Using the PIV Card Outside of the Federal Government

Dr. Russell J. Davis
Femtosecond Inc.

Introduction:

Before diving into the topics at hand it's worth defining a few properties that will be used throughout the paper [1].

Privacy is a property of individuals Confidentiality is a property of data Security is a property possessed by hardware and software systems and facilities

During the 1960's congress held hearings on a proposed National Data Bank (NDB). It was not funded for fear that a national ID might emerge and thereby erode privacy [2]. Today, the feared system of the 1960's is alive and well using the Social Security Number (SSN) to correlate confidential information. At the same time, identity theft is on the increase. However, not many years ago, it was common practice for checks to include SSN, names, and address. Yet at the time, identity theft was no where near the problem that it is today. After all, there are only 9 digits in an SSN so there are but one billion possible combinations. Have you ever been asked to provide the last four digits of your SSN to prove you are who you claim to be? Pause for a moment and ask yourself why is it that the loss of an SSN is so devastating to identity theft victims? I think the answer has to be that too many institutions are relaxing an individual's right to privacy by trusting that the SSN as proof of a person's identity. If e-commerce is to survive, this practice must stop.

This paper presents the case for strong Identification and Authentication for all citizens. The argument evolves around the government Personal Identity Verification (PIV) card, and the supporting infrastructure. Other government initiatives such as common driver's licenses are also examined. The argument follows: If you have my SSN and you cannot use it to impersonate me in any matter, then the SSN is of no value to you. If on the other hand, you can open lines of credit and can impersonate me based solely on my SSN, then the SSN is very valuable. Another question here is why should the SSN be so non-reputable?

By the Numbers:

In this section, we will explore how bad the identity theft trend is and why confidentiality is not preserved. Years ago, your driver's license number was your SSN. Now the numbers are different. However, this has resulted in yet another number that is accepted as non-reputable. Consider that the Secret Service reports that counterfeiting is on the rise. For years the US currency had a

consistent flavor. Yet, recently, the currency seems to go through continuous upgrades. Even so, there are periodic reports of large counterfeiting operations being shut down [3]. Given the problems trying to keep paper currency from being forged, how much protection can be afforded a piece of plastic with various etchings on it?

The Federal Trade Commission (FTC) received 635,173 consumer complaints last year, 246,570 of which were identity theft [4]. The problem is exasperated by the lack of law enforcement support. On a personal note, several years ago, I went out to get the morning newspaper. There affixed to my door was a note to Fedex and UPS claiming to be the homeowner working late hours, and please leave the package. I called the Fairfax County Police department and they seemed to be at a loss as to what to do. I tried in vain to convince them it was likely a case of a stolen credit card. I also pointed out that in some cases, the card numbers are taken from online underground sites. Their advice was to call back if a package arrived. I changed the note on my door advising Fedex and UPS not to leave a package without a signature. Sure enough, several days later a package arrived. Once again, I called the Fairfax County Police and this time they sent out a uniformed officer. I offered to let them set up a camera to see who picked up the package. I pointed out that that if the credit card number came from an online source, the camera could help them get a suspect and possibly crack a much wider case. The discussion was clearly beyond the officer's training. He took the package and I never heard back from the police. However, I did note in the newspaper's crime report that there was one incident in my neighborhood during that period. You guessed correctly, a stolen credit card was used to purchase online pornography.

What I learned from my experience was that cyber crimes were evolving faster than the ability of law enforcement to hold them in check. Furthermore, adding additional laws, when the current ones cannot be enforced, did not seem to be a viable solution. Again, someone's identity was based on a static number. In this case, a credit card number. Delivering the goods to a street address did not prevent the purchase from taking place. For everyone that reports an incident, how many cases go unreported?

I have one more personal experience from around the same time period that I'll share. I logged onto my on-line brokerage (name withheld) and received a curious error message. It was from the Brokerage firm's firewall stating that it did not trust my Internet Protocol (IP) address. At the time, I had an Internet Service Provider (ISP) that provided me a static IP address. In looking through the trace routes, I had concluded that I was victim to a man in the middle attack. I waited for about ten minutes, re-established my connected, and once I was satisfied that the path was correct, I immediately changed my password. What I found interesting is that my brokerage firm never alerted me to the fact that a known bad site was trying to connect using my account. That they blocked the site indicated they knew there was a hostile attack underway. Since then and a couple of years after the fact, I once could not log into the account. The number of password attempts was exceeded, and not of my doing. I suspect but have no

proof, that the man in the middle site was harvesting passwords and assuming that most users do not change their password, tried to exploit their holdings.

Similarly, credit card fraud is a costly business. While the major credit card companies are working with the smart card industry, there is still a lack of consumer acceptance. The thought of installing a smart card reader is too much for the average user. That the credit card companies are active in the smart card arena indicates they recognize the necessity of improving security. On-line purchases using credit cards typically rely on encrypted Secure Sockets Layer (SSL) for protection.

This brings me to the weakness that exists with most of the SSL implementations currently in use. The way they are typically set up is using the server side certificate to establish the encrypted session. When a user connects to a hostile site, every detail may look legitimate, including the site name (universal resource locator (URL)) and the lock (indicating an SSL session). Unfortunately, most users would not know they were connecting to a bogus site. The problem is that the server does not authenticate the client (user). Thus, a Domain Name Service spoof or other man in the middle attack can be effective. By requiring the client to have a certificate and associated private key, then bi-directional (two-way) authentication can take place as part of the SSL set up. Even if a bad actor had your confidential account login information, they could not establish the required SSL session to exploit their holdings (assuming of course that the server SSL is setup correctly).

The following figure depicts a typical man-in-the-middle attack. Here a typical attack, such as a Domain Name Service (DNS)) spoof, results in the Browser connecting to a bad actor's site instead of the intended web server. First, the user tunnels in to the Browser Bad actor's proxy machine using SSL (running on the default port 443). The actual connection could either 1) be from the Browser to the bogus server or 2) port 80 (exploiting un-patched browser holes).

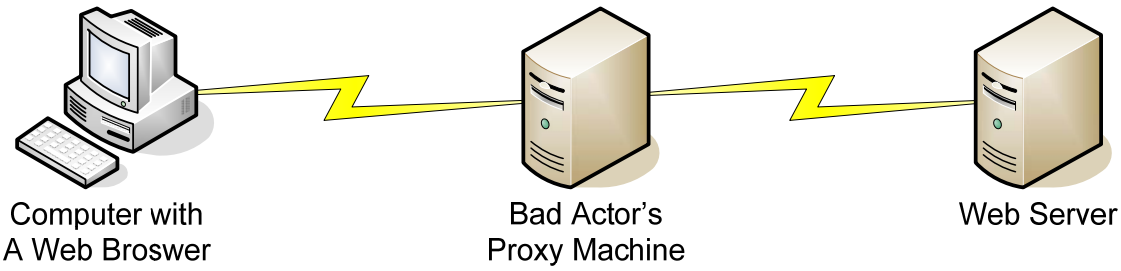

Figure 1 Man in the Middle Attack

Next the Bad Actor's Proxy Server connects to the intended web server again using SSL. In effect, when using port 443 there are two SSL connections between the Browser and the intended Web Server. Each screen and response is passed onto the next SSL connection.

Now consider how password (or a credit card number) authentication works. The Intended Web server asks for a password. This request screen is forwarded to the Browser. The user enters the password, this is then forwarded

to the Web Server and the bad actor is in. Moreover, the bad actor now has a copy of the user's password and can capture any information flowing between the user and intended Web Server.

Now consider a cryptographic challenge and response authentication mechanisms. These products could be a calculator device where a user enters in information and calculates the appropriate response; or they could be a token with a constantly changing value.

1. The User connects to the bad actor's server.
2. The bad actor's server forwards the request to the intended Web Server.
3. The Web server responds to the bad actor's server with a cryptographic challenge.
4. The cryptographic challenge is forwarded from the bad actor's server, to the Web Browser.
5. The user received the cryptographic challenge, enters this value into the calculator device, and responds to the bad actor's server with the appropriate challenge.
6. The Bad actor's server forwards the response to the Web server where the authentication is validated.
7. At this time, there is a secure session with a man-in-the-middle mediating all information flow.

Now consider a client side certificate. The certificate identifies the client user and the user has an associated private key. Additionally, the certificate could be software or resident on hardware. If the certificate is software tied to the local machine, then trying a secure session on another machine would require transferring the certificate and associated private key to the new machine. In contrast, if the certificate and private key are located on a hard token, such as a PIV card, then securely logging in from another machine requires only the hardware token.

1. The user logs into the Bad actor's server.
2. The bad actor's server then attempts to establish an SSL session with the intended Web Server.
3. The intended Web Server requests valid client side authentication.
4. As the Bad Actor's web page does not have a valid key, the second SSL connection cannot be established.

So what could a man-in-the middle do to a current session? The bad actor can be expected to do anything the legitimate user is permitted to do. If the user stores documents on a server then the user has write access and this is an avenue for back door exploitation. Alternatively, the Bad Actor may keep a session open long after the Browser thinks the session has concluded thereby conducting other nefarious activities.

You might ask, we if we can determine the location of the bad actor's proxy server, could we not block it at our firewall? One problem is that the bad

actor's proxy server may belong to some other unwitting victim. There are a significant number of Internet connected machines today that are acting as zombies [5]. That is, the machine is taken over by another exploit, such as a worm, and then used as a launch vehicle to attack other machines. The effect is that the attacks could come from any number of locations. Unlike the case where my brokerage firm blocked a single IP address, the network threats have since evolved.

The idea of a user connecting to a site that they think is legitimate is not a new concept. Consider that over 30 years ago, a couple of high school students wrote a program to mimic the login. By the time they were caught, they had the login information for over 100 users [6]. Clearly, an un-forgeable login would mitigate this type of attack.

There are now a large number of phishing attacks that target users through bogus emails. The user receives an email message that looks legitimate and includes a link to access a Web portal. Unfortunately, the link instead goes to some bad actor's site where the user is asked to provide confidential information. This information is then harvested and used to perpetrate identity theft. As there actually is no man in the middle, the victim could inadvertently divulge confidential information not knowing that the site is bogus. However, the reason this exploit can take place is that trust is placed on un-trusted email and the information captured is all that is needed to effect identity theft. Most email packages today incorporate the Secure Multipurpose Internet Mail Extensions (S/MIME) standard. S/MIME can provide email trust but requires users to have their own certificate.

Hardly a day goes by without more bad news from the privacy front. A laptop at the University of California was stolen with confidential information on 100,000 people [7]. And at the George Mason University in Virginia, confidential information on 30,000 students and faculty were stolen online [8]. Moreover, it would seem that during December, 2004, some Bank of America backup tapes containing confidential information on approximately 1.2 million government employees was lost [9]. As I was still a government employee during that time, I received the Bank's form letter. Included with the letter a one page checklist of things you could do to protect your identity. However, not one of their recommendations would have prevented the lost tapes. Why such sensitive information should be transported unencrypted is another matter. A question here is how much money do think those tapes could fetch on the black market? So like the million plus others on those tapes, I await the conclusion of this episode. But again, the risk exists because institutions will use the information without question.

In 1988 I published and presented a paper, "Exploring Computer Viruses." At the time, there were a number of security "experts" that argued viruses were no more than a curiosity and would never amount to a serious security challenge. I don't think anyone would argue that point today. Indeed, it is interesting to note that the risk is everywhere. Consider the Colorado Motor Vehicle Business Group was shut down by a virus and 4 – 5 million records following a complete software reinstallation had to be restored [10]. I once again find myself arguing

for a technology, this time the PIV card that ha1s a mixed backing from the security industry. Yet it was the security industry that initially warned us of the disaster that was sure to happen when the clocks rolled over to the year 2000.

E-Authentication:

In the 2002 President's Management Agenda (PMA), there are a number of goals listed. On pages 24-25 there is the following:

> "Agencies will undertake a Federal Public Key Infrastructure (PKI) to promote digital signatures for transactions within the federal government, between government and businesses and between government and citizens. The digital signature initiative should be coordinated with state and local governments as well as the private sector."

In this context, a PKI is used to generate digital certificates and revocation lists. The digital certificates work with a number of off the shelf vendor products including browsers and S/MIME enabled email. Within the E-Authentication environment, there are a number of sources where digital certificates can be obtained. These are referred to as Credential Service Providers (CSP). A feature of a well connected PKI offers is the ability to revoke digital certificates by identifying the bad certificates on a revocation list. Most modern PKI enabled applications will automatically check the requisite revocation list. This is possible because within the certificate is the Certificate Revocation List (CRL) distribution point where applications can get the CRL.

To facilitate the PMA, the Office of Management and Budget (OMB) established an initiative: "The Administration is committed to reducing the paperwork burden on citizens and businesses, and improving government response time to citizens" (M-04-04). The first step was to categorize the various applications government agencies interact with the public, four assurance levels were defined. The highest, level 4 are those devices that are hardware based. The PIV card in particular is a level 4 device. Table 1 depicts under what circumstances the various levels would be used. A key point is that federal employees and contractors will have the Assurance Level 4 PIV cards

Assurance Level	Description of when to use
Level 1	Little or no confidence in the asserted identity's validity
Level 2	Some confidence in the asserted identity's validity
Level 3	High confidence in the asserted identity's validity
Level 4	Very high confidence in the asserted identity's validity

Table 1 OMB M-0404 Assurance Levels

The OMB also provided tools to help agencies conduct risk assessments on their major application to determine what type controls should be applied. Much effort went into establishing e-authentication throughout the federal

agencies. Next, the National Institute of Standards and Technology (NIST) came up with a list of tokens that could be used to satisfy the various assurance levels defined by the OMB. Table 2 illustrates the tokens NIST identified.

Token	Description of when to use
Password tokens	can satisfy the assurance requirements for Levels 1 and 2
Soft cryptographic tokens	may be used at authentication assurance Levels 1 to 3, but must be combined with a password or biometric to achieve Level 3
One-time password devices	are considered to satisfy the assurance requirements for Levels 1 through 3, and must be used with a password or biometric to achieve Level 3
Hard tokens that are activated by a password or biometric	can satisfy assurance requirements for Levels 1 through 4

Table 2 NIST SP 800-63 Tokens for Meeting Assurance Levels

When HSPD-12 was issued, there was some (and perhaps still remains) confusion between e-authentication and HSPD-12. The bottom line is that federal employees and contractors will receive the PIV card (hard token). This is a level 4 device that can be used for all assurance levels (as noted in Table 2). So the only question regarding e-authentication is what level of assurance outside parties should have in order to authenticate to federal systems. And it will be some time before current applications that rely on passwords are converted over to accept the new PIV cards. However, for every conversion, that is one less password a user is burdened with remembering. How many passwords does the average user need to remember? This leads to the obvious question, why would we not want to actively encourage citizens and businesses to use hard tokens? The short answer is the cost. The HSPD-12 targeted federal employees and contractors. So how would the citizens gain access to the infrastructure deployed to support the PIV card? This is where you the reader can help. The more people that ask the same question, the faster the message will be conveyed.

PIV Card:

The PIV card is detailed in the NIST Special Publication 800-73. The credit card sized device includes a contact and a contactless chip (or one chip with both functions). The contactless chip is typically used to access facilities. The user places the card near a reader and the Card Holder Unique Identifier (CHUID) is read from the device. The CHUID is also digitally signed so that its integrity can be verified. The Physical Access Controls System (PACS) uses this information to allow (or block) facilities access. So at some point in the future,

high risk government facilities will have contactless readers that will work with PIV cards. It is worth mentioning that just because you may have a legitimate PIV card does not mean you will automatically be granted access to a government facility. The physical access security will configure the PACS to allow individual access only as needed. So how might the contactless chip help the average citizen? Consider those that must travel through major airports. Are there not Transportation Security Administration (TSA) personnel that work there screening passengers? As long as there are government employees in locations requiring high physical security controls, it is likely that there will be government contactless readers there. Would it not be beneficial to use this same technology investment to screen passengers? Right now there is a dedicated person looking at the photographic identification (typically a driver's license) to determine if a person is who appears on the identification card. Why not provide a stronger, machine readable format that allows passengers quicker access through airport security?

The contact portion of the PIV card includes a cryptographic processing capability. It includes storage for two biometrics of index fingers, the CHUID, a digitally signed security object and authentication certificate. The contactless portion can also include encryption and signature certificates with associated private keys. It is this second chip that offer interesting capabilities to strengthen the security necessary for electronic commerce. One of the biggest stumbling blocks for furthering e-commerce is people's distrust of online security. By providing a strong device that we can agree improves security, perhaps we will see a further acceptance of e-commerce. However, victims of identity theft may be reluctant to once again trust Internet security, regardless of how their identity was stolen.

What makes the combination card look attractive for non-government use is the investment in the federal infrastructure and the volume purchasing planned. If another technology is deployed for say driver's licenses, it will lack the volume discounts and could cost more while providing fewer functions. For example, the TSA is working on the Transportation Worker Identification Credential (TWIC). Would it not be beneficial to have a common infrastructure instead of a separate stove pipe? However, the real pay off would be in reducing (or eliminating) the dependence on a number (SSN) to represent an individual. By having a strong cryptographic module providing technical non-repudiation, then a bad actor will be less likely to perpetrate an identity theft. It really wouldn't matter if a bad actor had your password because it would be useless without the PIV card.

Before a PIV card can be used at a client workstation the computer must have a smart card reader. If you go to your favorite computer store today, they probably have no smart card readers in stock. Why do you suppose this is the case? Well to begin, who has a smart card? Without users with smart cards, there simply is no business case to include a reader. If the number of users with smart cards increased, then there would be a market driven business case to bundle smart card readers with new computers.

The PIV card includes interoperating with the Shared Service Provider hierarchical PKI. The certificates must include the common policy object identifier (OID) for the certificate policy extension within the certificates. It is this ability to quickly determine that a credential is still active that makes the PIV card so powerful. Consider a driver's license that the department of motor vehicles would like to revoke. How can they accomplish this? Without physical access to the badge, there is little they can do. If the person is pulled over for a traffic violation, a central database could flag the license as being invalid. However, the person could still pass airport security identification checks. Moreover, consider the fraudulent license. How can airport personnel determine that the licenses are bogus?

If you recall the 1998 Kenya embassy bombing, before the main blast, there were hand grenade explosions. This had the effect of getting people to look out their windows to see what was going on. It was not standard practice then to use a protective plastic window coat. Thus flying glass from the main explosion caused additional damage. More recently, there have been reports of stolen uniforms and identification badges [11]. Consider the following terrorist scenario. Some man made disaster takes place as a preamble to a planned larger attack. The first people on the scene are the first responders. For example, if there is a fire, one would expect to see firefighters and medical workers. The question is how do you verify first responders quickly and reliably? The message is clear, there needs to be some automated way to verify emergency workers, police, fire & rescue, and other first responders. If the only check is to look at a possibly bogus identification, then this is a soft underbelly for terrorists. The Department of Homeland Security (DHS), along with other agencies is exploring a number of technologies (including the PIV card). Consider a disaster scene where first responder credentials are quickly verified by a portable reader. This allows quick response to the disaster while preserving security.

In response to HSPD-12, the NIST promulgated Federal Information Processing Standard (FIPS) 201 on February 25, 2005. In this standard, federal agencies are required to conduct a Privacy Impact Assessment (PIA) in accordance with OMB M-03-22, when there is confidential information in identifiable format (IIF) pertaining to people. This would of course include SSN information. With the number of incidents involving the loss of SSN and other information, it's worth closing this section on a person's right to privacy:

> *In a landmark case involving a state statute restricting the use of birth control, Justice Douglas, writing for the court found the right of privacy to be implicit in rights afforded by the first, third, fourth, and fifth amendments to the Constitution.* [1]

PIV Algorithm Update:

The PIV card has many capabilities that can be used to improve security. In this section, we emphasize that the PIV card is best suited for identification

and authentication. By using a standard PIV card, the readers and infrastructure components can be the same. This will drive down costs as volume increases.

The NIST assumed the Secure Hash Algorithm (SHA-1), part of the digital signature process, had a computational complexity of 2^{80} (or 80 bits)[1]. A recent attack has reduced the computational complexity to under 69-bits. Assume the 56-bit key length Data Encryption Standard (DES) was broken in 1997. The difference in bit (69 – 56) is only 13 bits. If we apply a modification to Moore's Law[2], where the technology doubles every 18 months, then the 13 bits represents 19.5 years. Thus, if there re no other weaknesses found, the SHA-1 can be expected to survive no longer than 2016. This weakness is based on collisions. That is, we take two messages and we manipulate the white space so that the hash vales are the same. We then get the party to sign the seemingly good message and we have another bogus message that will equally validate.

So why worry? The Common Policy requires Public Key Infrastructure (PKI) records be retained for 10 years and 6 months. If we have digitally signed records, with long retention periods, then bogus signed documents can be generated in the future claiming legality based on past signatures. For example, consider a digitally signed Will. Forty years from now, the person dies with a small fortune amassed. Then ten people with digitally signed Wills appear. Which of the 10 are bogus? To be effective, the technology must stand the test of time. Based on this simplistic analysis, caution is advised for long retention period digital signatures until the new NIST algorithms are required (2010).

Where the PIV Card comes into its own is for identification and authentication. The Intelligence Reform and Terrorism Prevention Act of 2004 establish minimum standards for driver's licenses and birth certificates. Additionally, H.R. 418, if it passes, will require machine readable driver's licenses. It is clear that driver's licenses are undergoing change. This is worth exploring further. What is the most common use of a driver's license? It is perhaps the most widely used form of identification. Thus is has an established role in identification and authentication. Would it not make sense to extend the functionality to allow citizens cryptographic capabilities on their licenses? After all, the big expense is in verifying a person's identity before the state's department of motor vehicles in the first place.

What about the arguments against establishing a National ID? Unfortunately, the SSN has made the National ID a reality. The difference is that the SSN can easily be used to steal your identity. To preserve citizen privacy, the confidentiality controls in protecting National IDs need to be strengthened. The PIV card is a technology to accomplish this task. If we accept a person's digital credentials instead of their SSN, we will be reducing the risk associated with identity theft.

---

[1] Each bit doubles the number of unique values. For example, a 2-bit number has four possible values (00, 01, 10, & 11). Thus, 2^n can be represented by n bits.

[2] Gordon Moore, the co-founder of Intel, coined a law where the number of transistors that could be applied to a chip doubled every couple of years.

Summary:

This paper addressed the need for a hard token recommends the investment applied to the PIV card be expanded. The threat to computers and networks is greater than ever. If we are to address the challenges ahead in a cost-effective manner, then the PIV card is a viable solution. There are many overlapping areas where federal employees, such as the TSA, operate in facilities shared outside of the federal government. By using a common approach, cost and quality can be improved. HSPD-12 requires government agencies to report on those areas not addressed that should be included. Based on the abbreviated arguments presented, I believe the law makers need to provide the legal and financial backing for states to incorporate the PIV card infrastructure into their driver's license program. This will then provide the average citizen with a strong multi-factor cryptographic card for establishing identity and authentication. This in turn should start the long process to move away from depending on numbers to authenticate people.

References:

[1] Davis, Ruth M., Computers and People, *Privacy and Security in Data Systems*, pages 20 -26, March, 1974.

[2] Matley, Ben G.,"Computer Privacy In America: Conflicting Practices and Policy Choices," *Proceedings of the 1985 Symposium on Security and Privacy*, pp. 219-223.

[3] US Secret Service Press Release Pub 08-03, *Colombian Police And United States Secret Service Seize $20 Million In Counterfeit U.S. Currency*, 2003.

[4] Federal Trade Commision, *National and State Trends in Fraud& Identity Theft January - December 2004*, February 1, 2005.

[5] Tynan, Daniel, PC World, Zombie PCs: Silent, Growing Threat, July 9, 2004.

[6] Foster, Caxton C., Computers and Automation, *Data Banks – A Position Paper*, pages 28 – 30, March, 1971.

[7] Reuters, *U.S. Senator Seeks Safeguards After Identity Theft*, March 29, 2005.

[8] Mccullagh, Declan, Hackers steal ID info from Virginia university, CNET, January 10, 2005.

[9] Nowell, Paul, *Bank of America says tapes with customer data lost*, Associated Press, February 26, 2005.

[10] Barba, Robert, The Denver Post, Virus Puts Brakes on Licensing for the Week, Page B1, September 22, 2004.

[11] CBS News, Too Many Lost Uniforms & Badges. July 23, 2003.