Issue Paper
RAND Science and Technology

E-Mail Communication Between Government and Citizens

Security, Policy Issues, and Next Steps

C. Richard Neu, Robert H. Anderson, Tora K. Bikson

Modern network technologies—particularly electronic mail and the World Wide Web—offer the potential for significantly enhancing communication between government agencies and their citizen clients.[1] Because much of the communication between governments and citizens involves the transmission of sensitive information, however, the full potential of these new media will not be realized until means are developed for secure interactions.

The *technology* to support secure communications exists today. Similarly, the *physical and commercial infrastructure* for widespread digital communication—the public switched network, Internet service providers, and similar components—already exists or is being built. What does not exist, however, and does not appear to be imminent, is the *institutional, organizational, and administrative infrastructure* to support a potentially universal (i.e., available to any citizen who wants it) system for secure and binding e-mail communication between government agencies and citizens.

On November 6 and 7, 1997, with the sponsorship of the Markle Foundation, RAND convened a workshop in Washington, D.C. to begin a discussion of the character of the required infrastructure, who might plausibly provide it, how it might be financed, and what other policy changes—institutional, legal, programmatic—might be necessary to support secure communication between government and citizens. Attendees at the workshop included managers, policymakers, and analysts from a variety of government agencies at the state and federal levels and representatives of private-sector concerns that are users or providers, current or potential, of secure communications services. In this issue paper, we summarize some of the insights that the RAND organizers took away from that workshop and some of the questions that remain to be resolved.[2]

ELECTRONIC COMMUNICATION BETWEEN GOVERNMENT AND CITIZENS: WHY?

It is currently possible for citizens to access much government information on-line. Mainly, this information has a "bulk mail" character—reports, forms, or bulletins that are suitable in more or less the same form for all citizens. Less common are electronic communications of a personalized nature—communications that come from or are addressed to individual citizens and whose content is specific to these individuals. Examples of such communications are tax filings; applications for various licenses and permits; communications related to health, welfare, and

[1]With few exceptions, the considerations discussed here in relation to communication between government agencies and individual citizens are equally applicable to communications between government agencies and businesses.

[2]Consistent with the spirit of frank, off-the-record exchange that characterized workshop discussions, this issue paper does not attribute specific ideas or points of view to individual participants.

retirement benefits; and all manner of queries and responses relating to government programs. Today, this personalized communication is typically accomplished through postal mail and occasionally by telephone or in-person contact.

Federal, state, and local governments send or receive hundreds of millions of individualized communications every year. If even a small fraction of these communications could be transmitted electronically, the savings in printing, handling, and postage costs could be significant. Electronic documents might be more easily and cheaply processed and stored than their paper equivalents and automatically checked for completeness, consistency, and accuracy.

In many cases, citizens may find electronic documents more convenient than traditional paper documents.[3] Electronic documents can, for example, be filed, reproduced, abstracted, and forwarded by pressing a key. Recipients may also receive e-mail communications wherever they establish access to the Internet—potentially important for an increasingly mobile population that spends ever larger amounts of time away from permanent or registered home addresses. The asynchronous nature of e-mail communication also allows citizens to have the same round-the-clock access to government services and agencies that they are beginning to enjoy in their dealings with private-sector institutions such as banks, airlines, and catalogue retailers. Cheaper and more convenient communication with citizen constituents could provide a good basis for more responsive and more effective government services.

THE NEED FOR SECURE COMMUNICATIONS

Many government communications with individual citizens involve the transmission of sensitive information—tax information, records of health care, and entitlement to government benefits, for example. In some cases, communications between citizens and government agencies are also legally binding—tax returns, for example. Consequently, electronic communications between government agencies and individual citizens will have to be highly secure. More specifically, a system that supports extensive government-citizen communication will have to embody strong protections for

- *Privacy.* The information being transmitted cannot be read by unauthorized parties.[4]
- *Integrity.* The form and content of the message have not been altered.
- *Authentication.* Citizens and government agencies must be sure that they are in fact communicating with the intended party.

Electronic communications between government agencies and citizens will probably require more stringent protections than do traditional paper-based or in-person transactions. The scale and velocity of traditional transactions are limited by the very nature of these transactions: requests for information have to be submitted, information copied and mailed, and so forth. Breaches of security are likely to affect one citizen at a time. But as databases of sensitive information become increasingly accessible on-line, the consequences of a security failure may multiply. Rather than stealing a single Social Security or credit card number, a determined, skilled, and criminally inclined hacker might succeed in gaining access to files that contain identifying information for thousands of individuals. The same ease of access that makes electronic access to databases attractive in the first place could permit a malefactor to download large amounts of sensitive information or carry out hundreds of illegal transactions in seconds—much too quickly, perhaps, for authorities to recognize or to plug a breach.

Of course, nongovernmental users of electronic communications also require privacy, integrity, and authentication—in pursuing, for example, on-line commercial transactions. And some kinds of nongovernmental communication—the transmission of medical records, for example—may involve information as sensitive as anything kept in government files. Systems for secure e-mail communication are already being developed to serve the needs of these nongovernmental users. Government agencies may be able simply to piggy-back on this infrastructure, and it would certainly be wasteful to create a parallel infrastructure purely for government purposes. Ideally, a common infrastructure for secure governmental and nongovernmental e-mail communications will emerge.

But there is no guarantee that a secure communications infrastructure developed for commercial purposes will be adequate for government-related uses. In particular, there is no guarantee that privately developed systems

[3]See Robert H. Anderson, Tora K. Bikson, Sally A. Law, and Bridger M. Mitchell *Universal Access to E-mail: Feasibility and Societal Implications*, RAND, MR-650-MF, 1995.

[4]The importance the public attaches to privacy was illustrated in April 1997 by the outcry against and the subsequent discontinuance of a service offered by the Social Security Administration that allowed citizens to have immediate access via the World Wide Web to individualized Personal Earnings and Benefit Estimate Statements (PEBES). Even though the information required for on-line access—name, Social Security number, date of birth, and mother's maiden name—was the same as was required for in-person or postal access, many saw electronic transmission of Social Security–related information as insufficiently secure and open to potential abuse.

will provide the potential for universal access that must be a key feature of systems meant to facilitate communication between government and citizens. At the very least, government agencies will have to articulate—sooner rather than later—their needs for security, and undertake assessments of the degree to which independently developed approaches satisfy those needs. Government agencies might also play a useful role in promulgating security standards that can then be widely adopted by non-governmental users. (The U.S. Department of Health and Human Services, for example, has already established standards for the electronic transmission of personal medical information.) And, above all, government agencies will have to create a general policy environment that will encourage the development of secure and binding e-mail communications for all purposes.

THE ELEMENTS OF SECURE COMMUNICATION

Today, arrangements for secure digital communications often employ some form of *public key encryption* (PKE).[5] In such systems, each user has one or more key pairs, each comprising a "public" key that is known to his or her correspondents, and a "private" key known only to the user. These keys can be used in either of two ways: as encryption keys, to ensure the confidentiality of messages, or as signing keys, to confirm the identity of the sender.

When a correspondent encrypts a message with the recipient's public key, only the intended recipient can read (decrypt) the message by means of the recipient's private key. Similarly, if the correspondent "signs" the message using his or her private key, the recipient can use the correspondent's public key to check the signature and confirm that the message came from the named correspondent. By attesting to the origin and integrity of an electronic document, such "digital signatures" may, in appropriate circumstances, make the document binding on the sender (many states have enacted laws making digital signatures that meet certain standards the legal equivalent of traditional physical signatures).

At the heart of a PKE system are one or more so-called *certificate authorities* (CAs)—trusted institutions or organizations that "certify" that a particular public key is associated with a particular user. In essence, a CA establishes an "electronic identity" for each user of its services. For others to have confidence in this identity, a CA must also be able to provide nearly instantaneous verification that a particular user/public key pairing is still valid—that the user or other authority has not for some reason canceled a public key.[6] Usually, a CA will demand proof of identity—perhaps a driver's license, birth certificate, passport, or application form bearing a notarized signature—before issuing a digital "certificate" binding the public key to the user.[7] Typically, a CA will also provide customer services such as replacing certificates that have been lost or compromised, publishing directories of public keys, and assisting users who experience difficulties.

IDENTITY VERSUS AUTHORITY

By associating a public key with a particular user, the CA establishes the electronic *identity* of that user. To complete a system for secure communication, a government agency or commercial institution must grant this user, whose identity can now be verified, *authority* to access information, to make use of services, to carry out transactions, or whatever. Establishing authority will typically require additional measures beyond those necessary to establish identity. For authorization purposes, for example, a particular electronic identity may need to be associated with particular accounts or records that the user is allowed to access.

Authorization—associating electronic identities with specific records or accounts—may be performed directly by the agency or institution granting access to records or accounts. Although an organization or agency must retain the responsibility for establishing identities or authorities, it may contract out to a third party the processing of electronic records keeping track of those certifications. The organizations with responsibility for granting authorities are commonly (perhaps confusingly) called certification authorities, because they certify the right of particular individuals to access particular files or services. Current usage distinguishes between *identity certificates* and *authority certificates.*

The two functions—establishing identity and establishing authority—are distinct and quite separable. A CA issues an identity certificate asserting that a particular electronic identity is associated with a particular user. If a government agency or commercial institution accepts this assertion—if it believes that the CA did an adequate job of verifying the user's identity—it may then issue an authority certificate granting that user authority to execute specific transactions—for example, accessing a Social Security file or a bank account, filing an application or tax return,

[5]For one of many introductions to PKE, see *Cryptography's Role in Securing the Information Society*, National Research Council, Washington, D.C.: National Academy Press, 1996.

[6]If a private key is lost or compromised, a user must replace both public and private keys.

[7]Some CAs issue different kinds or levels of "certificates," depending on the kind of supporting identifying materials required.

placing an order, or registering a motor vehicle. Some CAs may both certify identities and authorize transactions within specified domains, but this combination is neither necessary nor necessarily efficient. Indeed, the processes required to issue the two kinds of certificates are likely to be quite different. Identity certification will typically require some direct, perhaps in-person, interaction with individual users. Authority certification will typically require routine processing of large databases and updating links between electronic identities and particular accounts or records.

An individual user may have more than one electronic identity, and each of these identities may be granted multiple authorities. For example, the same person may have the identity "Trustee of John Doe Trust with certain authorities granted thereto (for example, authority to initiate specified financial transactions) and the identity "staff member of the XYZ Corporation" with other authorities (say, building access or purchasing authority). The CA that establishes identity does not need to know what specific authorizations have been granted to or revoked from a particular user. If the CA granting authorization relies on another CA to establish identity, a trust relationship based on clearly understood standards and accountability must be put into place and maintained between the two CAs. In some cases, authorization may not require identification in any absolute sense. A merchant may, for example, authorize a purchase knowing the credit card or bank account to be charged but not the personal identity of the buyer. For most sensitive government-related transactions, however, it seems likely that personal identity will have to be clearly established before authorizations are granted, and any government agency relying on other CAs for establishing identity will need to be linked to these other CAs by a well-established "web of trust."

WHO CAN ACT AS CERTIFICATE AUTHORITIES FOR GOVERNMENT AGENCIES?

Widespread and versatile communication between government agencies and citizens will depend on a CA or group of CAs that can meet the following criteria.

- *Highly reliable identification of agencies and users.* The government activities that generate the highest volumes of individualized communications often require the transmission of extremely sensitive information. Government agencies and citizens will require a very high degree of confidence that they are in fact each communicating with the intended party.
- *Local presence.* To ensure reliable identification of users, CAs may require in-person interactions and perhaps the physical presentation of certain documents. This in-person interaction may have to be repeated periodically to maintain the validity of the digital certificate. If secure electronic communication is to be available to any citizen who desires it, then every citizen (e.g., within a city, state, or the entire United States for federal government applications) will have to have easy access to an office of a suitable CA.
- *Extensive customer service.* A system that allows secure electronic communication with government agencies for any citizen who desires it will require a robust customer service operation—to answer questions, to guide infrequent and perhaps unsophisticated users, and to restore or to replace lost or compromised certificates.

Although increased use of e-mail communication could result in significant cost savings for government agencies, it is unlikely that these savings would be large enough to justify the considerable expenses associated with any single agency's acting as a CA—especially as an identity CA—solely to support its own communications. And citizens would not be well served if they had to establish different electronic identities for every government agency they wished to deal with. If secure communication between government agencies and citizens is to become commonplace, therefore, some organization or organizations will have to provide CA services that make possible communications with multiple government organizations. Ideally, electronic identities provided by these CAs will also be useful for commercial or nongovernmental communications. But who will provide these communication services?[8]

A variety of private-sector actors may be well positioned to provide CA services for secure communications between government agencies and citizens.

In recent years, a number of **specialist firms** have begun to offer CA services. Verisign, GTE Cybertrust Solutions, Digital Signatures Trust Company, and Cylink are some of the early entrants into this market. Although all of these firms hope for future growth, all still serve relatively small and specialized populations. Whether they can or wish to expand their operations to the entire population—including many users who might require exten-

[8]Identifying suitable providers of CA services for interactions with the government is not of purely theoretical interest. The General Services Administration of the federal government has prepared a draft request for proposals for a "pilot demonstration" to provide CA services for a broad range of federal agencies.

sive customer service and may not generate much revenue—remains to be seen. Also open to question is whether CA firms oriented (at least today) primarily toward facilitating private commercial transactions will find it worthwhile to meet possibly specialized standards of identification certainty and authorization control required for citizen-government communication. Similarly open to question is whether citizens will wish to entrust the security of sensitive government-related transactions to commercial firms.

Banks may be well placed to provide CA services for government-citizen communication. Banks have ongoing trusted relationships with their customers and already go to some lengths to establish customers' identities. (It is a legal requirement in banking to "Know your customer.") Banks have many points of presence in almost all communities and, at least occasionally, deal face-to-face with their customers. The movement toward direct deposit of government benefits means that even low-income Americans are increasingly likely to have bank accounts and to be in routine contact with a bank. Banks are familiar with needs for data security, authenticity, and privacy. Moreover, banks are already closely regulated, and the extension of this regulation to include standards for identifying customers and universal access may not be a large step. Finally, many banks are moving toward creating electronic banking systems to serve their own customers. It may turn out that such bank infrastructures can be exploited for communications with the government at minimal additional cost.[9]

Other institutions that maintain continuing relationships with individual citizens might also be able to provide CA services. Consider, for example, large **health insurance providers or health maintenance organizations**. Such organizations routinely establish basic identity information on their members and patients. Increasingly, these organizations may desire to communicate sensitive information—diagnostic test results, payment information, appointment verifications, etc.—to doctors and patients electronically, and they may develop secure communications systems for their own purposes. Electronic identities established for these purposes might be sufficiently reliable for the transmission of sensitive government information. Indeed, the federal government is already drafting security standards for the electronic transmission of health-related information. These organizations also have legitimate needs for information relating to some government programs—Medicare, Medicaid, Social Security—and extending their on-line communications systems to allow direct citizen-government interaction may be a natural step.

In carrying out their missions, some government agencies and quasi-governmental entities have frequent or regular interactions with large numbers of citizens. They may, therefore, be plausible candidates for providing CA services to a broad population.

The Social Security Administration (SSA), for example, has a nationwide system for creating a kind of digital identity—a Social Security number (SSN)—that is already widely used to verify many kinds of transactions. Upgrading the Social Security number to a public/private key pair is perhaps not too farfetched to be considered, although there has been resistance in the past to allowing the Social Security number to become anything resembling a national identification number. The issuance of SSNs does not currently meet the standards for identity verification we have described for digital identity certificates by CAs.

The U.S. Postal Service (USPS) maintains a relationship with every address in the country (if not, strictly, with every individual), and most Americans live within a short distance of a post office. Government agencies and individual citizens have grown accustomed to entrusting confidential materials to the Postal Service for delivery. Over the years, a substantial body of law and regulation has created a special status for postal mail. The Postal Service is not liable, for example, for losses suffered because a letter is not delivered. Tampering with mail and using the mail to perpetrate fraud are federal offenses, and postal inspectors "with badges and guns" are empowered to deal with offenders. E-mail, of course, enjoys no such protections today, but many see the extension of at least some postal regulations to e-mail as useful in the maturation of the new medium. This extension might prove more natural or graceful if the USPS were chosen to manage a system for secure e-mail.

Finally, state **departments of motor vehicles** may deserve some consideration as CAs. After all, these departments issue the most commonly used means of identification in America today—drivers' licenses. Most also issue identification documents to nondrivers. Why not, some ask, extend this identification service to the electronic realm?

[9]In January 1998, the Office of the Comptroller of the Currency granted permission for the first time for a bank to provide CA services. A subsidiary of Zions Bank, Digital Signature Trust Company, is issuing digital certificates to facilitate electronic filing of legal documents. See Office of the Comptroller of the Currency News Release NR 98-4, January 13, 1998.

ONE CA, OR MANY?

Most government agencies communicating via e-mail (and most private firms, for that matter) will necessarily maintain unique processes for granting and verifying access authorizations. Although they may contract with other agencies or with outside firms for the actual authorization, they will establish authorization and access policies specific to their own requirements. The Health Care Financing Administration, for example, will presumably not rely on the Social Security Administration or the Internal Revenue Service, much less a private firm, to determine who will have access to a citizen's medical information.

But there is no reason for different government agencies to maintain their own procedures or to rely on different CAs to establish the identities of electronic correspondents. Indeed, life will be simpler for citizens if many government agencies can agree to accept identity certifications from a common set of CAs. One pair of public and private keys would work for many government transactions. There would be no need to establish one key for dealings with the IRS and another for dealings with the Social Security Administration. Ideally, identities established for government purposes would also suffice for nongovernmental commercial or financial transactions. A single digital signature would be adequate for multiple purposes, just as a single physical signature is today.

This does not imply, however, that a single CA must or should provide identity certificates for all citizens. If several CAs—perhaps a number of private firms specializing in CA services, a number of banks, and the USPS—all provided identification services that met established government standards for reliability and validity, there is no obvious reason why citizens should not be allowed to choose the CA whose services they found most convenient or attractive, just as consumers are now free to choose among long distance telephone carriers or Internet service providers. Competition among CAs might help to constrain the price of CA services and to maintain the quality of their customer service. Being deemed acceptable for communications with government agencies could be a valuable selling point for CA providers; a bank, for example, might attract customers to its on-line banking services by advertising that the same digital key that provides access to checking account balances is also accepted by the Health Care Financing Administration should a customer want to check on the status of a Medicare claim.

A choice among CA providers may also alleviate concerns among some citizens about the creation of a monolithic "big brother" capable of observing or monitoring all of a citizen's e-mail transactions. A citizen who feels more comfortable using one key to file tax returns, another to respond to census inquiries, and yet another to facilitate personal banking transactions and who is willing to put up with the inconvenience associated with establishing and managing multiple keys might welcome the existence of multiple providers of CA services.[10]

SOME ISSUES TO BE RESOLVED

Along the path to an infrastructure for routine, secure e-mail communication between government agencies and individual citizens, a number of potentially difficult policy issues will have to be dealt with.

Responsibilities of certificate authorities. In essence, a CA certifies that a particular public key is associated with a particular individual or authorization and has not been canceled or compromised. What happens if the CA gets it wrong or assigns keys to an impostor? Almost certainly, CAs must bear some legal or financial responsibility if communications are compromised because of their failures. Contracts offered by commercial CA firms today typically spell out in considerable detail the limits of the CA's liabilities in various circumstances. But no standards exist for such terms and conditions,[11] including a statement of which protections are adequate for communications involving government agencies. What sanctions will be applied in case of a security breach? And if a CA complies with government guidelines for verifying identity, can the CA be held accountable for subsequent lapses?

Managing and protecting private keys. Exactly how individual citizens will create, record, protect, and use their private keys has not yet been clearly worked out. These keys will be long strings of digits, impossible for anyone to remember, and a user will need some repository (a "digital wallet") for his or her keys. A convenient solution would be for a user to store keys in password-protected files on his or her personal computer. The user

[10]Apparently, existing legal restrictions on the actions of government agencies and assurances that information will not be inappropriately shared between government agencies are not sufficient in the view of some citizens. A representative from the IRS told workshop participants that many taxpayers resist providing the IRS with bank account numbers for the direct deposit of income tax refunds. Very stringent legal restrictions on IRS activities notwithstanding, these taxpayers apparently fear that providing information on their bank accounts might allow IRS personnel to pursue improper investigations of their financial activities.

[11]However, a task force on certification authority rating and trust, under the auspices of the Internet Council of the National Automated Clearing House Association (NACHA), is developing policies to allow government agencies to evaluate the reliability, trustworthiness, and performance of CAs. Representatives from state and federal government agencies, as well as from the private sector, are participating. See http://internetcouncil.nacha.org.

would simply choose the appropriate key for any transaction and activate the key by typing an easily remembered password. But several workshop participants warned against storing encryption keys on personal computers; in an increasingly networked world, it is too easy for someone else to read even supposedly protected files. And what about occasions when keys are to be used away from the user's home computer? Better, they argued, to keep keys on a smart card or other device that can be carried around and inserted into a computer only when needed. Current technology allows multiple keys to be stored on a single card. But if all electronic identities are stored on a single card, does this come too close to a "national identity card?" And who will establish a common format for electronic keys and the cards on which they are stored so that they can work in multiple situations?

The legal status of electronic transactions. There is widespread recognition that laws have not kept pace with technology in regard to digital communication. E-mail does not enjoy the same legal protection from interception as do postal mail and telephone communications. As a general matter, for example, it is not illegal today to intercept another person's e-mail. The contents of an e-mail exchange are discoverable in legal proceedings; postal mail or telephone conversations typically are not. And prohibitions against mail or wire fraud do not yet clearly apply to e-mail communications. Many of the protections that now apply to other forms of communication will have to be extended to networked digital communications if the latter are to carry sensitive information. Will the act of reading an official e-mail—such as a summons, a tax notice, or some other communication that requires the recipient to take action—be construed as proof that the message was received, much as a signature for certified postal mail is today? Could a subpoena be served by e-mail? And what responsibility will citizens have to check e-mail regularly for official documents?

Key escrow. There is current uncertainty and controversy about the laws and regulations that will govern the use of encryption for secure communication within the United States. Will users of so-called strong encryption be required to register their keys with "key escrow" facilities so that law enforcement agencies can decipher communications if necessary? If so, who will maintain these escrows? How and how well can these key depositories—arguably among the most attractive targets for the criminally inclined—be protected? Must escrow holders be independent of CAs or independent of government agencies (to minimize chances for abuse)? Under what circumstances can or should escrow holders be required to disclose keys to law enforcement personnel? Presumably, there should be no requirement for escrow of keys used purely for the purposes of establishing digital signatures, since such keys establish only identity and integrity of messages. But is it possible to guarantee that keys intended only for digital-signature purposes cannot also be used for encryption?

Multiple laws and standards. In the past few years, a number of states have enacted digital signature legislation that endows electronic documents meeting specified standards with the same status as traditional signed paper documents. Unfortunately, requirements for a valid digital signature vary from state to state. Little progress has been made toward national standards for shared trust that will facilitate cross-jurisdictional transactions. International standards are yet further off. Neither has progress been made yet toward security standards that will be acceptable for multiple government transactions. There is some question, in fact, about whether a single security standard for many government interactions is practical or desirable. Should, for example, information about recent traffic violations be protected at the same level as tax returns or health information? Making all communications with government agencies meet the security standards of the most sensitive would doubtless increase the cost and inconvenience associated with many communications. One might envision a hierarchy of digital authority certificates being granted, much like the confidential–secret–top secret security clearances used by the Department of Defense.

Who will pay? Secure communication will not be costless. Who will bear these costs? Will citizens who wish to communicate with government agencies via the Internet be required to pay Internet access charges and CA subscription fees just as citizens who wish to communicate with a government agency today are required to pay for postage or telephone service? Will CA services be available on a subscription basis (like basic local telephone service), and will it be feasible or desirable to charge users for actual usage (like long-distance telephone service)? Can or should the government provide basic CA services for any citizen willing to use a centralized government-managed service?

Relations among certificate authorities. To what extent will multiple CAs have to cooperate? A degree of interoperability would seem desirable so that by checking with his or her own CA a user might conveniently confirm the validity of a correspondent's public key, even if that key were issued by a different CA. This kind of interoperability will require that a "web of trust" develop among CAs and that all CAs in the web meet some minimum standards. By establishing standards for identities used for government transactions, government agencies might

help to build this web of trust. But which agencies, and which standards? And whose responsibility will it be to monitor CAs to guarantee that standards are being maintained? Is self-policing among CAs adequate for these purposes?

E-mail addresses. If government agencies begin to make extensive use of electronic mail for communicating with citizens, should steps be taken to provide every citizen with an e-mail address? What if an e-mail address changes? Should Internet service providers be required to provide forwarding services similar to those now provided by the USPS for first-class mail?[12] What security standards are needed for e-mailboxes and e-mail service providers?

Equal access to government services. The number of Americans with easy access to the Internet is growing rapidly. Convenient use of the Internet, though, still requires significant monetary investment for equipment and a significant temporal investment in learning. If government agencies begin to offer e-mail communications to cyber-advantaged citizens, what obligation do these agencies have to create opportunities for the less plugged-in? Traditional access through paper and telephonic channels for communication will remain available—certainly during a lengthy transition period, and probably indefinitely. But will that be sufficient to guarantee equal access for all citizens to government services? Will it be incumbent on governments to promote electronic access through public-use terminals or kiosks in, for example, libraries, post offices, banks, and government buildings? Can or should personnel be available to assist first-time or infrequent users of such equipment?

GETTING FROM HERE TO THERE

Routine, secure e-mail communication between government agencies and individual citizens will not become a reality overnight. Considerable groundwork must be laid: Standards for privacy, integrity, and authentication must be established; certificate authorities must be identified or established; a host of institutional, administrative, and policy questions have to be resolved; and, most important, accumulating experience and maturing laws, regulations, and practice norms will have to provide a foundation for trust in using e-mail for sensitive communications.

The task of creating a capability for secure communication between governments and citizens is a daunting one. How can we begin to put the necessary pieces in place?

[12]For more on this topic, see Anderson et al., 1995.

An incremental, experimental approach is key. Experience with on-line transactions is steadily accumulating. Users are gradually becoming comfortable with the notion of entrusting sensitive information to the Internet. Government agencies are learning about public expectations for service and security and about the procedures necessary to provide both. With attitudes and capabilities changing so rapidly, it will be important not to lock into a single approach to secure communications. The temptation to let the ever better become the enemy of the adequate will be strong. But the likelihood that we will get the system entirely right on the first try is vanishingly small, and there is little point in trying at the outset for a system that will meet all government demands. Much better to concentrate on functional requirements, and to experiment, starting with relatively undemanding applications and relatively nonsensitive information, and then to gradually strengthen systems and procedures until we are confident that we can handle the most complex transactions and the most sensitive data. We should figure how to renew dog licenses over the Internet before we attempt to file income tax returns.

Citizens should be able to "opt in." At least during a transition period when the security and reliability of on-line communication with government agencies is still being demonstrated, citizens must be able to "opt in" to such communications arrangements, positively choosing for their records or accounts to be accessible on-line. Simply allowing citizens to "opt out"—to block electronic access to their personal information by themselves or by anyone else—will probably be inadequate. It is premature to assume that citizens have sufficient understanding of the implications of on-line access and of procedures to control this access to make on-line access the default option.

"Out of band" communication will continue to be important. To provide adequate assurance of the identity of an individual, it is often useful to use a separate channel of communication for verification. For example, although application for a digital identity certificate might be made on-line or in person, the password or personal identification number (PIN) unlocking or activating the certificate might be sent by postal mail to the correspondent's registered home address. Similarly, requests to establish specific authority may be transmitted and verified through separate channels or through channels different from those used to exercise the authority. Particularly sensitive transactions may require confirmation through independent channels. All of this suggests that policy should aim to maintain and to utilize multiple channels for electronic communication: the Internet, automated telephone services, bank ATM networks, and the like.

Success will depend on education and training. Successful development and deployment of mechanisms for digital communications between citizens and governments will require extensive efforts to educate citizens regarding the advantages of new communications modes and associated protections for sensitive information. Training in how to establish, use, and protect a digital identity will also be key. Equally important will be establishing realistic expectations among users; just because e-mail can be transmitted nearly instantaneously, for example, users cannot expect instantaneous answers to queries. Current modes of postal and telephone communication—and all the procedures, customs, and expectations that go with them—have evolved over decades. The evolution of legal precedents, operational procedures, and social practices and norms relating to e-mail communication will also require time.

PARTICIPANTS IN WORKSHOP ON SECURE COMMUNICATIONS BETWEEN GOVERNMENT AND CITIZENS

November 6–7, 1997

Robert Anderson
RAND

Tora Bikson
RAND

Tom Carty
GTE Cybertrust Solutions

Denise Caruso
Analyst, commentator, and journalist

Stanley Choffrey
General Services Administration

Jon Cook
U.S. Postal Service

Michael Danziger
MasterCard

Catherine Gay
International Advisory Group

Richard Graveman
Bellcore

Dan Greenwood
Commonwealth of Massachusetts

Jodi Heilbrunn
RAND

Allan Heller
Health Care Financing Administration

Stephen H. Holden
Internal Revenue Service

Tessa Kaganoff
RAND

Brian Kahin
White House Office of Science and Technology Policy

Normal G. Litell
Visa USA

Jessica Litman
Washington College of Law, American University

Scott J. Lowry
Digital Signature Trust Co.

David Lytel
Sherpa Consulting Group

Lloyd Morrisett
The Markle Foundation

C. Richard Neu
RAND

Jim Omura
Cylink, Inc.

John A. Phillips
Aristotle Publishing

Nick Piazzola
Verisign

Bob Reisner
U.S. Postal Service

William Polk
National Institute of Standards and Technology

Dick Rothwell
U.S. Postal Service

Damian Saccocio
America Online, Inc.

Maria Sanchez
RAND

Joyce Somsak
Health Care Financing Administration

Judith Spencer
General Services Administration

Hugh Stevenson
Federal Trade Commission

Peter Weiss
Office of Management and Budget

Joan D. Winston
Trusted Information Systems, Inc.

RAND

1700 Main Street, P.O. Box 2138, Santa Monica, California 90407-2138 • Telephone 310-393-0411 • FAX 310-393-4818

1333 H St., N.W., Washington, D.C. 20005-4707 • Telephone 202-296-5000 • FAX 202-296-7960

IP-178 (1998)