Strategic Tasks for Government in the Information Age

Financial Cryptology Conference 1997
Anguilla, BWI
February 24-28, 1997

Presented by
Paul Lampru (Paul_L2@verifone.com)
Strategic Marketing for Electronic Commerce and Security
Financial, Healthcare and Government Markets
U.S. Division, VeriFone, Inc.

(The ideas expressed in this paper are those of the author and
do not necessarily represent those of VeriFone, Inc.)

Introduction

Today we are participating in a sea-change that may equal or exceed the social and economic impact we experienced when we transitioned from an agrarian economy to an industrial economy over one hundred years ago. Clearly government officials recognize the enormous opportunity this transition offers to dramatically reduce the cost of government services while improving their quality. As companies rapidly switch to information-based businesses, government support, leadership, and vision are needed to accelerate and guide the development of a commercial/government infrastructure that will support a new economy.

We should carefully consider the answers to several important questions before applying government's influence to support and channel the construction of new global economic and social infrastructure so that it serves our national interests.

- What is the driving technology force behind this paradigm shift to an Information-based economy?

- What are the key elements that might facilitate this transition?

- What are the dynamics of this shift?

Answering these questions could help shape government strategies to ensure that new "digital factors of production" are used to benefit national and global interests well into the next century. This paper proposes answers to these questions and presents ideas that might contribute to the development of an Electronic Commerce infrastructure in the United States.

Payment Technology Driving Forces

Beginning about 1994, two new electronic commerce forces started driving the U.S. toward the next generation of payment systems. The first force is a global push to replace magnetic stripe payment systems with chip card systems. The second is the development of the Internet for Electronic Commerce (EC). Two advocacy camps formed around each of these technology forces. Neither camp viewed the other as a potential competitor or rival; perhaps their attitude toward each other was benign indifference.

One camp aggregated around the Smart Card Forum and the second around CommerceNet and the Financial Services Technology Consortium (FSTC). For a year or so there was little interplay between these two camps. The Smart Card Forum focused on smart card applications for stored value, medical records, loyalty, etc. CommerceNet and the FSTC focused on developing technologies for Internet commerce and payment systems. In 1994-1995 it was difficult to tell if either or both camps would be successful.

Today it is clear which payment technology is the driving force. While chip card applications are under development around the world, the deployment of Internet/Intranet-based EC applications is exploding. Internet payment schemes are rich with diversity and imagination. There is no doubt the Internet is the driving force behind our movement toward the Information Age, and the next generation of payment technologies. Therefore, we should reflect on the fundamental reasons the Internet is growing exponentially while the movement to chip card applications (for example, Store Value Cards) is not moving as rapidly. Understanding the potential insight that could be gained from a careful study of the reasons for the unprecedented expansion of one camp compared to the other is important before developing government policies and allocating resources.

Payment Technology Driving Forces:
Stored Value Card Pilots

There are a number of reasons chip cards and particularly SVC applications are still under pilot development in the U.S. The reason that is perhaps the most fundamental is summarized below.

Open Chip Card systems are at a competitive disadvantage when marketed toward consumers who have wallets with well-entrenched ubiquitous magnetic stripe payment alternatives, and when they are based on a single proprietary application—primarily reloadable SVC applications—using proprietary networks.

It seems clear that a single application, especially one based on a proprietary network and on a proprietary payment scheme, will have great difficulty in generating enough profits to cover the cost of its infrastructure. The SmartCash lessons from the Atlanta Olympics pilot could be interpreted to support this hypothesis as well as other hypotheses that try to explain why this SVC pilot was not expected to be a profitable venture.

Payment Technology Driving Force:
Open Public TCP/IP-based Networks

The Internet is a fundamentally new communication platform that embodies the functionality of all the communications technologies ever developed. Examples of communications functionalities include the transport of handwritten words, printed words, digital words, voice, video, multi-media, hyper-media, etc. using one-to-one, one-to-many, many-to-one, and many-to-many communications technologies. In the history of modern communications, advances span decades, with each major technology having a tremendous impact on society. Today the functionality in virtually all the communications technologies ever developed is hitting our society at one time, embedded within an open, public TCP/IP-based network. Clearly, if each major communications technology developed during the last several hundred years has impacted our society in historically significant ways, the combination of all communications technologies hitting our society simultaneously is unprecedented.

Although the Internet is the driving force, chip cards and reader/writers (R/W) have an essential, albeit supporting role for EC over the Internet. Basically chip card technology can provide a portable, non-duplicable electronic token system to securely hold an individual's Private Key and Public Key Certificate (PKC). This token enables individuals to digitally sign electronic documents without being tied to a single computer. To the Smart Card Forum this is an "access" application. Within the context of Mastercard and Visa's SET protocol VeriFone refers to the chip card and R/W as PayPort^{tm}.

If PayPort^{tm} could be adapted as a Stored Value Card (SVC) system used to reload electronic cash at home using an Internet-based E-cash scheme, it is reasonable to believe that this platform could become a foundation for an even wider variety of chip card-based applications. For example, the PayPort^{tm} with a PKC could be used by patients, doctors, nurses, pharmacists, etc. to digitally sign electronic healthcare forms or to access healthcare records. It could be used to electronically vote or pay income taxes. Welfare recipients could be issued a chip card to download Food Stamps value into a SVC purse at an Internet kiosk. Grocery stores and merchants using "PayPort^{tm} terminals" at countertop could accept electronic cash and electronic benefits using the same Internet terminals that consumers use for cashless payments. In this scenario the PKC could evolve into a universal identification card enabling its owner to digitally sign electronic documents that were legally enforceable or to initiate payment transactions, business transactions, medical transactions, or educational transactions, etc.

Rapidly shifting to an open information-based, fully-interconnected digital society will enable countries to obtain an international strategic competitive advantage over economies that partially move toward open network systems or ones that continue to be based on proprietary networks. For example, consider the structure of the U.S. economy today. Although it is technologically advanced, over the long term it could not compete successfully against a fully-interconnected "digital economy". A simple comparison of the cost structures associated with operating and maintaining a "physical-retail" business connected by proprietary networks compared to a "virtual-retail" business connected by public networks suggests today's business models will be progressively disadvantaged. Nicholas Negroponte discusses this idea in terms of an economy based on "atoms" and one based on "bits" in his book, *being digital*. If this perception is true, then commercial and government support for the development of public networks (such as the Internet) should continue to be a national economic priority.

Open Public TCP/IP-based Networks

Key Elements

The potential of the Internet is far too important for government to passively monitor commercial developments, waiting for inequities, before using its influence. The Federal government can and should develop a national strategy that does not curtail commercial innovation but one that balances potential benefits between the public interest and private enterprise's profit potential. Such a strategy should be based on a Vision or an optimism that points our society toward the highest and best use of this new communications infrastructure. If the Internet is the driving force behind this paradigm shift, then focusing on the following four key elements might help government harness the Internet and lead to the formation of a national strategy:

- public key cryptology

- a national (commercial) public key Certification Authority infrastructure

- individual control and "privacy" of personal information in commercial databases

- chip card technologies

A discussion of the importance of each element follows.

Key Element:
Public Key Cryptology

The greatest value of the Internet is that it is a global, open network that provides ubiquitous connectivity; but this fact also makes the Internet worthless for Electronic Commerce without “security”. If there is a single “security” technology that extends across the spectrum of human interactions and stretches into the next century, it is Public Key Cryptology. The need for spontaneous, remote, non-refutable, and secure communications over the Internet cannot be achieved as completely or as elegantly by any other single technology. Public Key cryptology is one of the lowest common denominators for secure communications over public or private networks. By using a sufficiently large number of bits in the “Private Key”, communications over any network can be absolutely secure from a “brute force” attack on keys. For the vast majority of transactions, the use of public key cryptology for routine personal communications is analogous to using a battleship to escort a sailboat over open seas.

The potential value of public key cryptology to society could extend far beyond just securing the day-to-day Internet transactions for citizens, businesses, and governments. The full potential of public key cryptology lies in its dependency on a public key certification authority infrastructure. This dependency is also its Achilles’ heel. Consequently, a fundamental goal for government should be to ensure that the infrastructure for Public Key cryptology reaches its greatest potential value to society on an international scale. An argument to support these assertions follows.

Key Element:
National Public Key Certification Infrastructure (NPKCI)

Since Public Key encryption is extremely secure when key lengths are over 1024 bits, we should recognize that it is not the weakest message security link and focus our efforts on a much weaker link----the NPKCI. Today it is not clear how our Certification Authority (CA) infrastructure will inevitably organize itself. Competition and short-term revenue objectives are unduly influencing the evolution of the CA infrastructure. For instance, should the MasterCard and Visa CA architecture for issuing certificates linked to credit card numbers be a universal model for other certification applications? It is certainly appropriate for securing credit card transactions over the Internet. But does this suggest that every special application should construct a special purpose way to issue certificates? Is there not a common set of functions that certificates provide for all applications? We need a consensus on a common set of services which a National PKCI must provide to the Internet community in the broadest sense. Considering these common elements, a collective long-term vision for a national Public Key Certification architecture should emerge.

A simple vision for a NPKCI is that it should be based on a viable business model capable of providing low cost PKC to every person while minimizing the opportunity to fraudulently obtain a PKC. It should enable CA to establish reasonable and explicit liability limits. It should assure citizens and businesses that digitally signed documents will be upheld in a court of law. It should increase personal control and access to private information stored in third party databases. To achieve this set of goals the key component to manage is the design of an NPKCI. Since it must be based in law, it is important that government authorities monitor, influence and reinforce its ultimate architecture.

National Public Key Certification Infrastructure (NPKCI)
PKCI Architectures

There are at least two extreme architectures upon which a Public Key Certificate Infrastructure (PKCI) could be based—a "fully-distributed" architecture and a "hierarchical" architecture. A fully distributed architecture is one in which any organization may issue a Public Key Certificate (PKC) without cross certification. Under this model the PKC is useful "locally". A hierarchical CA architecture is one in which a single organization is the root for all Certificate Authorities. This model is inflexible and may not be achievable. While neither of these two extremes are practical, they are useful for framing alternate architectures. This paper proposes ideas for a hybrid National PKCI based on the elementary functions that a PKC provides.

National Public Key Certification Infrastructure (NPKCI)
PKC Elementary Functions

A PKC provides at least two elementary functions. First, a PKC provides personal identification so all parties may identify each other before a transaction is finalized. Second, a PKC can be used to authorize an individual to have certain "privileges", such as access to a bank account, authorization to purchase something, or permission to act on behalf of another. A PKCI organized around these two functions (that is, identification and authorization) would recognize two types of PKC—an Identification Certificate (ID-PKC) and an Authorization Certificate (AU-PKC).

For example consider an architecture where an individual's ID-PKC, not the CA is the "root" or the center of focus. Granted, an individual's certificate and a CA are not similar; but the idea is to create a hybrid hierarchy based on the ID-PKC—not the CA. This paper briefly describes how such an architecture might be organized and operate.

National Public Key Certification Infrastructure (NPKCI)
Maximum Identification Liability (MIL)

An ID-CA issues an ID-PKC (X.509) in accordance with its Certification Practice Statement (CPS). However, the ID-PKC includes a new data element called the "Maximum Identification Liability" value. The MIL establishes the ID-CA's maximum liability for guaranteeing that the information contained in a certificate correctly identifies an individual and the associated Public Key. An ID-CA may establish different liability limits for each individual.

In the event the ID-CA issues a certificate erroneously, the ID-CA is contractually bound to compensate a business for any loss it incurs as a result of the error up to the Maximum Identification Liability limit, as long as that business had "registered and linked" with the ID-CA before relying on that certificate. (See "ID-PKC Registering and Linking" below for an explanation of these terms.)

National Public Key Certification Infrastructure (NPKCI)
Credit Risk

Merchants and other parties dealing with consumers are always faced with credit risk, the possibility their customers will not repay a loan or a line of credit. Businesses reduce credit risk by obtaining a consumer's payment history. Three national credit bureaus in the United States provide consumer credit reports upon receipt of an electronic request containing information which uniquely identifies that consumer. Usually a business obtains ID information directly from the consumer when he submits an application.

A credit bureau uses the ID information transmitted by the business to retrieve that consumer's credit report from a database that may contain as many as 150 million credit report records. Often more than one credit report may match the criteria supplied by a business. In this case, multiple credit reports may be returned to the requester who must decide which report is related to his customer. The business—not the credit bureau--is responsible for properly identifying the consumer.

National Public Key Certification Infrastructure (NPKCI)
Identity Risk

Identity Risk is the risk that an ID-CA might issue an ID-PKC to an impostor or simply issue an ID-PKC in error even though it followed its CPS procedures carefully. Consequently, any business that relies on an ID-PKC may be entitled to recover losses attributable to an erroneously issued certificate—up to the Maximum Liability Limit (MIL) offered by the ID-CA. The MIL is a form of insurance that reflects the ID-CA degree of confidence that the information in the certificate correctly identifies the individual.

National Public Key Certification Infrastructure (NPKCI)

Residual Identity Risk

Before an Internet merchant establishes a relationship with a new customer, the merchant would use the value in the MIL field to calculate his "Residual Identity Risk". The Residual Identity Risk is simply the difference between the goods or services offered by a business and the Maximum Identification Liability offered by the ID-CA. If the Residual Identity Risk is too large, the merchant must decide either to accept that extra risk or require additional identification information. Here business rules could manage the merchant's Residual Identity Risk. In this way a merchant selling books might enter into a transaction with a potential customer based solely on the individual's ID-PKC. On the other hand, a merchant selling computers might require more identifying information than just the individual's ID-PKC.

National Public Key Certification Infrastructure (NPKCI)

ID-PKC Registering and Linking

The Maximum Identification Liability value offered by the ID-CA is a form of insurance. Consequently, a merchant must apply for this insurance and be accepted before the ID-CA can be held liable for subsequent losses. Requesting ID-PKC insurance is strictly at the option of the merchant. A process called "registering and linking" describes procedures to apply for ID-PKC/MIL insurance. The following are the five steps to "registering and linking".

1. The business checks the ID-CA's Certificate Revocation List (CRL) to verify that its customer's ID-PKC is still valid.

2. The business registers itself with the ID-CA by establishing a "tradeline" linked to the customer's ID-PKC. The "tradeline" is a credit industry term for the list of businesses on the credit report with whom a consumer has established relationships.

3. The ID-CA accepts a business's request for Identification insurance. For example, the ID-CA might establish risk management procedures to control the total value of its exposure for each new ID-PKC it issued or registered. If the ID-CA's cumulative risk limits are exceeded, the ID-CA might decline a request.

4. The ID-CA automatically establishes a "push" notification system to alert businesses with an established tradeline when the ID-CA determines an ID-PKC must be revoked. If a new ID-PKC replaces a revoked ID-PKC, this information is also pushed to all businesses with a tradeline. This procedure minimizes the need for a merchant to check the Certificate Revocation List (CRL) before

completing each transaction with a customer. The CRL is checked on the first transaction only.

5. The business who registers and links to an ID-PKC pays a fee similar to an insurance premium to the ID-CA.   There may be other types of fees, too.

National Public Key Certification Infrastructure (NPKCI)
Hypothetical Issuance of an ID-PKC

An ID-CA receives an application for an ID-PKC from a consumer. The ID-CA uses its Certification Practice Statement (CPS) and operating procedures to verify the identity of the individual. Considering the degree of confidence that the information in the application correctly identifies the applicant, the ID-CA establishes its Maximum Identification Liability (MIL) value and includes this value in the ID-PKC issued to the applicant.

Depending on the information an individual is willing to provide and the ability of the ID-CA to verify that information—either electronically or by physical presence, the ID-CA Maximum Liability Limit may differ by individual. It is important to note that the liability limit is related to only the *identity* of the applicant and has nothing to do with the applicant's credit risk, social status or national citizenship. This structure assumes every person has a universal right to obtain—or not to obtain—an ID-PKC from any ID-CA, irrespective of the individual's national citizenship or the business's national registry. Thus a citizen of any country could obtain an ID-PKC from any ID-CA. By accepting an ID-CA certificate the individual accepts the ID-CA governing rules disclosed during the application phase. Such rules might state the legal jurisdiction where disputes will be resolved.

National Public Key Certification Infrastructure (NPKCI)
Government Digital Signature Accreditation

If an authorized government agency reviewed an ID-CA's CPS and operating procedures and found they met "best practices" standards, the ID-CA could be granted a government "Digital Signature Accreditation". Such an Accreditation would insure that an individual's digital signature—created with a certificate from an accredited ID-CA—would be upheld in a court of law as a handwritten signature. In this situation the government authority would enforce a person's digital signature and, by implication, would be providing another "guarantee" that the ID-PKC was properly issued.

By granting a Digital Signature Accreditation the government would augment the ID-CA Maximum Identification Liability with the threat of criminal penalty for a person who obtained an ID-PKC by impersonation or by theft. It would be treated as another form of forgery. If appropriate, a court might find the impostor was personally liable for all damages that exceeded the ID-CA Maximum Identification

Liability amount (that is, the Residual Identity Risk). In any event, granting an Accreditation to an ID-CA would mandate a penalty fee the ID-CA would pay if it issued a fraudulent certificate even though it followed its CPS procedures.

National Public Key Certification Infrastructure (NPKCI)

Authorization Public Key Certificates (AU-PKC)

A Public Key Certificate (PKC) could be issued with or without an identification “guarantee” or MIL. An example is the MasterCard and Visa PKC that may be used to sign an Internet credit card purchase only.

An AU-PKC is a special type of PKC which is “registered and linked” to an ID-PKC as described previously. The AU-CA issues an AU-PKC to its customer to grant local privileges.

One of the primary uses for the ID-PKC is to enable a customer to digitally sign electronic applications for “membership” where the applicant’s identity must be established before services will be extended. For example, a consumer wants to apply for an electronic bank account. The bank requests that the customer complete and digitally sign an Internet home banking application. The consumer uses his ID-PKC to apply for an AU-PKC. Much of the information in the application is copied to the home banking account application enabling the customer to add only a minimum amount of information. The bank no longer needs to verify the individual’s identity. The bank would simply “register and link” the bank’s AU-PKC certificate to the ID-PKC thereby transferring Identity Risk to the ID-CA up to the MIL value.

If the ID-CA is accredited by the state to issue legally enforceable digital certificates, the AU-CA would have a government assurance that the potential customer is correctly identified. This assurance is based on the threat of criminal prosecution if the customer obtained an ID-PKC using false information.

Finally, if the AU-CA found these two levels of assurances insufficient, the AU-CA could begin any identification procedures it believed were necessary.

National Public Key Certification Infrastructure (NPKCI)

AU-PKC Revocation

Since the AU-CA grants privileges, it may withdraw those privileges by revoking its AU-PKC and posting that information to its Certificate Revocation List (CRL). Before revocation the AU-CA would send a “Closed Account Confirmation Notice” (CACN) to the customer with a reason his AU-PKC was revoked.

In addition to notifying the customer, the AU-CA would notify the ID-CA that its relationship with this customer was closed. At its option the AU-CA may include a reason the AU-PKC was revoked. When the AU-CA provides a reason for revocation, the ID-CA records and links this information to the individual's ID-PKC.

Occasionally an AU-CA may be forced to close a customer's account unilaterally for administrative or for punitive reasons. If the account was closed for punitive reasons the customer may elect to refute or to explain his side of the story. In this case the customer would send an electronic copy of the CACN to the ID-CA with his digitally signed rebuttal. The ID-CA would link the rebuttal to the original CACN and the individual's ID-PKC.

National Public Key Certification Infrastructure (NPKCI)

Privacy Control for ID-PKC Linked Information

Anyone with a ID-PKC has a right to obtain a copy of all ancillary information (that is, "tradelines", CACNs, etc.) that might be linked to his ID-PKC. He could do this by digitally signing a request form and sending it to the ID-CA. For instance, an individual may want to review information about himself periodically to make sure it is accurate and complete. Any changes an individual believes are necessary are digitally signed and sent directly to the ID-CA for review and action. The ID-CA decides if the requested changes should be made. In any event, the ID-CA replies explain all actions taken to the consumer. Finally, if an ID-CA has any information related to an individual's ID-PKC, that individual should have the right to require the ID-CA to "lock" his data record to prevent any information from being disclosed without his digitally signed authorization.

Assume for a moment that an NPKCI is based on the architecture discussed above in which a citizen is issued an ID-PKC. Furthermore, assume that the healthcare industry, as an example, constructs patient health record databases accessible over the Internet. Consider in this scenario that citizens have the same degree of privacy with their health records that they have today with their credit reports. Privacy rights groups and consumers will rightly perceive a significant erosion of "privacy" if cyberspace databases use the ID-PKC as the common link between all the electronic activities of an individual.

National Public Key Certification Infrastructure (NPKCI)

Privacy Controls for ID-PKC Linked Information

Government's Role

It seems appropriate that government should proactively influence the design of an NPKCI so that it encourages businesses to protect consumers' privacy. To accomplish this it is important that the public and private sectors work together to design NPKCI that increases a citizen's privacy and access to personal information. A government-industry goal should be to balance a consumer's right to privacy with a consumer's need to provide voluntarily and selectively personal information to businesses and government agencies before being authorized to receive benefits and services. If we can define an NPKCI infrastructure that is balanced in the eyes of the public and businesses, then a source of bitter contention could be mitigated to some degree. One possible way to achieve this balance is proposed below.

National Public Key Certification Infrastructure (NPKCI)

Privacy Controls for ID-PKC Linked Information

Direct Control of Private Information

Assume for purposes of discussion that a person's ID-PKC is linked to an AU-PKC. Assume the AU-PKC is linked to his personal healthcare database record stored in an Internet-accessible database. In this scenario the Trusted Third Party (TTP) database operator could offer a patient an Internet database location where he could store his personal healthcare records. The TTP database operator would warrant that no information contained in his patient record could be released without the patient's digitally-signed authorization message. As compensation the database operator charges the patient (or HMO, etc.) a storage fee for holding this information. Perhaps the database operator also charges a fee to a business or government agency the patient authorized to retrieve information.

In this scenario a patient would fill out an electronic form to give a doctor access to specific information in his electronic patient record. When the doctor needs to retrieve this information, the doctor digitally "endorses" the patient's authorization form and submits the request to the TTP database to obtain the information. A patient has absolute control over who has access to his medical records as well as the right to view his personal records over the Internet. This NPKCI business model provides any degree of privacy a consumer desires while enabling global access to his health records. In the general case the individual is able to directly authorize a business to retrieve only the information required to provide the services and benefits requested.

Key Element:

Chip Card Related Technologies

To generate a "digital signature", a secure, easily carried electronic token, such as a chip card or similar device, will be needed to hold an individual's Private Key and Public Key Certificate. Assuming the token is a chip card, there will be a need for chip card readers/writers wherever individuals need to digitally sign Internet transactions and documents—for example: a consumer's home, a doctor's office, a business or government office, a public phone, an Internet-connected kiosk, etc.

The consumer's home PC is expected to be the first place digital signatures will be generated in large numbers. Mastercard and Visa intend to use Public Key digital signatures to authorize credit card payments over the Internet. In any event a joint industry-government strategy is needed to encourage the long-term proliferation of chip card related technologies into consumers' homes, into businesses, and eventually into public sites for those without computers.

Dynamics of this Paradigm Shift

A clear understanding of the dynamic forces engaged in the shift to the Information Age is important before launching any significant government initiatives that might influence the competitive marketplace. While it is natural to focus on the push and pull between Microsoft and Netscape "battles", this should not cloud the government's perception of more fundamental opposing forces. The government's concern should be directed toward managing the transition from today's infrastructure to tomorrow's infrastructure. This battle is between old and new, status-quo and change. More specifically, it is the battle between the movement from Private Networks to Public Networks, from paper-based systems to electronic systems, from magnetic stripe payment technologies to chip card related payment technologies, from an economy of middlemen to an economy with fewer middlemen. It is the management of a paradigm shift taking place today that should be a primary focus for government. If there are realistic ways to manage a paradigm shift of the scale that appears to be happening today, perhaps one of those ways might be to construct a Vision of an ideal future.

Summary

There are a number of most important ideas presented in this paper. Foremost is that the Information Age is Internet-centric. Other technologies need to find their niche within the Internet. Proprietary networks may have special purpose uses, but their value in an open, public networked world will be somewhat reduced from the critical role they play today. The application of government resources should carefully but methodically accelerate the movement away from systems that use proprietary networks.

Another important idea is that the creation of a National Public Key Certification infrastructure is critical to realizing the full potential of the Internet. Today we seem to be constructing Certification Authorities that issue single-purpose certificates. We need a National Public Key Certificate infrastructure built around the ID-PKC and the AU-PKC.

It is certainly possible that the ID-PKC could evolve into a "national identification number" with all the Big Brother implications. Therefore, it is critical that we design features and privacy laws that prevent undesirable uses of the ID-PKC while allowing us to benefit from the enormous transaction efficiencies such a system might provide.