993 initiative proposed allowing the export of stronger encryption products which used the proposed key escrow idea.[4] While more recent proposals have modified the original 1993 initiative, permitting the

---

2. *Id.* at 1.

3. *See* 22 U.S.C. § 2778(a) (1994); 22 C.F.R. §§ 120.1, 121.1, 123 (1995). Congress, through the Arms Control Export Act (ACEA), has given the President the authority "to control the import and the export of defense articles and defense services." 22 U.S.C. § 2778(a)(1) (1994). The President designates certain products as "defense articles," which then constitute the U.S. Munitions List. *Id.*; *see* 22 C.F.R. § 121.1 (1995). Cryptographic systems or software "with the capability of maintaining secrecy or confidentiality of information" are included in Category XIII(b) of the U.S. Munitions List. *Id.* Further, the President may "promulgate regulations for the import and export" of items on the Munitions List. 22 U.S.C. § 2778(a)(1) (1994). These regulations are known as the International Traffic in Arms Regulations (ITAR), found at 22 C.F.R. §§ 120-130 (1995). The Munitions List is actually a part of ITAR, found at § 121.1. 22 C.F.R. § 121.1 (1995). To export an item included in the Munitions List, such as cryptographic software, one must obtain an export license from the Office of Defense Trade Controls of the Department of State. *Id.* § 123.1(a).

ITAR and ACEA are currently being challenged in the Northern District of California and the District of Columbia as unconstitutional. *See* Bernstein v. U.S. Dep't of State, C 95-0582 (N.D. Cal., filed Feb. 21, 1995); *see also Try Decoding the Latest in Munitions Wear*, CHI. DAILY L. BULL., Nov. 14, 1995, at 2 (stating that support for Bernstein's constitutional claims "also can be found in the government's own internal legal opinions questioning the regulation's constitutionality"); Jared Sandberg, *Judge Rules Encryption Software Is Speech in Case on Export Curbs*, WALL ST. J., Apr. 18, 1996, at B3 (stating that ruling clears way "for the judge to rule that the government's limitation on the export of encryption is unconstitutional"). *But cf.* Karn v. U.S. Dep't of State, No. 95-1812 (D.D.C. Mar. 22, 1996) (granting defendants' motion to dismiss APA claim as nonjusticiable, and granting defendants' summary judgment motion with respect to constitutional claims against ACEA and ITAR).

4. *See* White House Press Release, *Statement of the Press Secretary*, Feb. 4, 1994, *available at* http://library.whitehouse.gov (announcing "[n]ew procedures to allow export of products" using key escrow encryption).

export of stronger encryption products which use key escrow encryption remains central to the government's reform efforts.

This Recent Development critiques the most recent Clinton administration proposals to include key escrow in U.S. encryption export policy.[5] Part II outlines the major proposed changes to U.S. export policy.[6] Part III offers an overview of different approaches to key escrow.[7] Finally, the Administration's proposal is contrasted in Part IV with international efforts at implementing key escrow.[8]

II. PROPOSED CHANGES TO U.S. ENCRYPTION EXPORT POLICY

As part of the government's early efforts to modify encryption export policy through the use of key escrow technology, the National Security Agency (NSA) developed an initial implementation of escrowed encryption in a microelectronic chip called the *Clipper Chip*.[9] Although *Clipper* offered strong, exportable encryption, it was widely criticized on four accounts: (1) its encryption algorithm ("Skipjack") was classified,[10] (2) it required special hardware, (3) the government held the keys and (4) it did not accommodate user data recovery.

Following the *Clipper* initiative and the criticisms which followed, the government began working with industry personnel to develop a more flexible approach to key escrow that would address the objections raised over *Clipper* and meet the needs of users, industry and the government. In August 1995, the Clinton administration announced a new proposal to allow the general export of

5. Since this article was written, the Administration has issued a new key escrow proposal. For more information, see http://www.cosc.georgetown.edu/~denning/crypto.

6. For a discussion of the Clinton Administration's proposed changes to encryption export policy, see *infra* notes 9-37 and accompanying text.

7. For a discussion of key escrow approaches and products, see *infra* notes 38-46 and accompanying text.

8. For a discussion of international efforts to implement key escrow policies, see *infra* notes 47-58 and accompanying text.

9. *See* White House Press Release, *supra* note 1, at 1. *Clipper* is a "state-of-the-art microcircuit" which "scrambles telephone communications using an encryption algorithm." *Id.* For further description of the *Clipper Chip* and its key escrow system, see Dorothy E. Denning & Miles Smid, *Key Escrowing Today*, 32 IEEE COMM. 58 (1994), also available at http://www.cosc.georgetown.edu/~denning/crypto. *Clipper* advanced beyond the theoretical stage before it was eventually scuttled; for example, AT&T integrated the chip into a telephone security device to provide secure voice communications.

10. Because the algorithm is classified and not open to public review, outside experts were invited to examine the algorithm and to report their findings to the public. No weaknesses were found. *See* Earnest F. Brickell et al., *Interim Report: The SKIPJACK Algorithm*, SKIPJACK REV., July 28, 1993, *available at* http://www.cosc.georgetown.edu/~denning/crypto.

software encryption products with unclassified algorithms of up to 64-bit keys, provided that the products were combined with an acceptable key escrow mechanism.[11] Keys would be held by government-approved trusted parties within the private sector (not by the government as with *Clipper*), where they could support user data recovery in addition to authorized government decryption.[12] The proposal, which is still undergoing refinement as of March 1996, is already being used as a basis for granting general export licenses for key escrow products.

The first part of the Administration's proposal would allow the general export of encryption products using up to 64-bit keys. Under current U.S. export policy, software encryption products with keys longer than 40 bits are exportable only by obtaining a license from the Department of State.[13] Additionally, any vendor wishing to export such a product must apply for a separate license for each customer or obtain a special distribution arrangement.[14] By comparison, products with key lengths not exceeding 40 bits may be readily exported under general licenses administered by the Department of Commerce.[15] Consequently, many products devel-

11. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T OF COMMERCE, NIST 95-24, COMMERCE'S NIST ANNOUNCES PROCESS FOR DIALOGUE ON KEY ESCROW ISSUES (Aug. 17, 1995), *available at* gopher://gopher.nist.gov.79/0/.docs/.releases/n95-24.rel. As part of the proposal, the Administration also announced plans to develop a FIPS (Federal Information Processing Standard) for key escrow encryption implemented in software. *Id.* The standard would be used by federal agencies and other interested organizations in conjunction with FIPS-approved encryption techniques.

12. *Id.*

13. The ITAR Regulatory structure, discussed *supra* note 3, does not specifically differentiate between encryption software using more or less than 40-bit keys. However, after the Software Publisher's Association (SPA) urged the government to stream-line the export licensing process, the National Security Agency (NSA) agreed to expedite mass-market software for export if such software uses keys not longer than 40-bits. *See* U.S. DEP'T OF COMMERCE & NATIONAL SECURITY AGENCY, A STUDY OF THE INTERNATIONAL MARKET FOR COMPUTER SOFTWARE WITH ENCRYPTION (Redacted Copy of Original Secret Document) II-4 (1995) (on file with author). The 40-bit rule is sometimes referred to as the "SPA Agreement." *See* Ira S. Rubinstein, *Export Controls on Encryption Software, in* INTERNATIONAL CRYPTOGRAPHIC INSTITUTE 1995: GLOBAL CHALLENGES 11-12 (1995). Software using keys longer than 40-bits do not fall within this agreement, and the Department of State would retain jurisdiction. *See* 22 C.F.R. § 120.1(a) (1995).

14. *See generally* 22 C.F.R. § 123.1 (1995).

15. U.S. DEP'T OF COMMERCE & NATIONAL SECURITY AGENCY, *supra* note 13, at II-5 (stating that SPA Agreement "ensures transfer of licensing jurisdiction [of encryption software using up to 40-bit keys], after a one-time review by NSA, to the Department of Commerce, where the products are freely exportable"). After an initial review by the Department of State, the product may be granted a *commodity jurisdiction* transfer to the Department of Commerce. *Id.* There, it can be exported to most places without the need to obtain a license for each sale. For a

oped by U.S. companies for the international market use 40-bit keys.

The longer the key, the harder it is to break the code. Although 40-bit keys provide adequate protection for most applications, they are not foolproof. For example, in the summer of 1995, a French student cracked one in eight days, using 120 workstations and a few supercomputers.[16] The key gave him access to a dummy purchase order that had been encrypted with the overseas version of a popular program for browsing the World Wide Web.[17] Even though a substantial investment of resources was required just to crack a single message, many potential users regard the incident as an indication that 40-bit keys are unacceptably small.

As a result, some U.S. companies complain that they have lost sales to foreign competitors who were able to provide stronger encryption, including the Data Encryption Standard (DES),[18] which uses 56-bit keys. They cite the worldwide availability of products using DES and other encryption algorithms as evidence that export controls limit U.S. companies' competitiveness in the global market. As of December 1995, Trusted Information Systems of Glenwood, Maryland, had identified 497 encryption products from twenty-eight countries, 193 of which used DES.[19] In some cases, software vendors have been forced to build separate product lines for domestic and foreign sales in order to meet the demands of U.S. customers for DES or better encryption.

Some critics contend that the proposed increase from 40 bits to 64 bits is minimal, and that U.S. export policy should allow even greater key lengths. However, each additional bit doubles the number of possible keys and thus the effort required to crack a key. The proposed additional 24 bits, therefore, gives about seventeen million times better security. It would have taken the French student 136 million days—or about two billion computers in eight days—to crack a single 64-bit key. At the current rate of technological advancement, it will be several decades before the French stu-

---

detailed treatment of export controls as they apply to encryption software, see Rubinstein, *supra* note 13.

16. *See* Jared Sandberg, *French Hacker Cracks Netscape Code, Shrugging Off U.S. Encryption Scheme*, WALL ST. J., Aug. 17, 1995, at B3.

17. *Id.* The software was Netscape's "browser" program. *Id.*

18. For a general discussion of DES, see National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication (FIPS PUB) 46-1, Apr. 1977.

19. David M. Balenson, *Worldwide Survey of Cryptographic Products*, Presented at the International Cryptography Institute, Dec., 1995, *available at* http://www.tis.com/crypto/crypto-survey.html.

dent could break a 64-bit key in eight days with updated computers. 64 bits is therefore likely to provide a reasonably high level of security for at least the next twenty years.[20] Further, if a company sends out numerous messages per day, each encrypted with a different key, the task of an adversary to break all keys with the hope of finding some message worth reading becomes increasingly impractical.

For the near term, DES combined with key escrow can provide strong security while being implementable in exportable software products. Despite its age,[21] DES still offers robust encryption and may have a decade or more of useful life remaining. For the longer term, DES can be replaced with a readily exportable 64-bit algorithm.

As a balance against the increased acceptable key length, the Administration's proposal requires encryption products to provide acceptable key escrow mechanisms. Draft criteria for export of software key escrow encryption were issued in September 1995, and then refined and re-issued in November for comment.[22] Meetings were held at the National Institute of Standards and Technology (NIST) in September and December to discuss the criteria and to solicit comments from industry.

The proposed export criteria are intended to ensure that the government can, when lawfully authorized, readily access keys and decrypt intercepted communications and stored information in a timely manner. Accordingly, products must include information in the encrypted data that identifies the escrow agent(s) and the particular keys needed for decryption.[23] Further, keys must be held by escrow agents certified by the U.S. government or by foreign governments with which the U.S. government has formal agreements.[24] The conditions under which companies could hold their own keys has not yet been determined.

Under the criteria, compliant products must allow access to encrypted communications from both ends of the channel.[25] This al-

20. Not everyone agrees that 64 bits provides adequate encryption. A report by an ad hoc group of cryptographers and computer scientists recommends that keys be 75-90 bits long. Matt Blaze, et al., *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security* (January 1996), *available at* http://www.bsa.org/bsa/cryptologists.html.

21. DES is now about 20 years old. *See Encryption: Secret Plans*, ECONOMIST, May 6, 1995, at 80.

22. Draft Software Key Escrow Encryption Export Criteria (11/95 version), *available at* http://csrc.ncsl.nist.gov/keyescrow.

23. *Id.* at criteria 4.

24. *Id.* at criteria 3.

25. *Id.* at criteria 5 ("The product's key escrow feature shall allow access to the

lows communications sent both to and from a subject of investigation to be decrypted using only the subject's keys. Compliant products must also allow for the decryption of multiple messages during a period of authorized access without requiring repeated presentations of the access authorization to the escrow agent(s).[26]

Additionally, products must be designed to resist alterations that would circumvent or disable the key escrow mechanism.[27] The escrowed encryption functions must interoperate only with escrowed functions in other products and must not interoperate with products whose key escrow features have been altered or disabled. Exportable products will be allowed to use keys up to 64 bits long, but they must not provide multiple encryption modes that effectively increase the key length.[28] For example, the criteria will allow the use of DES, but not triple-DES, which uses two keys (112 bits) or three keys (168 bits).

The draft criteria for escrow agents, released at the December 1995, NIST meeting, address the requirements for escrow system integrity and security and for key access.[29] Escrow agents will be required to ensure the confidentiality, integrity and availability of key escrow information and the confidentiality of requests for that information.[30] Further, they will need to ensure due form of all requests and respond to such requests in a timely fashion.[31] Finally, they will need to maintain audit records of all events relating to the management and release of keys.[32]

To obtain a license under the new proposal, a vendor with a candidate product would submit the product to the Department of State for review. If the product is found to meet the criteria for export, it would be granted a *commodity jurisdiction*[33] transfer. It would then be exportable under a general license administered by the Department of Commerce.

---

key(s) needed to decrypt the product's ciphertext regardless of whether the product generated or received the ciphertext.").

26. *Id.* at criteria 6.

27. *Id.* at criteria 9 ("The product's . . . functions . . . shall not interoperate with the cryptographic functions of a product whose key escrow encryption function has been altered, bypassed, disabled, or otherwise rendered inoperative.").

28. *Id.* at criteria 8.

29. Key Escrow Agent Criteria, draft, Dec. 1, 1995, *available at* http://csrc.ncsl.nist.gov/keyescrow.

30. *Id.*

31. *Id.* at criteria 2.

32. *Id.* at criteria 9.

33. *See* 22 C.F.R. § 120.4 (1995).

Reaction to the government's proposal has been mixed. Trusted Information Systems (TIS) and TECSEC, Inc., submitted products for review and are likely to be joined by other companies; TIS has received approval for their *Gauntlet* firewall. Some major corporations which are adopting corporate key escrow policies to protect their own interests have stated that the government's proposal might meet their goals if they can hold their own keys. The Software Publisher's Association[34] and the Business Software Alliance[35] both issued statements calling for the liberalization of export controls independent of whether key escrow is used. A coalition of nearly forty public-interest groups, trade associations and representatives for industry led by the Center for Democracy and Technology (CDT) sent a letter to Vice President Gore in November 1995 saying that the proposal did not address the need for immediate liberalization of export restrictions and that it was no substitute for a comprehensive national cryptography policy.[36] The CDT-led coalition pledged to develop an alternative proposal within six months.

Despite these criticisms, we believe the proposal is a major step forward. It would allow a vendor to develop a single product line for both domestic and international sales, using software or hardware implementations of the 56-bit DES or an even stronger 64-bit algorithm. This step should facilitate the seamless integration of strong encryption into network and applications software, thereby making it cheaper and easier for businesses to encrypt their electronic transactions and proprietary data. Furthermore, this step will facilitate electronic commerce. If strong algorithms are implemented in both domestic and international products, businesses will be able to communicate securely with customers, suppliers, partners, investors and subsidiaries throughout the world.

Some vendors and users may not accept the 64-bit limit on keys. One company has stated that the proposal would not alleviate its need to continue manufacturing two product lines, because it uses 128-bit keys in its domestic products.[37] Some critics of the

34. SOFTWARE PUBLISHER'S ASSOCIATION, COMMENTS OF THE SOFTWARE PUBLISHER'S ASSOCIATION ON 11/95 DRAFT EXPORT CRITERIA FOR KEY ESCROW ENCRYPTION, Presented at the National Institute of Standard and Technology (NIST) (Dec. 5, 1995).

35. Robert W. Holleyman II, President, Business Software Alliance, *Encryption Export Policy and the U.S. Software Industry: Chipping Away at America's International Competitiveness*, Testimony at NIST (Dec. 5, 1995), *available at* http://www.bsa.org/.

36. A copy of the letter is available at http://www.cdt.org/.

37. NETSCAPE POLICY ON ENCRYPTION EXPORT (distributed at meeting at NIST, Dec. 5, 1995), *available at* http://www.netscape.com/newsref/ref/encryption_export.html.

limit argue that because access is possible through the key escrow system, there is no reason to restrict key size at all. The government's response has been to note that given the limited experience with key escrow, the strength afforded by 64-bit keys might pose significant national security risks. After key escrow systems have been more widely deployed and found effective, perhaps longer key lengths will be permitted. However, we believe that 64-bit keys are more than adequate for virtually all business transactions. The increased key length, combined with the key escrow concept, properly balance the competing interests of the government and the business community.

III. KEY ESCROW APPROACHES AND PRODUCTS

While there is no single approach to escrowed encryption, all methods follow a few general principles.[38] The data recovery key used with a particular encryption product is generated by or given to a trusted party sometime before the product is used. For example, it might be generated and escrowed while the product is being manufactured or when the product is initialized and registered with an escrow agent. The key could be unique to an individual product or user, or it could be shared by many users. Additionally, it could be held by a single escrow agent, or it could be split into several components, with each component held by a separate entity.

Whenever the product encrypts a document (or message stream), the product attaches to the encrypted document sufficient information to allow backup decryption. For example, the data encryption key might be encrypted under the data recovery key and placed in a document header. If the encryption key is later lost, then the user or an officer in the user's organization would give that information to the escrow agent and request assistance. After determining that the request is authentic, the escrow agent either would release the data recovery key (if it is unique to the user) or else use the key to determine and release the data encryption key. If an investigative or intelligence agency needs access to the key during the course of an authorized search or communications intercept, the agency would present certification of the legal author-

38. For a description of the characteristics of key escrow encryption systems and different proposals, see Dorothy E. Denning & Dennis K. Branstad, *A Taxonomy of Key Escrow Encryption*, 39 COMM. OF THE ACM, No. 3, Mar. 1996, at 34-40. The taxonomy, plus detailed descriptions of 30 systems, including all those mentioned in this article, can be found through http://www.cosc.georgetown.edu/~denning/crypto. *See also* Dorothy E. Denning, *Key Escrow Encryption: The Third Paradigm*, COMPUTER SECURITY J., Summer, 1995.

ity to access that information (normally a court order) to the escrow agents. Legitimate privacy interests can be protected through access procedures, auditing and other technical, legal and operational safeguards.[39]

The *Clipper Chip* represents one approach, implementing the Escrowed Encryption Standard (EES), a voluntary government standard for encrypting sensitive but unclassified low-speed telephone communications, including voice, fax and data.[40] Each chip has a unique data recovery key, which is split between two government escrow agents: the National Institute of Standards and Technology (NIST) and the Department of Treasury Automated Systems Division. Data are encrypted with the classified *Skipjack* algorithm, which uses powerful 80-bit keys. Products that implement the EES must use tamper-resistant hardware in order to protect the classified algorithms. They are generally exportable.

The *Clipper Chip* is a scaled back version of a more advanced chip, called *Capstone*, which the NSA developed for use in the *Fortezza* card (a PCMCIA[41] card). The goal was a small, affordable and extremely secure hardware token that would provide a full suite of cryptographic services for confidentiality protection, authentication and digital signatures.

Capstone implements the EES plus public-key cryptographic algorithms for the Digital Signature Standard and for generating and establishing session keys. A *Fortezza* PCMCIA modem card is also available so that encryption and decryption can be performed either as part of the transmission protocols or as independent service calls, for example to encrypt or decrypt files and electronic mail messages. The government plans to extend the scope of the EES to cover high speed communications over computer networks so the *Fortezza* and other *Capstone*-based devices will meet approved standards for use by federal agencies.

Clipper's key escrow system supports backup decryption by authorized government agencies, but does not help users with lost or damaged keys. *Fortezza*, on the other hand, was designed also to allow user data recovery. This is accomplished through the certifi-

39. With some approaches, key escrow is a service provided by the trusted parties that manage the public-key infrastructure and issue public-key certificates. Issuance of a public-key certificate may be conditioned on the user escrowing the corresponding private key with the certificate authority.

40. National Institute for Standards and Technology, *Escrowed Encryption Standard (EES)*, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS PUB) 185 (1994). *See also* Denning & Smid, *supra* note 9.

41. Personal Computer Memory Card International Association.

cate authorities which grant certificates for the public keys used for key establishment and digital signatures. Those same authorities escrow the user's corresponding private keys, which are stored on the *Fortezza* card; the keys can be recovered from the certificate authority in case the card is lost or the keys become corrupted.[42]

Some type of key escrow is a feature or option of several commercial products including Fisher Watchdog, Nortel's Entrust, PC Security's Stoplock KE, RSA Secure and TECSEC Veil. With all of these products, escrowing can be done within the user's organization. In some cases, it is integrated into the company's key management infrastructure. Bankers Trust has developed a commercial key escrow system, called *Secure KEES*, that uses third party escrow agents.[43] Keys, which are stored on hardware cryptographic tokens, can be split between multiple agents. TIS has developed a commercial key escrow system which could be used with either hardware or software encryption products.[44] National Semiconductor has proposed to implement the TIS system using their PersonaCard (a PCMCIA cryptographic card) with the goal of producing an exportable product with strong security and data recovery capability.[45] Other proposals have come from researchers at AT&T, Bell Atlantic, Cylink, Fortress U&T, Karlsruhe University, Massachusetts Institute of Technology, Royal Holloway and the University of Wisconsin. All of these products and proposals are covered by a taxonomy of escrowed encryption.[46]

The cost of key escrow is difficult to estimate, especially given the wide range of approaches. One approach, used by *Fortezza* and *Entrust* and adopted by several of the proposals, includes escrow with the services provided by public-key certificate authorities. Another, used by *Stoplock* and *Veil*, integrates escrow into the overall

42. Although *Fortezza* was developed as part of the NSA's Multilevel Systems Security Initiative (MISSI), the technology is available commercially. Support for *Fortezza* has already been added to AT&T's SecureAgent, Netscape's Navigator, Oracle's Secure Network Services and other products.

43. Bankers Trust Electronic Commerce, *Private Key Escrow System*, Presentation at the SPA/AEA Cryptography Policy Workshop, Aug. 17, 1995, and at the International Cryptography Institute, 1995: Global Challenges, Sept. 21-22, 1995 (on file with author); *see also* Secure KEES product literature distributed at NIST (Dec. 5, 1995).

44. Stephen T. Walker et al., *Commercial Key Recovery*, 39 COMM. OF THE ACM, no. 3, Mar. 1996, at 41-47.

45. William B. Sweet & Stephen T. Walker, *Commercial Automated Key Escrow (CAKE): An Exportable Strong Encryption Proposal*, National Semiconductor; *i*Power Business Unit, Sunnyvale, CA, June 21, 1995.

46. *See* Denning & Branstad, *supra* note 38.

key management infrastructure. With both of these approaches, the incremental cost of escrow may be relatively low.

Although the government's export proposal discussed above explicitly addresses software encryption, hardware products may also be considered for export. The advantage of hardware is that it generally offers greater security than software. In addition, it can better protect against tampering which would disable or circumvent the key escrow mechanism. For this reason, hardware products with key escrow might be approved for export with even longer keys. *Clipper* and *Fortezza*, for example, use 80-bit keys with *Skipjack*. Software has the advantage of being cheaper, but with mass production, the cost of hardware need not be prohibitive, especially if the encryption is combined with authentication mechanisms on a single token that can be used for access control and other security purposes (e.g., as with *Fortezza*).

We see a strong market for escrowed encryption products. In recognition of the threats posed by uncontrolled cryptography, some companies have already adopted internal security policies requiring key escrow. For example, at the International Cryptography Institute in September 1995, Nick Mansfield of Shell International reported that key escrow is used in Shell Group enterprises. Keys are escrowed by a trusted Shell service company on behalf of the shareholders and businesses, and this provides the shareholders with an independent ability to decrypt information should the need arise.

IV. INTERNATIONAL EFFORTS

Several products and proposals for key escrow have come from outside the United States. Governments and businesses worldwide are beginning to recognize the potential of key escrow for achieving information security without denying legitimate government access. In addition to providing confidentiality and emergency backup decryption, escrowed encryption is seen as a way of overcoming export restrictions, common to many countries, which have limited the international availability of strong encryption in order to protect national security interests. With key escrow, strong exportable cryptography can be standardized and made available internationally to support the information security needs of international business.

At a meeting sponsored by the Organization for Economic Cooperation and Development (OECD) and the International Chamber of Commerce (ICC) in December 1995, in Paris, repre-

sentatives from the international business community and member governments agreed to work together to develop encryption policy guidelines based on agreed upon principles that accommodate their mutual interests. The INFOSEC Business Advisor Group (IBAG), an association of associations representing the information security interests of users, issued a statement of seventeen principles that they believe can form the basis of a detailed agreement.[47]

These principles acknowledge the right of businesses and individuals to protect their information[48] and the right of law-abiding governments to intercept and to lawfully seize information when there is no practical alternative.[49] Businesses and individuals would lodge keys with trusted parties[50] who would be liable for any loss or damage resulting from compromise or misuse of those keys.[51] The trusted parties could be independently accredited entities or accredited entities within a company.[52] The keys would be available to businesses and individuals on proof of ownership[53] and to governments and law enforcement agencies under due process of law. Additionally, they would be available for a limited time frame.[54] The process of obtaining and using keys would be auditable, and governments would be responsible for ensuring that international agreements would allow access to keys held outside national jurisdiction.[55]

Further, the principles call for industry to develop voluntary, uniform and international standards, and for governments, businesses and individuals to work together to define the requirements for those standards.[56] The standards would allow choices about algorithm, mode of operation, key length and implementation in

47. INFOSEC Business Advisory Group (IBAG) statement, *available through* http://www.cosc.georgetown.edu/~denning/crypto/IBAG.txt.

48. *Id.* at principles 1-5.

49. *Id.* at principle 6 ("[L]aw-abiding governments have the right, in the prevention, investigation and prosecution of serious crime, lawfully to intercept and lawfully to seize information for evidential purposes only, where there is no practical alternative.").

50. *Id.* at principle 7.

51. *Id.* at principle 11 ("Where Trusted Third Party agents hold keys on behalf of businesses and individuals, they must accept liability for any direct or consequential loss or damage resulting from misuse or unauthorised [sic] disclosure of those keys.").

52. *Id.* at principle 7.

53. *Id.* at principle 8.

54. *Id.* at principle 10 ("Where Governments and Law Enforcement Agencies do obtain keys under such processes, they must only be available for a specified, limited timeframe.").

55. *Id.* at principle 9.

56. *Id.* at principles 12 & 13.

hardware or software. Products conforming to the standards would not be subject to restrictions on import or use and would be generally exportable.[57]

EUROBIT (European Association of Manufacturers of Business Machines and Information Technology Industry), ITAC (Information Technology Industry Association of Canada), ITI (Information Technology Industry Council, U.S.) and JEIDA (Japan Electronic Industry Development Association) also issued a statement of principles for global cryptography policy at the OECD meeting.[58] The quadripartite group accounts for more than ninety percent of the worldwide revenue in information technology. Acknowledging the needs of both users and governments, their principles call for harmonization of national cryptography policies and industry-led international standards.

Products conforming to the U.S. government's software key escrow export proposal would offer one set of options consistent with the principles identified by the international business community. Thus, it seems likely that if international standards are adopted, then U.S. vendors will be able to develop products that simultaneously conform to the international standards and to the export criteria.

V. SUMMARY

Key escrow offers a valuable service to individuals, organizations and society. By incorporating key escrow into its encryption export policy, the government would safely be able to grant export licenses for products using up to 64-bit keys without compromising national security. Key escrow benefits law enforcement and protects businesses from a host of problems—from misplaced keys to espionage. Further, the U.S. proposal is in line with various initiatives on the part of governments and industry worldwide which are leading toward policies and standards for key escrow.

Because the government's proposed key escrow program is voluntary, there is no guarantee that criminals will choose it over unescrowed encryption. Nevertheless, the program satisfies an important objective: terrorists and other criminals will be unable to take government-sponsored codes and turn them against the government and society. Further, it is hoped that government purchasing power combined with export controls will have some

57. *Id.* at principle 17.

58. EUROBIT-ITAC-ITI-JEIDA Statement, *available at* http://www.cosc.georgetown.edu/~denning/crypto.

positive influence on both the domestic and international market. Finally, responsible corporate participation will ensure that entirely inaccessible networks are not created, to the detriment of both government and industry.