



**Smart Card  
Alliance**

***Securing Identity and Enabling Employment  
Verification: How Do Immigration Reform and  
Citizen Identification Align?***

*A Smart Card Alliance Identity Council White Paper*

*Publication Date: May 2010*

*Publication Number: IC-10001*

**Smart Card Alliance**  
191 Clarksville Rd.  
Princeton Junction, NJ 08550  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

## ***About the Smart Card Alliance***

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit <http://www.smartcardalliance.org>.

Copyright © 2010 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

# TABLE OF CONTENTS

- 1 EXECUTIVE SUMMARY..... 4**
- 2 IMMIGRATION REFORM AND EMPLOYMENT IDENTIFICATION AND VERIFICATION OVERVIEW..... 5**
  - 2.1 INTRODUCTION ..... 5
  - 2.2 BACKGROUND..... 5
- 3 SECURING ENROLLMENT, CREDENTIALING, AND VERIFICATION OF WORK-ELIGIBLE PEOPLE ..... 7**
  - 3.1 DEALING WITH FRAUD ..... 7
    - 3.1.1 *Preventative Measures* ..... 7
    - 3.1.2 *Mitigating Measures* ..... 7
  - 3.2 SMART CARD TECHNOLOGY AND IDENTITY APPLICATIONS ..... 7
  - 3.3 A SOLUTION FOR THE IMMIGRATION REFORM/EMPLOYMENT ELIGIBILITY CREDENTIALING CHALLENGE..... 9
  - 3.4 BIOMETRIC OPTIONS ..... 10
  - 3.5 PRIVACY ..... 11
  - 3.6 EMPLOYMENT VERIFICATION ..... 12
- 4 USE CASES FOR ENROLLMENT AND USE..... 13**
  - 4.1 ENROLLMENT THROUGH EXISTING ORGANIZATIONS AND INFRASTRUCTURE ..... 13
  - 4.2 EXAMPLE PROCESS FOR UPGRADING THE SOCIAL SECURITY CARD ..... 13
  - 4.3 VERIFICATION PROCESS AT THE EMPLOYER ..... 14
- 5 CONCLUSIONS: THE MOST IMPORTANT CONSIDERATIONS FOR POLICY MAKERS..... 15**
- 6 PUBLICATION ACKNOWLEDGEMENTS..... 16**

# 1 Executive Summary

Immigration reform discussion over the last two centuries has been extensive and often polarizing, bringing out extreme responses to attempts for reform. One unintended consequence of the Immigration Reform and Control Act of 1986 (IRCA) has been the proliferation of fraudulent identity documents. Using fraudulent documents to obtain government benefits is seen as a threat to national security and undermines the integrity and fairness of all government programs and of the U.S. immigration system.

Little progress has been made in increasing the physical security of documents (such as Social Security cards and driver's licenses) to meet the 9/11 Commission's recommendations. A robust system of identification and secure identification documents is a key requirement that needs to be addressed in the immigration reform debate. This white paper provides considerations for stakeholders in the debate on how the use of smart card and biometric technology can provide a high level of confidence in the identity of the document holder and help to validate status and entitlement.

The Smart Card Alliance understands the importance of taking all aspects of the issue of immigration reform into consideration when making decisions and setting policy. Social, environmental, economic, legal, and political effects need to be addressed to determine the options from which to choose. This document limits itself to providing factual information to allow the reader to make educated and informed decisions.

An upgraded Social Security card incorporating biometric identity credentials enables a true authentication process that will benefit workers, employers, and government. Biometric identifiers link identity to the physical person, providing "something you are" as part of the identification process. A secure electronic credential can also protect the security and privacy of personal and biometric data stored on the card. Such a credential will enable three things:

1. Privacy is enhanced since the individual is in possession of the card and can control who can access the data stored in the card.
2. The legitimacy of the card can be confirmed through electronic authentication processes.
3. The system can easily scale to support large populations and many organizations.

Identity management is a fundamental issue for immigration reform. A solid immigration identity foundation is required to support any efforts to improve the immigration system, reduce administrative costs, fight immigration document and benefit fraud, and prevent identity theft. Industry-proven technologies and existing Federal government standards can be leveraged to create an effective immigration identity management infrastructure and implement flexible, secure, and cost-effective credentials in support of immigration reform.

The Smart Card Alliance believes that smart cards can be a foundational technology that creates strong identity credentials to protect our citizens' identities and facilitate the secure verification of identity, immigration status, and employment eligibility. A smart card-based Social Security card with biometric identity credentials incorporated into the document provides a secure identity credential. If policymakers proceed to reform immigration in the United States, we recommend that they consider:

- Developing and communicating a strong, clear privacy and security policy for immigration reform
- Leveraging existing government secure credential standards and procedures
- Using smart card technology to provide a highly secure and privacy-sensitive platform to support an identity management framework for immigration reform and employment eligibility verification

## **2 Immigration Reform and Employment Identification and Verification Overview**

### **2.1 Introduction**

This paper provides support for the use of smart card technology, assisted by biometric identity verification, for immigration reform and for employment identification and verification in the United States.

On December 15, 2009, Representative Luis Gutierrez (D-Illinois), along with 91 co-sponsors, introduced the Comprehensive Immigration Reform for America's Security and Prosperity Act of 2009 (CIR ASAP), H.R. 4321. This act marks the latest Congressional effort to address immigration reform. The last major reform took place in 1986, with the passage of the Immigration Reform and Control Act (IRCA). Several immigration reform initiatives have been introduced since the IRCA, but none have passed.

In March 2010, Senators Charles Schumer (D-New York) and Lindsay Graham (R-South Carolina) renewed a push for immigration reform aimed at an overhaul of the nation's immigration laws, outlining a plan to require U.S. citizens and legal immigrants to obtain a high-tech Social Security card linked to the cardholder's fingerprints or other biometric identifier.<sup>1</sup>

Immigration reform discussion over the last two centuries has been extensive and often polarizing, bringing out extreme responses to attempts for reform. One unintended consequence of the IRCA has been the proliferation of fraudulent identity documents. Using fraudulent documents to obtain government benefits is seen as a threat to national security and undermines the integrity and fairness of all government programs and of the U.S. immigration system.

While many different elements can affect both the debate over immigration reform and the eventual outcome, this white paper addresses one key question only: how to provide secure credentials and identity proofing using available technology. The answer to this question will help address the significant issue of fraud and support the development of an integrated, encompassing, and viable legislative proposal to reform immigration policy and rules in the United States.

### **2.2 Background**

In 1986, when the IRCA passed, an estimated 3.2 million<sup>2</sup> unauthorized immigrants were in the United States. As of January 2009, this number was estimated at around 10.8 million.<sup>3</sup> One of the negative results of IRCA's requirement that employers check employment eligibility was an exponential increase in the use by job applicants and acceptance by employers of fraudulent documents to indicate legal presence. The IRCA inadvertently created a booming counterfeit document market.<sup>4</sup>

The 9/11 Commission investigations showed that immigration violations were committed by one or more of the 9/11 hijackers. One of the conclusions of 9/11 Commission report<sup>5</sup> was that there is a need for standards for issuing birth certificates and other sources of identification, such as driver's licenses. This conclusion culminated in the provisions of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) that require the establishment of new standards to ensure the integrity of the three basic documents Americans use to establish their identity: birth certificates, state-issued driver's licenses and identification cards, and Social Security cards. The provisions include requirements to ensure that the applicant for an identity document is actually the person whom the applicant is claiming to be. The IRTPA also addressed the need for improved physical security surrounding the document issuing process.

---

<sup>1</sup> "Senators draft plan to rework U.S. immigration policy," *The Washington Post*, Thursday, March 18, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031803762.html>.

<sup>2</sup> Ruth Ellen Wasem, "Unauthorized Aliens in the United States: Estimates Since 1986," *CRS Report for Congress*, September 15, 2004, page 3, [http://www.immigrationforum.org/documents/crs/CRS\\_undocumented\\_2004.pdf](http://www.immigrationforum.org/documents/crs/CRS_undocumented_2004.pdf).

<sup>3</sup> "Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2009," Dept. of Homeland Security, January 2010, [http://www.dhs.gov/xlibrary/assets/statistics/publications/ois\\_ill\\_pe\\_2009.pdf](http://www.dhs.gov/xlibrary/assets/statistics/publications/ois_ill_pe_2009.pdf)

<sup>4</sup> Robert Suro, "Boom in Fake Identity Cards for Aliens," *The New York Times*, February 19, 1992, <http://www.nytimes.com/1992/02/19/us/boom-in-fake-identity-cards-for-aliens.html?pagewanted=all>.

<sup>5</sup> "The 9/11 Commission Report," <http://www.9-11commission.gov/report/911Report.pdf>

In 2006, an immigration reform bill was introduced that required the issuance of secure, machine-readable biometric documents<sup>6</sup> and included new biometric entry and exit requirements. This was followed in 2007 by another bill requiring the government to implement new entry and exit requirements and calling for greater interoperability among biometrics databases.<sup>7</sup> Since April 2006, U.S. Immigration and Customs Enforcement established 19 document and benefit task forces (DBTFs) to focus on detecting, deterring, and disrupting document and benefit fraud. From April 2006 through June 2009, DBTFs have initiated more than 2,130 investigations, helped bring about 1,534 indictments and 1,815 criminal arrests, and resulted in 1,293 convictions.<sup>8</sup>

Knowing that an individual is who that individual claims to be is essential to the success of any new immigration reform effort. Such a verification process is the only way to ensure that U.S. workers and legal immigrants are eligible for employment and that illegal immigrants are not. However, today there is no effective way for the nation's 7 million employers to realistically determine an individual's identity and status. Efforts around E-verify<sup>9</sup>, the Department of Homeland Security (DHS) system for employers to determine the eligibility of an employee to work in the United States, are an important step forward but do not get to the heart of the issue: Am I who I say I am, and how can I prove it?

The Social Security number system currently used to verify workers is paper-based, unless the number is checked through E-Verify or Social Security Online Verification (SSOLV). All that is required for verification is the number from an identification credential that is issued without the benefit of security features or electronic verification processes. For this reason, stolen Social Security numbers are widely available; in some cases, numbers are simply made up. Other identity credentials, including driver's licenses, are easily counterfeited or can be obtained through fraudulent means.

Little progress has been made in increasing the physical security of documents (such as Social Security cards and driver's licenses) that can be used for identification purposes to meet the 9/11 Commission's recommendations. Identification and identification document requirements are key elements that need to be addressed in the immigration reform debate. This white paper provides considerations for stakeholders in that debate on how a strong identity management platform is critical to the reform and how the use of smart card and biometric technology can provide a high level of assurance of the identity of a document holder and help to validate status and entitlement.

An upgraded Social Security card incorporating biometric identity credentials enables a true authentication process that will benefit workers, employers, and government. Biometric identifiers link identity to the physical person, providing "something you are" as part of the identification process. Equally important to the security and privacy protection of personal and biometric data is the requirement that both elements be tied to a secure electronic credential. Such a credential will enable three things:

1. The individual holds the data and can control who can access the data.
2. Electronic authentication of the credential can confirm its legitimacy.
3. The authentication capability can easily scale to support large numbers of individuals and organizations, depending on the requirements of the application.

The Smart Card Alliance understands the importance of taking all aspects of the issue of immigration reform into consideration when making decisions and setting policy. Social, environmental, economic, legal, and political effects need to be addressed to determine the options from which to choose. This document limits itself to providing factual information to allow the reader to make educated and informed decisions.

---

<sup>6</sup> 2006 – S.2611 (as amended).

<sup>7</sup> 2007 – S.1639.

<sup>8</sup> "Document and Benefit Fraud task forces expand to Houston and San Juan," U.S. Immigration and Customs Enforcement, August 26, 2009, <http://www.ice.gov/pi/nr/0908/090826washington.htm>

<sup>9</sup> U.S. Department of Homeland Security E-Verify Program, [http://www.dhs.gov/files/programs/gc\\_1185221678150.shtm](http://www.dhs.gov/files/programs/gc_1185221678150.shtm)

## **3 Securing Enrollment, Credentialing, and Verification of Work-Eligible People**

### **3.1 Dealing with Fraud**

A number of solutions are commercially available that can assist in dealing with identity fraud in the United States. Generally speaking, they fall into one of two categories: preventative measures or mitigating measures. Card authentication and cardholder verification are examples of preventative fraud measures, because effective authentication and verification mechanisms can prevent fraudulent transactions. If the preventative measures are ineffective, then compensating controls (mitigating measures) are needed to reduce the impact of fraud.

#### **3.1.1 Preventative Measures**

Preventative measures use authentication mechanisms to validate that a identity verification card is authentic or that the person presenting the card is the genuine cardholder. Three factors can be used for authentication:

1. Something you have (such as a credential)
2. Something you know (such as a personal identification number, or PIN)
3. Something you are (a biometric factor, such as a facial image, iris pattern, or fingerprint)

The more factors that are used to authenticate an individual in a transaction, the more reliable the authentication. The financial services world typically uses the first two factors for authentication.

In addition, authentication can be either static or dynamic. Static authentication always uses the same credential or data for validation. Dynamic authentication uses a different credential each time, and the credential used is typically transaction-specific. For example, in the payments industry, magnetic stripe cards validate the same static data with every transaction, while smart cards generate a different, dynamic security value for each authorization request, thereby improving security.

#### **3.1.2 Mitigating Measures**

Fraud mitigating measures address security gaps that fraudsters can exploit. A common cause for these security gaps is the poor performance of the chosen authentication solution. A typical scenario involves using these mitigating measures to address a current fraud attack based on patterns seen in previous fraud attacks. Fraud mitigating measures use information about past fraud trends to reduce the impact of future fraud trends.

### **3.2 Smart Card Technology and Identity Applications**

The selection of an identification (ID) technology is critical to the security of an identity application and system. The ID technology must be one that can both facilitate and reinforce the system's privacy and security design and goals. Many current ID or badging systems rely on technologies such as magnetic stripes or bar codes. Such technologies are no longer appropriate, since they cannot fulfill the requirement to provide strong security while guarding privacy. IDs based on these technologies are tamper-prone, can easily be counterfeited, and provide little or no protection for the information they carry.

A smart card looks very much like a typical credit card, but what makes it "smart" is the small computer chip built into the card. Unlike magnetic stripe or less secure RFID cards, the smart card's computer provides high levels of security and privacy protection, making the technology ideal for preventing fraud or false identification. With the embedded computer, smart cards have built-in tamper resistance and have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signature), and interact intelligently with a smart card reader. Smart cards can readily be used online and across networks and deliver very high levels of security over the Internet. They are also very convenient and easy for people to use.

Only IDs that use smart card technology have the strong security features that can enhance privacy protection in a well-designed and properly implemented system. Relying on smart card technology provides an identity management system with the following advantages:

- **Strong information protection.** Smart card technology protects identity data stored on the ID completely and constantly. Smart card-based IDs can encrypt the identity information stored on them and encrypt communications between the ID and the device that reads the ID, preventing eavesdropping. Smart card technology can lock the personal information on the ID, releasing it only after the owner authorizes the release by providing unique information such as a PIN, password, or biometric factor.
- **Strong ID security.** IDs incorporating smart card technology are extremely difficult to duplicate or forge. In addition to visual anti-counterfeiting and tamper-resistance features such as holograms, microprinting, and optical variable devices, smart card chips have built-in tamper-resistance. The chip in a smart card-based ID includes a variety of hardware and software capabilities that immediately detect and react to tampering attempts, countering possible attacks.
- **Sophisticated “on-card” processing.** Smart cards accomplish many identity management functions within the secure processing environment on the card itself. Smart cards store data, which they can then manage securely, protecting the information both while it is stored and while it is being accessed. On-card processing enables smart card-based IDs to perform on-card functions (for example, encryption, decryption, and other data processing) and to interact securely and intelligently with a card reader. These capabilities have particular importance when an identity management system relies on biometric information to verify the identity of an individual. Smart ID cards can securely store biometric information and do an on-card comparison with the captured biometric to verify an individual’s identity. This capability increases privacy: the individual’s stored biometric information never leaves the ID card (which remains in the individual’s possession) and the stored biometric is compared to the captured biometric within the smart card chip’s secure processing environment.
- **Authenticated and authorized information access.** Smart cards have a unique ability to process information and react to their environment. When secure card access is a requirement, only a smart card-based ID can verify the authenticity of the ID reader and prove its own authenticity to the reader. Smart cards can also verify the authority of the information requestor and grant access only to the information required by that particular request. Stored personal information can be protected further by a unique PIN or biometric factor that the cardholder provides before access is granted to the information.

Implemented properly, smart card technology strengthens the ability of any organization to protect the privacy of individuals whose identity the organization needs to verify. Unlike other IDs, smart card-based IDs can implement a personal “firewall,” releasing only required information and only when it is genuinely required. Smart cards are excellent guardians of personal information and individual privacy.

Smart card-enabled applications are becoming more prevalent in many of today’s businesses. The financial payments industry has moved to smart cards with the majority of regional financial organizations worldwide mandating that financial credit and debit cards be smart cards by a specific date. In addition, contactless smart card technology has been rapidly accepted for fast, convenient, and secure credit and debit payment transactions. Enterprises are issuing smart ID badges to employees to secure physical and logical access, and many government identity programs around the world are issuing smart card-based identity credentials to citizens. Smart card-based healthcare ID cards are also issued by many countries, including France and Germany, which have issued over 140 million smart healthcare ID cards to their citizens.

The Federal Government has also adopted smart card technology for its major credentialing initiatives. The Department of Defense Common Access Card uses smart card technology to credential all military and civilian personnel. The Department of State uses contactless smart card technology for the electronic passport. The Transportation Security Administration has issued biometric-enabled identity smart cards to all private and commercial transportation workers accessing all U.S. maritime ports under

the Transportation Worker Identification Credential (TWIC) program. Smart card-based identity credentials are now being issued to all Federal employees and contractors to help secure access to sensitive Federal facilities and information systems, in compliance with Homeland Security Presidential Directive 12. Existing standards (e.g., FIPS 201<sup>10</sup>) enable corporations and state and local governments to issue smart card-based identity credentials that are interoperable with those used by the Federal Government.

For all of these deployments, the use of smart card technology is essential to the integrity of the credentialing scheme. Smart cards are portable, personal security devices that can securely carry sensitive information, enable secure transactions, validate an individual's identity within a secure system, and verify that an information requestor is authorized to access the information carried on the card. Smart cards not only maintain the integrity of information stored on the card, they also make that information available for secure interactions with the overall system.

The smart card itself is only one component in a smart card-based system implementation. Security mechanisms are typically implemented in the card and at the operating system, software, and system levels, providing layers of security to protect the system and information within the system from unauthorized access. In any smart card system implementation, the issuer needs to determine the risks to which the system will be exposed and implement necessary security measures throughout the system to address those risks.

The government and financial payments industries have also led the way in establishing security evaluation and certification programs for the various layers of smart card security. Standardized evaluations and certifications use trusted third-party labs to verify empirically that specific threats are prevented to a defined level of effectiveness, providing issuers with the confidence that certified products meet specified security requirements.

By placing a secure smart card in the hands of the user, organizations can implement a layered security architecture that addresses expected security risks and implements an end-to-end chain of trust.

Organizations that need to verify identity find that concerns about privacy and the protection of personal information quickly emerge as key issues when new identity management systems are being considered. An organization's specific requirements for safety and security must be balanced against the need to protect the privacy of the individuals whose identities must be verified. This requirement—to identify people unequivocally while also protecting their privacy—shapes every discussion of how to design, build, or implement a new, secure identity management system.

### **3.3 A Solution for the Immigration Reform/Employment Eligibility Credentialing Challenge**

To implement an effective immigration reform/employment eligibility program, employers need to be able to determine whether a prospective employee is actually eligible to work. In addition, a robust identity proofing capability is needed to encourage employers to perform due diligence and limit the inconvenience and cost incurred by employers in the process of determining whether a person is eligible to work.

An identity management solution is not a silver bullet for all immigration management problems; however, it is the cornerstone of any solid solution. The Smart Cards Alliance firmly believes that smart cards provide the easiest, most cost-efficient, secure, and user-accepted method for solving the immigration identity management problem. Using a strong identity credential such as a biometrically enabled Social Security card that is issued in a secure manner and that includes proper vetting of the credential holder's identity, will support immigration reform.

The following examples illustrate how smart Social Security cards can address several key immigration/employment verification challenges.

---

<sup>10</sup> Federal Information Processing Standard (FIPS) 201 Personal Identity Verification of Federal Employees and Contractors, <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>, and "Personal Identity Verification Interoperability for Non-Federal Issuers," [http://www.idmanagement.gov/documents/PIV\\_IO\\_NonFed\\_Issuers\\_May2009.pdf](http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf)

- **Identity theft and benefit fraud.** Smart card technology supports capabilities that can help combat identity theft and benefit fraud. Immigrant identification information can be securely stored in the smart card chip, which has built-in tamper-resistance features that make it extremely difficult to duplicate, hack, or forge. Smart cards support advanced cryptographic methods to secure data on the card. In addition, smart cards can be used as secure tokens to provide authenticated access to information stored in online databases. Smart cards can also be used in conjunction with biometrics to provide the highest levels of secure identification. For example, a biometric template can be captured and compared on the smart card to a stored biometric template; this provides multi-factor authentication, preventing an unauthorized person from misusing another person's identification to prove work eligibility.
- **A unique identifier or multiple identifiers.** Many organizations agree that there is a strong need for a unique identifier to link immigration records across multiple institutions and within multiple departments in a single institution. The smart card can be used to securely hold the unique identifier, along with other identity information, and to provide multi-factor authentication. Smart card technology enables the use of distributed and federated applications in lieu of a central database. The use of smart cards and standards-based protocols would allow appropriate parties to have access to data across multiple data stores, with the assurance that the immigrant identity is verified, that the records retrieved belong to that immigrant, and that only persons who need the data can access it. (Proper security controls must also be implemented around the applications, databases, and environments that house electronic immigration data.) Smart cards can serve as a secure way to aggregate multiple identifiers across many different systems or organizations, linking them all on the smart card.
- **Form factors.** It is critical that the immigration identity management solution support the current environment and provide a form factor that can easily be leveraged as the immigration credential platform of the future. If the current Social Security card were upgraded—a recommendation made by the 9/11 Commission and included in the Intelligence Reform and Terrorism Prevention Act of 2004—a separate employment authorization credential for legal residents would not be required.

### 3.4 Biometric Options

Used in conjunction with smart cards, biometric technology can provide a very high level of assurance when confirming an enrolled individual's identity. Examples of biometric technology include fingerprints, iris patterns, facial images, and vein patterns. When an individual is initially vetted and enrolled in the program, one or more biometric samples can be registered. The biometric data that is used for subsequent matching is in a reduced digital format, called a template, that is processed from the original biometric data image. The template consists of only those features needed for the matching process, which are extracted from the original data. The template enhances privacy since it cannot be easily reconstructed into the original image. To further enhance privacy, advanced encryption techniques can be used to securely store the biometric template in the smart card's memory or in a central database.

When a person presents the smart card credential to a prospective employer (or other designated authority) to prove eligibility, the verifying party must have both the ability to read and process the information on the smart card and the biometric sensor hardware and software necessary to collect and process a biometric sample from the individual.

Three approaches can be taken to performing the biometric match during the identity verification process:

- Match from card at system
- Match on card
- Store on server and match on server

When the **match from card at system** approach is used, the biometric template is read from the card and a biometric sample is collected from the individual. The biometric matching takes place at a personal computer or other computing device, where the match result is determined. The advantage of this

approach is that no central database of biometric data is required, and the cardholder maintains possession and control over the biometric data.

Another approach, called **match on card**, collects a biometric sample and transfers the processed sample to the memory of the smart card. The microcontroller on the smart card then performs the matching process. Match on card has all of the benefits of the match from card at system approach. In addition, the enrolled biometric template never leaves the card, which further enhances privacy.

A third approach, **store on server and match on server**, stores the biometric data in a central database, instead of on the card, and performs the biometric matching at a central server. When the card is read, the unique identifier and the biometric template captured from the cardholder are sent to the central server. The unique identifier points to a specific record in the central database that contains the enrolled biometric template. The biometric match takes place at the server and the match result is returned to the remote location.

### **3.5 Privacy**

Designing a new identity management system is complex, and the requirement to balance security and privacy affects everything about a system design, from the policies and processes formulated to support and maintain the system to the system's architecture and the particular technology chosen to authenticate individuals. For example:

- The organization must have a privacy and security policy that clearly defines what personal information is to be collected, how the information will be used, who can access the information, how the information will be protected, and how the individual who owns the information will control its use and provide updates to the information.
- The enrollment and identity proofing process must verify that the information presented is accurate and protect the confidentiality and integrity of that information.
- The system must protect each individual's information at all times, including while the information is being stored and while it is being used.
- The ID an individual carries must protect its contents from being copied, altered, or hacked, to prevent unauthorized use, misuse, or disclosure of the personal information it carries.
- The exchange of data between the ID and whatever device reads the ID must be protected to prevent unauthorized capture and use of data to impersonate an individual.
- Access to personal information must be granted only after an issuer-defined authentication process. Only necessary information should be released and only to authorized systems or individuals.
- All personnel involved in using the system must be carefully trained and monitored to ensure strict conformance to the system's policies and practices. Compromising these policies and practices means compromising the identity management system itself.

Designing an identity management system to guard individual privacy therefore involves more than simply selecting a particular type of ID technology. The organization issuing the ID must design information privacy and security into the overall system, have the appropriate policies and processes in place to support the privacy and security requirements, and implement the technologies that deliver these features. Issuing organizations must also have established operational practices for monitoring and ensuring that privacy and security policies are implemented and strictly followed.

Smart cards offer all of this privacy enhancing functionality. Based on interoperable standards defined by the National Institute of Standards and Technology, smart cards put state-of-the-art technology to work to secure and protect each person's identity information. When partnered with biometrics, smart cards enable each person to definitively prove the person is who he or she claims to be.

### **3.6 Employment Verification**

In the early 1990s, the Federal Government initiated the Basic-Pilot employment eligibility verification system, which culminated in today's E-Verify program. It has become mandatory for certain public and private entities to use this program to support the electronic verification of documents proving identity and work eligibility.<sup>11</sup> This effort was initiated in part to address the use of fraudulent documents to prove identity and work eligibility. One of the enhancements currently being considered to address document fraud (and being implemented on a limited scale) is the verification of state-issued credentials, including photographs, with the issuing authority. With the introduction of a smart card immigrant credential, the Federal Government would not be required to rely on state and local agency information to determine whether a person's identity is correct.

The U.S. Citizenship and Immigration Services (USCIS) within the Department of Homeland Security (DHS) and the Social Security Administration (SSA) are already working together on the E-Verify program. Through E-Verify, employee information is first matched against SSA data and then, for non-citizens and some naturalized citizens, against DHS data.

An evaluation study<sup>12</sup> of the E-Verify program (completed over a year ago) revealed the limitations of the E-Verify system in determining identity fraud or misrepresentation by prospective workers. This study clearly showed the need for appropriate ID proofing to support the E-Verify program and assure that only eligible prospective employees are approved by the system.

---

<sup>11</sup> Form I-9, *Employment Eligibility Verification*, provides the list of acceptable documents that can be used for establishing identity and employment authorization.

<sup>12</sup> "Findings of the E-Verify Program Evaluation." Westat, December 2009, [http://www.uscis.gov/USCIS/E-Verify/E-Verify/Final%20E-Verify%20Report%2012-16-09\\_2.pdf](http://www.uscis.gov/USCIS/E-Verify/E-Verify/Final%20E-Verify%20Report%2012-16-09_2.pdf).

## **4 Use Cases for Enrollment and Use**

This section presents possible use cases for upgrading the Social Security card using existing organizations and infrastructure and enabling employers to securely and accurately check employment eligibility.

### **4.1 Enrollment through Existing Organizations and Infrastructure**

While deploying an identity system on the scale of the Social Security card is no small undertaking, upgrading the Social Security card to use smart card technology and include a biometric identifier is viable. Many countries have enrolled entire populations into similar identity systems by using regional enrollment centers.

The United States is fortunate in that installed technology and the current transportation infrastructure allow for easy communication and travel, which makes getting to regional enrollment centers convenient for most people.

In addition, both private and public organizations can carry out large-scale enrollment and issuance services. The Social Security Administration (SSA) offices located in every state can be used. U.S. Postal Service offices are conveniently located in all communities and are currently used to facilitate applications for U.S. passports. State Department of Motor Vehicles agencies, which currently issue driver's licenses and identity cards, can be leveraged to issue new Social Security cards. They have the necessary information technology and physical facility infrastructure and a staff that is already trained in enrollment and card issuance procedures.

Finally, there are private companies all over the United States with a network of thousands of credential issuance and biometric enrollment centers. These centers provide businesses and governments with convenient points of service for the background check and enrollment services related to screening applicants for employment in high security or sensitive occupations (for example, hazardous materials truck drivers, maritime workers, school bus drivers, day care workers, stock brokers, and airline pilots). This existing infrastructure can be leveraged for enrollment and issuance of a new, secure, biometrically enabled Social Security card.

### **4.2 Example Process for Upgrading the Social Security Card**

This section describes one process through which all Social Security cardholders could upgrade their records to incorporate a biometric identifier tied directly to the cardholder using a secure smart card solution.

The process begins with a letter from the SSA to the address of record for an individual. The letter includes an individual code that is not the individual's Social Security number (SSN). This code could be a bar code or a mathematical combination/representation of information including name, address or region, and SSN. Each code is unique and associated with only one Social Security record. The letter must be validated with the correct SSN, which needs to be provided by the individual. Therefore, if the letter is intercepted, the interceptor needs to know the SSN associated with the letter and record.

The letter offers a timeframe (perhaps two weeks to a month) during which the individual can come to an enrollment center, such as a post office, to upgrade the individual's Social Security record and card. The letter would include the address of the designated enrollment center. The individual would be required to bring the letter and other supporting documents to facilitate the upgrade.

At the enrollment center, the individual provides the letter (something they have), the associated SSN (something they know), and two forms of ID, at least one of which includes a photo. All Social Security records would thereby be protected and could not be claimed without the letter, the corresponding SSN, and proper photo identification.

All information provided by the individual is then processed, vetted, and verified by the SSA and DHS before a new biometrically enabled Social Security card is issued. No cards are issued at the enrollment center; all cards are mailed to the address of record.

Exception procedures would be required to handle individuals who lost their letters, never received their letters, or left them at home.

### ***4.3 Verification Process at the Employer***

The deployment of biometrically enabled Social Security cards to eligible citizens in the United States will enable any individual to be authenticated by any employer.

The employee authentication process is simple. The first step is for a new employee to insert the biometrically enabled Social Security card into a smart card reader. The employee then presents a biometric sample (e.g., a fingerprint or facial image) to the biometric sensor. The biometric information is matched within the card, not in an online database. This biometric match-on-card ensures maximum privacy for the employee. At the same time, the biometrically enabled Social Security card is automatically validated using a web browser interface to an online database, to ensure that the card is still valid.

Performing the one-to-one biometric match-on-card and online verification of the validity of the biometrically enabled Social Security card should take less than a few seconds. Employers can acquire the required equipment (e.g., a smart card reader and fingerprint scanner) or contract the process out to a designated authentication service.

## **5 Conclusions: The Most Important Considerations for Policy Makers**

It is crucial for government policymakers to understand the importance of identity management in addressing immigration challenges. As the national immigration agenda moves forward, solid identity standards and technology must be employed to meet the needs of new legal residents and employers. The Smart Card Alliance believes that smart cards should be used as a foundational technology to create strong identity credentials to protect our citizens and legal residents and to facilitate the secure verification of identity and employment eligibility.

The most important point is that identity management is a fundamental issue for immigration reform. Any efforts to improve the immigration system, reduce administrative costs, and fight immigration document and benefit fraud and identity theft must start by building a solid immigration identity foundation. Industry-proven technologies and existing Federal Government standards can be leveraged to create an effective immigration identity management infrastructure and implement flexible, secure, and cost-effective credentials in support of immigration reform.

The Smart Card Alliance believes that smart cards can be a foundational technology to an identity management approach that creates strong identity credentials to protect our citizens' identities and facilitates the secure verification of identity, immigration status, and employment eligibility. If policymakers proceed to reform immigration in the United States, we recommend that they consider using smart card technology to provide a highly secure and privacy-sensitive platform to support an identity management framework for immigration reform and employment eligibility verification.

Additional information is available online at [www.smartcardalliance.org](http://www.smartcardalliance.org).

## 6 *Publication Acknowledgements*

This white paper was developed by the Smart Card Alliance Identity Council to provide an overview of the importance of proper identification security to the success of immigration reform and to describe how smart cards with biometrics can be an effective technology.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Identity Council members for their contributions. Participants involved in the development of this white paper included: CardLogix; Cogent Systems; Deloitte & Touche, L.L.P., Audit and Enterprise Risk Services; Gemalto; IBM; Identification Technology Partners; IDmachines; IQ Devices; L-1 Identity Solutions.

Special thanks go to **Harold Kocken**, Deloitte, who led the white paper project, and to the following Identity Council members who contributed to the development of this white paper:

- **Sal D'Agostino**, IDmachines
- **Roland Fournier**, L-1 Identity Solutions
- **Walter Hamilton**, Identification Technology Partners
- **Harold Kocken**, Deloitte & Touche, L.L.P., Audit and Enterprise Risk Services
- **John McKeon**, IBM
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, CardLogix
- **Neville Pattinson**, Gemalto
- **Steve Rogers**, IQ Devices
- **Dave Walker**, Cogent Systems

### **About the Smart Card Alliance Identity Council**

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.