ATTACHMENT E: RFID SECURITY AND PRIVACY WHITE PAPER

The attached document is a white paper prepared to survey the issues surrounding RFID and security and privacy.

Table of Contents

List of Figures and Tables

1.0 Introduction and Summary

The RFID Security and Privacy Study was conducted in concert with the Feasibility Study. The security and privacy study has the following objectives:

- Investigate the security and privacy issues that arise from the proposed use of RFID Technology
- Assess the capability of available technology to resolve those issues
- Provide recommendations to help meet security and privacy requirements

The RFID Security and Privacy Study Report is presented as a discussion of these stated objectives. This report provides an enumeration of the security requirements desired of a near term deployment of the technology. Security and privacy risk assessments of the passive RFID System are provided, with a description of potential countermeasures to address the stated risks.

General analysis of RFID technology indicates that several mitigation strategies are available to alleviate privacy and security concerns. Security mitigation strategies include the use of encryption, implementation of anti-collision algorithms to ensure reader availability and data integrity, the use of filters and audit trails to permit detection of counterfeit tags or replay attacks, and education of tag holders about the use of physical shielding.

A number of privacy concerns related to the use of RFID-enabled documents are already being addressed within the Increment 2C design removing personal data from the tag and into a secure database. Additional privacy protection strategies include the implementation of Fair Information Practices, including educating the public about RFID technology and subsequent placement of tags in travel documents, assignment of a new a-ID number whenever a new or replacement a-ID is issued, and educating tag holders about the use of physical shielding that can prevent their tags from being read.

These strategies should be further evaluated during the design and development phase of Increment 2C in order to determine their effect on operational capabilities and to perform a business risk analysis prior to implementation.

2.0 RFID Security in Increment 2C

Section 2.0 of this report discusses RFID-related security issues as they apply to US-VISIT Increment 2C. The parameters of this security assessment are based on concepts detailed in the US-VISIT Increment 2C RFID Feasibility Study Final Report and are described in Section 2.2.

2.1 Security Objectives

The security objectives detailed in Sections 2.1.1 – 2.1.4 define the "information assurance requirements" of the RFID System. They draw upon industry best practices and adhere to the information security principles of confidentiality, integrity, availability, and non-repudiation. As such, they are desired goals for the deployed system. The security objectives presented in this section are addressed in context in further sections. Detailed explanation of the risks to these goals and proposed countermeasures to these risks are presented.

2.1.1 Confidentiality

Confidentiality is the assurance that only authorized entities share and access system resources and data.

The confidentiality objectives within the RFID System include:

- All data within the system should be protected from unauthorized access
- The algorithms for creating a-IDs can not be reverse engineered from known a-IDs
- Communications channels within the system should be protected from unauthorized access
- The data on the RFID Tags should be protected from access by unauthorized RFID Readers.

2.1.2 Integrity

Integrity is the assurance that data is complete, un-modified and authentic.

This principle introduces requirements to protect against the modification of system data and resources:

- RFID Tag data should be protected from unauthorized modification
- The RFID interrogation channel and subsequent RFID data trail between the RFID System components should be protected from unauthorized modification
- All data within the system should be protected from unauthorized modification
- The presence of multiple tags should not cause loss of system integrity
- Duplication of RFID Tags should be prohibited.

2.1.3 Availability

Availability is the assurance that authorized entities are able to access resources when needed.

The following availability requirements are relevant to the RFID System:

- All system components are operational 24 hours a day, 7 days a week
- The presence of multiple tags should not cause system outage
- The presence of multiple readers should not cause system outage
- Data accessed from the back end enterprise system should be available to multiple authorized personnel at any one time.

2.1.4 Non-repudiation

Non-repudiation is the assurance that a sender or recipient cannot deny data modifications and data transmissions.

The assurance of this principle allows for entities within a system to trust one another and trust data integrity. As such, we state the following requirements within this principle:

- Mutual authentication between the RFID Tag and RFID Reader should occur
- Mutual authentication between the RFID Reader and Middleware should occur

2.2 Security Risk Assessment of the RFID System

This security assessment focuses on an examination of risks inherent in RFID Systems employing Ultra-High Frequency Generation 2 (UHF Gen2) Standard passive tags and middleware communicating with Reader Protocol 1.0. While the UHF Gen 2 Tag Specification has been ratified, but not published as of this date, its characteristics have been extrapolated from the Class 1 published standard.

In addition, it is assumed that resident system data and communication channels between the RFID Middleware and Back End Enterprise Systems will be protected from unauthorized access and modification. The National Institute of Standards and Technology (NIST) issues Special Publications that are of assistance in this regard; these publications are available at http://csrc.nist.gov/publications/nistpubs/index.html. In addition, The Department of Homeland Security (DHS) issues policies, handbooks, and directives that should be consulted when considering system security implementations. Relevant references include (1) DHS MD 4300A, "DHS Sensitive Systems Policy Publication;" and (2) the DHS Sensitive Systems Handbook.

2.2.1 Counterfeit RFID Tag Attacks

RFID Tags are devices prone to several modes of physical attack, to include counterfeiting attacks which seek to duplicate legitimate tags through cloning or forgery. Several intrinsic characteristics of low-cost RFID Systems contribute to the prevalence of these attacks:

- By virtue of its inexpensive functionality, the low cost RFID Tag contains an unencrypted identifier that can be stolen for duplication efforts. For example, an attacker can gain physical or electronic access to the tag's identification number and generate a second, false tag with this same number. This illegitimate tag can be used to perform a replay attack in which the counterfeit tag is used to mimic the behavior of a valid tag.
- The RFID Tags in a deployment are usually manufactured in manner such that the information that provides a tag with its unique value is a predictable number amidst a series of numbers. An attacker could fabricate a meaningful number upon cracking the algorithm for generating the series.

2.2.2 Replay Attacks

The successful creation of counterfeit tags can inflict damage to the integrity of system data. An attacker can perform replay attacks with counterfeit tags, mimicking the valid arrival and departure of tags. Replay attacks on a grand level can ultimately lead to a Denial of Service (DoS) attack in which counterfeit tags are replayed to readers in excess form. Authorized readers are inundated with counterfeit tags presented at a high rate. They consequently fail and cannot read legitimate tags. DoS attacks constitute a serious threat to system availability.

2.2.3 Eavesdropping Attacks

Lightweight RFID Tags do not have the resources required to communicate with RFID Readers through encrypted channels.

Electronic access to tag contents occurs via eavesdropping by attackers in possession of rogue readers. A rogue reader is a reader that is not authorized to interrogate a tag or population of tags. Unsophisticated RFID Tags indiscriminately respond to RFID interrogation at the proper frequency and cannot differentiate between a rogue and authorized reader. In addition, legitimate communication between an authorized reader and tag takes place in clear text and can be intercepted by a rogue reader in the system's vicinity.

Finally, eavesdropping can occur on data flowing between readers and middleware access points. Both wired and wireless deployments of Reader Protocol 1.0 are susceptible to this attack.

2.2.4 Electronic Collisions

Electronic collisions constitute a threat to system integrity and availability. They occur when multiple RFID devices (readers and tags) respond to each other simultaneously, causing their communication signals to interfere with one another. Reader and/or Tag Collisions result in failed transmissions, lost data and faulty data integrity. In addition, readers are prevented from interrogating tags, a loss of system availability.

2.2.5 Introduction of Rogue Components

RFID Readers and Middleware Access Points are units placed in strategic physical locations. To meet functionality needs, they are placed in close proximity to areas in which they are able to contact tags via radio frequency emissions. An intruder could gain access to a physical location and add a rogue reader.

2.3 Mitigation Strategies for Security Risks

Countermeasures to counterfeit tags require an assurance of the confidentiality and integrity of tag data. Measures to prevent the disclosure or modification of tag contents include encryption and access controls. Unauthorized individuals, and rogue readers operating as their extensions, should be prevented from physically and electronically reading tags.

2.3.1 Encryption

Encryption is the conversion of plain, or clear, text into unintelligible form by means of a reversible, mathematically-based translation algorithm. Encryption capabilities can be provided through public (asymmetric) key and symmetric key algorithms. Symmetric key systems perform encryption and decryption functions with the same key. Asymmetric key systems rely on two different keys, both of which can perform encryption and decryption functions. Two parties communicating through these systems each possess one key in a pair of such keys. Outsiders cannot encrypt or decrypt a resultant communication line without the possession of one of these keys.

Both systems can provide confidentiality via encryption, non-repudiation, authentication and access control services. It is noted that the management of symmetric keys, and the maintenance of a public key infrastructure to support asymmetric keys, is accompanied with high overhead costs. In addition, keys embedded on tags are prone to physical attacks, the success of which can lead to cloning.

2.3.2 One-Way Hash Locks

A hash is a one-way function that converts a variable-length block of data into a fixed-length value called a “hash code.” It cannot be reversed. A hash function known only to two parties provides two principles; it authenticates the sender and it provides integrity assurance for sent data.

Weis et al. describe a method by which access control can be achieved via a one-way hash function lock. In their proposal, a tag would store the hash of a unique key as the tag’s *meta-ID* and subsequently enter a “locked state.” The key value and the *meta-ID* value would be stored in a back-end enterprise system. Upon interrogation by a reader, the tag would respond with this *meta-ID*; a legitimate reader would consult with the back-end database, retrieve the key that matched the *meta-ID* value and transmit the key value to the tag. The tag, upon computing a hash on the received key value, would compare the resultant hash value with the stored hash value. A successful match would in essence authenticate the reader to the tag. The tag would enter an “unlocked” state and transmit its full functionality to nearby readers. It should be noted that this proposal does not protect from eavesdropping by rogue readers during the “unlocked” state. In addition, the holders of tags can still be tracked with *meta-ID* values.

2.3.3 Physical Shielding Sleeve (The Faraday Cage)

A Faraday Cage is a metal mesh or foil container that is impenetrable by radio signals of certain frequencies. It can be used to shield a tag from unwanted eavesdropping, but requires owner compliance for use. A physical shield around the tag can serve as a potential threat to availability and integrity if it is not removed to allow legitimate readers to perform their scans. For example, users may fail to remove the tag from its shielding sleeve in the vicinity of authorized readers; the readers cannot identify the now unavailable tag. Data integrity is also compromised, as the RFID System does not record the tag.

2.3.4 The Selective Blocker Tag

Many RFID readers implement anti-collision algorithms. These functions allow for a reader to talk with a single tag without interference from nearby tags that are also responding to the reader’s interrogation signal. Because these algorithms allow tags to be read singly, they are referred to as “singulation protocols.” RFID Systems operating at the UHF range usually employ the silent tree-walking singulation protocol for anti-collision.

The silent tree-walking protocol utilizes a binary algorithm that queries tags bit-by-bit; it resembles a depth-first search of a binary tree. RFID tags bear Unique Identifiers (UIDs) of a fixed bit-length; each bit is represented as a “0” or a “1”. The number of queries performed on a tag by a reader at a single point in time is related to the nature of all tags that are concurrently responding to the reader’s interrogation signal. A population of 96-bit tags is represented by a binary tree of 2^{96} nodes, each node representing a UID. Each node, branches out into two child nodes; one child represents a “0” bit and the other a “1” bit. The reader traverses through the tree, in recursive depth-first form, until a tag is singularized and read. It then performs recursion queries at previously traversed nodes at which there are “children” branching out on either side; this is essentially a point at which a collision of tags has occurred.

Juels et al. propose an extension to the silent tree walking singulation protocol to allow for a tag to hide and reveal itself to a reader at the appropriate times. Described as the “selective blocker tag”, it simulates the full set of possible tag numbers in a given tree. As a reader queries tags in a tree at a given node X for their next bit value, the selective blocker tag responds positively for both children of that node (i.e. it broadcasts both a “0” and “1”). The resultant simulation of all possible tag numbers in a tree causes the reader to collide at all points in a tree. A reader can be assumed to fail after querying several hundred nodes in a tree. It is prevented from reading the tag.

The costs for implementing this functionality would involve slight modifications to circuits and would utilize an approach similar to the EPC tag standard “kill” command to password-protect the selectiveness of the blocker tag. An authorized reader could use a Personal Identification Number (PIN), or password, to disable the simulation behavior and legitimately read the tag.

2.3.5 EPC Tag PINs

Juels describes an alternative method to control access to tags with a simple challenge-response authentication mechanism. This technique strengthens the resistance of tags to counterfeiting, specifically to cloning attacks.

EPC Class 1 Tags have PIN-controlled access to several sensitive functions, including “write,” “sleep” and “kill.” However, this PIN access was originally envisioned to allow readers to authenticate to tags. The Juels proposal twists this inherent capability in EPC Tags to allow for reverse authentication of tags to trusted readers.

A resultant challenge and response communication line between the tag and the trusted reader ultimately results in mutual authentication of both entities.

A realistic vulnerability of this scheme is the risk of PINs being harvested from tags, either physically or electronically. Electronic attacks, which involve PIN-guessing techniques, can be addressed by disabling a tag after a number of incorrect PINs. It is additionally anticipated that PIN lengths will increase from 8 to 32 bits with the Class 1 Generation 2 Tag Specification; this will statistically increase the complexity of “guessing” PINs. Juels also proposes that deployed tags have periodic PIN changes, much like standard system passwords are changed every ninety days per best practices. This last proposition introduces administrative costs and considerations.

2.3.6 RSA Countermeasures

RSA Laboratories has proposed two techniques to address the tag eavesdropping problem. The first, developed by researchers at the Massachusetts Institute of Technology (MIT), modifies the silent tree walking singulation protocol to eliminate reader broadcast of tag data. A second proposal involves tags in possession of multiple identities. The tag emits different identifiers over time; only legitimate readers are able to distinguish valid identifiers from pseudo-identifiers.

As of this writing, these two RSA techniques have not been deployed in RFID vendor production lines for tags or readers.

2.3.7 Anti-Collision Algorithms

Tag collisions can be prevented with the use of anti-collision algorithms that essentially “singularize” a tag from a population of tags. RFID systems operating at 915 MHz generally implement the silent binary tree-walking algorithm as a singulation technique.

Although anti-collision algorithms are helpful commodities, their implementation nonetheless introduces significant tradeoffs that can potentially lead to less efficient and more costly systems. These tradeoffs include:

- The speed which a tag may be read
- The range at which a tag may be read
- The bandwidth of the outgoing reader signal
- The bandwidth of the incoming tag signal
- Tag and Reader Cost

These tradeoffs introduce risks to the system's availability and integrity. If a reader is not able to interrogate properly or if the tag is not able to respond properly, data can be potentially missed.

2.3.8 RFID Distribution and Assignment

Reader Collision generally occurs in environments where there is a dense population of readers that interfere with one another. Sarma et al. propose that frequencies should be allotted to a group of readers over a period of time through a centrally or distributed controlled approach. This would allow specific readers to operate at specific times at specific frequencies. Interference would be eliminated with this scheduled specificity. Ultra high frequency bands would additionally allow for multiple frequency slots, and consequently, multiple instances of reader-to-tag communication lines.

This approach has drawbacks that originate from the fact that low-cost tags do not have the intelligence to discriminate between multiple readers attempting communication with them. One reader may start to perform an action on a tag and fail to complete the action before its allotted time expires. A new reader may take hold of the tag in the next time period and perform additional actions on the tag, without knowledge of previous reader actions. The lightweight tag does not have the sophistication to recognize or prevent these actions. Sarma et al. suggest that reader-to-tag transactions remain brief and atomic to account for this drawback.

2.3.9 Secure Reader Protocol 1.0 Implementations

Reader Protocol 1.0 is the EPCglobal generated and industry accepted standard for defining communication between RFID Middleware and RFID Readers. The protocol is specified in three distinct layers, as depicted in Figure 2-1.

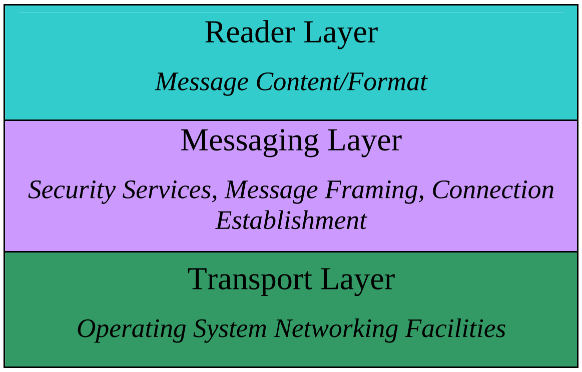
Reader Layer
Message Content/Format
Messaging Layer
Security Services, Message Framing, Connection Establishment
Transport Layer
Operating System Networking Facilities

Figure 2-1 Reader Protocol 1.0

The specification of the protocol allows for multiple alternate implementations of the Messaging Layer. A particular implementation is termed a Messaging/Transport Binding (MTB). Alternate implementations of MTB allow the RFID System to support different types of wired transport, to include Ethernet and Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802 Local Area Network/Metropolitan Area Network (LAN/MAN) Standards. The security context possibilities of the middleware and reader communication mode are therefore indicated by the technology used to implement the MTB.

An IEEE 802 LAN/MAN (Wireless) Standard MTB Implementation such as IEEE 802.11 Wireless LAN can provide shared key authentication and privacy services with the Wired

Equivalent Privacy (WEP) algorithm. Additionally, as IEEE 802.11i becomes prevalent in wireless LAN products, Wireless Protected Access (WPA) 2 can provide Advanced Encryption Standard (AES) encryption of the data packets for wireless transit.

Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL), are two protocols which can provide authentication and encryption controls. Authentication would address the risks of rogue readers and access points, while encryption would address the eavesdropping risk.

Other MTB implementations of consideration include Virtual Private Networks (IP Security Protocol) and Web Services Security (WS-Security). The former is limited in that interoperability issues can arise when client and server software originates from different vendors. The use of WS-Security can result in increased reader computation requirements and can therefore be a potential bottleneck to efficiency.

It is noted that the use of public or symmetric key technologies, as implemented with these described methods, results in overhead costs for key management. Software key certificates stored on readers and access points must be protected from unauthorized disclosure lest the software keys be stolen, implemented on rogue devices, and used to illegally authenticate to legitimate devices. Readers and access points should therefore be placed in environments with appropriately implemented physical and electronic access control measures.

2.3.10 Physical and Environmental Controls

Readers and access points are additionally threatened by natural and structural hazards, to include fire, flooding, fault induction, and power interruption/loss. These physical threats should be addressed very carefully, making certain to adhere to industry accepted physical environment controls. All devices should have back-up/emergency power sources to ensure that the availability of the system is not compromised. Contingency plans should be developed such that the system remains functional in the event of internal component failure. Relevant requirements in these control families are noted in the Requirements Traceability Matrix (RTM) for United States Visitor and Immigrant Technology (US-VISIT) Increment 2C, a document produced using NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems (DRAFT).

2.4 Security Conclusion and Recommendations

This paper presents the security considerations relevant to the deployment of a low cost RFID System. Requirements for the assurance of system confidentiality, integrity, availability and non-repudiation are postulated per industry best practices. Risks to meeting these requirements are discussed, as well as possible countermeasures to these risks, developed as proposals in both academic and research environments. These countermeasures offer a hybrid of potentially lightweight solutions, as well as more expensive solutions for future deployments with less costly circuit power.

Table 2-1 summarizes the aforementioned risks inherent to the RFID System, mapped to the impact they have on our security objectives. It additionally provides a synopsis of countermeasures to control the exploitation of these risks.

Risks	Security Objective(s) Impact(ed)	Countermeasures
Counterfeit Attacks	Confidentiality Integrity	Encryption EPC Tag PINs Physical shielding sleeve One-Way Hash Locks Selective Blocker Tag
Replay Attacks	Availability Integrity	EPC Tag PINs Physical shielding sleeve One-Way Hash Locks Selective Blocker Tag
Eavesdropping Attacks	Confidentiality	Encryption EPC Tag PINs Physical shielding sleeve Selective Blocker Tag RSA Countermeasures
Electronic Collisions	Availability Integrity	Anti-collision Algorithms RFID Distribution and Assignment
Rogue Components	Availability Confidentiality Integrity Non-repudiation	Secure Reader Protocol 1.0 Implementations Physical and Environmental Controls

Table 2-1 RFID System Risks, Their Impacts and Countermeasures

2.4.1 Recommendations

Near-term deployments of a RFID System shall take care to address the overarching security requirement of due diligence. This requirement implies that best practices are implemented after a cost/benefit analysis of possible implementations. This section provides minimum recommendations to assist in this stead. General system recommendations are given as follows:

- The system should implement physical security measures, well documented as controls in guidance available through NIST.
- The system should adhere to information assurance requirements mandated in DHS Department of Homeland Security (DHS) Management Directive (MD) 4300, DHS Information Technology Security Program, DHS Sensitive Systems Policy Publication 4300A and the DHS Sensitive Systems Handbook.
- Back end enterprise systems should offer protection against unauthorized access and improper modification.
- Contingency plans should be developed to ensure availability of the overall system, including RFID readers.
- System administrators should maintain and review audit trails for accountability and investigative procedures. In addition, the system should implement physical and electronic access controls.

RFID System-specific recommendations are given as follows:

- The communication line that extends from readers to middleware to enterprise systems should remain confidential using encryption technologies.
- Unnecessary tag functionalities should be disabled (i.e. "kill" commands) to avoid tag tampering in the field.
- System stakeholders should be able to physically control and track tags from manufacturing to disposal.
- Readers should implement anti-collision algorithms, which help ensure reader availability and data integrity.
- The system should apply filters and audit trails so that administrators can examine faulty data for possible counterfeit or replay attacks.
- The system should mitigate DoS attacks based on a large volume of tags.
- Tag holders should be educated about the proper use of the physical shielding sleeve.

3.0 RFID Privacy in Increment 2C

RFID privacy issues fall into two broad categories: data privacy and location privacy. Data privacy involves control over personal information contained on the tag and in associated database(s). Location privacy involves control over the information regarding the individual's physical location and movement. Security controls that protect data privacy may not address location privacy and vice versa. For example, "one-way hash lock," described in Section 2.3.2, prevents unauthorized readers from accessing the UID on the tag, preserving data privacy, but location privacy is not protected if that same tag produces a unique hash value any time it is interrogated by a reader. A different security control, "Selective Blocker Tag," described in Section 2.3.4, preserves location privacy by interfering with a reader's ability to read data on the tags in its vicinity. However if the data on the tag is maintained in a non-protected format, removing or disabling the "blocker tag" may compromise the individual's data privacy.

This section of the report addresses RFID-related privacy issues as they apply to US-VISIT Increment 2C. The deployment and operations concepts are described in US-VISIT Increment 2C Proof of Concept – Concept of Operations Phase 1, January 3, 2005, and serve as the basis for this analysis. The relevant elements of the operations concept are:

- Tags will be passive, i.e., will not transmit any information until queried by a reader antenna;
- The information contained on the tag will be restricted to UID
- Information on the tags will not be encrypted, i.e., any reader utilizing the proper protocol between 868 and 956 MHz will be able to query the tag and receive the number stored on the tag;
- The tags will be factory programmable, meaning that the serial numbers on the tag will be immutable and part of the physical structure of the tag; and
- Information moving from the antenna to the reader and then to the host computer will be moving over landline and/or in encrypted form.

The UHF tags operating between 868 and 956 MHz can be read from distances of up to 30 feet away.

The RFID implementation in US-VISIT Increment 2C raises both data privacy concerns and location privacy concerns. Many of these concerns arise from the fact that an individual traveling to the US will be issued an RFID-enabled travel document or token (a-ID) and will carry it outside the border inspection area. The nature of government-issued identification and travel documents raises special privacy concerns because of the distinctive relationship between the issuing government, the document, and the individual who is the subject of the document. This portion of the report examines how these privacy concerns arise and ways in which US-VISIT can mitigate them.

Section 3.1 below provides a general overview of privacy objectives for US-VISIT Increment 2C and the basis for these objectives. Section 3.2 describes privacy risks associated with RFID deployment on Increment 2C. Section 3.3 addresses specific data privacy issues in the proposed deployment. Section 3.4 addresses location privacy issues. Section 3.5 discusses possible mitigation strategies for issues identified in Sections 3.3 and 3.4. Conclusions and recommendations are in Section 3.6.

3.1 Privacy Objectives

Privacy objectives for Increment 2C can be stated as follows:

- Protect the data privacy of visitors
- Protect the location privacy of visitors
- Give confidence to visitors that their privacy is being protected

Most privacy protection regimes in the United States, Europe and elsewhere are based the same core set of Fair Information Practices. In the United States these were first codified in 1973 by an advisory committee in the then-Department of Health, Education and Welfare[1] and became the basis for the Privacy Act of 1974. Fair Information Practices continue to serve as a basis for federal and state privacy legislation that governs collection and use of personal information in the United States.

Current studies of privacy in RFID implementation have focused on the use of RFID for supply chain management and the privacy issues that arise when an RFID-tagged product moves from the control of the seller to the purchaser or consumer. On November 20, 2003, a group of eight consumer privacy and civil rights organizations issued a position paper on the use of RFID in consumer-facing applications.[2] The position statement was endorsed by 37 other organizations and individuals worldwide who are involved with privacy and civil rights. The position statement identified several RFID deployment practices that threaten privacy and civil liberties. These practices and their impact on data and location privacy are summarized in Table 3-1.

The privacy and civil liberties groups propose that several Fair Information Practices be made mandatory in RFID deployments:

- **Openness and transparency**. Those who implement RFID systems should make public their policies and practices involving the use and maintenance of RFID systems, and there should be no secret databases. “Individuals have a right to know when … items …in the … environment contain RFID tags or readers. They also have the right to know the technical specifications of those devices. Labeling must be clearly displayed and easily understood. Any tag reading that occurs … must be transparent to all parties. There should be no tag reading in secret.”
- **Purpose specification**. Those who deploy RFID systems should give notice of the purposes for which tags and readers are used.

[1] Secretary’ s Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens*, Washington, DC, 1973. Available online at <http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

[2] RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, November 20, 2003, available at <http://www.privacyrights.org/ar/RFIDposition.htm>.

- **Collection limitation**. The collection of information should be limited to that which is necessary for the purpose at hand.
- **Accountability**. Those who deploy RFID systems are responsible for implementation of this technology and the associated data. They should be legally responsible for complying with the principles discussed here. An accountability mechanism must be established. There must be entities in both industry and government to whom individuals can seek redress when these provisions and/or the organization's stated practices have been violated.
- **Security safeguards**. There should be security and integrity in transmission, databases, and system access. These should be verified by outside, third-party, publicly disclosed assessments.

EPCglobal has also published a set of privacy guidelines for the deployment of RFID systems in consumer-facing applications. These guidelines include many of the same Fair Information Practices identified above: providing consumers notice about the presence of tags, enabling consumers to disable or remove tags, providing information about EPC and RFID technology, and publication of notices about the retention, use and protection of any consumer-specific data generated through operations, either generally or specifically with respect to EPC use.[3]

However, the discussion of Fair Information Practices and RFID in the pure consumer environment does not take account of the fact the relationship between the consumer and the RFID-tagged consumer product is different from a relationship between an individual and an RFID-tagged travel or identification document or token. In the commercial environment, the (tagged) product belongs to the consumer after it is purchased, and the consumer may use, alter or destroy it in any way that is consistent with the law. For example, if a consumer disables an RFID tag, as proposed by EPCglobal, he or she may not be able to take advantage of post-sale services such as returns or warranty service, but under current law there is no prohibition against voluntarily refusing to participate in such programs. The consumer can also use a substitute product if he or she does not wish to purchase one that includes an RFID tag and a functional substitute is available.

The ownership and control relationship surrounding identification and travel documents and their subject individual are significantly different from those between consumer and a commercial product. Identity and travel documents do not belong to the person to whom they are issued but remain the property of the issuing agency.[4] It is illegal to alter identity and travel documents in any way.[5] In order for an identity or travel document to be valid, the individual must accept the document as issued by the issuing government authority, and there is no acceptable substitute. As a result, consumer-initiated privacy protection strategies available in the commercial world, such as refusing an RFID-enabled item or disabling the tag on an RFID-enabled item, are not

[3] EPCglobal, Inc., *Guidelines on EPC on Consumer Products*, available at <http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html>.

[4] The United States passport contains the following statement: "**U.S. Government Property**: This passport is the property of the United States Government. Upon demand made by an authorized representative of the United States Government, it must be surrendered." (Emphasis in original. Location of statement in the passport varies by date of issuance.)

[5] The United States passport contains the following statement: "**Alteration or mutilation of passport**: This passport must not be altered or mutilated in any way. Alteration may make it INVALID and, if willful, may subject you to prosecution (Title 18, U.S. Code Section 1543). Only authorized officials of the United States or of foreign countries, in connection with official matters, may place stamps or make statement, notations, or additions in the passport. You may amend or update personal information for your own convenience on page 7." (Emphasis in original. Location of statement in the passport varies by date of issuance.)

applicable to RFID deployments in identity and travel documents. The individual's inability to alter or refuse RFID-enabled documents or token places increased responsibility on the issuer of such documents to provide privacy protections as part of the issuance and use process.

RFID Practice	Data Privacy Concern	Location Privacy Concern
Hidden placement of tags	Tags can provide information about objects purchased, owned, or carried by the individual without the individual's knowledge or consent	Individual's location can be determined from location of tag readers without the individual's knowledge or consent; individual movement can be tracked via networks of readers
Unique identifiers	Items can be linked to individuals at the time of purchase; history of an item can provide history of individual use and/or activities involving the item	Individual's location can be recorded with fine-grained accuracy by associating the location of a specific item with a specific individual
Massive data aggregation	Tags can provide the means to link information about purchases, post-purchase behavior, financial condition and other personal information from a variety of unrelated sources	Location information can be combined with information about purchases and other behavior
Hidden readers	Tags can be read and information collected by owners of readers without the individual's knowledge or consent	Individual's location can be determined and movement tracked without the individual being aware that this is happening
Tracking and profiling	Fine-grained profiles of individuals can be built by aggregating information related to multiple tagged items and by linking information about purchase, ownership and behavior with information from other sources	Individuals can be tracked by following tags with a mobile reader or through a network of fixed-position readers with known locations

Table 3-1 Privacy Issues in Consumer-Facing RFID Deployments

3.2 Privacy Risk Assessment of the US-VISIT RFID Deployment

RFID deployment on US-VISIT raises both data privacy and location privacy issues. Data privacy issues arise if personal information or information that can be associated with visitor status is stored on the tags. Data privacy concerns have been mitigated to a significant degree in Increment 2C implementation by moving personal data from the tag to a secure backend database. However, some concerns remain, including the UID itself if an algorithm for deriving this number uses data associated with the individual, e.g., birth date or passport number. Data privacy issues also arise because personal data about the tag holder is contained in databases associated with US-VISIT, and because tag numbers can serve as "anchors" to various new databases that can be built by entities that may or may not be associated with the US government. Location privacy issues arise because of the "promiscuous" nature of the tags being deployed, which allows them to be read by any reader at the appropriate frequency and tags in the selected frequency range can be read from several meters away.

Data privacy and location privacy risks are specifically discussed in the sections that follow.

3.3 Data Privacy Risks

Data privacy issues in the use of a-ID involve control of personal information.. Personal data in the RFID system may reside on the tag and/or in associated backend databases, and risks arise when there is possibility for an unauthorized entity to gain access to this data. Additional issues can arise if tags can be re-written.

3.3.1 Data On Tag

In the proposed Increment 2C implementation, no personal data is stored on the tag. If the tag number (UID) is randomly generated, no data can be gathered about the individual by reading the tag. If the UID is generated via an algorithm that uses personally identifiable information as its basis, knowledge of the number generation algorithm may permit "decoding" of the tag number and provide information about the individual to whom the tag was assigned unless the UID is protected, e.g., via encryption.

Random assignment of UID and placing personal data into a secure backend database alleviates the concern that personal data will be gathered by reading the tag or by eavesdropping on the communication between the tag and the reader. If UID is acquired by someone without access to the government's backend databases, the unauthorized reading will produce only the tag number and not the associated personal information. Nevertheless, depending on how many other tags that respond between 868 and 956 MHz are carried by an individual, and particularly if part of the UID identifies either DHS or US-VISIT as an issuing entity, a visitor carrying a US-VISIT issued a-ID may be identified as a visitor simply by virtue of carrying the tag. If identified as a visitor, he or she might become a target for theft or coercion.[6]

In addition to the number assignment scheme, the government should consider whether an individual will be permanently associated with a single a-ID number or whether a different number will be issued every time an a-ID is issued, e.g., because the previous document/token has expired or has been compromised. If the same number is permanently associated with an individual, this number can facilitate profiling and tracking by serving as an "anchor" to a variety of information from government and non-government sources.

[6] A description of crimes against tourists in Florida and of the measures taken to prevent such crimes can be found in U.S. Department of Justice, Office of Community Oriented Policing Services, *Crimes Against Tourists*, p. 16, found at http://www.cops.usdoj.gov/mime/open.pdf?Item=1306. Crime-prevention measures include removal of special rental car license plates and prohibition on rental car company stickers, which make automobiles identifiable as ones driven by tourists.

3.3.2 Tags as "Pointers" and "Anchors" for Databases

By serving as a pointer to associated database entries, UID can serve as a way to create virtually unlimited profiles of individuals. a-ID was specifically selected for use on US-VISIT to facilitate correlation between various pieces of information about individual visitors, correlation between different individuals who might be traveling together, and between individuals and vehicles in which they are traveling. If someone acquires a UID with access to backend databases, whether or not this access is used for a lawful purpose, the dossier of personal information will become available. The extent of the dossier will depend on the extent to which access is limited by security measures within backend systems.

In addition to profiles built using databases associated with US-VISIT, the number produced when the tag is read (either the true UID or the hash if UID is encrypted) can be used as an "anchor" for new databases, e.g., a database of individual purchasing habits or border crossing history. These databases may be compiled by entities that do not have any association with the US government and used for commercial, criminal, or other purposes. While this may seem like an issue outside the scope of US-VISIT's concern, the creation of databases accessible via tag numbers would be possible only because visitors have no choice about accepting a tag on the a-ID if they wish to visit the U.S.

3.3.3 Re-writable Tags

If a tag has the capability of being re-written, there is a possibility that an unsuspecting visitor may become an inadvertent accomplice of someone who wishes US law enforcement authorities to believe he or she has left the country. Until biometric verification is installed for pedestrian and vehicular exit traffic, the only tracking at exit is the tracking of a-IDs. If a tag is reprogrammed with a different number before a visitor leaves the US, the backend databases will contain incorrect information and potentially subject the individual involved to unwarranted scrutiny or punishment on future visits. Additionally, a re-writable tag could be modified to incorrectly alert CBP officers to watch list hits while allowing the truly dangerous individuals to slip past by "swapping" a-IDs.

3.4 Location Privacy Risks

Location privacy risks arise when a tag number is associated with a physical location and time. The location of a tag can be identified either by a mobile tracking system or by a networked system of fixed-position readers connected to a centralized database. Once location information is obtained, it can be used in data mining and other value-added applications.[7] Location privacy issues are a particular concern in the Increment 2C implementation because the operational concept requires that tags be readable from a significant distance without any action by the individual carrying the a-ID.[8]

Location privacy issues arise in various contexts. Sometimes location identification is an essential part of a product or service that an individual wishes to obtain. For example, use of

[7] A framework for analyzing location privacy can be found in James C White's *People, Not Places*, Masters Memo Prepared for the Electronic Privacy Information Center, Spring 2003, found at <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf>.

[8] See US-VISIT Increment 2C RFID Feasibility Study Final Report, Section 2.0, RFID Feasibility Study Objectives.

stored-value card for travel on public transportation or use of an electronic toll-collection device involves and implicit acceptance by the individual that his position will be known and recorded at the time the device is used. There are also devices that produce location information as a by-product of their intended function. For example, use of a cell phone produces location information because the service provider must track the phone's location in order to route calls. A third category of devices can provide location information without an individual being aware that any transaction or query has taken place because location information is not associated with the function provided by the item. RFID used on identification or travel documents falls into this last category because an unprotected tag can be read in any location where a reader is available, but providing location information is not relevant the document's intended function of managing border crossings and may not be anticipated by the individual carrying the document.

By using RFID tags that respond to any reader interrogating them at the correct frequency, the government opens the possibility that location privacy of the individual carrying the RFID-enabled document or token may be compromised. Effective tracking and profiling by law enforcement officials, criminals and commercial entities may be possible because the tag number is all that is required to place an individual at a specific location. Moving personal data from the tag into a backend database does not address the location privacy concern. In fact, even if the tag number is encrypted, location privacy may be compromised if the tag responds with the same encrypted response every time it is read.

The location privacy risk is exacerbated by the government's desire to be able to read tags from a distance of several meters in moving vehicles in order to facilitate traffic flow across the border.[9] Tag numbers can be acquired as the individual crosses the border or at a later time. Because tags in the Increment 2C deployment do not require close proximity for reading, readers can be deployed openly or they can be effectively camouflaged by being placed in or close to objects such as doorways, security cameras, or traffic lights. Since the location of these fixed readers will be known, a network of strategically placed readers will provide information about an individual's movement, enabling tracking of individual visitors. Additionally, because the tags can be read from a significant distance, mobile readers may be able to track them without being seen.

3.5 Mitigation Strategies to Preserve Data and Location Privacy

Both data and location privacy issues discussed above can be mitigated through actions by the government. Table 3-2 below presents a summary of these mitigation strategies and their relationship to the privacy objectives they address.

3.5.1 Implementing Fair Information Practices

Fair Information Practices, particularly operational transparency, are an important part of addressing privacy in RFID deployments for identification and travel documents. The government should adopt a policy of clearly identifying documents that carry RFID tags. The US-VISIT privacy policy should be modified to include an explanation about what RFID is, where the tag is located on the travel document, when and how it will be read, frequency of operation, what information is transmitted by the tag, how the information will be used, and to

[9] See US-VISIT Increment 2C Feasibility Study Final Report, Section 2.2, Study Scope.

whom the information may be disclosed. This explanation should be provided to visitors at the time the a-ID is issued and made available at all border crossing points.

The government can also ensure that government-controlled readers and the area in which readers are operating are clearly marked. This might include signs stating that an individual is entering a border area and that US travel documents can be remotely read within this area. Readers might also include a light or some other signal that indicates a-ID has been read.

In addition to implementing open and transparent practices with respect to RFID-enabled documents, the government also needs to implement security and accountability measures to protect information associated with a-ID tokens. These measures can be discussed in public documents such as the US-VISIT privacy policy, and the Privacy Impact Assessment and System of Records Notice for the system where a-ID numbers will be stored.

3.5.2 Issuing random numbers for a-ID

To minimize the possibility of profiling and tracking by unauthorized entities, the government can adopt a policy of randomly assigning UID when a new a-ID is issued for the first time or re-issued as a result of document expiration or revocation. A new a-ID number with every new a-ID, the new number can be associated with the individual in databases related to US-VISIT, but would make it more difficult for rogue trackers or profilers to continue aggregating data about the tag holder. The government can also provide information to individuals about what they should do if their a-ID is lost or stolen, or if they suspect their tag information has been compromised.

The policy could also prohibit the assignment of the same a-ID number to the individual more than once. This would follow recommendations of International Civil Aviation Organization (ICAO) working group on machine-readable travel documents (MRTDs), which has recommended against issuing a single number to be permanently associated with the individual, in part because of the difficulties that would be experienced by both the individual and the border security officers if the number is compromised.[10] If the tag number identifies DHS or US-VISIT as an issuing agency, visitors should also be given information about what to do if they feel they have been targeted because they are visitors.

3.5.3 Physical shielding of a-ID

Because of the special nature of travel documents or tokens, the RFID must remain active and unaltered. In order to prevent the tags from being used for anything other than the authorized purpose, the government can consider providing information to visitors about effective shielding for RFID-enabled documents. (See discussion of the physical shielding sleeve in the Security section of the report.) ICAO identified possible approaches to physical shielding in its discussion of MRTDs.

> "There are methods of preventing unauthorized reading. One such method is that a State (or other organization) wishing to issue Contactless IC may consider giving holders the advice to keep their MRTD in a metal jacket when not in use. This will completely

[10] ICAO, Technical Advisory Group on Machine Readable Travel Documents, “Use of Personal ID Number as Passport Number,” May 2004.

> prevent unauthorized reading. The MRTD must be removed from the metal jacket for authorized reading.” [11]

Notifying individuals about ways to shield their a-ID would have the advantage of giving individuals an opportunity to make sure that the a-ID is used only for its intended purpose without raising either data privacy or location privacy concerns.[12]

3.6 Privacy Conclusions and Recommendations

The use of RFID in travel document or tokens raises data privacy and location privacy issues. Both data privacy and location privacy risks are present in the deployment of a-ID in Increment 2C. Mitigation strategies that minimize the impact of the proposed deployment on individual privacy are summarized in Table 3-2. These strategies include the use of Fair Information Practices, care in assignment of a-ID numbers, and providing visitors with information about physical shielding of RFID-enabled documents. Each of these mitigation strategies needs to be evaluated in the operational context to understand its potential effect on the performance of the US-VISIT program and on the cost and process of deployment.

Mitigation Strategy	Data Privacy Addressed?	Location Privacy Addressed?	Confidence Provided in Privacy Protection?
Fair Information Practices	Yes	No	Yes
Random a-ID number	Yes	No	Yes
Physical shielding	Yes	Yes	Yes

Table 3-2 Mitigation Strategies for Privacy Protection

4.0 References

- A. Juels. Strengthening EPC Tags Against Cloning. Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2780.
- A. Juels, R.L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. *8th ACM Conference on Computer and Communications Security*, pages 103-111. ACM Press, 2003.
- Auto-ID Center (now EPCglobal, Inc.). Auto-ID Reader Protocol 1.0 *(Work in progress)*. Available at: http://www.epcglobalinc.org/WD-reader-protocol-200309051/4861_0.htm.
- EPCglobal, Inc., *Guidelines on EPC on Consumer Products*, available at <http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html>.

[11] .Ibid.

[12] It should be noted that shielding a-ID might compromise the quality of data or efficiency of border traffic flow if the individual neglects to take the a-ID out of its protective covering in the border area. Shielding might also hinder authorized law-enforcement related surveillance activities.

- EPCglobal SAG Security Working Group. Threat Assessment and Security Survey for Reader Protocol *(Work in progress).* Available on request by E-mail: dbailey at rsa security dot com.
- International Civil Aviation Organization, Technical Advisory Group on Machine Readable Travel Documents, “Use of Personal ID Number as Passport Number,” May 2004.
- NIST Computer Security Special Publications. Available at: http://csrc.nist.gov/publications/nistpubs/index.html.
- RSA Laboratories. Securing RFID Tags from Eavesdropping. Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2118.
- S. Sarma, S. Weis, and D. Engels. RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems*, pages 454-470. Lecture Notes in Computer Science, 1999.
- S.A. Weis, S. Sarma, R. Rivest, and D. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Computing*, pages 201-212, 2004.
- White, James C. *People*, *Not Places*, Masters Memo Prepared for the Electronic Privacy Information Center, Spring 2003, found at <http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf>.