

**Radio Frequency Identification Technology (RFID):
Securing the Homeland through Next Generation Identification
Technology**



Prepared for
The IT Security Community and our Customers

Prepared by

Lunarline, Inc.
1875 I ST, NW, Suite 500
Washington, DC 20006
www.lunarline.com

11 August 2006

By Matt Metheny, PMP, CISSP, CAP, CISA

Abstract

This paper discusses the next generation identification technology, also known as Radio Frequency Identification (RFID), and the Homeland and National Security Initiatives that have adopted RFID-based identification to protect the nation against terrorist threats. The proposed standards needed support these initiatives are also discussed, and how a RFID will enhance the current system, resulting in an overall more secure, regulated, identification system. We will also look at the privacy concerns surrounding the RFID technology implementation, and the security safeguards that need to be integrated into the system and processes to ensure they adequately protect privacy information.

Table of Contents

Radio Frequency Identification Technology (RFID):.....	1
Securing the Homeland through Next Generation Identification Technology.....	1
Introduction.....	4
Introduction to RFID Technology.....	5
Legislation.....	6
Intelligence Reform and Terrorism Prevention Act of 2004.....	6
Real ID Act of 2005.....	7
Next Generation Identification Initiatives.....	7
National ID (Real ID Act of 2005).....	8
E-Passport.....	8
United States Visitor and Immigration Status Indicator Technology (US VISIT).....	9
Privacy Concerns.....	9
Appendix A: Driver License and Identification Cards.....	14

Introduction

Radio Frequency Identification (RFID) technology is considered the next generation of identification technology. RFID as an application for identifying U.S. citizens and foreigners provides a more reliable form of identification than those currently used because it is less susceptible to counterfeiting or replication. There are several initiatives that have been developed to take advantage of the benefits provided by RFID technology such as the National ID (Department of Homeland Security) and the E-Passport (Department of State).

The establishment of RFID-based identification cards sets the standard for a secure, regulated, identification system designed to protect the nation against terrorist threats. The National ID through the passing of the “The Real ID Act of 2005” (H.R. 418) created the requirements for all states by May 2008 to introduce through the Department of Motor Vehicles (DMV), a Homeland Security approved, electronic machine, readable ID that will be required by all American citizens, legal aliens, and foreigners visiting the U.S. The National ID will include RFID technology to allow it to be electronically read through machines at places such as airports, banks, federal buildings, and U.S. borders.

Introduction to RFID Technology

RFID technology has found valuable uses in several industries over the past decade such as transportation, supply-chain management and defense. As the RFID technology evolves, it is continuously finding new applications and benefits in new and existing industries. The basic function of RFID is to store data in a tag (also known as a transponder) that can be retrieved at some point of time in the future based on the specific application requirements. An RFID system usually consists of three major components: the antenna, reader device (or transceiver), and a transponder that is embedded with a single chip processor and is electronically programmed. The antenna transmits a radio signal between the reader device and the tag where the data is either read from or written to the device, depending on mode of operation for the tag (active tags offer read/write capability, and passive tags are read-only).

The use of an RFID system should be considered only when the application is cost-effective and provides some relative benefit (it is not a wise business decision to put a 50 cent tag on a 5 cent piece of equipment). RFID is expensive to implement, and requires extensive expertise in the design, development, and installation of RFID systems because of the sensitivity the technology has with the surrounding environment (e.g., water and metal). To ensure the application of RFID does not receive interference with other short-wave RF technologies, the adoption of RFID is tightly controlled by international standards organizations that seek to ensure interoperability, and to clearly define specifications. EPCglobal and the ISO [International Standards Organization] are the two key bodies charged with RFID standards (http://www.cbronline.com/article_news.asp?guid=501806F2-1E9D-4A59-97CB-B078CDEE410D, para. 7).

RFID has found both proponents and inhibitors within society. The proponents see RFID as an advanced identification technology that enables additional information to be attached to an item, therefore creating smart items that can be quickly found (solving the needle in the haystack problem). However, inhibitors seek to block RFID adoption because of the fear of misuse and invasion of privacy. RFID can come in different shapes and sizes, making it very useful, but also very scary if used in the wrong way (the “Minority Report” concept). Later in this paper, we will discuss the privacy issues with RFID, and the technologies that have been developed to address these concerns.

The federal government has found a wide range of uses of RFID, both in the defense and homeland security sectors. The federal government has introduced several initiatives that take advantage of the benefits of RFID. One such initiative includes the Homeland Security Presidential Directive 12 (HSPD-12), which seeks to create a common federal government-wide identification card.

The common federal identification cards, known as personal identity verification (PIV) cards, will provide a secure form of identification for federal employees and contractors to be used for physical access control to federal buildings, and logical access

to information systems. “PIV Cards must be personalized with identity information for the individual to whom the card is issued, in order to perform identity verification both by humans and automated systems. Humans can use the physical card for visual comparisons, whereas automated systems can use the electronically stored data on the card to conduct automated identity verification” (NIST, p. 5). The centerpiece of the PIV card will be a passive RFID chips which will contain information such as passwords to fingerprints, and be used for an employees access to logging into computers, accessing computer rooms, encrypting transmitted data, access control information system, and roles-based privileges for accessing information. The new technology will provide a government-wide, secure authentication system that is both portable and interoperable between departments and agencies (http://www.gtsi.com/pdfs/7229_hspd12_white_paper.pdf?ShopperID=c1b00811-5085-426f-a914-9b24f4136532, paras. 3-4).

Legislation

The legislation that was passed following the attacks of September 11 created a requirement for a standardization process in the issuance of identification documentation, and was a critical step in the adoption of RFID as an alternative to the current identification technology. The legislation laid out specific guidelines for the requirements that must be included in the standardized National ID system, and requires the States to implement the new forms of identification, which was previous, a state-by-state initiative by May 2008. The National ID system includes several forms of identification that will be provisioned under legislation and regulated through federal standards such as birth certificates, passports, social security cards, and drivers’ licenses.

The implementation of the National ID system is a continued effort that has created a national strategy for initiatives that leverage next generation identification technologies. The national strategy provides security measures to reduce the threats posed by terrorists groups through cross-organizational initiatives such as border and identification documentation security. The improvement of security through these initiatives is provided by technologies such as RFID that offer a method of real-time identification and authenticity of individuals and thereby preventing fraudulent activity.

Intelligence Reform and Terrorism Prevention Act of 2004

Following September 11, the 9-11 Commission issued a report that outlined the events that occurred surrounding September 11, 2001 and recommendations for the preparedness and response of future terrorist attacks. The recommendations detailed in the report identified the need for stronger security measures for drivers’ licenses. “The federal government should set standards for the issuance of birth certificates and sources of documentation, such as drivers’ licenses. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to

ensure that people are who they say they are and to check whether they are terrorists” (9/11 Commission, 2006, p. 390).

The results found in the 9/11 Commission Report were captured in a bill passed by Congress shortly after September 11 that included provisions to ensure that identification documentation provided stronger security measures, therefore limiting fraudulent activities by terrorists groups. As noted in Title VII, Section 7211-7212, the results for greater security measures and minimum document requirements and issuance standards for identification information were imposed on States to implement. These requirements not only included strengthening the documents themselves, but also the process used for issuing them. For example, the States will be required to validate and verify a person’s Social Security Number, if they are eligible, prior to the issuance of identification documentation such as drivers’ licenses.

Real ID Act of 2005

The Real ID Act of 2005 contained provisions that replaced those that were included in the Intelligence Reform and Terrorism Prevention Act of 2004, but were never implemented. Under this new legislation, the Department of Homeland Security (DHS) will be responsible for establishing the standards for drivers’ licenses and identification cards issued by the States.

The Real ID Act requires all States to uniformly implement the proposed standards by May 2008. The proposed standards being developed by DHS includes both the technology enhancements to reduce forgery, tampering, or duplication, and issuing procedures that will lower the likelihood that terrorists would be issued legitimate documentation by mistake. The standards and requirements that are being established by DHS for implementation by the States include:

- Minimum identification document requirements
- Minimum issuance standards
- Special requirements for non-drivers licenses such as identification cards
- Procedures for documentation verification
- Administrative requirements such as photo identification, social security number validity, out-of-state drivers license termination, employee training programs, information sharing between States, and security clearance requirements for drivers’ license producers

Next Generation Identification Initiatives

The post-9/11 homeland and national security initiatives will have a tremendous impact on the future of identification technologies such as RFID. The evolution of next generation identification technologies will prove to be an essential asset for supporting anti-terrorist legislation. The challenges in the business of protecting the nation will be minimized through identification technology advancement and standardization.

National ID (Real ID Act of 2005)

The National ID system is a national security enhancement that will function as a national identifier built around the state drivers' license through the Real ID program. The concept of the National ID is already implemented in other countries, and if successfully implemented in the United States would create a universal identifier that can be used to globalize efforts for portable travel documents such as VISAs and passports. The federal ID standards are a critical part of DHS's arsenal of efforts that seek to prevent terrorists and illegal immigrants from freely living within the United States undetected. The federal standards developed for the Real ID program encompasses three main areas related to the data on the National ID, what information or documentation must be checked prior to issuing a National ID, and how the information will be shared between the States.

The federal government through legislation and anti-terrorism laws are working to improve national security through the enhancement of the most commonly used forms of identification such as the drivers' license, Social Security cards, and birth certificates with the integration of RFID technology. The RFID technology is considered the central component selected to meeting the federal standards outline by the Department of Homeland Security for federally accepted National IDs. Three years following the enactment of the Real ID Act, Federal agencies are prohibited from accepting s State-issued driver's licenses or identification cards unless the State issuing drivers' licenses and identification cards conform to the standards (see Appendix A) specified in the new law [Real ID Act of 2005] (http://www.ssa.gov/legislation/legis_bulletin_051305.html, paras. 4-5)

E-Passport

The security at borders and airports is important because they are the last form of defense against illegal immigrants and terrorist entering into the United States. Based on this understanding the State Department and DHS have identified the benefits offered by a machine readable passport that can be used to quickly identify a person requesting access. The Department of State will begin issuing E-Passports as part of a pilot program in late 2006 that will include RFID identification information to ensure its authenticity, especially against duplication or counterfeiting.

The next generation RFID-enabled passports will offer another level of protection against identify-theft from stolen passports, and border officers are provided another method for guaranteeing the identity of the passport-holder. The chips will securely store the same data displayed on the photo page of the passport such as name, date of birth, gender, place of birth, passport issue and expiration date, passport unique identifier, and a digital photograph. The digital photograph is an important addition because it can be analyzed by biometric devices that use facial recognition technology at International borders for a more accurate analysis or compared against government terrorist or criminal

databases for quick identification of suspected individuals (U.S. Department of State, para. 4).

United States Visitor and Immigration Status Indicator Technology (US VISIT)

The Department of Homeland Security and State Department are jointly working together to implement a DHS border protection program (US-VISIT) that uses advanced technologies such as RFID and biometrics to enhance security measures at ports of entry.

The US-VISIT program goals are:

- “Enhance the security of U.S. citizens and visitors”
(http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0385.xml, para. 9)
- “Facilitate legitimate travel and trade”
(http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0385.xml, para. 9)
- “Ensures the integrity of the U.S. immigration system”
(http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0385.xml, para. 9)
- “Protect the privacy of U.S. visitors”
(http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0385.xml, para. 9)

The US-VISIT program seeks to identify visitors who travel for business or personal recreation and want to temporarily come to the United States. US-VISIT applies to all visitors entering the U.S., regardless of the country of origin or whether they are traveling on a VISA, by air, land or sea
(http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0385.xml, para. 4). Through this initiative identifying information is collected on visitors prior to being allowed to travel to the U.S., and gives border protection officers more information to interrogate the visitor’s identity before trying to gain entry into the U.S. This program will provide a more expedited method for evaluating travelers, which increasing the security of the nations most vulnerable entry points.

Privacy Concerns

Every new technology has both proponents that believe the technology will provide some benefits, and inhibitors that try to prevent the adoption of the technology because they are either uneducated about the overall benefits or threatened by the results of the technologies success. RFID has received the same attention as other new technology introductions because of the concerns over privacy and the leaking of personal information. These issues have caused both state and federal legislators to seek

a full investigation into the potential threats and vulnerabilities associate with RFID's adoption.

There are many groups that are lobbying legislators to create laws that prevent RFID from being widely used because of the potential concerns associated with privacy-related information. The ACLU [American Civil Liberties Union] favors legislation that limits RFID use and requiring notice of any RFID use because of the dangers of criminals accessing the private information of individuals. They are also concerned about the type of information that might end up on some RFID tags (Boulard, 2005, pp. 22-23).

Not all RFID implementation should be banned, and many privacy groups do not want to prevent the complete use of RFID. The primary concern with the unlimited adoption of RFID is the lack of control and regulation of RFID integration. There is a universal belief that necessary safeguards have to be put into place to prevent possible privacy issues from becoming a reality. Many observers of the RFID technology believe that privacy concerns being raised by RFID can be addressed through privacy and computer crime legislation that also applies to other current and future technologies (Boulard, 2005, p. 23).

The institution of security safeguards is critical to lowering the risk of privacy and security threats from being exercised. Before precautions to RFID implementations are evaluated there needs to be a fundamental understanding of what risks should be considered, and how they are prioritized against their relative impact. As part of the evaluation process it is essential to evaluate the privacy and safety threats associated with the use of RFID technology. After the threats have been weighed against an acceptable threshold, mitigation factors can be implemented to address the privacy concerns.

The enhancement of mitigating controls must start with a requirement drawn from legislation (laws), policy, or regulator guidance either directly or indirectly related to the specific technology or information being protected. The broad range of RFID technology implementations makes regulating RFID difficult, however, with industry standardizations and government watchdogs' in-place, monitoring can be achieved against security threats and privacy issues. The advancement of enhancement privacy controls can also help restrict the abuse of the technology, and create capabilities that support the laws and guidelines developed in partnership between government and industry.

The security of RFID is also an overarching mechanism that should be integrated from the conceptualization of the RFID system. The technical, operational, and management controls should be considered during security requirements definition, and should be both part of the application and the process that support the non-functional requirements of the system. Through a clear definition of the vulnerabilities, adequate countermeasures can be establishment to minimize the impact variables.

In response to the Homeland and National Security Initiatives, privacy has been a claim by privacy advocates against the implementation of RFID in the E-Passport, and in

support of the National ID. The issues with privacy are claims by those less educated on the safeguard that were part of the design to protect personal information. There is a need for government agencies implementing RFID implementations to meet legislative requirements to educate the public regarding the technology, and how security has been integrated to ensure protection of privacy information.

The E-Passport adoption is still receiving public opposition against deployment because of the concern regarding privacy information and integrated security safeguards. The E-Passport requires special protective measures that should include data confidentiality requirements against spoofing, forgery, or duplication. The security requirements also mandate additional authentication protection to confidentiality of stored data. Confidentiality protection for privacy data is important because both RFID and biometrics are highly-sensitive technologies, and must afford special protection for data carried on the E-Passports (Juels, Molnar, & Wagner, 2005, p. 2).

Conclusion

The improvements of RFID technology will create more and more opportunities for its introduction into society. The Homeland and National Security sectors have already seen benefits from the use of RFID, and have continued to invest in initiatives such as the National ID and E-Passport that need advanced tracking and identification processes that are reliable and secure. Through the integration of RFID, many other technologies have found benefits to extend their capabilities, and enable them to take advantage of the extensibility offered by RFID to meet their specific business requirements. RFID has also been the question of scrutiny by many privacy groups that see advanced identification capabilities as both a threat and an opportunity for criminals to steal personal information. The information carried within the RFID components, if not adequately protected, could produce privacy issues. To address this concern, security has also found to play an important role in RFID applications to ensure data confidentiality is maintained and risks are limited.

References

- 109th Congress. (2005). Real ID Act of 2005. Retrieved on June 3, 2006 from <http://www.ombwatch.org/regs/2005/hr418.pdf>.
- 9/11 Commision. (2006). The 9/11 Commission Report. Retrieved July 15, 2006 from <http://www.gpoaccess.gov/911/index.html>.
- Ascierto, R. (2005). EPCglobal ratifies first RFID software standard. Retrieved on June 7, 2006 from http://www.cbronline.com/article_news.asp?guid=501806F2-1E9D-4A59-97CB-B078CDEE410D
- Boulard, G. (2005). RFID: Promise or Peril? Retrieved on July 9, 2006 from https://www.ncsl.org/programs/pubs/slmag/2005/05SLDec05_RFIDBadges.pdf
- Electronic Privacy Information Center. (2006). National ID Cards and REAL ID Act. Retrieved on June 30, 2006 from http://www.epic.org/privacy/id_cards.
- General Accounting Office. (2005). Retrieved on July 5, 2006 from <http://www.gao.gov/new.items/d05551.pdf>.
- Juels, A. Molnar, D., and Wagner, D. (2005). Retrieved July 26, 2006 from <eprint.iacr.org/2005/095.pdf>
- Mohan, K.S. (2005). Your Guide to HSPD-12 (Homeland Security Presidential Directive). Retrieved on June 8, 2006 from http://www.gtsi.com/pdfs/7229_hspd12_white_paper.pdf?ShopperID=c1b00811-5085-426f-a914-9b24f4136532
- Schneier, B. (2005). REAL ID. Retrieved on June 8, 2006 from http://www.schneier.com/blog/archives/2005/05/real_id.html.
- United States. Congress. Congressional Budget Office. (2005). H.R. 418 REAL ID Act of 2005 Cost Estimate. Retrieved July 13, 2006 from the Congressional Budget Office Web site: <https://www.cbo.gov/showdoc.cfm?index=6072>.
- United States. Department of Homeland Security (2006). Fact Sheet US-VISIT. Retrieved on July 17, 2006 from the Department of Homeland Security Web site: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0385.xml
- United States. Department of State (2006). United States Issuing New Electronic Passports in Pilot Program. Retrieved on July 15, 2006 from Department of State Web site: <http://usinfo.state.gov/gi/Archive/2006/Feb/27-535.html>.

United States. Department of Commerce. National Institute of Standards and Technology (NIST). Computer Security Division. (2006). Biometrics Data Specification for Personal Identify Verification. Maryland: National Institute of Standards and Technology.

United States. Department of Commerce. National Institute of Standards and Technology (NIST). Computer Security Division. (2006). Interfaces for Personal Identity Verification. Maryland: National Institute of Standards and Technology.

United States. Department of Commerce. National Institute of Standards and Technology (NIST). Computer Security Division. (2006). Personal Identify Verification (PIV) of Federal Employees and Contractors. Maryland: National Institute of Standards and Technology.

United States. Social Security Administration (2005). Social Security Legislative Bulletin. Retrieved on July 9, 2006 from the Social Security Administration Web site: http://www.ssa.gov/legislation/legis_bulletin_051305.html.

Appendix A: Driver License and Identification Cards

The standard requirements the State must include on each driver's license and identification card were outlined by the Department of Homeland Security as follows:

- The person's full legal name;
- The person's date of birth;
- The person's gender;
- The person's driver's license or identification card number;
- A digital photograph of the person;
- The person's address of principle residence;
- The person's signature;
- Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes; and,
- A common machine-readable technology, with defined minimum data elements.

About Lunarline, Inc: Lunarline, Inc. is a Service Disabled Veteran Owned Small Business (SDVOSB) that specializes in Information Security (IS) and Information Assurance (IA). Lunarline, Inc. designs, develops, integrates, maintains, audits, and documents the security for systems, telecommunications, and software throughout the Federal Government. Lunarline Inc. has a successful track record of providing risk-based/Information Security services to our customers. From risk assessments to providing support for an entire Federal Agency's Information Security Program, Lunarline Inc. has ensured our customers' systems and programs exceed Federal and DoD security requirements.