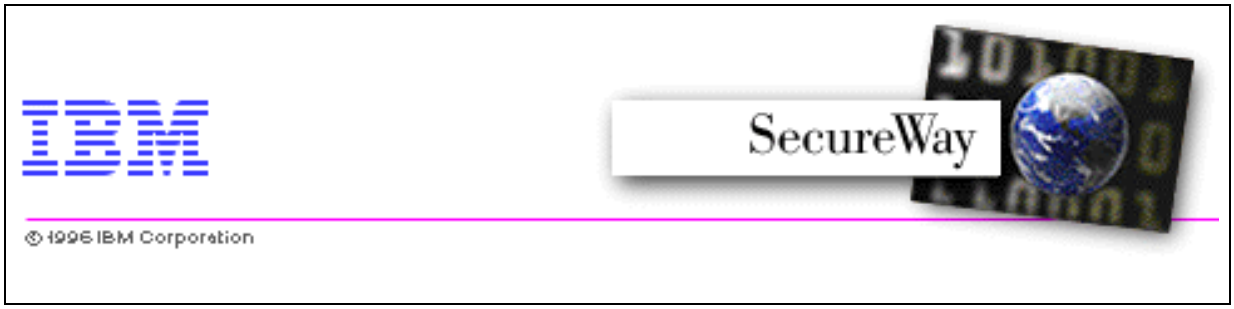

THE NEED FOR A GLOBAL CRYPTOGRAPHIC POLICY FRAMEWORK

For the first time, government, industry, consumer groups, civil liberties groups, and the media around the world appear to agree it is time to reform public policy on cryptography. The central question is how to best balance the need for stronger cryptography with the need of governments to promote public safety and global and national security. This paper puts forth IBM's belief that: In order to provide our customers with the strongest security possible while supporting governments around the globe in their roles, industry must invest immediately in the development of a Global Key Recovery Framework.

THE NEED FOR A GLOBAL CRYPTOGRAPHIC POLICY FRAMEWORK

AN IBM POSITION PAPER

INTRODUCTION

For the first time, government, industry, consumer groups, civil liberties groups, and the media around the world appear to agree it is time to reform public policy on cryptography. With the advent of the Global Information Infrastructure (GII) and its applications in electronic commerce, customers around the world increasingly demand that assets they maintain and communicate electronically be secure. The 1996 report of the U.S. National Research Council, *Cryptography's Role in Securing the Information Society*, concludes that without the strong cryptography to provide security for the GII, U.S. national and economic security will be at risk. The report balances this by noting that illegitimate use of cryptography poses substantial threats to national and public security.

The central question is how best to balance the need for stronger cryptography with the need of governments to promote public safety and global and national security. How should governments embrace cryptographic use without harming basic individual rights and the protection of electronic assets on the GII?

In this IBM paper, we take two conclusions as given -- (1) that strong cryptography should be more widely available; and (2) that governments have a legitimate need for applying certain conditions to cryptographic use in order to perform their constitutionally or statutorily mandated duties. To balance these competing goals, IBM believes the following: *In order to provide our customers the strongest security possible while supporting governments around the world in their roles, industry must invest immediately in the development of a Global Key Recovery Framework. The cryptographic key recovery methodology available today that offers the greatest security to legitimate GII users, while permitting government access under valid authority without unnecessary risks to GII users' right to privacy is a* ***key recovery system.***

Investment in key recovery systems must be made now. It will take several years to establish such a framework globally that will fully support pervasive key recovery use. If the world's principal supplier nations of cryptographic products and technologies do not act quickly, then other suppliers of non-key recovery products will begin to win market acceptance for their products, putting the future of cryptographic product supply from North America, Europe, and Japan at risk.

IBM Position on Clinton Administration Policy

On October 1, 1996, the Clinton Adminsitration announced a shift in American policy treatment of cryptographic technology and products. ***IBM applauds this initiative as a major first step forward on a journey that governments and industry must make together in promoting security for the Global Information Infrastructure. The announcement leaves a number of questions unanswered and which cause IBM concern, but we are prepared to work with other companies, customers and other private sector groups, as well as the Administration, the Congress, and governments around the world to ensure that these issues are addressed.***

IBM supports the Administration announcement for the following reasons:

- The Administration recognizes the commercial nature of cryptography through the transfer of export licensing jurisdiction from the State Department to the Commerce Department. All provisions of law governing commercial technology and products -- which differ substantially from the Arms Export Control Act, the statute that has previously governed the export of encryption products as munitions items -- should be applicable following the transfer of licensing jurisdiction. This should include provisions of law governing foreign availability.

- IBM supports the Administration statement that controls on domestic use of cryptography will not be imposed. This policy statement will be one of the central criteria by which we will evaluate the regulatory and legislative implementation of the Administration's announcement. It will be tempting for some to try to use export controls to encourage the deployment of key recovery as a means to impose controls on domestic use. IBM will oppose such attempts. Widespread use of key recovery technologies in the domestic market should only occur where there is a need perceived by cryptographic users for such technologies.

- IBM supports the immediate liberalization of exports of non-key recovery products at the 56 bit level. However, the Administration limits this relaxation to a period of two years, a limitation we believe will be unworkable. We expect other countries will move quickly to match the U.S. action in order to allow their own companies to remain competitive with U.S. exporters. We therefore expect 56 bit DES availability to proliferate rapidly, as it previously has begun to do.

  Further, IBM and other U.S. cryptographic exporters will have to address customer questions about the two year limit. These will include whether we will be able to provide service and support for installed 56 bit products after it expires and whether they will be able to expand their applications as the number of their sites or software

"seats" continues to grow. This situation could adversely effect American exporters. As non-American sources of 56 bit products grows (as noted in the preceding paragraph), customer uncertainty about the two year limit could lead some customers to non-U.S. suppliers. American exporters may be at a disadvantage; therefore, IBM asks the Administration to withdraw the two year limitation.

- The October 1 statement does not overtly dictate conditions or requirements for key recovery. The announcement indicates that exports of key recovery products based on any algorithm of any key length will be permitted (prior Administration proposals imposed requirements that either a specific technology or algorithms of no greater key length than 64 bits be used as a condition of export). IBM views the most recent Administration announcement as evidence that they will encourage ***industry-led solutions, rather than government-mandated ones,*** a major step forward.

  Still, IBM has a major reservation about this portion of the announcement. The conditions attached to the two year liberalization of 56 bit exports will not be viewed constructively by many companies and other private sector groups, and hence, will hinder rather than help. As we and others have communicated to the government, private sector investment in key recovery has already begun for commercial reasons. The Administration should reconsider this part of their policy change. It would be better if liberalization were granted in recognition of these pre-existing investments, rather than due to what many will regard to be market-distorting tactics.

We welcome the stated intent of the Administration to work with industry to develop a policy framework that will promote this framework in a constructive manner. The remainder of this paper addresses the elements that should be addressed as the U.S. and other governments consider how to promote the rapid deployment and standardization of such key recovery products and technology. In the United States and other countries, it will be important to build a national consensus around these elements. We encourage a full public discussion.

Congress will be an important player in this discussion, since legislation is needed in order to effect some of these recommendations. IBM supported the movement of legislative initiatives in the 104th Congress that addressed encryption issues. We intend to continue working with the leadership in Congress and the sponsors of those initiatives to improve and broaden them to include the elements addressed in the following set of recommendations.

IBM Recommendations for a "Global Key Recovery Framework"

Recommendation 1: *IBM recommends that governments support "Key Recovery", where unlimited key length solutions may be exported and widely used around the world.*[1]

IBM does not make this recommendation lightly. It is unclear yet that key recovery will be widely endorsed as a global standard, especially if in the course of the next few years, unlimited strength non-key recovery solutions from uncontrolled sources of supply begin to become pervasive in the world market.

Nevertheless, IBM believes that a number of information technology users have begun to view key recovery techniques as a possible solution to their concerns about the loss, destruction, or compromise of keys that they hold today and the associated costs they absorb in managing those keys. Further, we believe it possible that if key recovery products begin to be used widely enough around the world, then over time, the world's principal cryptographic suppliers will standardize on key recovery solutions. With more time, given the desire of customers of these suppliers to standardize their own internal systems and those of their own customers and business partners, market forces will eventually make key recovery systems the global norm, including in domestic use. We do not know whether this premise will hold in practice, but given the importance of the issues at stake, we are prepared to invest in the development of key recovery products.

Recommendation 2: *Governments of the world's principal cryptographic technology and products supplier countries -- especially those in OECD countries -- should agree as quickly as possible on a "Global Key Recovery Framework".*

Throughout the post-World War II era, governments have tried to control access to and use of sophisticated products and technologies for security reasons. Experience demonstrates that such controls work only when governments of countries that serve as the principal sources of these products and technologies all agree on the means by which to effect these controls. The nature of technology -- particularly in a global and fast-moving technology like electronics -- is such that governments' control systems are inevitably challenged by the portability of the technology and its speed of development. Thus, agreements among supplier countries must be sufficiently adaptable to changing circumstances and broad enough in terms of coverage of supplier countries that the agreements and the means chosen to implement them can be effective.

---

[1] We assume most readers of this paper understand the differences between key recovery and key escrow, between single key and partial key approaches, and between public and private key management systems. For readers who may not, we have included a discussion (Attachment A) that explains them.

Frankly, we are skeptical, based on past history on the encryption export control issue, that a multilateral agreement that is truly effective will be negotiated. Governments view cryptography so differently that it will be difficult to get anything more than a superficial agreement multilaterally. It does seem possible, however, that a set of bilateral agreements may be negotiated, and we regret this, since such agreements seem to us to be less likely to conform to the principles of this suggested Framework than would an open multilateral agreement. Nevertheless, IBM will continue to support the negotiation of a multilateral agreement in the future as the best way to assure consistency of encryption export control treatment from country to country.

Recommendation 3: *Governments should agree not to control the legal use of cryptography domestically.*

This recommendation will be controversial in a few countries. Nevertheless, we strongly support the individual user's freedom to choose security solutions most appropriate to the protection of his or her electronic assets and right to privacy. Further, we note the conclusions of the U.S. National Research Council report which notes the paramount necessity of maintaining the integrity of important national assets like national power grids, banking and financial systems, and air traffic control systems. The administrators of such systems should have the autonomy necessary to determine the level of security that best meets their needs.

Recommendation 4: *Governments should agree that interoperability between key recovery and non-key recovery systems will be permitted in perpetuity.*

We recommend above that governments should not control the domestic use of cryptography. Some customers will never be comfortable with any key recovery system. We expect this to be particularly true in the individual user environment. Given the needs of individuals for privacy and of all users for security, and given that a number of them will not opt for key recovery-based cryptographic solutions, it will be vital that their computers be able to communicate with those that are based on key recovery.

We note as well that for many larger customers, conversion from installed bases (sometimes called "legacy systems") of non-key recovery systems to key recovery systems will not happen overnight. In order to provide them with the smoothest possible migration path to key recovery, their installed systems must be able to work with the newer systems that they procure.

Recommendation 5: *Assuming adequate key recovery is supported, governments should impose no export restrictions on the algorithm key length of key recovery products or on algorithms to be used for key recovery products.*

We believe governments in the OECD countries agree with this principle. Key recovery techniques can easily meet government requirements for accessing encrypted files and communications in clear text regardless of a key recovery product's key length or the algorithm used.

Recommendation 6: *The ability of Key Recovery Service Providers (KRSPs) to perform effectively is critical. It is likely that KRSPs will be required to receive permission to offer key recovery services. Criteria for granting permission for them to operate should be limited to (1) the ability to provide timely access to government authorities upon presentation of valid authority to gain such access; (2) establishment of a satisfactory audit trail mechanism to show where key recovery information has been lawfully transferred; and (3) the ability to protect the confidentiality of all lawful requests for key recovery information.*[2] *This latter point applies in particular to cases where users wish to retain their own key recovery information. Self-retention should be permitted based on the self-certification that such users are able to meet these performance criteria. Governments may impose penalties on self-retaining users for miscertifications.*

KRSPs will be a central component of a Global Key Recovery Framework. Their ability to provide timely access to key recovery information will be vital both to their customers' needs for recovering keys and for governments to acquire legitimate access. Their ability to do so will likely require some form of authorization. Governments must avoid the temptation to overregulate them -- thereby imposing perhaps unreasonable costs on their operations. IBM believes one good way to avoid this temptation would be for governments to authorize independent organizations to license agents to operate. Another equally valid approach would be for governments to approve several authorization agents -- preferably in the private sector -- to perform such functions with KRSPs being able to choose between their services.

Whether governments elect to authorize KRSPs on their own or to permit private organizations to do such authorizations, it is important that the process created by which KRSPs are authorized to operate is not so cumbersome that it creates a disincentive for moving to a Key Recovery Infrastructure. Clearly, the most important requirement for authorization is a KRSP's demonstrated ability to provide timely access to keys. Creating an audit trail mechanism for tracking the lawful transfer of key recovery information is also

---

[2] While IBM believes a Global Framework involving international agreements should address these issues, readers should note Recommendation 12 which calls for immediate licensing of key recovery products for export when those products are supported by acceptable Key Recovery Service Providers either domestically or in other countries.

important. And, given that KRSPs will often want to retain their own key recovery information, we recognize the potential that in some isolated cases, individuals in the parent company of the may at times be the subject of an investigation. In such cases, the KRSP must provide a sufficient level of certainty to government investigators that their investigation will not be compromised.

Recommendation 7: *Key recovery information should be accessible from a network of KRSPs only under contractual terms between the KRSPs and their customers or to government agencies upon presentation of valid legal authority to acquire such access.*

Demand for key recovery services derives principally from those customers who are concerned about losing their keys through forgetfulness (principally individual users) or through such events as natural disasters or the willful or negligent acts of employees or through the death of an employee. KRSPs, we believe, will find a significant market in the private sector for their key recovery services. KRSPs will only succeed, however, when they can assure their customers -- via contract -- that their customers' key recovery information will not be compromised.

The exception to this would occur when a government investigative agency, upon presentation of valid legal authority to acquire such access, would request key recovery information from the KRSP. In the United States, such authority would normally be presented in the form of a wiretap order or search warrant. Other countries' constitutional and legal frameworks provide for other, but similar, kinds of authority.

Recommendation 8: *Framework governments should agree that key recovery information will only be permitted under the terms of lawfully or constitutionally prescribed government access.*

Key recovery information, in the hands of government authorities, can expose sensitive information related to an individual's right to privacy or to an individual's or organization's intellectual assets. Constitutional and legal protections must therefore be strictly observed, including the conditions under which a search warrant, wiretap, or similar authority is granted to government agencies. Further, other conditions, such as the duration and investigatory scope of such authorization, must be observed. Without such guarantees, users will have no confidence in a key recovery system.

Recommendation 9: *Governments should agree that the international exchange of lawfully acquired key recovery information should only be done on a government to government basis. No government should ever ask an agent resident in another country for access to key recovery information. Framework member countries should engage in Mutual Recognition of the other members' duly licensed key recovery agents. Mutual Recognition Agreements (MRAs) should be negotiated between*

Framework member countries under which the principle, "Once authorized, globally authorized" should be applied to Key Recovery- Service Providers.[3]

Key Recovery Service Providers will be licensed by their own governments or by trusted private parties who will perform the KRSP licensing role. They have no obligation to other governments. If a government in one country wishes to acquire access to key recovery information in another country, then it should contact the government of the second country. The second government, in this case, would only be permitted to request key recovery information subject to the authority it has acquired under law.

Mutual recognition among Framework member countries of each other's licensed KRSPs is important from several perspectives. First, it is unrealistic to expect that all countries will cooperate with establishing this Framework. Second, governments in the Framework should benefit from a higher degree of confidence in a global key recovery system which relies only on a network of authorized Key Recovery Service Providers. Further, customers themselves, at times, may not wish to have all of their key recovery information held in their own countries, due to possible concerns about unauthorized invasions of privacy or industrial espionage. And, some privacy rights advocates question whether governments who do not want to be bound by international agreements may engage in secret agreements with the weaker members of a regime for unacceptable exchange of key recovery information -- in other words, the system's strength could only be as strong as its the protections offered by its weakest member. A key recovery system that permits customers to choose among KRSPs in a global framework is a powerful protection against this concern.

Recommendation 10: *Governments should agree to permit the export of key recovery products to international customers when these products support adequate key recovery through acceptable KRSPs. This may involve one time product reviews by government agencies as a condition of approval prior to its initial export. Governments must provide sufficient resources to key recovery product providers to inform them of what their specific requirements for timely access are.*

Consistent with the other recommendations in this paper, key recovery products that conform to government access needs should be licensed for export when they are linked to licensed KRSPs. Note that it is not necessary that the KRSPs be in the country of

---

[3] "Mutual Recognition Agreements" is a term of art used in trade policy negotiations internationally. Normally, MRA's address, for example, product safety requirements. The phrase, "once tested, globally approved" would, for example, apply to a situation where a product approved for use by the testing body in one country would be permitted to be used without duplicate testing in others. We are suggesting the same approach for KRSP authorization in order to promote faster implementation of the Key Recovery Framework.

importation, since the key recovery technology will easily allow for them to be in countries other than that in which a cryptographic product user is located.

Recommendation 11: *Key recovery approaches that are designed around more than one source of key recovery must be authorized by Framework member countries.*

As is explained in Attachment A to this paper, key recovery systems designed to support key recovery from more than one KRSP provide the greatest level of security to GII users of any key recovery system. Such approaches provide an affordable and scaleable solution -- regardless of format chosen -- that will benefit product suppliers, KRSPs, and individual and corporate users alike.

Recommendation 12: *Governments should act immediately to support the development of products and services that support the Framework. Support should include adopting legislative reforms as needed, revising regulations to support the recommendations above, government purchasing policy, and immediate licensing of key recovery products for export in certain cases.*

Governments have many tools to promote their interest in the development of a Global Key Recovery Framework as fast as possible. Speed is of the essence, since standardizing on key recovery quickly and globally is desirable as an alternative to the availability of non-key recovery strong cryptographic products from other countries.

Legislative and, perhaps in a few cases, constitutional reforms may be required in some Framework countries. For example, in most countries, the liability of KRSPs for unauthorized disclosure of keys or key recovery information should be addressed legislatively where contractual terms may not address these liability issues adequately. However, it should also be noted that key recovery systems supported by more than one source of key recovery information largely address those liability issues involving inadvertent or willful and improper disclosure of key recovery information. When users utilize such systems fully; i.e., by relying on more than one KRSP as the source of all the key recovery information required to reconstruct keys, then it would require the acts of more than one individual to improperly disclose key recovery information. Liability exposure for KRSPs is therefore likely to be limited either to instances (1) where there is a conspiracy among several KRSPs or (2) where, in the case of self retention of keys, an employee or group of employees without authorization disclose such information (e.g., information contained in personnel files that should be protected under privacy laws). Governments' legislation should address these issues.

Our recommendations also require quick action to update and revise regulations to promote development of a key recovery system. Governments should also consider the use of public procurement for their own uses as a way to encourage private sector

development of the technologies, as well to provide a useful test bed for key recovery approaches.

Finally, it will take time for governments to agree either multilaterally or bilaterally on how best to do it. We therefore call on individual governments to take steps immediately to authorize the export of key recovery products when those products are supported by acceptable Key Recovery Service Providers either domestically or in other countries.

Recommendation 13: *We recommend that governments should continue to explore the possibilities presented by "differential cryptography" solutions systems.*

IBM and Lotus have suggested that the approach adopted by the Lotus Notes version 4.x product is less than an ideal solution. However, the "differential cryptography" approach embodied in the Lotus approach did address the requirements of a number of Lotus's customers. Governments should continue to explore whether such solutions can be more elegantly applied in the future.

CONCLUSION

IBM hopes that our recommendations will help to point the way for governments, industry, and others to find common ground for resolving the policy issues regarding the use of strong cryptography in the GII context. The stakes involved in this global public discussion are enormous -- ranging from the rapid and complete initialization of the Global Information Infrastructure, to the protection of vital national assets and information, to how best to protect public safety and global and national security, to the question of which country or countries will be the cryptographic technology leaders of the future. We believe that our recommendations will lead to a positive solution for the broadest number of parties interested in the future of cryptographic use.

ATTACHMENT A

A Layman's Guide to Various Underlying Cryptographic Concepts

Cryptographic technology is inherently difficult to understand. The concept of "key escrow" itself is fairly easy to grasp, since escrowing of cryptographic keys may be likened to a homeowner giving a copy of the key to his house to a trusted neighbor in case the homeowner should inadvertently lock himself out of his house. However, even in such a common case as this, there is a potential vulnerability for the homeowner. He may trust his neighbor, but others -- such as members of the neighbor's own family -- may acquire unacceptable access to the key. For example, a person wanting unauthorized access to the homeowner's key may try to bribe the neighbor's son or daughter to provide the unauthorized person with a copy of the key. Thus, under this kind of escrowing system, there is a single point of vulnerability.

Cryptographers have developed several ways to address this problem, one being the "split key" approach to escrowing of keys. For example, many homeowners have more than one lock on their houses. So, the homeowner may simply take one of the keys and give it to a neighbor and give the other to another neighbor. This is a little more cumbersome in case the homeowner locks himself out, but it is more secure. The person seeking unauthorized access would have to bribe two neighbors. Still, these two sources of vulnerability may pose an unacceptable degree of risk for a homeowner who may have a multimillion dollar art collection. Transferring keys themselves generates what many will consider to be unacceptable risk.

Cryptographers are now beginning to work on so-called "key recovery" approaches as an alternative to such key escrow systems. Under these systems, no key is ever transferred to another party. In the homeowner analogy, keys would be kept only by the homeowner. To understand key recovery, it is better to think of a combination lock on the front door of a house. In this case, there is a series of digits -- say, a 6-digit combination -- which the homeowner may give to his neighbor. Again, however, this kind of approach would be little more secure than giving an actual key to the neighbor.

However, it is not necessary that the homeowner must provide all 6 digits to a neighbor. He may elect to give 3 digits each to 2 neighbors, 2 digits to 3 neighbors, even 1 digit each to 6 neighbors. No single neighbor would have the entire combination. Under more advanced forms of key recovery, means are readily available to ensure that in the first case, the 3 digits could be done randomly and in no particular sequence. Therefore, a neighbor who has 3 digits would not know in which sequence they would appear in the combination, and neither would he necessarily know who the other neighbors are who have the other 3 digits. For him to break the combination would require the same kind of massive work effort as if he were to try out all variations of a 6 digit combination.

Cryptographers have other ways of adding even greater security for such information, by providing a protective shield of sorts to protect even the confidentiality of the 3 digits. This would be similar to the homeowner providing the 3 digits to each of two neighbors in a sealed envelope. If the sealed envelope were ever broken into, then it would be known that an unauthorized access attempt had been made.

Of course, in the world of cryptography, key recovery systems are much more complex. Instead of just 6 digits being shared among neighbors as in the above example, there are a verly large number of digits that go into the construction of a key. Attempting a massive assault on such key lengths is difficult and costly, and for very strong encryption products, virtually impossible to achieve. Also, putting the digits themselves in random order through various applications of cryptographic techniques is complex, as is the cryptographic equivalent of the homeowner envelope.

A recovery system that relies on multiple sources for key recovery information in order to reconstruct keys offers many advantages over key escrow systems -- for example, they are less expensive to implement, since there are no large databases being created of keys that must be retained over a period of time. Further, the only person who has access to the actual keys, and the means by which to reconstruct the keys, is the owner of the data. However, under valid court ordered authority, law enforcement officials may acquire access to key recovery information and using the key recovery technology, would be able to reconstruct keys -- but only under the terms of the court authority.