The Legal Report

U.S. Advisory Panel Meets on Key Management Infrastructure

Richard L. Field
Contributing Editor, JIBC Legal
field@pipeline.com

Richard Field is an attorney and legal consultant in Cliffside Park, New Jersey, U.S.A. He chairs the Electronic Commerce Payment Committee of the American Bar Association.

In this month's Legal Report I reprint an excellent and insightful meeting report by John A. Thomas, first posted on 9 Dec 1996 to the cyberia-l list. The meeting was the first of the Technical Advisory Committee to develop a U.S. Federal Information Processing Standard for a federal key management infrastructure. The meeting report hints at the growing rift between the positions of U.S. government and industry in defining the appropriate limits of an encryption key recovery system for storage and/or communication of messages.

The meeting came three days after a notable letter was sent by the Business Software Alliance to U.S. Vice President Al Gore, criticising the U.S. government's new encryption export policy. The Alliance, a leading software industry group whose members include IBM, Microsoft, Apple Computer, Novell, and Adobe, backed away from its initial support of the Clinton administration's policy. It claimed that the government backtracked between its 1 Oct 1996 announcement of the new policy and its 15 Nov 1996 Executive Order implementing further details of the policy. More fundamentally, the Alliance no longer supports key escrow or key recovery systems for encrypted real-time communications, but only for stored communications and data. As you would assume, this is a major problem for law enforcement.

President Clinton's new policy shifts administration of cryptography exports from the U.S. State Department, under its International Traffic in Arms Regulations and Munitions List, to the Department of Commerce, under its Export Administration Regulations. Normally, such a move would signal an easing of export restrictions. However, the Executive Order imposed a number of strict new conditions on the Department of Commerce, including a requirement that the exporter will work to institute satisfactory key recovery techniques as a condition to obtaining export approval.

Under ordinary circumstances (as set out in the U.S. Constitution), these types of changes would require the approval of the U.S. Congress. Congress, however, permitted the Export Administration Act to expire in 1994, and since then the President has unilaterally extended enforcement of the Act's provisions on an emergency basis, under authority granted by Congress to the President under the International Emergency Economic Powers Act.

We have not yet heard the last word on U.S. cryptography export policy. The U.S. Congress has shown signs of rebellion against the President's recent unilateral actions, and will likely begin serious debate in early 1997. And a draft report by the President's own top advisors, entitled "A Framework for Global Economic Commerce", reportedly advocates a free market approach that conflicts with existing Administration cryptography policies.

Further documents from the FIPS Advisory Panel meeting are available at .

- Richard L. Field, field@pipeline.com

11 December 1996

FIPS key recovery meeting (long)

John Taber and I attended the first meeting of the technical advisory committee to develop a Federal Information Processing Standard (FIP) for the federal "key management infrastructure." The meeting was held December 5 and 6, 1996 near the Dallas/Fort Worth Airport. Although the official documents referred only to "key recovery" instead of "key escrow", representatives used both terms interchangeably.

The committee is an advisory body to the Dept. of Commerce. Its recommendations pass through the National Institute of Technical Standards (NIST). The charter states membership will be no more than 24, so the ten "federal liaisons" present are apparently not considered members of the committee. The chairman is Stephen Kent, chief scientist for information security at BBN Systems.

The other members of the committee were employees of various computer and computer-security firms, including Sun Microsystems, Microsoft, Intel, Lucent Technologies, Cisco Systems, Digital Equipment, IBM and Motorola. Some security related firms were Trusted Systems, GlobalKey, and CygnaCom. Officials from Chase Manhattan Bank and Visa were also present. The only academic member was Dorothy Denning of Georgetown University.

The government liaisons included Michael Gilmore of the FBI, Jan Manning of NSA, and representatives of NIST, the Federal Reserve Bank, and the Defense Information Systems Agency. Some representatives were from agencies having no apparent need for cryptography, and therefore key recovery, such as the Small Business Administration and the Social Security Administration. Kent later questioned why the SBA would need key recovery when it had no need to store encrypted data. SSA needs encryption only when it receives confidential information over insecure systems.

Mary Good of the Commerce Department opened the meeting with a speech charging the committee to develop a federal key-recovery standard that can be extended to "public policy". Good urged the committee to confine itself to technical issues only, and arrive at a standard that could be implemented and would not be merely theoretical. Good also asked for "transparency" in key recovery, and a couple of the government liaisons mentioned this as well. Kent's opening remarks included the comment that the FIPS would only deal with crypto key recovery, not recovery of digital signatures, or with public key certification.

Most of the rest of the first day was taken up with introductions and comments by the members and liaisons. The general tenor of comments from corporate representatives was that key recovery had not been important to their customers, and while they did not oppose a key recovery standard for the government, they did oppose any effort to make it mandatory or make it a requirement for export. Some differed on whether an export requirement would be a problem.

Some typical comments follow. GlobalKey (which runs a private encrypted mail system) said using key escrow would be against is policy, and its customers would not accept it. Oracle stated it had had no requirement for key escrow from customers and saw no need for key escrow from its customers. It supported software-only solutions, and emphasized they must have no classified content. Motorola stated it was important not to impact the performance of wireless systems. Motorola advocated an open system supporting multiple algorithms and opposed the trusted third-party concept. Microsoft said it was pragmatic, willing to provide key recovery if customers want it, but it definitely does not want it mandated, nor tied in with export licensing. The Digicom member assumed the committee was not concerned with individual privacy rights vis-a-vis the corporate employer's power to recover an employee's encrypted message.

Jan Manning of NSA and Patricia Edfors of Treasury said the government had a corporate interest in key recovery like any other business, as well as for national security or law enforcement purposes. Manning agreed there was no place in the FIPS for concern over individual privacy rights and urged the committee to avoid privacy issues.

Kent said another issue the committee would face was the timeliness of any response required to a key-recovery request. Gilmore of FBI says the FBI's need for timeliness would vary, depending on the investigation. Denning said that data other than law-enforcement related messages could need timely recovery, citing encrypted medical data, or

encrypted data from some kind of sensor. Another parameter for timeliness would be the number of requests made in a given time.

Although the issue was not explicitly debated, the commercial members seemed to feel that key recovery should be directed to stored data, while the government representatives were clearly using the term to cover both stored data and communications. Someone asked how session keys in a communication system were archived, and Denning remarked she didn't know of any system which archived session keys. The following morning, Kent said the issues included key recovery for storage, key recovery for communications, and key recovery for staged delivery (email). This seemed to remove the doubts some members had about the scope of the proposal. We were left wondering how key archiving could possibly work in communications networks. Consider a system where encrypted packets arrive in any order, with different keys and different key expirations.

After a commenter asked for clarification of who the users of the new standard were assumed to be, Kent stated: "The government wants the FIPS so that industry will produce products that government can use, and others will use as well." When another commenter pointed out that a user could defeat a key-recovery system with superencryption or other means, Kent said "...we have to be willing to let [that case] slip through the cracks."

Some participants attempted to distinguish between key backup and key recovery, the latter being the case where the parties to the communication are themselves unwilling to give up keys. Denning responded that "key recovery _is_ backup." The distinction seems to be about who is a party to the communication--the corporation whose employee has lost his keys, or the employee himself. Confusion on this point may exist because the members didn't distinguish the case where an entity using key recovery doesn't care about it in particular cases, but another entity, government, very well might.

Kent asked if the new standard should require a data recovery field in encrypted messages or files, and if so, should there be check for integrity of this field. Requiring a recipient to check this would encourage senders to use the standard. Someone asked how a recipient could check if a sender were, in fact, escrowing data, even if the field were present. Others said requiring a data-recovery field would make compatibility difficult for older systems, or "...those choosing not to use key recovery." Some expressed concern for the impact on system performance of sending extra bits. Miles Smid of NIST once referred to the data-recovery field as a "LEAF," invoking some laughter from those recalling Clipper's "law-enforcement access field."

Following a question on interoperability with systems not using the standard, Manning of NSA said the new export law required products to interoperate only with products using key recovery. This brought some irritated responses from the commercial members. One asked if the government had some bottom line the committee would have to accept if there were to be a FIPS. Manning said NSA had some requirements, and he assumed the FBI did as will. Kent suggested the government side put together a position paper. A member then asked who the customers of FIPS were supposed to be; given the government's special requirements, why was industry input even needed? Smid of NIST said industry input was needed, or no one would build systems for the government to use; also, the government may be involved in key recovery in commercial systems where "...public safety is involved." (It seemed plain that "public safety" in this committee is a code word for "law enforcement").

Kent suggested that if private parties want to operate key-recovery services (apparently meaning escrow services), they would have some negligence defense if they used a federal standard.

On the following day, December 6, Dorothy Denning presented a high-level schematic of key recovery associated with key fields and encrypted data. The schematic was thrown together the night before. She promised to make it available on her web page (www.georgetown.edu/~denning/).

Patricia Edfors of Treasury spoke about federal public key infrastructure pilot projects. She also described an "Emergency Access Demonstration Project," which was to "demonstrate the viability of key recovery, as a security service, for federal business applications." The project is to last 9-15 months, beginning August 1996. There will apparently be participation between certain government agencies and some private firm. Edfors said no attempt would be made to recover digital signature keys, create a key management infrastructure, or mandate which cryptography is used. However, "export requirements" will apply to all plans.

Kent wondered why the government would need key recovery for itself. He seemed to feel that key recovery for an individual's worksation is a data protection issue (backups) rather than true key recovery. Members mentioned a few cases where an employee was unable to decrypt his files, but no one knew of a case where an organization was unable to obtain shared data (e.g., a database), because it was encrypted. Other members seemed reluctant to accept his distinction. They seem to view key recovery as a way to audit proper use of organization assets by employees, or to protect the organization from malicious acts of employees, or to recover data if a custodian is run over by a bus.

Discussions continued to frame the issues for the project and assign functional tasks for sub-committees. Gilmore of the FBI said most key-recover issues would arise (for law enforcement) in the context of search warrants, not wiretaps, although the latter could be very important. In a question as to how long escrowed or archived keys should be kept, Gilmore said as long as the data existed, which might be indefinitely. When pressed, Gilmore said this was because some crimes have no statute of limitation. We thought some members might be mentally calculating storage requirements for session keys in a large communications system, if key storage and indexing was to be indefinite.

Manning of NSA said the National Archives, for example, would have to have access to recovery keys forever. No one asked why the National Archives might be archiving encrypted data.

Boland of GlobalKey also asked about keys to encrypted voice or video. No one seemed to have thought of this before.

Kent wrapped things up with a list of issues for discussion at the next meeting. These included:

```
--the threat model
--interoperability
--key recovery agents
--performance issues, computation and bandwidth
--algorithm independence
--enforcement measures
```

The next meeting will be held in the San Francisco area on February 19 and 20, 1996. Before then the members will confer by email and attempt to set up working groups to present papers on particular topics.

The meeting ended with an opportunity for public comment. None was offered.

Our opinion was that the only reason for the existence of this project was the insistence of the government, primarily the law enforcement and state security agencies. Private industry seems to feel there is little demand for a key-recovery standard, since those needing it can implement it themselves. Industry representatives were obviously worried about export restrictions requiring key escrow, and possible attempts to make it mandatory in some way. As corporations use encryption more and more, there will obviously be a need to develop key recovery systems inside the firm. The justification for a federal standard, however, seems weak.

We felt that this project would probably end in failure, through inability of the industry and government parties to compromise, or if a standard did issue, few private firms would use it. It's even doubtful a standard could be completed and adopted before private systems are firmly in place. Is the whole thing just more of the government's increasingly delusional effort to control private cryptography, or does someone besides the security agencies really want a standard?

The committee will post information at www.crsc.nist.gov. We can fax a copy of the materials handed out. We'll try to answer any questions by email (or phone, if you're really in a hurry).

John A. Thomas jathomas@NETCOM.COM
Dolce & Thomas, L.L.P.