Backgrounder

Published by The Heritage Foundation

No. 1946
June 27, 2006

Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft

Alane Kochems and Laura Keith

Identity theft has become a hot topic in today's society, with television commercials oversimplifying and trivializing the threat by focusing on the potential financial consequences. Identity theft is a more serious threat than someone draining a grandmother's bank account. False or fraudulent documents could help terrorists enter the United States and establish themselves in preparation for an attack on the country. Since this country relies primarily on identity-based security systems, secure identity documents are critical to national security.

Taking advantage of the available technologies could help to minimize the inherent weaknesses in an identity-based security system. To secure documents from fraud, policymakers need to examine carefully the available technologies, reviewing their capabilities, requirements, infrastructure demands, and costs. They should also consider how these technologies could affect individual privacy and fundamental liberties. Finally, policymakers should work in conjunction with the private sector and other stakeholders to create a compendium of best practices that uphold the principles of federalism while ensuring a successful strategy for identity security.

Types of Identity Documents and Their Uses

"Identity document" refers to a wide variety of documents—from birth certificates to credit cards—that are used for many purposes. Because of this variety, it

Talking Points

- Securing identity documents is essential to preventing terrorists from entering the United States.
- The United States relies heavily on identity-based security systems to secure the border and protect infrastructure. However, identity documents used in the United States are quite vulnerable to misuse, as demonstrated by the 9/11 hijackers, who used identity documents to enter United States repeatedly on non-immigrant visas.
- Improving homeland security will depend heavily on improving the reliability and security of state and federal identity documents.
- A variety of technologies are available that could be used to improve the reliability of identity documents.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/bg1946.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies of the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

is important to distinguish between base identity documents, also known as breeder documents, and secondary identity documents.

For instance, an acceptable national base identity document is a birth certificate. Internationally, a passport is typically considered a base identity document. Secondary identity documents (e.g., driver's licenses, credit cards, immigration visas, and green cards) are obtained by showing proof of the base identity documents. Base identity documents can also be used to obtain access to specific data or secure locations at the workplace.

Types of Document Fraud

With so many types of identity documents, there inevitably are many ways to perpetrate fraud. Successfully replicating or emulating a base document increases the likelihood of obtaining legitimate secondary documents—or, rather, secondary documents that appear legitimate even though they are based on the false base documents. It is also possible to obtain legitimate secondary documents without base documents. Securing an identity document is a vital first step for a terrorist or anyone else who wants to enter the United States illegally.

Tactics for entering the United States using illicit documents include traveling on fake, stolen, or forged passports; hiding past travel by acquiring a new passport by claiming that the old passport was lost, stolen, or damaged; and traveling under "legitimate" passports that have been purchased blank and filled in with false personal data. Terrorists have also used legitimate means to enter the United States, including entering as students, requesting political asylum, and avoiding immigration inspection upon entrance.[1] These tactics highlight the need for security professionals to be able to validate identity documents, not just generally to be on the lookout for fraudulent papers.

The Problem

Behind every type of identity document should be a person. In this country, proof of a person's legal existence is often required for transactions and for access to places and things. From obtaining passports and visas to protecting critical infrastructure, security systems must be in place to ensure that the person requesting access to a location or information is actually the person indicated by that person's identity document. Currently, security officers have very limited means of validating documents and verifying that they are based upon legitimate breeder documents.

For example, the 9/11 hijackers used identity documents to enter United States repeatedly on non-immigrant visas. While these men could and should have been stopped for many reasons, their use of student and visitor visas was not one of those reasons. In fact, many known terrorists who have lived in or have been extradited from the United States entered legally and had legitimate green cards. In other words, they claimed immigrant status and were on the "path to citizenship."[2]

Another potential weakness in relying on identity documents is the personnel who issue the documents. Are the guards and other personnel responsible for identity documents and access doing their jobs effectively and faithfully, or are they scoping out weaknesses in the system? For instance, in May 2004, workers at department of motor vehicles (DMV) centers in northern Virginia were selling driver's licenses on the side to people who were in the country illegally. Despite legislation that tightened loopholes, two more workers from the same DMV centers were arrested and convicted a year

1. Thomas R. Eldridge, Susan Ginsburg, Walter T. Hempel II, Janice L. Kephart, and Kelly Moore, *9/11 and Terrorist Travel*, Staff Report of the National Commission on Terrorist Attacks Upon the United States, August 21, 2004, p. 59, at *www.9-11commission.gov/staff_statements/911_TerrTrav_Monograph.pdf* (June 15, 2006). The legitimate entrances highlight problems with current U.S. visa, immigration, and border policy that could be resolved through comprehensive reform. See James Jay Carafano, Ph.D., "Safeguarding America's Sovereignty: A 'System of Systems' Approach to Border Security," Heritage Foundation *Backgrounder* No. 1898, November 28, 2005, at *www.heritage.org/Research/HomelandDefense/bg1898.cfm*.

2. James Jay Carafano and Paul Rosenzweig, *Winning the Long War* (Washington, D.C.: The Heritage Foundation, 2005), p. 67.

later.[3] In addition to the nation's border, access to and protection of critical infrastructure also rely to a great extent on identity-based systems.

Current ID Validating Technologies

Basing a security system on identity documents is a convenient but flawed method of providing security. However, a wide range of available technologies could improve the ability of security systems based on identity documents to discriminate and verify identities accurately. Marking and radio frequency identification (RFID) tagging are two main types of such technology.

Better use of the technology holds promise for improving identity document standards and for hindering, if not preventing, criminals and terrorists from using identity documents for nefarious purposes. Policymakers should carefully examine the technologies available for securing identity information, including their capabilities, requirements, infrastructure demands, costs, and how they would affect individual privacy and fundamental liberties.

Marking. Marking something as a signal of authenticity has been used for thousands of years. The Romans used unbroken wax seals imprinted with the ruler's insignia to verify that messages and orders had not been revealed or tampered with. Although still used on the occasional wedding invitation, this ancient technology is not fit for today's security challenges. However, two types of advanced marking—digital and metal—could be used to apply a security layer to identity documents, thereby linking different layers of security or information to the document to verify its authenticity.[4]

Digital marking involves storing information as an image. This could be a Social Security number or biometric information like a facial image or fingerprints. The digital mark consists of a layer in the card and is only machine-readable (i.e., invisible to the naked eye). Bar codes, laser engraving, microprinting, and watermarking are all types of digital marking. Cards with digital watermarks are designed to limit the validity of the ID and thus adapt to changing information requirements.

Digital watermarking has been used widely in the media industry to prevent piracy and on the Internet to secure Web sites and personal computers from hackers. The concept behind all digital watermarking technology is the same: A machine "reader" reads the watermark and checks the information against a database, such as terrorist watch lists.

Holograms are metal devices implanted in identification cards to allow a machine or a human eye to authenticate the document. Holograms do not connect automatically to other information or databases. The metal hologram is durable and can be adapted to new technologies or demands. The concept behind markings such as holograms is to provide an eye-readable or machine-readable marking that will prove effective and durable.

Because holograms can be read by the human eye, their use does not require that expensive equipment be provided to every local, state, and federal law enforcement officer. Instead, the hologram can be instantly authenticated, whether at the local DMV by a small machine or on a rural road by the human eye. This is particularly important to small communities that may not be able to afford machines for every field officer. A hologram can last up to 10 years, which keeps down upgrade costs, unlike many other technology solutions. Hologram technology is also reasonably mature.

RFID Tagging. Already popular for retail store security systems, an RFID tag has the capability to "talk" to its homing device, up to two meters away. For example, if someone tries to shoplift from the local mall, the tag in the item sets off alarms when the shoplifter carries it through the security point. The homing device that controls settings for the identification tag can be mobile or fixed. A tag can store and relay only minimal information. The amount and types of information stored depend on

3. Jerry Seper, "Virginia DMV Official, Wife Held," *The Washington Times,* July 13, 2005, at *www.washtimes.com/national/20050713-121905-3495r.htm* (April 10, 2006).
4. Digimarc Corporation, "Enhancing Personal Identity Verification with Digital Watermarks," 2004, p. 4, at *csrc.nist.gov/piv-program/FIPS201-Public-Comments/digimarc.pdf* (June 15, 2006).

the type of encryption, the tag's memory, and the format of the stored information.

Research into RFID technology began in the United States in the early 1940s as a means by which to track allied and enemy planes. By the 1970s, the technology was used to track nuclear materials.[5] Today, RFID technology has spread throughout the public and private sectors. Due to its versatility, people are now starting to use it in identity documents as well.

The technology behind RFID consists of a chip embedded in a tag and an antenna that transmits information from the chip to a reader that is hooked up to a database. Three types of tags exist: passive, semi-passive, and active. A passive tag does not contain a power source (e.g., a battery) and must be activated by another source. A semi-passive tag does not actively transmit, but it can store information. An active tag contains an individual power source, and its data can be updated or reconfigured throughout its lifecycle.[6]

A wide variety of information in various forms may be stored on the chip. Financial institutions are using RFID technology to fight credit card fraud. The RFID technology is being developed to enable personal credit cards to be authenticated more accurately through read-once codes rather than the standard code that stays with the card for its lifecycle. This changing code, transmitted mere inches from the machine "reader," could reduce the risk of consumer credit card fraud.

A similar system could be used to secure base identity documents or even secondary identity documents. Information, ranging from biometrics to tracking data on entries into and exits from the country, could be stored on the chip. Most uses in government and the private sector continue to center around tracking physical materials, although the Department of State is considering using the technology in electronic passports and the Department of the Treasury is reviewing its use for access control and records management.[7] The Department of Homeland Security (DHS) also plans to use it for the automated US-VISIT program, which tracks visitors' entries into and exits from the United States.[8]

Although a relatively mature technology, RFID tags have been adopted only in approximately the past decade. The use of RFID technology continues to grow. The commercial sector and government agencies are working together to set standards and guidelines for more secure IDs, which are mandated by Homeland Security Presidential Directive 12[9] and the Intelligence Reform and Terrorism Prevention Act of 2004.

The central challenge for policymakers who wish to use RFID technology remains privacy. Most policy research in this area focuses on consumers and what happens to the information stored on the RFID chip once items have been purchased. Using RFID technology to authenticate identity documents raises concerns about the data collected by the tag, what data it stores, and how it stores the data. The Privacy Act of 1974, which addresses the "retrieval of personal information" rather than its subsequent use, may provide guidance on how RFID technology can be used.[10]

Current Legislation

In recent years, Congress has noted the need for secure identity documents. The Intelligence Reform

5. U.S. Government Accountability Office, *Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO–05–551, May 2005, p. 4, at *www.gao.gov/new.items/d05551.pdf* (June 15, 2006).
6. *Ibid.*, pp. 6–7.
7. U.S. Department of Commerce, "Radio Frequency Identification: Opportunities and Challenges in Implementation," April 2005, p. 16, at *www.technology.gov/reports/2005/RFID_April.pdf* (June 15, 2006).
8. U.S. Department of Homeland Security, "Radio Frequency Identification Technology," fact sheet, at *www.dhs.gov/dhspublic/display?content=4307* (May 1, 2006).
9. George W. Bush, "Policy for a Common Identification Standard for Federal Employees and Contractors," Homeland Security Presidential Directive HSPD–12, August 27, 2004, at *www.whitehouse.gov/news/releases/2004/08/20040827-8.html* (June 20, 2006).
10. U.S. Government Accountability Office, *Information Security*, p. 23.

and Terrorism Prevention Act of 2004 called on the DHS and the State Department to integrate travel documents with other intelligence for fighting terrorism and to support DHS and State Department field offices with appropriate technology.[11] In 2005, Congress took measures to strengthen national security by using identity cards. An amendment in the 2005 appropriations bill authorizes the Department of Homeland Security to set federal standards for all state driver's licenses. It does not require that states add more information to driver's licenses, but it does set stricter security standards for the identity document—security standards that reach beyond the physical document itself.

Privacy Concerns. Privacy is a prominent concern in the discussion of how best to secure identity documents. Are the data stored on one large database or just on the ID itself? Generating IDs might be more difficult if the information is stored only on the electronic ID. The processes for gathering and authenticating the information remain, but resources would be able to focus on gathering and authenticating rather than physically protecting a large infrastructure system. In addition, abuse of personally identifiable information by individuals involved in ID fraud or by the government, even with the best intentions of securing the information, is a serious concern.

Congress should give serious thought to how the government can assist in safeguarding information from wrongdoers while maintaining government access to information needed to carry out legitimate law enforcement, capture terrorists and prevent terrorism, and combat other threats to national security.

Much of the public debate about information sharing and analysis uses the word "privacy" in a manner that is imprecise and misleading. For example, many of the most vocal privacy advocates assert that any time government obtains or uses information that someone would prefer not to disclose to the government constitutes a violation of the person's constitutional "right to privacy." However, the Supreme Court has flatly rejected this claim that the Fourth Amendment can "be translated into a general constitutional 'right to privacy.'"[12]

Congress's efforts to regulate private information should be understood in constitutional context. Congress has been struggling with creating a legal framework that protects personal information while allowing the data to be used for security purposes. One such attempt is the proposed Data Accountability and Trust Act (H.R. 4127). Introduced in October 2005, the bill calls on the Federal Trade Commission to "protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information and to provide for nationwide notice in the event of a security breach." Implementation of such legislation should be crafted to address privacy and security concerns adequately.

The federal government is not alone in its quest for good security policy that balances privacy concerns. Many states from California to New York are debating legislation in their legislatures to mitigate privacy infringements unwittingly created by federal policies.[13]

Some advocates of privacy policies expand the definition of private information far beyond constitutional and legal definitions. In the context of personally identifiable information, their view is that debate should not center on simply keeping undisclosed personal information hidden or secret. Rather, they seek to extend the legal concept of privacy under U.S. civil law to information that an individual has disclosed to another in the course of

11. The Intelligence Reform and Terrorism Prevention Act of 2004 was signed into law on December, 17, 2004. For an excellent summary of the bill and its relation to preventing fraudulent identity documents from authentication, see Susan Ginsburg, *Countering Terrorist Mobility: Shaping an Operational Strategy*, Migration Policy Institute, Independent Task Force on Immigration and America's Future, February 2006, pp. 122–125, at *www.migrationpolicy.org/pubs/MPI_TaskForce_Ginsburg.pdf* (June 15, 2006).

12. *Katz v. United States*, 389 U.S. 347 (1967). Furthermore, the word "privacy" is not even in the Constitution.

13. For a list of active legislation, see Massachusetts Institute of Technology, RFID and Privacy, "Federal & State Government," at *http://rfidprivacy.mit.edu/access/happening_legislation.html* (May 1, 2006).

a commercial or governmental transaction—even to data that are publicly available. In this sense, privacy is about notice, fairness, and consequences rather than about what is withheld or hidden.

Personal Information Trustee. As a solution to the privacy problem, some industry experts have suggested a program that would rely on trusted, authorized private-sector organizations to hold and safeguard an individual's identification and other personal information.[14] Rather than a national database or a government agency holding information used to confirm identity (e.g., birth certificate information, Social Security numbers, and mother's maiden name), the individual citizen would designate one of several authorized private companies to hold the information as a trustee. All of the individual's personal information would reside with just one information trustee. In addition to fulfilling the individual's request to provide his or her personal information to specified third parties, the trustee's responsibilities would include monitoring and analyzing patterns of normal, legitimate use of the individual's personal information to recognize and prevent identity fraud and other abuse.

Because the financial services industry suffers enormous financial losses from the fraudulent use of identity documents, many financial services companies have invested in the technologies and techniques needed to mitigate losses through pattern analysis. For example, instead of tracking personal and account data, credit card companies monitor the normal frequency and amounts of a cardholder's transactions. Once the cardholder's normal pattern is broken, many companies will not authorize a new transaction. The company typically suspends the account until the cardholder has verified that the card has not been stolen.

In a personal information trustee program, a set of companies that seek to become trustees would be authorized and certified by the government. With the appropriate credentials, a trustee company would then be authorized to keep individuals' personal information and monitor patterns of personal information dissemination to prevent fraud. The decision of whether or not to disseminate an individual's information would be controlled by that individual, not by the trustee or the government.

A personal information trustee program would provide an additional privacy firewall similar to the ones already created by private financial companies. As a personal information trustee, a company would perform fraud detection and analysis on the usage patterns of the information entrusted to it. The government would be able to access and search the same information—in the aggregate—for patterns related to terrorism and other national security threats as part of normal counterterrorism and similar intelligence activities. Such efforts would not delve into the details of any personally identifiable information without credible evidence of a specific threat.

These respective roles for the personal information trustee and government would require legislation imposing severe penalties for illicit use of personal information and ensuring that the information analyzed by a government agency for counterterrorism and similar intelligence purposes would not pinpoint an individual without credible evidence of a specific threat. For example, the Electronic Communications Privacy Act of 1986 expressly authorizes the FBI and other government agencies to obtain data on individual activities (telephone call detail information) for pattern behavior analysis to investigate terrorist activity.[15]

Congress could build on such legislation by, among other things, making any unauthorized dissemination by the trustee of personal information a felony. This would strengthen any information trustee program introduced to secure identity while facilitating smart tactics for identifying terrorists and thwarting terrorism.

Cost Concerns. Cost is another policy concern. Currently, the private sector is shouldering the burden for research and development of these technologies because industry members are still the primary

14. See, for example, K. A. Taipale, "Science and Technology: Identity Theft: Policy Implications," Presentation at The Heritage Foundation, November 2, 2005, at *www.taipale.org* (June 26, 2006).

15. See 18 U.S. Code § 2709(a–b).

customers. Specific cost projections are difficult to find, but some reports claim that implementing RFID technology alone could cost $17 billion.[16]

Clearly, any government contracts awarded to private companies for implementing security measures required by Congress and the Administration should have congressional oversight. The government agencies administering the contracts should perform due diligence. If a personal information trustee program is implemented, Congress should enact legislation that fosters competition among the authorized personal information trustees while ensuring oversight of a range of companies offering such services.

Infrastructure

Infrastructure starts where the technology is manufactured and ends at the point of verification. Today, most identification verification occurs when one person examines with unaided eyes the documentation (e.g., photo ID or birth certificate) of another.

As more technologies become available to assist in securing identification documents, approaches to identity verification need to change. Securing identification through stored information pushes the boundaries of traditional infrastructure. The machines and manufacturing techniques must be protected so that criminals and terrorists do not copy the technology or exploit it for subversive purposes.

In addition, the stored information itself may become a target. Policymakers need to consider what data they will require from people, where they will store the data and for how long, how they will transfer the information onto the ID document, and how they will authenticate it. Securing infrastructure for one company or government entity is difficult; securing infrastructure for an entire nation is even more challenging.

Protecting physical infrastructure is also a concern. Before implementing one system or one part in a system of systems, parameters for security requirements that ensure proper accessibility and restrictions must be set in place to regulate the manufacturers and issuers of secure identification documents. Such requirements could include background checks on employers and physical security restraints on equipment or property.

What Next?

As the country struggles to protect itself against identity theft and to ease the validation of identity documents, it should take a principled approach that fosters both security and fundamental liberties. Policymakers need to decide whether it is better to take an approach driven by personal responsibility and the initiatives of each government agency or one driven by a federal, national focus. Specifically, policymakers should:

- **Push for creative ways to combine technologies to use their full capabilities.** Rather than focus on one technology as the silver bullet, policymakers and members of industry should focus on ways to adapt existing technologies and systems so that they complement one another to create more effective solutions. Within the realm of secure identification technology, there is much room for collaboration of technologies. For instance, new software could be used to harness the capabilities of old technology. Another approach is to combine various technologies into a "system-of-systems"—one network with many parts—to create a more effective security blanket.
- **Analyze the costs and benefits of each technology, including the necessary infrastructure, infrastructure protection, and fundamental civil liberties concerns.** This analysis should also take into account the costs and benefits of implementing more than one technology as part of a system-of-systems approach. For example, moving from paper to electronic security systems might necessitate changes in security policy.
- **Respect principles of federalism.** Allowing states to retain the power to design and imple-

16. Alice Lipowicz, "Coalition Objects to RFID Chips for Drivers Licenses," *Government Computer News*, January 23, 2006, at *www.gcn.com/online/vol1_no1/38073-1.html* (May 2, 2006).

ment security standards for their own identity documents may be the only course consistent with the U.S. federal system. The federal government, of course, can set the standards for federal identity documents and promote national standards and best practices, which the states can choose to accept. The states would need to fund the implementation of their chosen security measures. However, the federal government could provide funding to encourage them to adopt the national standards and best practices. Many states are already using new technologies to manage their driver's licenses and could serve as models for other states.

- **Collaborate with stakeholders to create a compendium for best practices.** Creating a collection of best practices would give private entities guidance on what the government believes are the best security practices without mandating specific fixes for problems. With a best-practices collection, organizations and state and local governments can choose a set of security standards that best meet their needs. The private sector has already formed consortia to set best practices and policies for the use of identity security technology. The public sector should work closely with these organizations to avoid wasting time and resources reinventing the wheel.
- **Work with the private sector in research, development, and implementation of policy and technology.** All government agencies, including the DHS, State Department, Department of Transportation, Department of the Treasury, and Social Security Administration, should work with the private sector to implement current and future policy mandated by Congress. Attempting to move forward without collaborating with the private sector in research, policy, and regulation would hinder progress in dramatically improving the secure identity environment. At the same time, Congress should seriously consider how government policy can enable access to the information needed to address national security threats while preventing the misuse of that information.

Conclusion

Document fraud is a national problem with international consequences. Successfully securing identity documents is possible through the collaboration of every level and branch of government and the private financial and technology sectors.

Congress and the Administration should take advantage of technology to strengthen the nation's security, but technology alone will not protect U.S. citizens from the fraudulent use of credit cards or the next terrorist attack on U.S. soil. The technology needs to be combined with an effective policy that is flexible enough to adapt to the next generation of requirements and based on solid principles that protect privacy and fundamental liberties. Securing the identity documents that lay the foundation for U.S. security systems is the right place to start.

—Alane Kochems is a former Policy Analyst for National Security and Laura Keith is a Research Assistant in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. Brian Walsh, Senior Legal Research Fellow in the Center for Legal and Judicial Studies, contributed to this paper.