Protecting Identities and Stopping Crime with Digital eIDs

IIIII A Brief for Policy Makers

http://www.gemalto.com/public_sector/

gemalto
security to be free

Table of Contents

Protecting Identities and Stopping Crime with Digital eIDs

A Brief for Policy Makers

Trust in an identity is fundamental to our society, enabling individuals to interact with government agencies, businesses and one another.

Yet in today's technologically advanced and interconnected world, trust in and protection of identity has become increasingly problematic in the United States:

- Identity Theft has been the number one consumer complaint to the Federal Trade Commission for more than 10 years in a row, which estimates as many as 9 million people have their identities stolen every year[1]
- More than 535 million U.S. personal data records have been breached since 2005 when public disclosures first became required by law in California[2]
- Fraudulent use of identities costs government agencies billions; the Department of Justice estimates Medicare fraud alone is $60 billion per year[3]
- Stolen or fraudulent identities are so widely used globally in illegal drug trafficking, money laundering and terrorist financing, that policymakers mandate customer identification programs for financial institutions and other regulated companies under the Bank Secrecy Act and USA PATRIOT Act
- 40% of registered online identities are fake, according to industry estimates[4]

Clearly problems with identity theft and fraudulent use of identities are rampant, and they are hurting individuals, businesses and government programs through direct losses to fraud, remediation costs and time. According to a 2010 report from the U.S. Department of Justice, it takes 130 person-hours to rebuild a digital identity after it has been compromised.

One of the primary factors underlying these problems is the lack of security in government-issued identity credentials.

---

1 "About Identity Theft,» FTC website, August 18, 2011, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

2 "Chronology of Data Security Breaches 2005 – Present," Privacy Rights Clearinghouse website, August 21, 2011, http://www.privacyrights.org/data-breach#2

3 "Knowing who you are; could save the US billions ," Secure ID Coalition blog, April 6, 2011, http://www.secureidcoalition.org/index.php/news/blog/35-blog/85-knowing-who-you-are-could-save-the-us-billions-

4 "Infographic: 40% of Online IDs are Fakes," ReadWriteWeb Enterprise, August 31, 2011, http://www.readwriteweb.com/enterprise/2011/08/infographic-40-of-online-ids-a.php

For example, Social Security cards have no security features, even though a Social Security number is one of the primary and most frequently used personal identifiers in America. U.S. Senators Charles Schumer from New York and Lindsey Graham from South Carolina have also cited the lack of security in Social Security IDs as a major barrier to the implementation of immigration reform.[5]

Driver's Licenses issued by all U.S. jurisdictions are also a primary identification document in our society. As fraudsters continue to make realistic simulations of many of the state's issued driver's licenses and ID cards, little has been achieved to improve the basic document. Adding a chip to the document will exponentially increase the difficulty to counterfeit it and also bring new cost savings to states in regard to consolidating how they interact with their citizens. Presently states issue multiple identity documents to citizens for many purposes such as additional fishing, hunting, concealed carry licenses, benefits such as Medicaid, WIC, etc. All of these programs could be consolidated into one multi-application eID on the driver's license and reduce how many times a state collects and maintains identity information. Privacy protections come with the chip technology to ensure only the minimal information required to gain access to a service is used, unlike today's plastic version where all their PII is visually readable off the printed card to any person.

Similarly, Medicare and other health insurance ID cards lack security features, exposing all stakeholders to pervasive fraud problems. According to a recent Ponemon Institute study, nearly 1.5 million Americans have been victims of medical identity theft with an estimated total cost of $28.6 billion – or approximately $20,000 per victim.[6] Further evidence of the significance of the medical fraud problem is the allocation of $1.7 billion for fraud detection in the 2011 U.S. Health and Human Services Department budget.[7]

There are many government programs, however, in the United States and other countries that are protecting identity and re-establishing trust by implementing electronic versions of secure documents such as passports, national ID cards, drivers' licenses or healthcare cards. These "eID" credentials are now equipped with an electronic component based on smart card technology that is either embedded within the card or – as in the case of passports – within the cover or a polycarbonate data page.

eIDs provide stronger security than their conventional counterparts to prevent counterfeiting or alteration of documents and to protect citizens' privacy and identities. They also enable "two-factor authentication" for more secure delivery of online services for eGovernment, eHealth and eCommerce. "Two-factor authentication" is the use of something you have — the eID — in addition to something you know — a PIN code or password — in order to access information or conduct transactions. Another eID security option is to use something you are, a biometric such as a digital picture or fingerprint, as a second or even third authentication factor.

This brief discusses the progress in the United States in using and establishing eID digital identity credentialing, and explores other opportunities to use eIDs that are under consideration.

---

[5] "The right way to mend immigration," by Charles E. Schumer and Lindsey O. Graham, *Washington Post*, March 19, 2010

[6] Survey conducted by The Ponemon Institute in February 2010

[7] "HHS Budget Makes Smart Investments, Protects the Health and Safety of America's Families," Feb 1,2010, http://www.hhs.gov/news/press/2010pres/02/20100201a.html

eID in the United States: ePassports

The most advanced eID program in the United States and the rest of the world as well is the electronic passport, or ePassport. An estimated 90 countries are now deploying ePassports with highly secure features to prove the authenticity of the document, the presenter of the document, including their identity and country of origin.

The ePassport illustrates many of the reasons why eID credentials are more secure, and while this initiative targets national security and the global war on terror, the same technology and methods can be used to protect identities and reduce the risk of fraud in any government-sponsored program.

The U.S. ePassport is the same as a traditional passport book with the addition of a small, embedded integrated circuit (or chip). In the United States and many other countries, the chip is embedded in the back cover. The embedded chip is a secure microcontroller with advanced cryptography and built-in sensors to detect attacks.
The chip stores:

- The same data visually displayed on the data page of the passport
- The passport holder picture stored in digital form
- The unique chip identification number
- A digital signature to detect data alteration and verify signing authority

These features and the computer-chip make U.S. ePassports more secure than traditional passports. First, it provides border protection officers with a new tool to more tightly tie the bearer's identity to the ePassport by adding the electronic version of the printed document in the chip. (See illustration) Second, the secure microcontroller chips incorporated into the booklet significantly increase the difficulty of passport forgery. This is because unlike traditional paper-only passports, when the ePassport is personalized and issued, the data which has been written to the chip is electronically signed using a digital signing key. This is the digital equivalent to a public notary's seal certifying a document. Once manufactured, personalized and digitally signed, no information in the chip can be changed.

ePassport

What happens at passport control:

1. The officer swipes the data page through a special reader to read the two lines of printed characters on the bottom of the data page. This provides a key that's unique to the passport and lets the process proceed.

2. The officer holds open the passport over another reader, then checks his view of the passport owner (a), with the photo in the passport (b), and all the data from the passport (including photo) on the monitor (c).

   The data on the monitor also verifies the passport was issued by a legitimate authority, and that it has not been altered.

Layers of security:

3. A chip is embedded into the back cover. It contains data that cannot be read without the security key as shown in step one above.

4. When the passport is held over the reader (no contact is necessary), a radio field from the reader wakes up the chip, and the encrypted data is transferred to the reader, allowing the officer to conduct his visual check.

Privacy protection:

5. A thin radio shield can be sandwiched between the front cover and the first page. Whenever the passport is closed—for instance, in a pocket or briefcase—the digital information in the chip cannot be read. The shield will not set off airport metal detectors.

Source: Gemalto

The Federal eIDs: PIV and CAC Cards

Perhaps the best model for how to better protect identities and establish trust with eIDs is the U.S. federal government's own credentialing standard, the Personal Identity Verification (PIV) card issued to all federal employees and subcontractors, and the Department of Defense version, the Common Access Card (CAC). Like the ePassport, the PIV and CAC eIDs are smart cards with embedded microprocessor chips that make them highly secure and useable for many different applications.

Driven by the issuance of Homeland Security Presidential Directive 12 (HSPD-12) in 2004, the U.S. federal government has invested significant effort and resources in implementing robust, interoperable and governmentwide credentialing processes and technologies. The resulting standard, Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, provides a framework of the policies, processes, and technology required to establish a strong, comprehensive program.

In addition to vetting identities and issuing millions of PIV cards, federal agencies have developed an infrastructure for using these interoperable credentials to support additional functions including:

- Physical security, including facility access and video analytics
- Logical security, including network and application access
- Incident monitoring and response
- Encryption and protection of sensitive data

State and local governments and other organizations can leverage the federal program. Two publications — Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers (issued by the Federal CIO Council in May 2009) and PIV-I Frequently Asked Questions — provide states, local jurisdictions, and commercial organizations with applicable standards and guidance.

The PIV framework provides a strong foundation for planning and implementing any eID program at any level of government. In addition to its strong identity security and multi-application capabilities, it has a number of advantages for any government enterprise looking to better protect individual identities and reduce losses from fraud, including:

- Mature federal standards
- Supporting framework of policies, processes and technologies
- Availability of compliant commercial off-the-shelf (COTS) GSA approved
- Testing standards and laboratories at NIST and other labs
- Ability to use a single, interoperable and secure credential across multiple application areas

Bi-partisan Bill Proposes an eID for Medicare Beneficiaries and Providers

An eID not only protects individuals, it can be used to fight fraud. To combat a reported $60 billion loss to waste, fraud and abuse within the Medicare system, a bi-partisan group of U.S. senators and representatives led by Senators Mark Kirk (R-IL) and Ron Widen (D-OR) have introduced legislation to use existing “smart card“ technology to protect seniors.

The Medicare Common Access Card Act of 2011 (S. 1551 and H.R. 2925) would establish a pilot program to develop a secure Medicare card using smart card technology to protect seniors’ personal information, prevent fraud and speed payment to doctors and hospitals. It is estimated that upgrading the Medicare system with globally proven smart card technology could save the American taxpayer $30 billion or more per year in fraud and waste reductions.

A Medicare eID would stop fraud and save money by:

- Preventing phantom billing: the beneficiary, the provider and their Medicare eIDs must be present to process a transaction
- Reducing Medicare identity theft: an eID protects the identities of beneficiaries because the card must be present to make a claim, it is protected by a PIN code and it cannot be forged, alternatively the PIN can be replaced with a biometric matched in the card
- Reducing administrative errors: accurately identifies and confirms eligibility for both beneficiary and healthcare provider

In a system that is riddled with fraud, waste and abuse, the bill's co-sponsors suggest that knowing who is receiving services and who is providing them could significantly lower costs. They point out that the current Medicare card has virtually no security features and clearly displays the individual's Social Security number. Not only can the outdated Medicare card be easily duplicated, fostering fraud within the Medicare system, but its public presentation of social security numbers creates further risk of identity theft among seniors.

Medicare Common Access Card

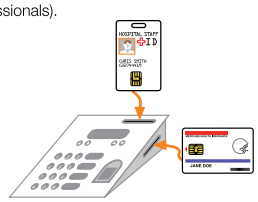
1. Medicare beneficiaries and service providers receive a secure ID card .

The smart card contains a computer chip that fights fraud and protects privacy.

What's stored on the ID card:

- A unique Medicare identity.
- A digital picture of the healthcare professional.
- A PIN code (beneficiaries) or biometric (professionals).
- Match on card software: PIN or biometric stays in the card.

2. At the doctor's office, both the ID cards are inserted into the reader. The chip on the card electronically confirms the card is legitimate.



3. The doctor confirms his or her identity by touching the biometric reader, and the beneficiary by entering a PIN code, proving both were there.

4. Transaction is confirmed and a secure authenticated information packet is sent to the payment processor.

Source: Gemalto

The idea was stimulated by looking at the Department of Defense (DoD) Common Access Card or the CAC, as a model for a secure eID to replace today's insecure Medicare cards. The DoD CAC incorporates multiple security features including the owner's picture, signature, and an embedded micro- processor chip. The difference in security features on each of these cards result in dramatic differences in the level of security and information protection. DoD's CAC has never been counterfeited, while the Medicare Card is an easy target.

A smart card-based Medicare CAC would protect our seniors from identity theft and reduce fraud in the Medicare system by upgrading the Medicare card to use the same underlying technology and standards as the DoD CAC. One very important additional protection from identity theft and abuse in Medicare is to remove the senior's printed social security number from the card and embed it securely into the chip. It would only be securely communicated once the senior authenticates their presence to the card at the point of transaction. This inexpensive eID proposal would eliminate a significant amount of fraud in the Medicare system and save taxpayers billions of dollars in the first full year of deployment.

U.S. Senator Mark Kirk has produced a video, *Medicare Fraud and the Common Access Card Explained*,[8] and the AARP has also endorsed the Medicare Common Access Card proposal.[9]

---

[8] "Medicare Fraud and the Common Access Card Explained," by Senator Mark Kirk, YouTube.com, September 2011, http://www.youtube.com/watch?v=lvn02O8En54&feature=player_embedded

[9] AARP.com, September 2011, http://www.aarp.org/about-aarp/press-center/info-09-2011/aarp-joins-bipartisan-effort-to-prevent-identity-theft-of-medicare-beneficiaries.html

A Biometric Social Security Card

U.S. Senators Charles Schumer from New York and Lindsey Graham from South Carolina have proposed an eID, a biometric Social Security card, as an essential component of immigration reform.[10]

In their view, one of the major difficulties with immigration reform is the fact that there is no reliable way for employers to verify that prospective employees are in the United States legally and eligible for employment.

That could change, however, if all U.S. citizens and legal immigrants who want jobs were required to obtain a high-tech, fraud-proof version of the Social Security card that citizens already have.

The eID technology envisioned for Social Security would be similar to the PIV card, with the addition of a unique biometric identifier stored only on the card. This would prevent anyone from using or stealing someone else's card. It would also have the same protections against counterfeiting or altering cards that are already proven in other eID programs.

Employers would be able to use a card reader to verify that the card is authentic and that the person presenting the card is actually its owner and is eligible to work in the United States.

In addition to its potential benefits for controlling immigration, a Social Security eID would help to protect citizens against identity theft because the card owner could use the card as digital proof of his or her ownership of the Social Security number. Again the printed social security number would be removed from the card and embedded securely in the chip to protect the Citizen's privacy and protect them from Identity Theft.

State Level eIDs and First Responders

Many state and local organizations point to the PIV-I standard and the availability of over 500 PIV-compliant products currently on the General Services Administration (GSA) Approved Products List as ways to achieve a more holistic approach to issuing eIDs and improving their own business processes. Two publications—*Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers*[11] (issued by the Federal CIO Council in May 2009) and *PIV-I Frequently Asked Questions*[12]—provide states, local jurisdictions and commercial organizations with applicable standards and guidance.

More than 16 states are currently planning or implementing some form of PIV-I strategy.[13]

During the April 2010 National Association of State Chief Information Officers (NASCIO) Digital Identity Workshop, a working group was established to put together a charter for a NASCIO Digital Identity Working Group. Many states and jurisdictions already use components of PIV-I policy or process, such as strong identity vetting procedures, public key infrastructure (PKI), and smart cards within their enterprises. These existing components can be leveraged to establish interoperable digital identities.

---

[10] Schumer, Lindsey, *Washington Post*

[11] "Personal Identity Verification Interoperability for Non-Federal Issuers," Version 1.1, Federal CIO Council, July 2010, http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf

[12] "Personal Identity Verification Interoperable (PIV-I): Frequently Asked Questions (FAQ)," Version 1.0, CIO Council, June 28, 2010, http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf

[13] "Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses," The Smart Card Alliance, February 2011, http://www.smartcardalliance.org/pages/publications-piv-i-for-non-federal-issuers

One of the principal drivers has been a joint effort between local, state and federal government agencies to determine a way to securely identify emergency responders, especially during a crisis for disaster situation. Known as First Responder Authentication Credential (FRAC) programs, these PIV-I eID credentials are being used in regional and national interoperability exercises sponsored by the Federal Emergency Management Agency (FEMA) and for piloting operations in other areas, such as accessing federal systems.

Early state adoption of PIV-I credentials and infrastructure in the Commonwealth of Virginia, the State of Colorado and the State of Illinois has established baselines for achieving interoperability with federal credentials, services and systems.

eID credentials issued by states can be made more widely applicable, be used more efficiently and enhance citizen privacy. States can move from issuing multiple credentials for a variety of state programs to issuing a single, multi-purpose, trusted PIV-I credential.

An eID for Electronically Prescribing Controlled Substances

On March 24, 2010, the Drug Enforcement Administration (DEA) published an interim final rule (IFF) in The Federal Register. In the new regulation, users of e-prescribing systems for controlled substances would prove their identities with two of the following three factors: something you know (password); something you have (token); something you are (biometric).

The IFF states, "Authentication based only on knowledge factors is easily subverted because they can be observed, guessed, or hacked and used without the practitioner's knowledge. In the interim final rule DEA is allowing the use of a biometric as a substitute for a hard token or a password."

As a very high assurance identity credential, an eID based on PIV-I would meet and exceed the authentication requirements mandated by the DEA.

eIDs and The National Strategy for Trusted Identities in Cyberspace

The White House Administration correctly recognizes that there are very real problems of identity management, privacy and security in our society today, especially on the Internet, and they are bringing a much needed focus to bear on solving the problems with the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative.

The NSTIC guiding document explains that the need for such a strategy is due to the rising tide of identity theft, online fraud and cyber intrusions, the proliferation of usernames and passwords that individuals must remember, and the need to deliver online services more securely and efficiently.

The vision is for a new Identity Ecosystem that will better protect people's identities and eCommerce transactions on the Internet. The NSTIC initiative is very practical in its approach because it limits the federal government's role to being an enabler, facilitator and accelerator of the Identity Ecosystem development. It specifically states government will not impose mandates or be the owner of the identities. There is a clear recognition that many different public and private stakeholders will be involved in working out the specifics of the identity framework and ultimately putting it to use.

While an Identity Ecosystem is intentionally broad in scope, providing a wide range of trusted identity constructs and identity protection technologies, it indicates that for high-value identities such as for banking or health care, some type of eID would be required. It mentions smart card technology as the kind of technology appropriate for an identity medium, or a personal security device to protect identities in online transactions and prevent others from stealing or misusing identities.

One way to make high-value identity transactions both secure and easy to use is the familiar approach of a card and PIN as an identity medium; however, to achieve high levels of security, the card must include smart card technology to carry PKI credentials, biometrics and other security features. Other important advantages are that this would create a portable identity medium, and it provides a secure environment that is independent from the PC, thereby side-stepping issues involved with PC, website and service provider hacker threats.

An Identity Ecosystem that includes smart card technology as an identity medium for high-assurance online identity transactions will provide a very strong and proven foundation for protecting identities in cyberspace in a secure, privacy sensitive manner. This foundation can be put in place without reinventing the wheel. From its PIV and PIV-I activity, the federal government has already established a set of best practices, standards and technology solutions for smart card-based identity management and authentication that can be adapted to this initiative.

The Role of Government: Setting a Higher Standard for Identity and e-Commerce Protection

150 years ago there were several competing standards for the gauge, or width, of railroad tracks. When the federal government funded the first transcontinental Railroad in 1863, it mandated the use of standard gauge tracks. That settled the issue and within four years all of the major rail systems in the United States had converted to standard gauge.

In 1933, after the private ownership of gold coins, bullion and certificates by American citizens was outlawed, the value of the Federal Reserve's gold swelled from $4 billion to $12 billion but there was no place to store it. To secure the national treasure, the federal government built the U.S. Bullion Depository at Fort Knox, Kentucky. Even today it still holds roughly 2.5% of all of the gold ever mined.

In retrospect, decisions to standardize the railroad track gauge and to build a secure gold depository seem obvious. Today, however, our society's interconnections, citizen and government interactions, and commerce are increasingly electronic transactions. Yet the problems that need government leadership are the same: standards and security.

Unlike our nation's gold reserves, our $10 trillion per year of Internet-based e-commerce[14] cannot be placed into a single depository. Nonetheless, the need to protect e-commerce transactions and the identities of individuals participating Internet-based transactions or government-funded programs is just as acute.

Government at all levels must provide the leadership for standards and infrastructure that can:

- Protect individual's identities in cyberspace
- Facility and secure e-commerce
- Prevent fraud and abuse which is rampant in important federal programs like Medicare

[14] April 15, 2011, Launch of the National Strategy for Trusted Identities in Cyberspace, U.S. Secretary of Commerce Gary Locke, http://www.nist.gov/nstic/launch-transcript.html

The U.S. federal government has already established that eIDs, based on smart card technology and potentially biometrics, solve these problems and ensure that security and privacy requirements are met for individuals while maintaining trust and preventing fraud. Today smart card eID technology secures:

- The U.S. and global electronic passport program
- The U.S. federal government interoperable Personal Identity Verification (PIV) card, used to secure both physical facility and information system access
- The first responder identity credentials, being developed under the offices of the Federal Emergency Management Agency (FEMA), the Department of Homeland Security (DHS) and cooperating state and local governments

Federal, state and local government leaders need to take decisive action to broaden the use of eIDs to solve the problems facing our Internet connected and e-commerce based society:

- Support the Medicare CAC Card bill to help eliminate $30 billion annually in waste and fraud from the Medicare program
- Set standards for high assurance Internet identity production in transactions comparable to the federal government's own PIV program
- Prioritize the use of high assurance smart card-based eIDs for other government programs such as Social Security and driver's licenses to help prevent fraud and abuse and protect individual's identities

eIDs based on current established federal smart card standards and proven technology provide a strong foundation for achieving all of these goals.

If you are involved in managing a government program and would like more information about how eID can achieve these goals for you, please consider contacting Gemalto North America. We would be happy to provide you with ideas on how you can benefit with eID, drawing from our experience in the U.S. PIV, CAC and ePassport programs as well as dozens of other eID projects around the world.

If you are involved in managing a government program and would like more information about how eID can achieve these goals for you, please consider contacting Gemalto North America. We would be happy to provide you with ideas on how you can benefit with eID, drawing from our experience in the U.S. PIV, CAC and ePassport programs as well as dozens of other eID projects around the world.

Interested in learning more?

To speak with a Gemalto representative please call 888.343.5773 or send a message to noramgov@gemalto.com

Gemalto, Inc.
Arboretum Plaza II
9442 Capital of Texas Highway North, Suite 400
Austin, TX 78759

The world leader in digital security

http://www.gemalto.com/public_sector/

gemalto
security to be free