

DANIEL E. TURISSINI
PRESIDENT
OPERATIONAL RESEARCH CONSULTANTS, INC.
TESTIMONY BEFORE
THE SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
COMMITTEE ON GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

SEPTEMBER 9, 2003

Mr. Chairman and Members of the Subcommittee,

Thank you for this opportunity to appear before the Subcommittee to discuss issues relating to *Advancements in Smart Card and Biometric Technology*.

By the mere fact that this subcommittee is holding hearings on a topic such as Smart Cards and Biometrics, it stands to reason that the Government is truly focused on the requirement to ensure the integrity of sensitive or confidential information. As such, it is worth noting that this task is complicated by the fact that the same information to be protected must also be circulated among a limited, but frequently changing, audience of specifically named people. It must be provable who (by name, not simply office) the provider of a piece of information is and it must be provable that no one has modified the information subsequent to its issuance. There must be no question as to exactly when the information was published. There must be a means of reviewing the history of any particular document, in terms of who did what to it, and when, as it was developed and circulated. There must also be a means to archive all information securely as well as a means to recall the information from the secure archive at a later time. The systems and technology used to accomplish these objectives must be easy to use and suitable for senior executives, managers, and workers at all levels. Reliability must be very high. And there is a requirement for the system to support the mobility of some of its users. For speed and convenience, the system must be electronic, not paper. Taken individually, these are considerable tasks. Taken as a whole, they appear to require Herculean effort. However, appearances can often be misleading. This undertaking is achievable, the tools and technology currently exist, and some are already being leveraged by certain government agencies. Those available tools are Smart Cards for the storage of digital credentials (among other data) and Biometrics to achieve the highest certainty of credential protection.

With the events of today's society such as the information fog preceding September 11, 2001 and the recent virus attacks, there is an urgency to these requirements that permits little time for invention or development. The past several years have seen significant advancements in the development and production of smart card technology and biometrics has seen significant progress. Further, the integration of these technologies into legacy and current generation environments has grown correspondingly. Unfortunately, the policies and acceptance of these technologies have progressed at a

much slower pace. To a large degree, this resistance to smart cards and biometrics has been due to fears of the loss of privacy and images of “big brother.” Such fears are not without merit. However, such fears do not have to be realized if the proper approach, policies, procedures and education is proliferated.

The Goal of Security

Security by definition is “*something which guarantees or safeguards.*”¹ With regard to Information Systems Security, it is defined as: “*The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.*”² That which is to be guaranteed or safeguarded is primarily the information asset residing within an enclave, enterprise, database, desktop, laptop, etc. Thus, Information Security applies to anyone using a computer, PDA, cell phone, and so on. In other words, it applies to most everyone in American society today.

There are numerous facets to Information Security that wage a continual tug-of-war, such as protection, privacy, availability, and so on. There are also a plethora of less than ethical individuals using malicious code to wreak havoc on their target du jour, as well as the unsuspecting. The news recently was once again filled with reports of viruses and worms spreading to businesses and households alike. To quote a September 1, 2003 article by Chris Taylor of Time magazine, “*worms spring from the minds of virus writers, who could be sitting at any computer in the world. Most spread because we do careless things like open e-mail attachments from strangers, but some have evolved to spread through computer networks on their own — like plague bacilli that have become airborne.*”³

The key piece of Mr. Taylor’s article is the statement that “*we (people in general) do careless things like open e-mail attachments from strangers.*” This does not, and should not, have to be the case. The ease with which nefarious code writers proliferate malicious code is a travesty that does not have to be. Still, our Government has not taken advantage of the significant investment already made in digital certificate technology, a technology that can present an enormous roadblock to such worms and viruses as ‘Blaster’ and the ‘I love you’ virus, and the like. By embracing this existing infrastructure, transactions that do not originate from an entity authenticated with a credential from a known, trusted authority, can easily be discarded and we will all live to see another digital day.

The target we should all be striving for is to attain the highest level of security, without sacrificing availability to authorized parties, and without encroaching upon the civil liberties under which our country was founded and has operated for over two hundred years. Moreover, it is critical that we all understand that we cannot allow technology to

¹ New Concise Dictionary, Lexicon Publications, 1997

² Federal Information Security Awareness, *Definition of Information Systems Security*, Department of the Interior, National Business Center, Internet: http://www.doiu.nbc.gov/itsecurity/fissa/content/text_only/module1/topic2.htm

³ Taylor, Chris, *Attack of the World Wide Worms*, TIME Magazine, September 1, 2003

be the driving force behind the policies governing their use. Instead, it must be common sense, sound policies and prudent laws that dictate how technology can complement and augment the safeguards and protections already in place. Too often, a new technology is devised and we make the mistake of compromising our processes and procedures so that the new technology can be used. This is analogous to building a brand new automobile in order to properly accommodate a newly invented radio. If the radio cannot be produced so that it can be integrated with an automobile, it must not be a *car* radio. If a technology or device requires the comprehensive reconfiguration and reconstruction of the existing resources, policies and procedures, it is not a proper fit.

Privacy issues

It is with good reason that most people in the today's society are skeptical of a universal identification card that contains vital personal information. Or, that they have fears of their personal data residing in a database somewhere that can potentially be 'hacked' into, causing their data to be compromised. Unfortunately, in the haste of the Internet boom vast amounts of personal data were willingly and/or unwittingly made available by individuals themselves, marketing groups, businesses, even some Government agencies, and a whole host of others. Now, we are left with trying to lock-down as much as possible while simultaneously reeling back in that which has escaped. Society's collective sense of being jaded by the Internet is quite well founded. However, the Internet was never intended to afford privacy to anyone. Quite to the contrary, the Internet was devised for the **open** sharing of information to anyone and everyone with a connection. Nonetheless, this is the state we are currently in, and some measure of privacy is still attainable.

Properly managed digital credentials can provide the additional security needed to afford all parties a high level of confidence that individuals attempting access to resources are who they claim to be or that the actionee of a transaction can be identified and non-repudiated. This can be achieved without compromising or infringing upon the privacy of the individual. It is simply a matter of adhering to established standards, policies and procedures to enforce the proper use and integration of the technologies, and laws to provide the requisite ramifications for transgression.

Smart cards and Biometrics

Smart cards afford an obvious benefit, mobility. By possessing a credential that can authenticate that an individual is who they claim to be, regardless of where they are, is highly beneficial. This un-tethers the individual from the desktop or laptop and frees them to move from station to station. And because there are such requirements within the Federal Government such as FIPS (Federal Information Processing Standard) to ensure such functionality as the token being tamper proof, for example, among other requirements, the level of assurance can remain consistent. However, with digital transactions smart cards are only as effective as the credential the card is protecting.

Biometrics provide a uniqueness of the persons identification, ‘something you are.’ Advancements have led to the ability to distinguish an individual by their fingerprint, voice, face, eye, entire body, and more. More importantly, devices are being developed that can use multiple biometric ‘signatures’ to exponentially increase the accuracy of identification and decrease the possibility of a ‘false positive’ or incorrect identification.

With both smart cards, as mentioned previously, and biometrics, legal non-repudiation is challenged because digitally there is no difference between the credential presented and the one stored for comparison. However secure, if the credential or the biometric ‘signature’ resides in a database, someone other than you has access to your credential. To extend this legal argument further, it is not necessary to prove that someone *did* or *did not* have access to your credential or biometric data. But rather, *could* someone, such as an administrator, have accessed your data? Or even the reverse of that argument, is it a categorical impossibility that no one other than the owner of the data had access to it? This is why the policies, guidelines and laws play such a critical role. Each piece of the equation, the card, the reader, the biometric, the credential, policies, the consequences, are all an equally important factor to the sum of the security solution.

For instance, with symmetric key generation the owner of the credential must know or have contact with all those in the community with which they are presenting their digital credential. This is because they must share their credential with that person and that person must subsequently ‘recognize’ that credential as being from its appropriate owner. This quickly becomes an arduous process when dealing with a community of any substantial size. To solve this issue, we must look beyond the physical and think in the “digital dimension.”

Asymmetric key technology offers both identity assurance and privacy. An individual’s identity is represented by a key pair. Properly managed, the private key is created and retained by the owner and only by the owner. The public key is then freely distributed to a public repository(s) where it can be accessed by anyone known or unknown. Despite being based on complex cryptographic technology and mathematics, the user experience is quite simple. To identify one’s self, the individual applies an algorithm using their private key and presents the result, a ‘hash.’ At the other end of the transaction, an algorithm is applied using the individual’s public key. If the resulting hash matches, the recipient can be assured of the identity of the initiator, and knows that the transaction was not altered or tampered with between the time it was created and the time it was received.

In a vast community of users such as the Internet it is much more feasible to leverage asymmetric key technology where distribution and retrieval of public keys can be readily achieved, and the protection of the private key can be managed to the level of assurance desired and that technology permits. The Internet can be used as it was designed, for the **open** sharing of information without the loss of protections or privacy.

Implementation

Federal agencies must lead the implementation of meaningful and efficient security into Internet/ Intranet operations to protect sensitive information and billions of dollars in transactions each day, as well as the privacy of its citizenry. A digital credential acquired from a certified “trusted third party” recognized and accepted both internally and externally as trustworthy is the front-runner to achieve these requirements. Once adopted, increasingly mature internal policies can be developed to ensure only those designated as authorized can gain access to resources while facilitating expedited secure communications with partners, vendors and citizens. And, equally important, the advancement of technologies such as smart cards and biometrics can be focused on enhancing existing security tools to ensure to a great degree that the individual presenting his or her self is, in fact, who they claim to be. Combined with asymmetric key technology, smart cards *and* biometrics provide ‘three factor’ protection of that digital credential.

- Something one knows, (pin or a password);
- Something one has, (smart card); and
- Something one is, (biometrics).

As the factors of the credential protection increase, so too does the assurance level that the individual is who they claim to be. Conversely, the probability that the individual is being ‘spoofed’ or mimicked by an intruder or interloper decreases.

The Department of Defense (DoD), as Mr. Scheflen has stated/will state, has been rapidly deploying the DoD Public Key Infrastructure (PKI) for the exchange of unclassified information leveraging smart card technology in the form of the Common Access Cards, and has piloted an external certificate authority (ECA) or trusted third party. Further, to meet the objectives of Federal-wide interoperability, the Defense Information Systems Agency has established a Federal Bridge Certificate Authority (FBCA) compliant commercial root which holds a non-agency specific Government OID (object identifier). This “Government commercial root CA” has been established to sign the subordinate ECAs. Additionally, the General Services Administration (GSA) has established the Access Certificates for Electronic Services (ACES) program, an infrastructure poised to provide digital certificates to the citizenry for use with various Government services such as Social Security Administration, Health and Human Services, etc. These infrastructures represent a prime example of best practices for ensuring authentication, confidentiality, data integrity and non-repudiation via digital certificates employing smart card technology.

Summation

The technologies necessary to attain digital security in our open society are available. Asymmetric credentials fully support non-repudiation and ensure user privacy coupled with multiple levels of credential protection based on the requisite security need. In more simple terms, providing each citizen the means by which they can authenticate themselves using something they know (password), something they have (smart card), and something they are (biometric) can begin today. Further, this does not have to be

done at the expense of anyone's civil liberties. However, to do so we must embrace the technology available today and continue to evolve these technologies as advancements emerge and technologies mature. The infrastructure to mitigate much of the risks associated with digital transactions is fielded. With your support, the ACES, DoD PKI, and DoD ECA programs can be embraced to avoid many of the problems that stand in the way of the President's eGov initiatives. Instead of continually reinventing the mousetrap, we need to use the mousetrap we have and continually enhance that trap to remain one step ahead of the mice. Through proper integration and configuration, security can be achieved and inalienable rights protected. Leveraging these technologies is not a panacea. It is an achievable undertaking that will "provide for the common defense, promote the general Welfare, and secure the blessings of liberty to ourselves and our posterity."⁴

Thank you for your time and the opportunity to present a viewpoint into this extremely important issue.

⁴ The Constitution of the United States of America