

Other PIV Card Uses

Dr. Russell J. Davis, PMP
Femtosecond Inc.
9747 Water Oak Drive
Fairfax, VA 22031-1029

Abstract

Executive branch agencies and departments are investing in Personal Identity Verification (PIV) technology. This paper explores a number of current and evolving security risks and discusses how the PIV technology could be used to reduce overall risk. This paper presents an overview of the threats to electronic commerce, a discussion how the PIV infrastructure could be expanded to reduce security threats, and describes some of PIV components. While there are other security solutions to these problems presented, the focus is limited to PIV. One threat expanded upon, identity theft, is so successful due in part to our relaxation of Identification & Authentication (I&A). We trust a Social Security Number (SSN) or a credit card number with little proof that the owner of this information is the party we are communicating with. By incorporating strong I&A, and making privacy decisions predicated on the strength used in determining I&A, the value of unauthenticated confidentiality information will deteriorate.

Forward

Security controls that operate within the same memory space have the potential to be bypassed [1]. With the number of large corporations falling victim to hacker attacks, one must ask if the current security controls are adequate. The large corporations that are known victims certainly have significant security control investments. Yet, bad actors continue to find ways to exploit weaknesses. Many security problems stem from the basic design principles used in developing systems and applications [2].

Not long ago, SSNs were on personal checks, military discharge certificates, and driver's licenses. Yet identity theft was not the threat that it is today. What has changed? In the past, just knowing an SSN and other confidentiality information was not enough to steal an identity. In contrast, today this information makes obtaining credit terribly easy. If in addition to knowing a name, SSN, date of birth (DOB), and other identifying information, strong I&A was required for obtaining credit; then the value of the confidentiality information would be reduced. In this paper, the PIV is examined as a candidate technology for implementing strong I&A.

The PIV comes at a time when the National Intelligence Reform Act (NIRA) requires a common

driver's license format. Within congress pending legislation, such as H.R. 418, if enacted, will require minimum standards for issuing driver's licenses to include a machine readable capability. If the driver's licensing efforts can utilize the technology and infrastructure deployed to support PIV, then we could have a basis for mitigating many of the threats to information assurance and e-commerce. The benefits and challenges needed to combine the State and Federal identity efforts are presented in this paper.

Introduction

On-line commerce continues to grow in use and importance. The e-commerce potential to grow is inhibited in part due to consumer's fear of security threats [3]. This fear is compounded by evolving security threats that threaten the ability to maintain e-commerce. This paper describes some of the challenges and explores how PIV technology could be promulgated outside of government to help citizens.

To better appreciate what is at risk, consider the Great Depression. By most accounts, the Gross National Product (GNP) fell from by over 40%, from 1929 to 1933. Unemployment rose to over 25% of the workforce. And the Great Depression lasted over 10 years. Examples of government regulatory oversight established in response include the Federal Deposit Insurance Corporation (FDIC) in 1933 and the Security and Exchange Commission (SEC) in 1934. We have seen the stress placed on government spending whenever there is an economic downturn. Programs are cut or delayed and debt increases. Inevitably, military spending usually takes a disproportionate budget cut when compared to programs such as Social Security. And we have seen the impact of reduced military spending as we try to fight the war on terrorism on multiple continents. Is not an objective of our enemies to reduce our war fighting capability and does reducing military spending not effectively achieve this goal? One question is can a cyber attack effectively cause another Great Depression? If so, how would we fund our homeland security, war on terrorism, and military expenses?

Consider that the FDIC requires insured banks to maintain a certain reserve for failed loans. It uses the Bank Insurance Fund (BIF), Savings Association Insurance Funds (SAIF), and Available for Sale (AFS) investment portfolios to cover bank

failings. If a serious cyber attack resulted in significant losses, would these safeguards be sufficient? In the next session, we will look at some known exploits and further the argument that actual losses and overall risk is greater than recognized.

The Dangerous Landscape

The technology we use to automate our business practices now accommodates unscrupulous bad actors presenting them with new ways to extract profit from their crimes. Moreover, given the number of prosecutions versus successful attacks, the bad actors appear to be gaining the upper hand. If e-commerce is to continue, customers and businesses must have confidence in the security provided. To recognize the importance of consumer confidence, one need only recall the newsreels showing the hollow faces standing in line to withdraw their bank funds following the '29 stock crash. Perhaps the most important goal any financial regulatory agencies offer is to ensure consumer confidence is safe and sound. This confidence must be preserved in light of ever changing technology.

Typically, improved controls are applied only after a significant loss. For example, the Rifkin *Fed Wire* transfer scam [4] that precipitated tighter security controls being applied to Fed Wire. Today, we would look at old *Fed Wire* controls then in place as inadequate. However, the new controls were only put in place following an incident. Reacting to incidents rather than proactively preventing them seems to be the most common approach to security.

A continuing security challenge is to predict what controls can be applied that will lessen exposure to evolving threats. For example, with the advent of automatic teller machines, banks have discovered a cheaper, faster, and arguably better method for providing service to customers. Since their inception, additional controls, such as security cameras were deemed necessary. Still, the ATM model has proved successful, in part because users are required to access a physically controlled ATM machine, possess a valid ATM card, and must know their personal identification number (a.k.a., a PIN or password). Compare this with the losses incurred with credit card fraud. Many of us know people who had a credit card used for fraudulent purchases. But how many people know of a person victimized using the ATM?

So how do credit cards and ATM cards differ? In general, the mere presenting of a credit card to a vendor is usually enough to authenticate a transaction, without requiring additional information from a customer. But two separate and distinct steps (possession of the card and a valid PIN) are required

to validate an ATM card transaction. In this example, the ATM card used two-factor authentication while the credit card uses single factor. These examples provide an idea of the challenges that confront the electronic banking and e-commerce.

For electronic banking, the first significant difference is the media that information traverses. In the case of credit cards, the store typically uses a phone or data connection to transfer information. With e-banking and e-commerce, the Internet is typically used to communicate information. So how safe is the Internet? Robert T. Morris Jr. [5] first demonstrated to the world just how connected (and vulnerable) the Internet was back in 1988. Late that year, he released the infamous "Morris Virus" (a.k.a. "Morris Worm") onto the Internet. Within hours, the Internet was on its knees. One need only visit the Department of Energy's Computer Incident Advisory Capability [6] to see that the same exploits, such as buffer overflows, used in '88 still trouble us today. Although the vulnerabilities used in the Morris Worm were widely known, there was no serious effort to plug the holes until after the fact.

Unlike the ATM that is physically controlled and the credit card reader that is located in the store, the consumer's home computer is outside the control of the bank. The home computer, along with the user's internet connection, provides an alternative path into consumer and bank assets. There are no controls on how consumers use their computers at home and there is the potential for significant loss during a simultaneous attack. That is, as the number of successful attacks occur, the greater the likelihood for business insolvency. Someone has to absorb the loss. A significant difference between traditional brick & mortar and e-commerce is that e-commerce transactions take place in a very short period of time. Whereas a bank teller could only process a finite number of people per hour, the e-commerce equivalent can facilitate many more transactions.

Another challenge is in trying to get meaningful information regarding actual online crimes. In a typical risk assessment, loss estimates are often based on the known history of similar losses. However, a business cannot report significant losses and hope to maintain its position in the industry. Consider the case of Egghead Online. In December 2000 they reported that a hacker had penetrated their online system [7]. The resulting customer fear caused the company to lose their market position. In conclusion, the last of the bankrupt company was dissolved during 2001 [8]. So the incentive for a company to report exploited vulnerabilities is bankruptcy? It is reasonable to expect businesses not

to report losses so the true extent of cyber attacks can only be estimated. In such an environment, one must look deeper to objectively determine overall risk.

To examine some Internet exploits, one need only look at the Denial of Service Attack Extortion attempts against on-line gambling. The first significant wave of cyber attacks were denial of service related. The trend now is for bad actors to exploit holes in home computers and then use these as robots (bots) to launch distributed denial of service attacks. Bad actors have used worms for propagating onto many computers for the purpose of launching distributed denial of service attacks [9]. The reality is that home computers will continue to remain a security challenge and perhaps the overall Internet weak link for some time to come. For example, many users are unaware that their machines are running rogue programs [10]. If the machines at home can be used to attack other sites; how long will it be before these machines are used to make obligations on-line? Here are indications that Bot networks (Botnets) are actively being used to exploit cyber crimes. In at least one case, a worm was used to create a 30,000 computer botnet [11]. The compromised IP addresses were then sold.

If we are to maintain the benefits of online commerce, we must do a better job providing enhanced security for home computers. To this end, the smartcard technology used to meet Homeland Security Presidential Directive 12 [12] could be extended to the public. Then consumers will have a strong security control for establishing Identity and Authentication necessary for on-line commerce. Indeed, the Department of Homeland Security (DHS), plans to issue 200,000 PIV cards to non-federal first responders in the Washington, DC area [13]. In all likelihood, this will be extended to all first responders throughout the US.

Consider that most of the Internet e-commerce today relies on Secure Socket Layer (SSL) where the Web portal has a certificate and the client uses a password to authenticate the user. This implementation allows customers to conduct their business from most (firewalls may block certain high risk IP address) Internet locations. However, if a bad actor gets the customer's account and password information, what is to prevent them from conducting nefarious transactions? If a bad actor has access to a large number of compromised home computers, bogus transactions can be launched from any number of locations thereby defeating a firewalls ability to block known hostile IP addresses. Moreover, bad actors have discovered a number of methods for gaining controls over consumer computers and

information. Consider, the latest Phishing attacks have demonstrated how easy it is to get people to provide information when they think they are connecting to a legitimate web portal. There are estimates that 60% of all internet users have visited a phishing attack link and that 15% have been tricked into providing data [14]. There are a number of ways compromised home computers can be used to disrupt our economy.

Today, Identity Theft is an increasing problem. Consider the first step in stealing an identity is to obtain personal information on the target individual. Many have suggested that identity theft results mostly from dumpster diving. That is when discarded paper with personal information is retrieved from trash receptacles. Similarly, stolen mail is often cited as another major source of information. The large number of phishing attack victims will certainly result in a significant increase in identity theft. One could argue that the Internet user should have known better (blame the victim); however, there have been a number of identities put at risk on a much larger scale that the Internet user had no control over. Consider the following partial list of incidents where there was theft or loss of personal information: 1.4 million credit card numbers from DFW Shoe Warehouse [15]; 200,000 client files from Ameritrade [16]; 30,000 students and staff at George Mason University [17]; 59,000 at a California University [18]; Bank of America tapes with 1.2 million government employees lost [19]; University of California laptop stolen with 100,000 identities [20]; 280,000 possible victims at LexisNexis [21]; and, 145,000 SSNs at ChoicePoint [22]. While it is easy to argue that more could have been done to protect individual's privacy; it would be unfair to argue that these victim companies are not committed to preserving their customer's privacy. With little more information than a SSN tied to a person, an identity can be stolen. As the Federal Trade Commission (FTC) points out "Social Security numbers play a pivotal role in identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims" [23]. It was not many years ago, identity theft was not the serious threat that it is today. With credit given based on little more than a name and SSN, it is easy to open bogus lines of credit in the name of some unsuspecting victim. The FTC statistics for 2004 indicate that: *Credit card fraud (28%) was the most common form of reported identity theft followed by phone or utilities fraud (19%), bank fraud (18%), and employment fraud (13%). Other significant categories of identity theft reported by victims were government documents/benefits fraud and loan fraud. And that: The percentage of complaints about "Electronic Fund*

Transfer” related identity theft more than doubled between 2002 and 2004 [24]. If businesses & financial institutions also required smartcard generated digital signatures, then knowing an SSN would not offer the same risk it does today.

It is widely accepted that we can always do more with security. Many security products focus exclusively on software based controls. However, a computer starts in a deterministic with the most privileged programs (those in the Basic Input/Output System (BIOS)) loaded first. The BIOS typically includes a flash memory update so software programs that start in the BIOS are the first to load. Following the BIOS programs, software such as the boot sector on the bootable media is loaded next. If these programs cannot be trusted, then operating system controls alone may not adequately enforce security [25]. If a home computer is infected (or compromised), typically additional back doors are installed. With multiple back doors, getting the bad actor out of the machine may not be feasible (short of a complete re-installation). To illustrate this point on a larger scale, a virus disrupted the Colorado state motor vehicles offices causing them to re-install the base software and reload 4-5 million records [26]. This would indicate that the attack was so severe that correcting the problem was not a cost effective alternative.

The federal and state governments have a number of laws against identity theft with more in the planning stages. However, laws alone have not proved to be an adequate deterrent for bad actors. The ability to enforce existing law is difficult and the types of attacks are changing.

The types of attacks discussed exploited known vulnerabilities. Often, exploit tools are readily available as soon as vulnerabilities are known. If a bad actor exploits a vulnerability before the home computer user gets the problem fixed, there may have any number of back doors installed on their machine. As bad as the time to fix exploits is, should we ever be confronted by a serious state sponsored cyber attack the exploit(s) used may not be known. The software and hardware products in use today are large, complex, and potentially harbor vulnerabilities yet uncovered. A state or large terrorist organization sponsored effort might uncover exploitable vulnerabilities. This is why defense in depth, using multiple controls, may offer the best protection.

The Smartcard Solution

Perhaps the biggest challenge with user’s home computer is to provide adequate protection. The near-term ability for vendors to improve security, especially with the rush to market driven design, is

difficult. What a smartcard offers is a hardware computer isolated from the desktop computer. A compromised desktop computer cannot corrupt the isolated smartcard device. For example, because it operates in an isolated space, a smartcard is typically immune from a computer virus [27]. With a smart card, we have a single hardware control that is less vulnerable to host computer software attacks. Moreover, the software is most effective when it is first to execute. A hardware smart card, working with software, provides enhanced security over exclusive software solutions.

A smart card by itself does not necessarily equate to a secure solution. To enhance I&A the smartcard should be tied to a person. If the smartcard were issued and personalized by a state driver’s license organization or by a bank, then there would be some assurance that the holder of the smartcard is the person they claim to be. The resulting form of authentication exceeds that of typical password approaches. Passwords have typically been used to authenticate users to systems, applications, and networks. However, there are a number of issues associated with password only authentication. First, the password is vulnerable to attacks such as shoulder surfing, keyboard capture, and network sniffing attacks. As the password is a single factor authentication mechanism, once a bad actor gets a password, little else is needed for nefarious activity. Another problem with passwords is the number of passwords users need to remember. While there are some password synchronization schemes, multiple passwords have been the rule rather than the exception.

The importance of hardware based protection is not lost on the software industry. For example, Microsoft’s Longhorn operating system, will work with hardware protected encryption keys. Additionally, there is at least one product that claims to work with the PIV card and includes BIOS security. In this case, as the BIOS loads first, the security software would be the first programs loaded into memory and therefore more resistant to being bypassed. Another advantage is that the BIOS is maintained in flash memory and is not readily modifiable from the operating system. Thus, for these machines the boot process will include a hardware based controls.

Another challenge is having the software development community utilize the security capabilities that currently exist. For example, many of the security vulnerabilities being exploited are based on buffer overflows. Yet, the 80386 processor that has been in wide spread use for years uses interrupt 5 for a “Bounds Check.” That is, the BOUNDS

instruction checks the array index against the bounds. If the index is greater than the limit, interrupt 5 is triggered. So why do we see so many buffer overflow problems when there is hardware mediated approaches readily available? Given the need for vendors to get their products to market, the overall security design gets varying emphasis. For example, from a vendor's point of view, what good is a security strong product if the opportunity to market the product has expired? When the competition can sell security-less products and capture market share the business case for enhanced security wanes. We also suspect that getting applications to work correctly in the first place is challenging enough. Trying to add sound security to the application adds yet another degree of complexity not uniformly practiced. Typically, customers are unaware of security flaws until after the products have been deployed. At that time, the patch management process disproportionately impacts the customer. For customers purchasing software, the product features and not the cost to implement an emergency patch (or patches) are considered.

In addition to the BOUND instruction, the 80386 processor includes four rings in its architecture (0-3 with ring 0 being the most secure). Ring 0, the most privileged, would be reserved for a security kernel and perhaps memory management. Ring 1 would contain most of the remaining operating system code. For programs operating in a less privileged ring, they can execute a CALL instruction and request a service in another ring. Effectively, the processor includes hardware mediated access control instructions. The software instructions to develop solid security are readily available as part of the microprocessor chip. However, designing code to operate correctly with security functionality is more complex than code written with relaxed security. Additionally, there may be a slight performance impact in adding security functionality to applications. So how can one determine if an application or system includes adequate security? While there are independent ways to have products evaluated, these take time and are not free. One method is to rely on the Common Criteria Evaluation and Validation Scheme. Under this approach, products are verified to have a given Evaluation Assurance Level (EAL). While this does not guarantee there are absolutely no security problems, it does reduce the risk of significant problems. To provide a non-computer analogy, a potential car buyer might review the Consumer Reports assessment of new cars prior to making a purchase.

Today, smartcard and contactless chips offer the physical isolation to protect select programs from compromised hosts. By having an island of protected

security on the smart card, the more trusted functions can be performed (often cryptographically) on the isolated chip. Given that operating systems now recognize smart card readers, we expect to see additional smart card security features combined with operating systems to provide enhanced security. This is a first and important step for ensuring security.

Going back to the SSL example where a bad actor is launching a man-in-the-middle attack. SSL can also be configured to require a client side certificate. The client side private key would only reside on the smartcard device. Before any transaction could take place, the client and server would establish a mutually authenticated secure session. That is, the server authenticates to the client, and the client authenticates to the server. Additional controls, such as logons, would take place following mutual authentication. As a man-in-the-middle would not have the requisite client side keys, a proxy could not take place, thereby providing powerful protection against this and DNS poison attacks.

HSPD-12

On August 27, 2004, President Bush signed Homeland Security Presidential Directive (HSPD-12). The goal was to have a single identification badge to provide strong identification and authentication for government employees and contractors. The identification badge referred to as the Personal Identity Verification (PIV) card will be verified by any federal agency or department. The technology includes machine readable information for accessing facilities and information systems. Thus the PIV card works with an infrastructure funded by federal agencies and departments. The infrastructure is based on standards and guidelines published by the National Institute of Standards and Technology (NIST). It addresses many of the statutory requirements found in the E-Government Act of 2002 and Privacy Act of 1974,

One path explored in this paper is to expand the PIV infrastructure to accommodate citizens. As will be discussed later, the PIV card requires a personnel adjudication process. While these processes are well defined for the federal employees and contractors, the non-government processes remain undefined. For federal employees and contractors, a National Agency Check with Inquires (NACI) is required. This investigation includes national criminal history check conducted by a fingerprint classification through the Federal Bureau of Investigation (FBI). It will be interesting to see how the PIV cards issued to first responders address this issue. Nevertheless, we suggest that the states driver's license and identification card is the logical

place for PIV card issuance. That is, before a driver's license is issued, supporting identification and an in-person picture is required. If the PIV cards are used for states driver's licenses then citizens would have a readily available strong I&A control that could be used to ensure the identity of those claiming to own a credit card or SSN.

With HSPD-12 signed, there is a common infrastructure that could accommodate states issuing drivers' licenses. There would be some data field changes required but the approach would build on the existing work funded at the Federal level. By getting users digital certificates generated by state departments of motor vehicles, there would be strong confidence that an on-line person is who they claim to be. Moreover, if state driver licenses are not tied to strong cryptographic technology, such as that provided by smartcards, then the licenses will remain vulnerable to counterfeiting.

What Would Be Required

Although the PIV card was specified for government employees and contractors, non-government use is encouraged: *"This recommendation has been prepared for use by federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright"* [28]. Thus, the federally funded technology could be used by non-government users. This section describes some changes that could be made to facilitate the expanded use. For a common discussion, consider a state issuing driver's licenses using PKI credentials and a PIV card.

First, the public will not be subjected to the same background checks that government employees and their contractors are. It is therefore important to differentiate the card holder as a citizen. There are obvious changes to the printed matter that could help. The distinguished name (DN) would be the first obvious change. The current DN naming for contractors requires an affiliate included after the government organization the contractor works for. Perhaps an extension of Citizen could be used to readily identify the card holder as a non-government person.

The second area would be in the Card Holder Unique Identifier (CHUID). This is a signed object that is on both the contact and contactless chips. Within the CHUID, there is 25-byte Federal Agency Smart Credential – Number (FASC-N) [29]. Prior to the FASC-N, there was another identifier defined by the Security Equipment Integration Working Group (SEIWG-12) [30]. In the past, this string included the person's social Security Number (SSN) in the form of

binary coded decimal (BCD) digits. The FASC-N requires 40 characters be encoded using 5-bits per character, this results in a 200-bit (25-byte) FASC-N. The FASC-N is backward compatible with the SEIWG-12 so this could impact an individual's privacy if implemented incorrectly. Whereas the SEIWG-12 required the cardholder's SSN, the FASC-N does not have to include a SSN, and it is strongly recommended that implementers not use the SSN.

Some other fields are agency code, system code, credential number, personal identifier (this is the field that would contain the SEIWG-12 SSN), organizational identifier, individual credentials issued (how many times your credential was reissued), organizational category, a person/Organization association category, and a credential series. The other fields are separators and error checks.

Fortuitously, the Government Smart Card Interagency Advisory Board had the foresight to allow the PIV card to be extended for public use. There are of course additional changes that could be made to ensure that a non-government worker is not granted access to a restricted area (particularly with the access control subsystem described later). However, by the same token, wouldn't it be nice to place your driver's license next to a contactless reader and get quicker access at the airport? Given that the Transportation Security Agency has personnel working at all major airports. Therefore, much of the PIV infrastructure will already be in place.

PIV Functional Areas

Personal Identity Verification has three functional areas: the front end subsystem; card issuance and management subsystem; and the access control subsystem. This section briefly discusses each functional area. That is, the PIV can be viewed based on functional area. The front end subsystem is that where users interface with daily. The card issuance and maintenance subsystem is the area where the PIV cards are issued, replaced, and revoked. The access control area consists of the rules that allow users to enter restricted areas or access restricted information systems.

Front end System

The front end subsystem includes the PIV Card, card and biometric readers, and personal identification number (PIN) input device. The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource. The PIV card includes a contact and contactless chip, various mandatory and optional data elements, and printed material requirements. For privileged operations, the PIV card uses an 8-

character Personal Identity Number (PIN). If less than 8-characters are used for the PIN, the remaining characters are padded with 0xFF (this is represented by all 1's).

Currently, any contact smart card reader must be used in conjunction with a keyboard or pad that allows numbers to be entered. The PIV cards work with a card management system (CMS) that keeps track of every assigned PIV card. That is, the CMS keys are specific to each card personalized. There are two types of smart card readers used in the front end system. The first reader complies with the Personal Computer/Smart Card (PC/SC) specification [31]. PC/SC focuses on the personal computer and the reader attached to it. The PS/SC standard is also starting to address contactless smart cards. Eventually there could be one standard to address both the contact and contactless smartcard chips. However, currently the second reader works with the contactless chip and must comply with ISO/IEC 14443. So the front end subsystem consists of the components and processes that users directly interface with on a daily basis.

Figure 1 depicts some of the front end components that a user would interface with. The top part illustrates a contactless reader shown connecting to a keypad. This would normally be a facilities access point such as to a restricted access computer room. The bottom part illustrates the connections to a personal computer. In addition to a smart card reader, some personal computers will include a biometric reader. Eventually, there could be facilities access readers that include a biometric reader. As the fingerprint biometric is maintained within the contact chip, a PC/SC contact reader would be required to support a fingerprint biometric.

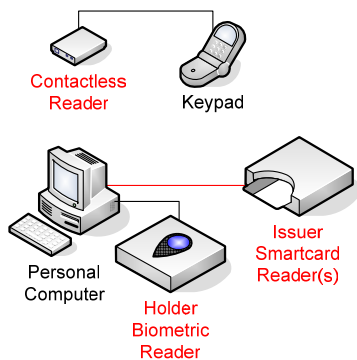


Figure 1 Front End Subsystem

Card Issuance and Management

Components responsible for identity proofing and registration, card and key issuance and

management, and the various repositories and services required as part of the verification infrastructure. The identity proofing and registration process for government employees and contractors require the person appear at least once in person. A Form I-9 (Employment Eligibility Verification) is completed. The application process includes capturing the applicant's finger prints. Before government employees and contractors can get a PIV card personalized, they must complete a National Agency Check (NAC). They then have up to six months to complete a NAC with Inquires (NACI). The original FIPS 201 included a requirement for the office of inspector general to complete a certification and accreditation. However, this requirement was eliminated by way of the FIPS 201 Errata sheet.

Card Maintenance is necessary to ensure that the PIV cards and associated information are kept current. If a card is damaged, lost, or the cardholder changes jobs, the new information must be distributed within the PIV management subsystem. Key to this is maintaining the status of the authentication certificates. Once an authentication certificate is revoked, the revocation is published on revocation lists or provided to OCSP responders. Thus, whenever an authentication certificate is checked, its status is quickly determined by the relying party's applications.

Card renewal is the process of extending the current PIV card. The PIV card can continue up to a maximum of five years. The card holder must still have a current NACI on file and the PIV card expiration date must not be exceeded. This later date is initially set during when the PIV card is first initialized.

Card re-issuance is when the full registration process must be completed. This requires a new PIV card and personalization. However, if the current cardholder has a valid NACI, then there is no need to conduct a new background check. Periodically, users forget their PINs. To reset the PIN, the user must go back to the card issuer and have the retry counter set. At that time, the cardholder's biometrics must be verified. It should be noted that the biometrics verified could be the photograph on the PIV card and not necessarily the fingerprints. The last condition is when a cardholder is terminated. For example, an employee separates from federal service. In these cases, the card should be collected and destroyed.

The PIV card contains key pairs for authentication. It can also support other key pairs for card authentication, encryption, and digital signatures. To ensure that revoked key information is made widely known, in a short time, and to a number of

heterogeneous platforms, the PIV architecture uses a Public Key Infrastructure (PKI).

PKIs have been deployed in a number of environments. The basic parts are based on the X.509 standard. While some implementations describe a number of components, a PKI consists of a certification authority (CA) that issues certificates and revocation lists; a directory that holds end entity information such as certificates and revocation lists; and some type of registration authority (RA) that acts as a front end for end entity registration. The RA communicates securely with the CA. The CA and directory are typically servers, while the RA can be either a server or a client. Many agencies and departments have extended the PKI model to include key management (includes a key escrow or other recovery mechanism).

When a certificate is created, there is a multistage process involved. Typically, for authentication and digital signature key pairs, the keys are generated locally on the PIV card. The private key never leaves the PIV card, while the public key is exported for inclusion in a certificate request. The certificate request includes a number of certificate extensions using the Basic Encoding Rules (BER) or Distinguished Encoding Rules (DER) expressed in Abstract Syntax Notation One (ASN.1) [32].

The RA sends a certificate request to the CA, where it is checked. If the checks are successful, the CA will digitally sign the certificate request creating a certificate. In the PIV architecture, there is a common government root operated by the General Services Administration (GSA). Every compliant PIV authentication certificate can be validated to this root. The approved Shared Service Providers (SSP), operate and maintain the intermediate certification authorities. There are a few scenarios for card issuance and maintenance. Two approved approaches are role based and system based implementations. It is also possible to have additional approaches that first require approval. As departments and agencies deploy their PIV systems, the processes used must be detailed in the RA Practices Statement (RPS). Currently, SSPs are typically not performing the RA functions. Additionally, if encryption is used, a Key Management Policy (KMP) and Key Management Practices Statement (KMPS) will likely be required. Before logical access can be used, departments and agencies must first complete their RPS, have a compliance audit conducted, and have these approved by the Federal Policy PKI Authority.

Access Control

The PIV card can provide strong I&A. However, there still needs to be access controls applied to facilities and information systems. For example, just because a PIV card is used to strongly identify and authenticate the cardholder, this does not automatically entitle the cardholder unrestricted access. Facilities access would include restrictions for a number of areas such as computer rooms, hazardous material storage areas, locations where investigatory information resides, personnel records storage, and procurement records. Likewise, information systems processing sensitive information would be restricted to those requiring access and restricted to all others. That is the physical and logical access control systems, the protected resources, and the authorization data. So the access control subsystem is some computer mediated process that allows or restricts access. For example, a user might be allowed read access to a database but not write access. This is an example of access control of a computing resource. Access control systems are administered by system and security administrators.

There is typically a separation of duties between facility and logical (computers and networks) access control administration. Once users and PIV cards are authenticated a set of permissions is used to allow or restrict access. Different applications and systems may use different mechanisms to determine access. For example, role based access control could be defined for a set of users. Moreover, there may be external events that temporarily allow access. For example, during a fire, first responders would require physical access to areas they would normally be restricted from entering. The trigger event to enable these temporary roles (first responder during a fire) might be a fire alarm. When the fire alarm is triggered, first responders would automatically be granted access to the effected areas. Another example of a trigger based rule would be restricted access during evenings, holidays, and week-ends. Most card holders could be denied access during non-working hour access.

The access control subsystem uses the PIV card only for the identification and authentication of the card holder. Once a card holder completes I&A the access control subsystems is used to determine what rights or privileges the card holder has. The access control information is not contained on the PIV card but is located in other supporting applications or systems.

Consider how passengers are currently screened at airports today. There is a person that looks to see if the passenger has a ticket and has a valid looking photo identification card. The photo

identification could be a fake or the individual might be wanted by law enforcement. In contrast, airports might use an unattended kiosk requiring multi-factor authentication (PIN, PIV Card, & possibly a fingerprint biometric). Once authenticated, the access control subsystem could pull information regarding what passengers have tickets to ensure that the person authenticated is the ticket holder. This would be combined with a solid record of the people (accountability) that have passed the security checkpoint. The result would be less chance that passengers will run through security and thereby require the airport to be shut down during the investigation. Expanding on this example, consider a person trying to flee the country. Law enforcement could request that their authentication certificate be revoked using the key compromise reason code. That is, when an authentication certificate is revoked, there is a reason code used to explain why the certificate was revoked. By using a key compromised code, it indicates that the card holder is using a compromised card. At the airport security check point, if any authentication certificate is revoked due to key compromise then the airport security personnel could detain the person pending further investigation. This would provide a powerful law enforcement control able to quickly flag cardholders as suspect. Once a person has been identified as having a key compromised credential, the access control subsystem can implement additional processes. For example, it could immediately notifying security personnel that a person needs to be detained. It can work cooperatively with video cameras and facilities lockdown devices to record, observe, and control the person's movement.

The combined access control subsystem and PIV card authentication could be used on a much wider basis. Consider a driver pulled over by police in another state. Getting police records and revoking drivers licenses across state lines today is challenging and time consuming. In contrast a PIV card can be revoked in less than 18 hours. By providing police mobile units with PIV card readers, they could determine in real time if a PIV card was revoked or not. Again, if the card holder has a revoked authentication due to key compromise, the officer could detain the person pending further investigation.

The PIV card optionally supports encryption keys. If these are used, then encryption can be used as a further access control mechanism. Sensitive information with respect to confidentiality can be encrypted so that only a limited group can decrypt the information. This in effect prevents unauthorized access to the plain text information. There are also products that encrypt on-the-fly all information that

goes into a protected folder. So even if a computer is stolen, the sensitive information is not compromised. Using encryption does not use a typical access control subsystem. Instead, it relies on commercial products that implement encryption using the PIV card to protect the keys. Other examples of encryption include email packages supporting the Secure Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Internet Protocol Security (IPSec).

Conclusion

The risk of identity theft and other malicious attacks is increasing. The consequences of not addressing the problem could include increase business bankruptcies, economic recession, or at worse, and economic depression. If the driver's licensing efforts can utilize the technology and infrastructure deployed to support the federal PIV, then we could have a basis for mitigating many of the threats to information assurance and e-commerce. A PIV card combined with enabled software could provide citizens with a security control that moves us away from dependence on unauthenticated SSNs.

References:

1. Hoffman and Davis, Security Pipeline Interface (SPI), *Proceedings of the Sixth Annual Computer Security Applications Conference*, 1990.
2. Davis, Russell, *Exploring Computer Viruses*, Proceedings of the Fourth Aerospace Computer Security Applications Conference, IEEE Computer Society, pages 7-11, 1988.
3. Salam, et al, *Trust in E-Commerce*, Communications of the ACM, pages 73-77, Feb, 2005.
4. Greguras, Fred, *Corporate EFT: Vulnerabilities and Other Audit Considerations*, IPC Business Press Volume 3, Number 3, May, 1981.
5. Echin, M. W. and Rochlis, J. A., With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988, Communications of the ACM, June, 1989.
6. <http://ciac.llnl.gov/ciac/index.html>
7. Harris, Ron, *Online technology retailer Egghead.com hacked*, Associated Press, December 22, 2000.
8. Rosencrance, Linda, *Egghead.com finally cracks, shuts shopping site*, Computerworld, October 29, 2001.
9. Levy, Elias and Arce, Ivan, *Criminals Become Tech Savy*, IEEE Security & Privacy, pages 65-68, April, 2004.
10. Gottesman, Ben Z. and Karagiannis, A false

- sense of security, pages 72-77, PC Magazine, February 22, 2005.
11. Leyden, John, The Register, *Botnet used to boost online gaming scores*, December 21, 2004.
 12. Office of the Press Secretary, the White House, August 27, 2004.
 13. Lipowicz, Alice, GCN Post-Newsweek Tech Media Staff, *First responders to get biometric IDs*, April 6, 2005.
 14. Glascock, Stuart, TechWeb, *IT Vigilance Urged to Fight Malware, Bots, Root Kits*, April 27, 2005.
 15. Associated Press, Columbus, Ohio, *DSW Data Theft Much Larger Than Estimated*, April 20, 2005.
 16. Fredrix, Emily, *Ameritrade Loses 200,000 Client Files*, Associated Press.
 17. McCullagh, Declan, *Hackers steal ID info from Virginia university*, CNET, January 10, 2005.
 18. San Francisco Reuters, *Calif. University Says 59,000 Affected by Hackers*, March 21, 2005.
 19. Swartz, Jon and Block, Sandra, *Underground market for stolen IDs thrives*, USA Today, page 1B, March 3, 2005.
 20. Reuters, U.S. Senator Seeks Safeguards After Identity Theft, March 29, 2005.
 21. Associated Press, Dayton, Ohio, *LexisNexis begins notifying possible victims*, April 19, 2005.
 22. Vlahos, Kelley Beaucar, *Embattled Data Collector a Big Homeland Security Contractor*, Fox News, February 27, 2005.
 23. Prepared Statement of the Federal Trade Commission on *Identity Theft and Social Security Numbers*, Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce, September 28, 2004.
 24. *National and State Trends in Fraud & Identity Theft January - December 2004*, page 3, Federal Trade Commission February 1, 2005
 25. Davis, Russell, *Peeling the Viral Onion*, Proceedings of the 14th National Computer Security Conference, pages 417-428, 1991.
 26. Barba, Robert, *Virus puts brakes on licensing for the week*, The Denver Post, page B1, September 2, 2004.
 27. Yang, Yi-Jen, *The Security of Electronic Banking*, Proceedings of the 20th National Information Systems Security Conference, pages 41-52, October, 1997.
 28. NIST Special Publication 800-73, *Interfaces for Personal Identity Verification*, page 1, Dated April, 2005
 29. Technical Implementation Guidance: Smart card enabled Physical Access Control System, version 2.2, Government Smart Card Interagency Advisory Board, July 30, 2004.
 30. NIST Interagency Report 6887 - 2003 Edition, Government Smart Card Interoperability Specification Version 2.1, July 16, 2003.
 31. www.pcscworkgroup.com.
 32. International Telecommunication Union, *Abstract Syntax Notation One (ASN.1): Specification of basic notation*, ITU-T Rec. X.680 (2002) | ISO/IEC 8824-1:2002.