National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-98

Guidelines for Securing Radio Frequency Identification (RFID) Systems

Recommendations of the National Institute of Standards and Technology

Tom Karygiannis
Bernard Eydt
Greg Barber
Lynn Bunn
Ted Phillips

NIST Special Publication 800-98

Guidelines for Securing Radio Frequency Identification (RFID) Systems

Recommendations of the National Institute of Standards and Technology

Tom Karygiannis
Bernard Eydt
Greg Barber
Lynn Bunn
Ted Phillips

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2007

US Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Robert C. Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the US economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. Special Publication 800-series documents report on ITL's research, guidelines, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-98
Natl. Inst. Stand. Technol. Spec. Publ. 800-98, 154 pages (April 2007)

Acknowledgments

The authors, Tom Karygiannis of NIST, and Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips of Booz Allen Hamilton, wish to thank Steven Fick, Rick Korchak, Kate Remley, Jeff Guerrieri, Dylan Williams, Karen Scarfone, and Tim Grance of NIST, and Kenneth Waldrop and Beth Mallory of Booz Allen Hamilton. These individuals reviewed drafts of this document and contributed to its technical content.

The authors would also like to express their thanks to several experts for their critical review and feedback on drafts of the publication. These experts include V.C. Kumar of Texas Instruments; Simson Garfinkel of the Naval Postgraduate School; Peter Sand of the Department of Homeland Security; Erika McCallister of MITRE; and several professionals supporting Automatic Identification Technology (AIT) program offices within the Department of Defense (DoD), especially Nicholas Tsougas, Fred Naigle, Vince Pontani, Jere Engelman, and Kathleen Smith.

During the public comment period we received helpful comments from the following Federal Government agencies: the US Departments of Defense, Health and Human Services, Homeland Security, Labor, and State; the Office of the Director of National Intelligence; the Office of Management and Budget; and the General Services Administration. We also received several helpful contributions from commercial industry, including comments from EPCglobal, VeriSign, and Priway.

Finally, the authors wish to thank the following individuals for their comments and assistance: Brian Tiplady, Daniel Bailey, Paul Dodd, Craig K. Harmon, William MacGregor, Ted Winograd, Russell Lange, Perry F. Wilson, John Pescatore, Ronald Dugger, Stephan Engberg, Morten Borup Harning, Matt Sexton, Brian Cute, Asterios Tsibertzopoulos, Mike Francis, Joshua Slobin, Jack Harris, and Judith Myerson.

Table of Contents

List of Appendices

List of Figures

List of Tables

This page has been left blank intentionally.

Executive Summary

Like any information technology (IT), radio frequency identification (RFID) presents security and privacy risks that must be carefully mitigated through management, operational, and technical controls in order to realize the numerous benefits the technology has to offer. When practitioners adhere to sound security engineering principles, RFID technology can help a wide range of organizations and individuals realize substantial productivity gains and efficiencies. These organizations and individuals include hospitals and patients, retailers and customers, and manufacturers and distributors throughout the supply chain. This document provides an overview of RFID technology, the associated security and privacy risks, and recommended practices that will enable organizations to realize productivity improvements while safeguarding sensitive information and protecting the privacy of individuals. While RFID security is a rapidly evolving field with a number of promising innovations expected in the coming years, these guidelines focus on controls that are commercially available today.

RFID is a form of automatic identification and data capture (AIDC) technology that uses electric or magnetic fields at radio frequencies to transmit information. An RFID system can be used to identify many types of objects, such as manufactured goods, animals, and people. Each object that needs to be identified has a small object known as an RFID tag affixed to it or embedded within it. The tag has a unique identifier and may optionally hold additional information about the object. Devices known as RFID readers wirelessly communicate with the tags to identify the item connected to each tag and possibly read or update additional information stored on the tag. This communication can occur without optical line of sight and over greater distances than other AIDC technologies. RFID technologies support a wide range of applications—everything from asset management and tracking to access control and automated payment.

Every RFID system includes a radio frequency (RF) subsystem, which is composed of tags and readers. In many RFID systems, the RF subsystem is supported by an enterprise subsystem that is composed of middleware, analytic systems, and networking services. RFID systems that share information across organizational boundaries, such as supply chain applications, also have an inter-enterprise subsystem. Each RFID system has different components and customizations so that it can support a particular business process for an organization; as a result, the security risks for RFID systems and the controls available to address them are highly varied. The enterprise and inter-enterprise subsystems involve common IT components such as servers, databases, and networks and therefore can benefit from typical IT security controls for those components.

Implementing the recommendations presented in this publication should help organizations improve the security of their RFID systems.

Personnel responsible for designing RFID systems should understand what type of application an RFID system will support so that they can select the appropriate security controls.

Each type of application uses a different combination of components and has a different set of risks. For example, protecting the information used to conduct financial transactions in an automated payment system requires different security controls than those used for protecting the information needed to track livestock. Factors to consider include:

- The general functional objective of the RFID technology. For example, does the system need to determine the location of an object or the presence of an object, authenticate a person, perform a financial transaction, or ensure that certain items are not separated?

- The nature of the information that the RFID system processes or generates. One application may only need to have a unique, static identifier value for each tagged object, while another application may need to store additional information about each tagged object over time. The sensitivity of the information is also an important consideration.
- The physical and technical environment at the time RFID transactions occur. This includes the distance between the readers and the tags, and the amount of time in which each transaction must be performed.
- The physical and technical environment before and after RFID transactions take place. For example, human and environmental threats may pose risks to tags' integrity while the tagged objects are in storage or in transit. Some applications require the use of tags with sensors that can track environmental conditions over time, such as temperature and humidity.
- The economics of the business process and RFID system. The economic factors for RFID systems are different than those for traditional IT systems. For example, many RFID tags offer few or no security features; selecting tags that incorporate basic security functionality significantly increases the cost of tags, especially if encryption features are needed. Also, the operational cost of some basic IT security controls, such as setting unique passwords and changing them regularly, may be higher for RFID systems because of the logistical challenges in managing security for thousands or millions of tags.

For RFID implementations to be successful, organizations should effectively manage their risk.

Like other technologies, RFID technology enables organizations to significantly change their business processes to increase efficiency and effectiveness. This technology is complex and combines a number of different computing and communications technologies. Both the changes to business process and the complexity of the technology generate risk. The major risks associated with RFID systems are as follows:

- *Business process risk.* Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable. For example, a warehouse that relies solely on RFID to track items in its inventory may not be able to process orders in a timely fashion if the RFID system fails.
- *Business intelligence risk.* An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system. For example, an adversary might use an RFID reader to determine whether a shipping container holds expensive electronic equipment, and then target the container for theft when it gets a positive reading.
- *Privacy risk.* Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. As people possess more tagged items and networked RFID readers become ever more prevalent, organizations may have the ability to combine and correlate data across applications to infer personal identity and location and build personal profiles in ways that increase the privacy risk.
- *Externality risk.* RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people. For example, an adversary could gain unauthorized access to computers on an enterprise network through Internet Protocol (IP) enabled RFID readers if the readers are not designed and configured properly.

Organizations need to assess the risks they face and choose an appropriate mix of management, operational, and technical security controls for their environments. These organizational assessments should take into account many factors, such as regulatory requirements, the magnitude of each threat, and cost and performance implications of the technology or operational practice.

Privacy regulations and guidance are often complex and change over time. Organizations planning, implementing, or managing an RFID system should always consult with the organization's privacy officer, legal counsel, and chief information officer.

When securing an RFID system, organizations should select security controls that are compatible with the RFID technologies they currently deploy or purchase new RFID technologies that support the necessary controls.

To be most effective, RFID security controls should be incorporated throughout the entire life cycle of RFID systems—from policy development and design to operations and retirement. However, many RFID products support only a fraction of the possible protection mechanisms. Tags, in particular, have very limited computing capabilities. Most tags supporting asset management applications do not support authentication, access control, or encryption techniques commonly found in other business IT systems. RFID standards specify security features including passwords to protect access to certain tag commands and memory, but the level of security offered differs across these standards. Vendors also offer proprietary security features, including proprietary extensions to standards-based technologies, but they are not always compatible with other components of the system. Careful planning and procurement is necessary to ensure an organization's RFID system meets its security objectives.

This page has been left blank intentionally.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

These guidelines have been prepared for use by Federal agencies. They may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidance made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

This publication seeks to assist organizations in understanding the risks of RFID technology and security measures to mitigate those risks. It provides practical, real-world advice on how to initiate, design, implement and operate RFID systems in a manner that mitigates security and privacy risks. The document also provides background information on RFID applications, standards, and system components to assist in the understanding of RFID security risks and controls.

This document presents information that is independent of particular hardware platforms, operating systems, and applications. The emphasis is on RFID systems that are based on industry and international standards, although the existence of proprietary approaches is noted when they offer relevant security features not found in current standards. Readers are encouraged to supplement this document with vendor publications and other materials if interested in further pursuing proprietary approaches.

Section 6 provides a brief overview of privacy laws and regulations that pertain to Federal agencies. Privacy concerns involve legal and policy issues that are addressed more thoroughly in the documents referenced in that section. Security and privacy concerns are not entirely separable. For instance, security mechanisms designed to protect data confidentiality also serve privacy interests. On the other hand, approaches to privacy protection that involve the temporary or permanent disabling of RFID technology may introduce a security vulnerability because of the potential for these mechanisms to be used in an unauthorized or unanticipated fashion.

This publication primarily focuses on asset management, tracking, matching, process control, and supply-chain RFID applications. RFID technology is also used in contactless smart cards that support personal identification, access control, and automated payment applications. While this document provides

information relevant to contactless smart card applications, it does not address the advanced authentication and cryptography features that are incorporated into many of them.[1]

This document has been created for executives, planners, systems analysts, security and privacy professionals, and engineers who are responsible for Federal government business processes or information technology (IT) systems. Professionals with similar responsibilities outside the government should also benefit from the information this document provides. The document addresses both the needs of those considering an RFID implementation and those with an existing RFID system. The document is also useful for researchers, students, market analysts and others who seek an overview of RFID technology and related security issues.

1.3 Document Structure

The remainder of this document is organized into seven major sections:

- Section 2 provides an introduction to RFID technology and the major components of RFID systems.
- Section 3 provides an overview of types of RFID applications. It then explains how organizations can identify application requirements to help determine which RFID technology would be most effective for a particular application.
- Section 4 discusses some of the major business risks associated with implementing RFID technology.
- Section 5 explains the various RFID security controls, including their benefits and limitations.
- Section 6 provides a brief overview of privacy regulations and controls, particularly as they pertain to Federal agencies.
- Section 7 provides recommendations that organizations using RFID systems can follow throughout the system life cycle, from initiation through operations to disposition.
- Section 8 presents two hypothetical case studies that illustrate how the concepts and recommendations introduced earlier in the document could work in practice.

Readers that are already familiar with RFID and primarily are interested in the security aspects of the technology may wish to skip Sections 2 and 3 of this document and start with Section 4.

The document also contains several appendices with supporting material:

- Appendix A contains more detailed information on common RFID standards and their security mechanisms.
- Appendix B contains a glossary.
- Appendix C contains an acronym list.
- Appendix D lists print resources and online tools and resources that may be useful references for gaining a better understanding of RFID technology and security.
- Appendix E contains information on permissible radio exposure limits.

[1] The distinction between RFID tags and contactless smart cards is becoming more difficult to define because the computing resources and security functionality of RFID tags is increasing over time. RFID tags and contactless smartcards often use the same air interface standards and techniques for wireless communication.

- Appendix F contains an index of terms used in the document.

This page has been left blank intentionally.

2. RFID Technology

This section provides an introduction to RFID technology. It begins with a discussion of the benefits of RFID relative to other automatic identification and data capture (AIDC) technologies. It then reviews the basic components of RFID systems and provides background information needed to understand later material in the document. Readers who already have a strong understanding of RFID technology and applications can skip this section and the discussion in Section 3 about RFID applications.

2.1 Automatic Identification and Data Capture (AIDC) Technology

Identification processes that rely on AIDC technologies[2] are significantly more reliable and less expensive than those that are not automated. The most common AIDC technology is bar code technology, which uses optical scanners to read labels.[3] Most people have direct experience with bar codes because they have seen cashiers scan items at supermarkets and retail stores. Bar codes are an enormous improvement over ordinary text labels because personnel are no longer required to read numbers or letters on each label or manually enter data into an IT system; they just have to scan the label. The innovation of bar codes greatly improved the speed and accuracy of the identification process and facilitated better management of inventory and pricing when coupled with information systems.

RFID represents a technological advancement in AIDC because it offers advantages that are not available in other AIDC systems such as bar codes. RFID offers these advantages because it relies on radio frequencies to transmit information rather than light, which is required for optical AIDC technologies. The use of radio frequencies means that RFID communication can occur:

- Without optical line of sight, because radio waves can penetrate many materials,
- At greater speeds, because many tags can be read quickly, whereas optical technology often requires time to manually reposition objects to make their bar codes visible, and
- Over greater distances, because many radio technologies can transmit and receive signals more effectively than optical technology under most operating conditions.

The ability of RFID technology to communicate without optical line of sight and over greater distances than other AIDC technology further reduces the need for human involvement in the identification process. For example, several retail firms have pilot RFID programs to determine the contents of a shopping cart without removing each item and placing it near a scanner, as is typical at most stores today. In this case, the ability to scan a cart without removing its contents could speed up the checkout process, thereby decreasing transaction costs for the retailers. This application of RFID also has the potential to significantly decrease checkout time for consumers.

RFID products often support other features that bar codes and other AIDC technologies do not have, such as rewritable memory, security features, and environmental sensors that enable the RFID technology to record a history of events. The types of events that can be recorded include temperature changes, sudden shocks, or high humidity. Today, people typically perceive the label identifying a particular object of interest as static, but RFID technology can make this label dynamic or even "smart" by enabling the label to acquire data about the object even when people are not present to handle it.

---

[2] AIDC technologies are also known as Automatic Identification Systems and Automatic Identification Technologies. The terms "automated" and "automatic" are often used interchangeably.

[3] Other AIDCs include smart cards, optical memory cards, contact memory buttons, and satellite tracking systems.

2.2 RFID System Components

RFID systems can be very complex, and implementations vary greatly across industries and sectors. For purposes of discussion in this document, an RFID system is composed of up to three subsystems:

- An *RF subsystem*, which performs identification and related transactions using wireless communication,
- An *enterprise subsystem*, which contains computers running specialized software that can store, process, and analyze data acquired from RF subsystem transactions to make the data useful to a supported business process, and
- An *inter-enterprise subsystem*, which connects enterprise subsystems when information needs to be shared across organizational boundaries.

Every RFID system contains an RF subsystem, and most RFID systems also contain an enterprise subsystem. An RFID system supporting a *supply chain* application is a common example of an RFID system with an inter-enterprise subsystem. In a supply chain application, a tagged product is tracked throughout its life cycle, from manufacture to final purchase, and sometimes even afterwards (e.g., to support targeted product recalls).

The characteristics of RFID enterprise and inter-enterprise subsystems are very similar to those of any networked IT system in terms of the types of computers that reside on them, the protocols they support, and the security issues they encounter.

Sections 2.3 through 2.5 review each of the subsystems in more detail.

2.3 RF Subsystem

To enable wireless identification, the *RF subsystem* consists of two components:

- RFID *tags* (sometimes referred to as *transponders*), which are small electronic devices that are affixed to objects or embedded in them. Each tag has a unique identifier and may also have other features such as memory to store additional data, environmental sensors, and security mechanisms.
- RFID *readers*, which are devices that wirelessly communicate with tags to identify the item connected to each tag and possibly associate the tagged item with related data.

Both the tag and the reader are two-way radios. Each has an antenna and is capable of modulating and demodulating radio signals. Figure 2-1 shows a simple RF subsystem configuration.

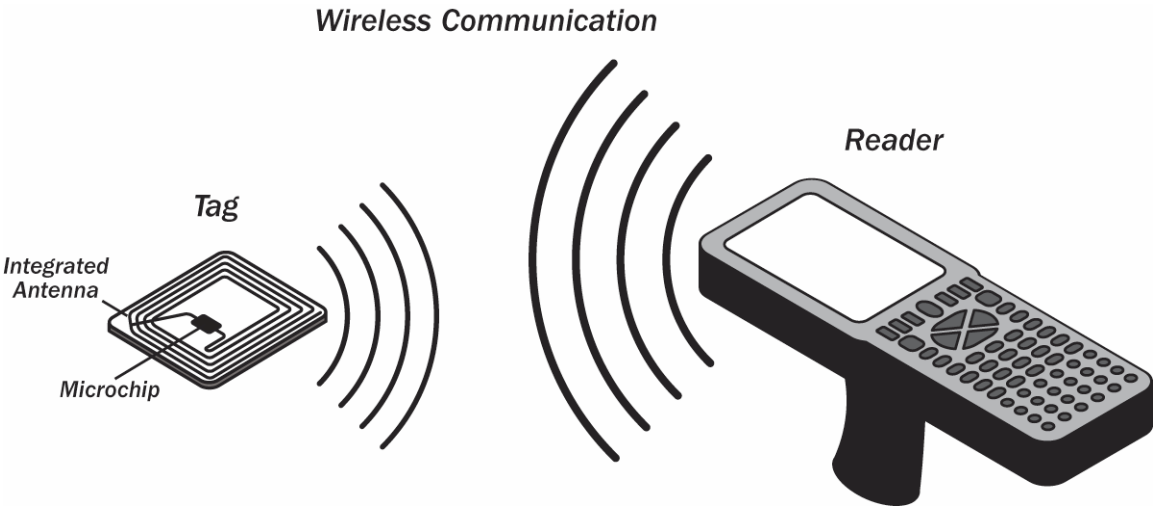

Figure 2-1. An Example of a Simple RF Subsystem

Sections 2.3.1 and 2.3.2 discuss tag and reader characteristics in more detail. Section 2.3.3 explains the fundamentals of tag-reader communication.

2.3.1 Tag Characteristics

The market for RFID tags includes numerous different types of tags, which differ greatly in their cost, size, performance, and security mechanisms. Even when tags are designed to comply with a particular standard, they are often further customized to meet the requirements of specific applications. Understanding the major tag characteristics can help those responsible for RFID systems identify the tag characteristics required in their environments and applications. Major characteristics of tags include:

- Identifier format,
- Power source,
- Operating frequencies,
- Functionality, and
- Form factor.

Sections 2.3.1.1 through 2.3.1.5 examine these characteristics in detail.

2.3.1.1 Identifier Format

Every tag has an identifier that is used to uniquely identify it. There are a number of data formats available for encoding identifiers on tags. System designers often want to use identifiers that have a standard structure, with certain groups of bits representing particular fields. A tag identifier format that is used across many industry sectors is the Electronic Product Code (EPC). This format was developed by the industry group EPCglobal. EPCglobal is a joint venture between Global Standards One (GS1), which was formerly known as European Article Numbering (EAN) International, and GS1 US, which was formerly known as the Uniform Code Council (UCC). The tag identifier format consists of four data fields:

- The *Header*, which specifies the EPC type,

- The *EPC Manager ID*, which uniquely identifies the organization that is responsible for assigning the object class and serial number bits (often the manufacturer of the item),
- The *Object Class*, which identifies a class of objects, such as a certain model of television set, and
- The *Serial Number*, which uniquely describes the instance of that class of objects (e.g., a particular television set).

Using a standard identifier format makes it easier for organizations to decode identifiers. When a machine reads a standard identifier, it can parse the identifier and decode its fields. The machine may need to request information from a remote computer to look up an identifier. When the database is distributed across several organizations and many servers, a standard identifier format with specified fields greatly facilitates the look up process. Therefore, standard identifier formats should be used whenever an RFID system will be used across multiple organizations.

If an organization does not expect its tag identifiers to be read by external parties or is concerned that the association of a tag with the organization or specific classes of objects is a business or privacy risk, then it may choose to develop and implement its own identifier format that does not reveal this information. Options include random or serialized identifiers that do not reveal information about the tagged item (e.g., its object class). Such identifiers can be encoded on many standards-based tags. These tags reserve memory for standard identifier formats but the memory does not have to be used for that purpose.

The data format chosen for an RFID system should be adequate for the entire life cycle of the system. Certain data formats may not have enough bits to uniquely encode all the tags that will be used in a particular application. For example, a supply chain RFID system may need longer identifiers to identify the large number of items that it will manage. The identifier data format also has security implications. For example, standard formats such as EPC allow an adversary to quickly obtain intelligence about a business activity by decoding the manager and object class fields.[4]

2.3.1.2 Power Source

Tags need power to perform functions such as sending radio signals to a reader, storing and retrieving data, and performing other computations (e.g., those needed for security mechanisms). Tags can obtain this power from a battery or from electromagnetic waves emitted by readers that induce an electric current in the tags. The power requirements of a tag depend on several factors, including the operating distance between the tag and the reader, the radio frequency being used, and the functionality of the tag. In general, the more complex the functions the tag supports, the greater its power requirements. For example, tags that support cryptography or authentication require more energy than tags that are limited to transmitting an identifier.

Tags are categorized into four types based on the power source for communication and other functionality:

- Passive,
- Active,
- Semi-active, and
- Semi-passive.

[4] The US Department of Defense (DoD) has mitigated this risk by using a serialized single-field tag identifier. This serialized identifier does not reveal any information about the object with which it is associated.

A *passive tag* uses the electromagnetic energy it receives from a reader's transmission to reply to the reader. The reply signal from a passive tag, which is also known as the *backscattered signal*,[5] has only a fraction of the power of the reader's signal. This limited power significantly restricts the operating range of the tag. It also means that passive tags can only support data processing of limited complexity. On the other hand, passive tags typically are cheaper, smaller, and lighter than other types of tags, which are compelling advantages for many RFID applications.

An *active tag* relies on an internal battery for power. The battery is used to communicate to the reader, to power on-board circuitry, and to perform other functions. Active tags can communicate over greater distance than other types of tags, but they have a finite battery life and are generally larger and more expensive. Since these tags have an internal power supply, they can respond to lower power signals than passive tags.

A *semi-active tag* is an active tag that remains dormant until it receives a signal from the reader to wake up. The tag can then use its battery to communicate with the reader. Like active tags, semi-active tags can communicate over a longer distance than passive tags. Their main advantage relative to active tags is that they have a longer battery life. The waking process, however, sometimes causes an unacceptable time delay when tags pass readers very quickly or when many tags need to be read within a very short period of time.

A *semi-passive tag* is a passive tag that uses a battery to power on-board circuitry, but not to produce return signals. When the battery is used to power a sensor, they are often called *sensor tags*. They typically are smaller and cheaper than active tags, but have greater functionality than passive tags because more power is available for other purposes. Some literature uses the terms "semi-passive" and "semi-active" interchangeably.

2.3.1.3 Operating Frequencies

The radio frequencies at which a tag transmits and receives signals have implications for:

- **Tag performance characteristics, including operating range, speed of tag reads, and RFID data transfer rate.** In general, as a tag's operating frequency increases, its signals are able to carry more data.[6] As a result, higher frequency readers are also able to read more tags in a given period of time. In addition, RFID systems that operate at ultra high frequency (UHF) and microwave frequencies are typically designed to have a longer operating range than LF and high frequency (HF) systems.[7] For most applications, the increased speed and operating range are considered advantages. One exception is applications for which security or privacy is a significant concern, such as those that involve financial transactions or personal data. In these cases, the ability of an adversary to read the data more quickly and from a longer distance typically is considered a risk that requires mitigation.

---

5 Passive tags that transmit ultra high frequency (UHF) or microwave signals typically rely on backscattering to communicate. Passive tags that transmit low frequency (LF) or high frequency (HF) signals typically are inductively coupled and do not communicate via backscatter.

6 For example, EPCglobal Class-1 Generation-2 UHF RFID technology can read tags at a speed of up to 640 kilobits per second. This data transfer rate can allow up to several hundred tags to be read per second.

7 UHF and microwave RFID systems are typically designed to operate outside the near field of the electromagnetic signal – i.e., beyond a small number of wavelengths. This permits these systems to have a longer operating range than LF and HF systems, which generally operate in the near field. For example, EPCglobal UHF RFID systems have an operating range of up to 3 meters (m), which is significantly greater than UHF wavelengths of between 0.1 m and 1.0 m. ISO/IEC 14443 HF systems have an approximate range of 7 to 15 centimeters (cm), which is significantly less than the HF wavelengths of between 10 and 100 meters. Recent advancements in near-field UHF RFID have improved the read rate and performance around liquids and metals.

- **The ability of the tag's signal to penetrate materials.** As a general rule, higher frequencies are less able to penetrate substances such as metals or liquids than lower frequencies. Depending on the application, the penetration capabilities of a particular frequency can be either a benefit or a shortcoming. For example, LF communication typically is a requirement when tags are placed inside an animal (or humans, in some emerging medical applications) because RF attenuation in living tissue, which is mostly water, increases significantly as frequency increases. In applications in which security is a significant concern, an organization may want to use a frequency range than can be blocked by a particular material because this enables effective security shielding that might not otherwise be available. Table 2-1 summarizes the ability of RF signals to penetrate various substances.

- **The likelihood of radio interference.** Radio interference is another reason why transmitted signals may not be properly received. Determining the potential sources of radio interference for a particular RFID implementation requires a site survey. RFID systems may experience radio interference from other systems that operate in the same or nearby frequency band. Interference often is exacerbated when using high power readers or when many readers are collocated. Table 2-2 lists potential sources of interference for RFID systems.

- **The international portability of tags.** The types of systems that use various portions of the electromagnetic spectrum can differ from jurisdiction to jurisdiction because not all regulators assign the same frequencies for the same purposes. If an RFID application requires transporting tags across multiple regulatory jurisdictions, then the system needs to use a frequency range permitted in all of the jurisdictions. Regulations impacting RFID often change, so organizations that use or plan to use RFID technology internationally should monitor relevant developments. Currently, there are frequencies within the LF, HF, and UHF bands that are permitted in most jurisdictions. Also, some tags are frequency-agile, so they can respond to one frequency in one jurisdiction and another in a different jurisdiction.[8]

[8] For example, EPCglobal Class-1 Generation-2 tags operate in the UHF band from 860 to 960 megahertz (MHz). In the United States, regulations permit operation from 902 to 928 MHz. In Europe, the typical operating range is from 865.6 to 867.6 MHz. Some US and European readers can be tuned to corresponding permitted frequencies, but the tags will respond to both.

Table 2-1. Impact of Selected Materials on RF Transmissions[9, 10]

Material	LF 30-300 kilohertz (kHz)	HF 3-30 MHz	UHF 300 MHz-1 GHz	Microwave > 1 GHz
	125 or 134 kHz (common US RFID usage)	13.56 MHz[11] (Worldwide ISM band)	433.5-434.5 915 MHz[12] (common US RFID usage)	2.45 GHz[13] (Worldwide ISM band)
Clothing	Transparent	Transparent	Transparent	Transparent
Dry Wood	Transparent	Transparent	Transparent	Absorbent
Graphite	Transparent	Transparent	Opaque	Opaque
Metals	Transparent	Transparent	Opaque	Opaque
Motor Oil	Transparent	Transparent	Transparent	Transparent
Paper Products	Transparent	Transparent	Transparent	Transparent
Plastics	Transparent	Transparent	Transparent	Transparent
Water	Transparent	Transparent	Absorbent	Absorbent
Wet Wood	Transparent	Transparent	Absorbent	Absorbent

Table 2-2. Common Sources of RF Interference

Frequency Range	RFID Applications	Possible Interference Sources in US
Less than 500 kHz	Access control, animal tagging, automobile immobilizers, EAS systems, inventory control, and track and traceability applications	Maritime radio and radio navigation applications
1.95 MHz - 8.2 MHz	EAS systems	Aeronautical radio, amateur, land mobile, maritime mobile radios, and radio location applications
13.553 - 13.567 MHz	Access control, item-level tagging, EAS systems, and smart card applications	ISM applications and private land mobile radio
433.5 - 434.5 MHz	In-transit visibility and supply chain applications	Amateur radio and radio location applications
902 - 928 MHz	Railcar, supply chain, and toll road applications	ISM applications including cordless phones and radio location
2.40 - 2.50 GHz	Real-time location systems (RTLS), and supply chain applications	ISM applications including Bluetooth, cordless phones, and Wi-Fi as well as radio location, and satellite technologies

9 S. Lahiri, *RFID Sourcebook*. Pearson Education, 2005.

10 In the table, transparent is used to indicate that the material allows radio waves to propagate through it without a significant loss of energy. Absorbent specifies that radio waves propagating through the material will have a significant loss of energy. Opaque indicates that radio waves will be blocked, reflected, or scattered.

11 This is the designated center frequency for the frequency band of 13.553-13.567 MHz, which is an Industrial, Scientific, and Medical (ISM) band that is available worldwide. ISM bands are also used for consumer applications.

12 The designation 915 MHz represents the frequency band of 902-928 MHz, which is an ISM band in North and South America. Contrarily, 433.5-434.5 MHz is not an ISM band in North and South America, but RFID systems in the United States can use this band subject to restrictions in the US Federal Communications Commission (FCC) Part 15 rules.

13 The designation of 2.45 GHz represents the center frequency of the 2.400-2.500 GHz frequency band, which is an ISM band.

2.3.1.4 Functionality

The primary function of a tag is to provide an identifier to a reader, but many types of tags support additional capabilities that are valuable for certain business processes. These include:

- **Memory.** Memory that is nonvolatile enables data to be stored on tags and retrieved at a later time. This memory is either write once, read many (WORM) memory or re-writeable memory, which can be modified after initialization. Non-volatile memory enables more flexibility in the design of RFID systems because RFID data transactions can occur without concurrent access to data stored in an enterprise subsystem. However, adding memory to a tag increases its cost and power requirements. Section 3 discusses RFID application requirements and provides additional information about the circumstances under which the use of re-writable memory would be a desirable approach. In general, when this document refers to memory, it is referring to non-volatile memory. In contrast, volatile memory, which is also used in tags, supports tag computations and does not retain data after it is powered down.

- **Environmental sensors.** The integration of environmental sensors with tags is an example of the benefit of local memory. The sensors can record temperature, humidity, vibration, or other phenomena to the tag's memory, which can later be retrieved by a reader. The integration of sensors significantly increases the cost and complexity of the tags. Moreover, while many tag operations can be powered using the electromagnetic energy from a reader, this approach is not workable for sensors, which must rely on battery power. Tags integrated with sensors typically are only used with high-value, environmentally sensitive, or perishable objects worthy of the additional expense.

- **Security functionality, such as password protection and cryptography.** Tags with on-board memory are often coupled with security mechanisms to protect the data stored in that memory. For example, some tags support a *lock* command that, depending on its implementation, can prevent further modification of data in the tag's memory or can prevent access to data in the tag's memory. In some cases, the *lock* command is permanent and in other cases, a reader can "unlock" the memory. EPCglobal standards, standards developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and many proprietary tag designs support this feature. Some RFID systems support advanced cryptographic algorithms that enable authentication mechanisms and data confidentiality features, although these functions are most commonly found on RFID-based contactless smart cards and not tags used for item management. Some tags offer tamper protection as a physical security feature.

- **Privacy protection mechanisms.** EPCglobal tags support a feature called the kill command that permanently disables the tag from responding to subsequent commands. The primary objective of the kill command is to protect personal privacy. Unlike the lock command, the kill command is irreversible. The kill command also prevents wireless access to a tag's identifier, in addition to any memory that may be on the tag. While the lock command provides security, the primary objective of the kill command is personal privacy. RFID tags could potentially be used to track individuals that carry tagged items or wear tagged articles of clothing when the tags are no longer required for their intended use, such as to expedite checkout or inventory. The ability to disable a tag with the kill command provides a mechanism to prevent unauthorized access to and illegitimate use of product information stored in the tag.

2.3.1.5 Form Factor

The *form factor* of a tag refers to its shape, size, packaging, and handling features. To a large extent, a tag's form factor is determined by the characteristics previously discussed, such as power source and functionality. Some important aspects regarding a tag's form factor include the size of the tag, the weight

of the tag, and the method by which the tag is affixed to and removed from its associated object. Tags typically vary in size from smaller than a postage stamp to about the size of a common document stapler. Active tags typically are significantly larger and heavier than passive tags because they have an onboard power supply. Tags that integrate environmental sensors are also larger and heavier than those without this functionality. While increasing the computing functionality of a tag increases its cost and power requirements, it may not have an impact on its form factor because the microchip on a passive tag is one of the tag's smallest components. On most passive tags, the largest component on the tag is its antenna.

Tags can be attached to items using an adhesive or can be embedded within the item. The primary concern when a tag is attached to an item is how easily it might be detached, whether accidentally or maliciously. Tags attached to items also are more vulnerable to harsh environmental conditions such as dust, debris, humidity, precipitation, and extreme temperatures. However, the vulnerability is intentional in some cases. For example, RFID tags known as *frangible tags* allow users to deactivate tags by tearing the tag's antenna from its circuitry. Organizations can create frangible tags on-site using a printer similar to the one shown in Figure 2-2. Tags that are embedded in objects (e.g., smart cards, animal tissue, plastic housing) are less vulnerable to tampering and environmental conditions.

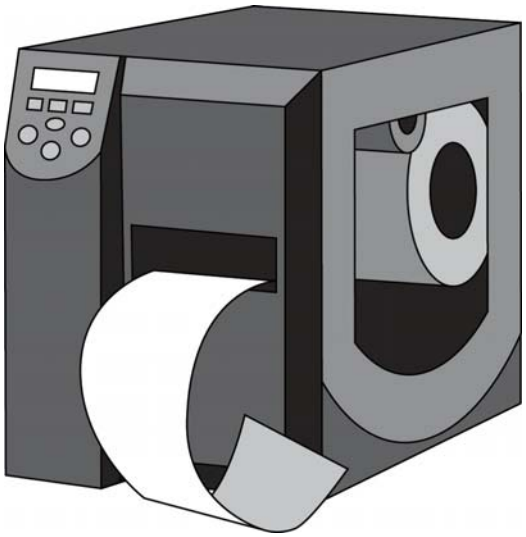

Figure 2-2. RFID Tag Printer

2.3.2 Reader Characteristics

The tag and the reader must comply with the same standard in order to communicate. If a tag is based on a proprietary design, a reader must support the same communication protocol to communicate with that tag. In many cases, if proprietary tags are used, only proprietary RFID readers from the same vendor can be used. Reader characteristics that are independent of tag characteristics include:

- Power output and duty cycle,
- Enterprise subsystem interface,
- Mobility, and
- Antenna design and placement.

These reader characteristics are discussed in Sections 2.3.2.1 through 2.3.2.4.

2.3.2.1 Power Output and Duty Cycle

In most cases, standards and regulations will determine the permitted power output and duty cycle of the readers. A reader's *duty cycle* is the percentage of time that the device is emitting energy over a specified period. For example, a reader that communicates for 30 seconds every minute has a 50% duty cycle. Readers that communicate with passive tags need greater power output than those that communicate with active tags because the signal must be strong enough to reach the tag and enable the backscatter to return to the reader. In general, readers with greater power output and duty cycles can read tags more accurately, more quickly, and from longer distances, but the greater power output also increase the risk of eavesdropping.

2.3.2.2 Enterprise Subsystem Interface

All readers have an RF subsystem interface to communicate with tags. Most also have a second interface to communicate with the enterprise subsystem. The enterprise subsystem interface supports transfer of RFID data from the reader to enterprise subsystem's computers for processing and analysis. In most cases, the enterprise subsystem interface is used for remote management of the readers. The interface may be a wired (e.g., Ethernet) or wireless (e.g., Wi-Fi or satellite) link. Many systems use Simple Network Management Protocol (SNMP) to monitor the readers and alert administrators of conditions that warrant attention.

2.3.2.3 Mobility

A reader's interface with an enterprise subsystem may be wired or wireless. Most wired readers are in fixed locations and support applications in which the tags approach the reader. Some wired readers offer limited mobility using cables. Figure 2-3 shows a reader portal that reads tags on a pallet of boxes moving through the portal. Figure 2-4 shows reader antennas mounted above each toll lane in a series of toll booths. As vehicles pass through one of the toll lanes, the reader reads a transponder that is attached to that vehicle's windshield.

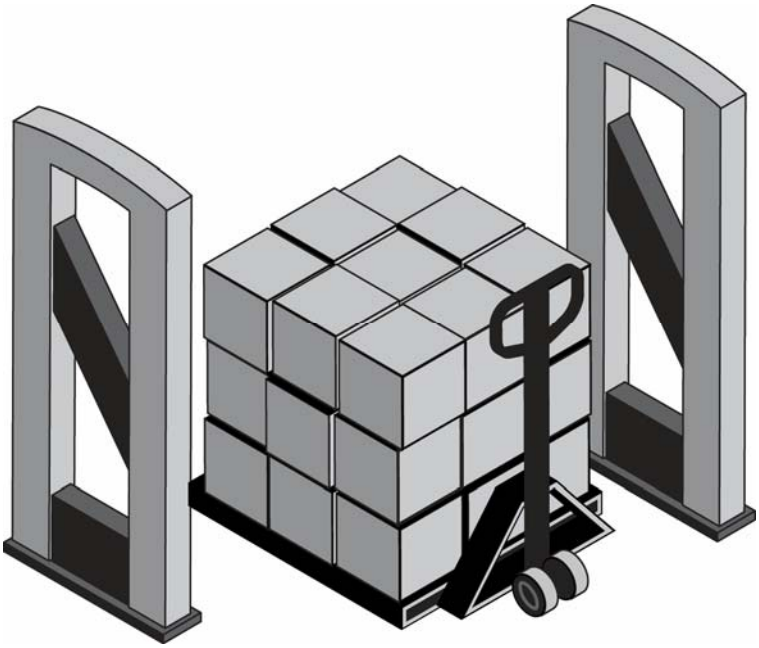

Figure 2-3. Fixed Reader in Item Management Application

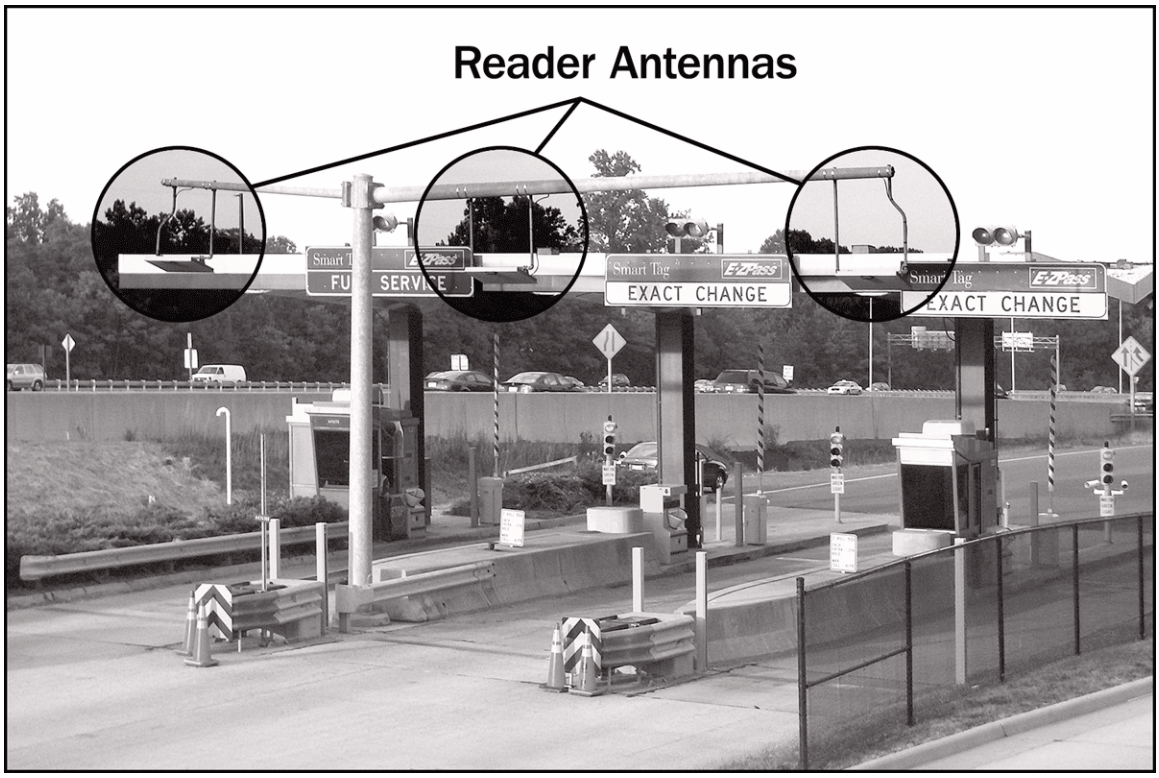

Figure 2-4. Fixed Reader in Automatic Toll Collection Application

In contrast, wireless readers support applications in which personnel must move around to read tags.[14] Figure 2-5 shows an example of a mobile handheld reader. A mobile reader usually uses different communications protocols on its RF and enterprise subsystem interfaces, even though both interfaces are wireless. Institute of Electrical and Electronics Engineers (IEEE) 802.11, also known as Wi-Fi, is a common protocol for the enterprise subsystem interface, although it is also used for the RF interface on some active tag implementations. The most common RF interface protocols are defined in ISO/IEC standards, which include ISO/IEC 14443, ISO/IEC 15693, and the ISO/IEC 18000-series.

Figure 2-5. Mobile Handheld Reader

[14] Wireless protocols are also used on the enterprise subsystem interface when an organization decides not to extend the wired infrastructure to the reader.

2.3.2.4 Antenna Design and Placement

Readers use a wide variety of antenna types. Each type has a different coverage pattern. To reduce the likelihood of eavesdropping and minimize interference with other radios, the coverage should only encompass a range sufficient to communicate with the intended tags. Antennas may be integrated into the device or may be detachable. Readers that support detachable antennas are better suited for applications that require specific coverage areas because an antenna can be selected or customized to meet those requirements.

Antennas can be mounted for a particular application. Figures 2-3 and 2-4 in Section 2.3.2.3 show examples of item tracking and automatic toll payment applications. Antennas can also be mounted on forklifts to identify items when they are moved from one location to another. In industrial applications, antennas are often placed in tunnels around a production line's conveyor belt.

2.3.3 Tag-Reader Communication

Tag-reader communication is achieved by using a common communications protocol between the tag and the reader. Tag-reader communication protocols are often specified in RFID standards. Prominent international standards include the ISO/IEC 18000 series for item management and the ISO/IEC 14443 and ISO/IEC 15693 standards for contactless smart cards. The most recent EPCglobal Class-1 Generation-2 standard is essentially equivalent to the ISO/IEC 18000-6C standard. A more detailed explanation of RFID standards can be found in Appendix A on RFID Standards and Security Mechanisms.

Tag-reader communication characteristics that affect performance and security include:

- How tag-reader communication is initiated,
- How a reader identifies particular tags, and
- How far away a tag or reader's signal can be reliably detected or interpreted.

These are discussed in detail in Sections 2.3.3.1 through 2.3.3.3.

2.3.3.1 Communication Initiation

Tags and readers can initiate RF transactions in two general ways:

- **Reader Talks First (RTF).** In an RTF transaction, the reader broadcasts a signal that is received by tags in the reader's vicinity. Those tags may then be commanded to respond to the reader and to continue transactions with the reader.
- **Tag Talks First (TTF).** In a TTF transaction, a tag communicates its presence to a reader when the tag is within the reader's RF field. If the tag is passive, then it transmits as soon as it gets power from the reader's signal to do so. If the tag is active, then it transmits periodically as long as its power supply lasts. This type of transaction might be used when it is necessary to identify objects that pass by a reader, such as objects on a conveyer belt.

Readers and tags in an RFID system typically operate using only RTF or only TTF transactions, not both types. Active tag TTF operation may be easier for an adversary to detect or intercept, because active tags send beaconing signals even when they are not in the presence of a reader. The adversary could eavesdrop on this communication without risking detection because in TTF transactions the adversary never has to send a signal to ascertain the tag's presence.

2.3.3.2 Singulation

Singulation is the process by which a reader identifies a particular tag. This capability is critical whenever multiple tags are in close proximity. For instance, when a reader issues a command to modify a tag's memory, neighboring tags should not accidentally execute the same command. Similarly, when a reader sends a query to a tag, the reader should not receive a response from multiple tags.

In the EPCglobal Class-1 Generation-2 standard, the singulation protocol requires the reader to broadcast commands to all tags within its operating range. By issuing additional commands, the reader may limit interrogation to tags with specific memory contents. Tags respond with a random number. Once the reader acknowledges this number, verifying that no tag collision has occurred, the tag will transmit its unique ID to the reader. The reader may then request another random number that it uses to address the tag in subsequent communication. The random number has significantly fewer bits than the tag's identifier, which simplifies the processing of later transactions and prevents transmission of the unique identifier by the reader.

Some RFID technologies do not support singulation. For example, ISO 11784/11785 animal tracking tags have no collision detection or avoidance mechanism because multiple tags are not usually read in close proximity for this type of application.

2.3.3.3 Signal Propagation Distance

The communications link between a tag and a reader typically is bi-directional. The reader transmits a signal to a tag over the *forward channel*. The tag responds on the *back channel*, which is also called the *reverse channel* or *backscatter channel*. When RFID systems use passive tags, signals on the forward channel typically are much more powerful than those on the back channel. Therefore, signals on the forward channel can be detected or properly received over longer distances. This difference has important implications for RFID communications security, including both the vulnerability of RF subsystem traffic and the mechanisms used to protect it. Some relevant operational ranges related to various communications objectives are:[15]

- **Nominal operating range**, which is the distance, often specified by standard, over which authorized transactions are expected to occur;
- **Back channel eavesdropping range**, which is the distance over which a rogue receiver can reliably interpret a tag's response to a legitimate reader;
- **Rogue skimming (or scanning) range**, which is the distance over which a rogue reader operating above regulated power limits can reliably communicate with a tag;
- **Rogue command range**, which is the distance over which a rogue reader can execute a tag command that does not require the reader to successfully receive information from the tag;
- **Forward channel eavesdropping range**, which is the distance over which a rogue receiver can reliably listen to the transmissions of an authorized reader; and
- **Forward channel traffic analysis range**, which is the distance over which a rogue receiver can detect the presence of a reader's signal without having to reliably interpret its content.

[15] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, February 2006.

Eavesdropping ranges can be significantly greater than the nominal operating ranges listed in product literature. For example, ISO/IEC 14443 tags have a typical operating range that is usually between 7 and 15 centimeters.[16] However, security researchers have used a portable, low-power device to demonstrate that the rogue scanning range of an ISO/IEC 14443 contactless smart card is at least 25 centimeters (cm).[17] Researchers have also successfully eavesdropped on ISO/IEC 14443 communications from distances up to 15 meters using fixed antennas and receivers that were tuned to the frequency of interest.[18]

If the potential adversary does not need a reply from a passive tag to achieve its objective, then the adversary can be much farther away. For instance, for many tags, a reader does not need to receive a message from the tag before writing to the tag's memory. This attack is not possible for certain commands in EPCglobal Class-1 Generation-2 tags, because mandatory cover-coding requires the reader to receive a key from the tag before issuing a command.[19] *Cover-coding* is a technique used to obscure the content of messages from readers to tags and is described in more detail in Section 5.3.2.1.

Similarly, an adversary can be farther away if that adversary obtains information from the mere detection of the signal, even if the signal is too weak to reliably decode. The presence of a signal indicates that RFID activity is occurring, which an adversary could use to infer that a shipment has arrived. An adversary may also be able to determine the number of transactions taking place even if that adversary cannot identify the nature of those transactions, but this nonetheless could be used infer the level of business activity. This type of intelligence gathering is called *traffic analysis*, and it can be performed over much greater distances than eavesdropping.

2.4 Enterprise Subsystem

The *enterprise subsystem* connects readers to computers running software that can store, process, and analyze data acquired from RF subsystem transactions to make the data useful to a supported business process. For example, an RFID system in a retail clothing store has an RF subsystem that can read the identifier associated with each tagged garment. The enterprise subsystem matches the identifier to the garment's record in a database to determine its price and the number of other items of a similar type that remain in inventory. Some simple RFID systems consist of an RF subsystem only (e.g., RFID-based key systems in which a reader can make an access control decision without access to other computers). However, most RFID systems have both an RF subsystem and an enterprise subsystem.

The enterprise subsystem consists of three major components, which are shown in Figure 2-6, and described in Sections 2.4.1 through 2.4.3:

- Middleware,
- Analytic systems, and
- Network infrastructure.

---

16 The operating range depends on the magnetic field strength of the reader. Source: K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. Munich: John Wiley & Sons Ltd., 2003, pp. 240-241.

17 I. Kirschenbaum and A. Wool, "How to build a low-cost, extended-range RFID skimmer," in *Fifteenth USENIX Security Symposium*, 2006, pp. 43-57.

18 J. Guerrieri and D. Novotny, "HF RFID Eavesdropping and Jamming Tests," Electromagnetics Division, Electronics and Electrical Engineering Laboratory, National Institute of Standards and Technology, Boulder, Colorado, Report Number 818-7-71, 2006.

19 The affected commands are *kill*, which disables all subsequent tag commands; *write*, which is used to write information to a tag's memory; and *access*, which is necessary to lock memory. The technique, in effect, makes the rogue command range equivalent to the back channel eavesdropping range, thereby significantly reducing the threat of rogue commands.

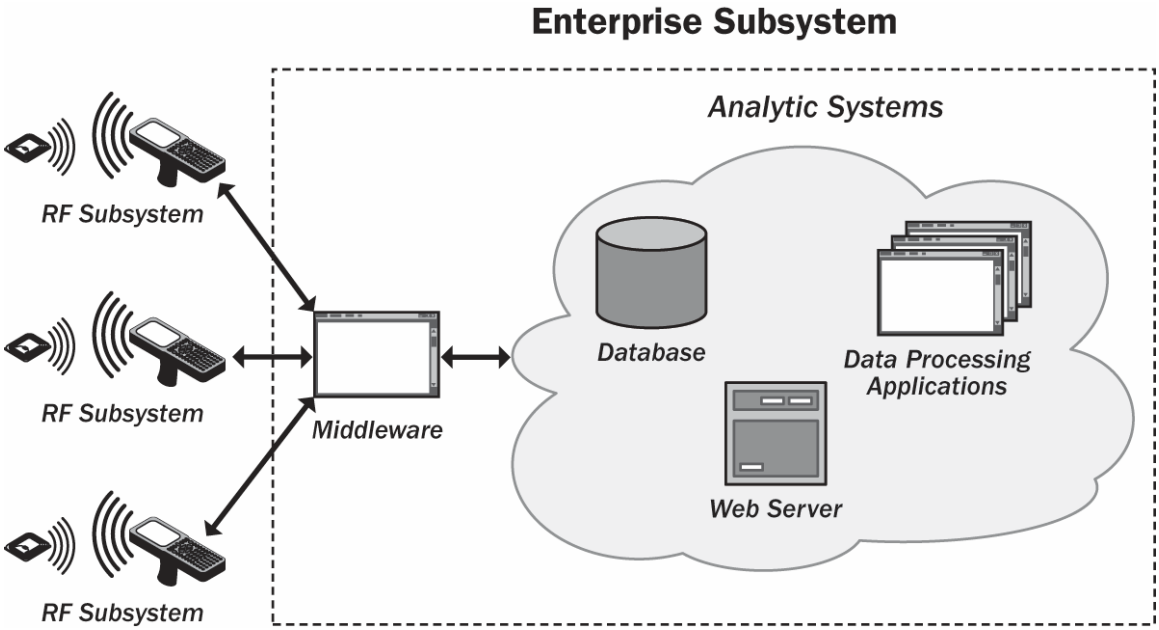

Figure 2-6. RFID System Architecture

2.4.1 Middleware

RFID *middleware* is responsible for preparing data collected from readers in the RF subsystem for the analytic systems that directly support business processes. Middleware hides the complexity and implementation details of the RF subsystem from the analytic systems. This allows the developers and users of the analytic systems to focus on the business implications of RFID data rather than the intricacies of wireless communication. For example, middleware filters duplicate, incomplete, and erroneous information it receives from readers. Middleware filtering is especially useful for applications in which large numbers of tags are in close proximity and for challenging RF environments, such as those containing reflective materials. The middleware can immediately transfer the filtered data to the analytic systems or aggregate and store it for later retrieval.

System administrators also use middleware to monitor and manage readers. For example, system administrators use middleware to adjust the power output and duty cycle to reduce the number of transaction errors. Many middleware products also support event-based triggers that perform actions automatically under certain conditions. Middleware transaction logs help with the identification of anomalous behavior, which could help an organization detect unauthorized use of the RFID system. Many middleware products also provide additional features, such as support for printing RFID labels that provide benefits beyond data and device management.

2.4.2 Analytic Systems

Analytic systems are composed of databases, data processing applications, and Web servers that process the data outputs of middleware based on business requirements and user instructions. They contain customized business logic for each business process they support. For example, the analytic systems of an RFID system supporting logistics may include customized rules for automated inventory management, procurement, shipping, receiving, and billing.

Analytic systems are often enterprise applications that draw inputs from multiple sources, many of which may not involve the RF subsystem. For example, some RFID systems are designed to co-exist with or complement existing AIDC systems (e.g., bar code technology). Analytic systems also correlate RFID data with non-RFID business records imported from other databases, such as records from business partners, customers, logistics service providers, and suppliers. Therefore, analytic systems are often based on commercial database software or legacy applications[20] that support processing of data other than RFID data. Analytic systems that are a part of the EPCglobal Network and process data based on tags that comply with EPCglobal standards are called *EPC Information Services (EPCIS)*.

2.4.3 Network Infrastructure

Network infrastructure enables communication between the RF and enterprise subsystems, as well as among components of the enterprise subsystem. Some important characteristics of network infrastructure include:

- The physical and logical topology of the network, and
- Data communications protocols.

2.4.3.1 Physical and Logical Topology

The *topology* of a network describes how network computing elements are physically and logically connected to each other. *Physical topology* describes the network's cable plant or air interfaces. *Logical topology* describes how the communications links between devices are arranged. Network communications devices often are configured so that the logical topology is different than the physical topology. For example, communications equipment can be configured to create *virtual private networks (VPN)* that logically combine and segment physical networks to achieve performance and security objectives.

The physical topology of a network infrastructure supporting an RFID system depends on the physical location of the components in its enterprise subsystem. For example, the RF to enterprise subsystem connections are physically located near readers.

The appropriate physical location of middleware servers depends on the level of traffic generated by the readers. If RFID transactions are relatively infrequent (e.g., an access control system with relatively small numbers of users), then the location of middleware is not critical. In this context, the middleware can be placed in a central location to serve multiple readers. If the business process requires large numbers of tags to be read quickly (e.g., multiple checkout stations in a busy store), then middleware is located near the readers to avoid latency problems and data throughput restrictions associated with many wide area networks. In some cases, middleware capabilities are incorporated into the communication switches to which the readers connect, so RFID-related traffic does not need to traverse even a single device before it is filtered and processed. This configuration is often termed an *edge processing network* because the switches are considered at the network's edges.

The physical location of analytic systems usually depends on how an organization manages its enterprise applications. If the analytic systems are dedicated to the RFID application, then organizations often place these systems near readers and middleware. On the other hand, some organizations locate their analytic systems in remote data centers to take advantage of the centers' physical security, on-site technical

[20] In this context, legacy applications are computer applications that significantly predate the RFID system and are not designed to process data in formats that middleware supports. In this situation, data has to be converted into a format that the legacy application can interpret.

personnel, and business continuity infrastructure (e.g., electric generators, enterprise data backup, high-availability communications equipment). If the analytic systems integrate both RFID and non-RFID information systems, then it is unlikely that the location of the RF subsystem will significantly influence the location of the analytic systems.

When the enterprise subsystem components are distributed across an organization's network, the resulting physical topology can be complex, but depending on the network's configuration, the logical topology might be relatively simple. Many organizations create *virtual local area networks* (VLAN) for the distributed enterprise subsystem devices that make them appear to each other as if they were on the same network segment. VLANs reduce latency that causes performance problems on networks with large numbers of time-sensitive transactions. They also isolate traffic from other systems, which improves security.

2.4.3.2 Data Communications Protocols

Data communications protocols are a critical component of a network's performance, reliability, and security. A complete discussion of data communications protocols is beyond the scope of this guide, but readers should be able to distinguish between *link-layer* and *network-layer* protocols to understand how RFID enterprise subsystem network infrastructures work and are secured. *Link-layer* protocols specify how devices communicate with each other over a common medium, or link. *Network-layer* protocols (sometimes called *internetwork* protocols) describe how data traffic is routed across multiple network links, possibly over many types of media.

The most common link-layer protocol connecting RFID enterprise subsystem components is Ethernet (IEEE 802.3), which is the same link-layer protocol used to connect most office computers to local wired networks. Ethernet has no built-in security functionality, which means other complementary data communications protocols must provide any required protection.

In most RFID implementations, data communication within the enterprise subsystem is wired communication. The exception is mobile readers, which connect to the enterprise subsystem using a wireless link-layer protocol, such as Wi-Fi (IEEE 802.11).[21] Wi-Fi's characteristics are significantly different than the link-layer protocols supporting communication between tags and readers. In particular, Wi-Fi equipment supporting Wi-Fi Protected Access (WPA) includes numerous security features, such as strong authentication and encryption.[22]

The most common network-layer protocol for enterprise subsystem communication is the IP. Since most modern computers are IP-enabled, enterprise subsystem components, such as middleware and analytic systems, can easily communicate across the enterprise and over external networks, including the Internet. The ability to communicate with a diverse range of computers and their application services also represents a security risk. IP-enabled enterprise subsystem components are subject to the same protocol attacks as any other IP-enabled computer.

2.5 Inter-Enterprise Subsystem

The *inter-enterprise subsystem* connects enterprise subsystems together when information needs to be shared across geographic or organizational boundaries, such as in a supply chain application. Not all RFID systems contain inter-enterprise subsystems. The largest government inter-enterprise subsystem is

[21] IEEE 802.11 is also used for communication between readers and some types of active tags.

[22] For additional information on IEEE 802.11 security, such as differences between WPA and WPA Version 2, see S. Frankel, B. Eydt, L. Owens, and K. Scarfone, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.* NIST Special Publication 800-97, February 2007.

currently the US Department of Defense's (DoD) Global Transportation Network. The DoD improves its logistics and operational efficiency by tracking DoD assets and personnel from their origin to their destination.

While many potential methods for building inter-enterprise subsystems exist, EPCglobal's inter-enterprise approach is a standards-based architecture that has broad industry support and publicly available documentation for review. This section focuses on EPCglobal's approach to the inter-enterprise subsystem for illustrative purposes, but the basic functional requirements described in the discussion of the EPCglobal standards would also apply to any alternative inter-enterprise subsystem architecture.

2.5.1 Open System Networks

RFID systems with inter-enterprise subsystems are called *open* or *online systems* because multiple entities have the ability to access tag-related information. In contrast, RFID systems that operate entirely within an enterprise, and thus have no inter-enterprise subsystem, are called *closed* or *offline systems*. EPCglobal is developing standards for an open infrastructure that will share data associated with EPCs over the Internet among participating organizations that agree to share such data.

To create an open system, each participating organization grants partner organizations access to its analytic systems. The access can occur over a network dedicated for this purpose, a public network such as the Internet, or a VPN that emulates the characteristics of a dedicated network using the infrastructure of a public or shared network. Both dedicated networks and VPNs are sometimes called *extranets*, to denote that information is shared outside the enterprise, as opposed to *intranets*, which are restricted to internal users. To enable extranet access, the implementing organization likely modifies its network firewall to permit RFID-related traffic to traverse the enterprise network boundary and also creates access privileges for external users on the analytic systems themselves. Companies typically sign agreements or memoranda of understanding that describe the roles and responsibilities associated with the access before enabling it.

Figure 2-7 shows how various EPCIS might be connected in an open system network.

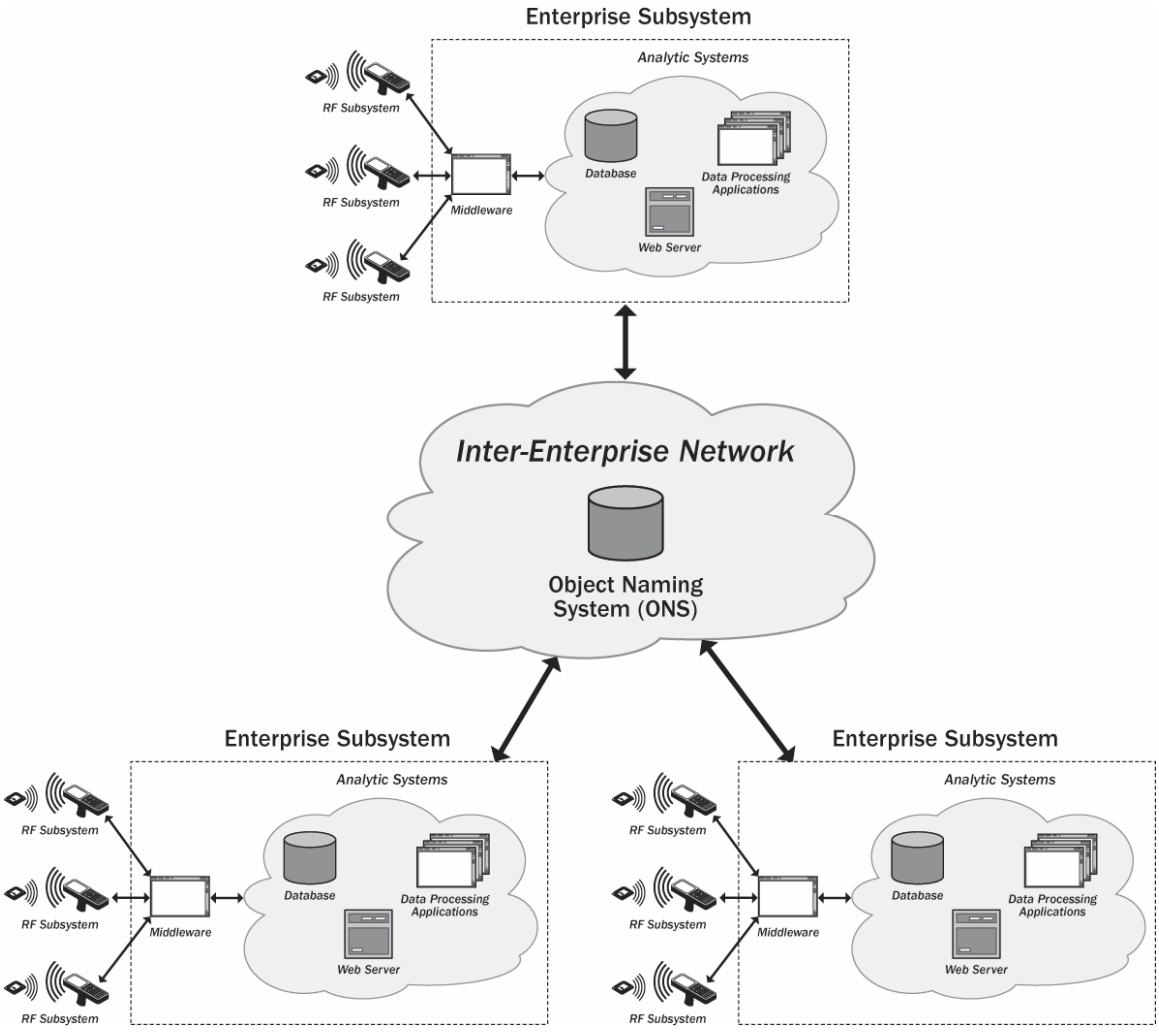

Figure 2-7. Inter-Enterprise Architecture

2.5.2 Object Naming Service (ONS)

Finding information about a tagged object in an open system is a challenge because the information could be located in any one of a number of analytic systems. To solve this problem, EPCglobal created the Object Naming Service (ONS), which is a global distributed database of EPC tag identifiers. Users query the ONS with a particular EPC, and the ONS returns the address information from the EPCIS that contains information associated with that EPC. The user then queries the EPCIS directly to obtain the desired data. The ONS is a resolution mechanism that directs an EPC query to where information associated with that EPC can be found on the network. In order to do that, the ONS utilizes two tiers of resolution services coordinated with the segments on the EPC string: the Root ONS and the Local ONS.

- The Root ONS is a community service administered by EPCglobal that provides an authoritative lookup service indexing all EPC Managers with the addresses of their Local ONS.

- The Local ONS is a software component maintained and operated locally by EPCglobal Network members. The Local ONS provides the authoritative database in which all EPCs issued by a specific EPC Manager are indexed with the addresses of their EPCIS location.

When a member of the EPCglobal Network queries the network for information about an EPC, the Root ONS utilizes the EPC Manager Number segment to direct the EPC query to the EPC's data owner (i.e. the EPC Manager). From there, the EPC Manager's Local ONS utilizes the object class segment to direct the query to the EPCIS that stores information for that EPC.

The ONS extends the Internet's Domain Name System (DNS) to support resolution of an EPC with its corresponding EPCIS. ONS EPC resolution works similarly to the name resolution that Internet users employ whenever visiting Web sites or sending e-mail messages, but with some significant differences, which are presented in Table 2-3.

Table 2-3. Comparison of Traditional DNS and ONS Resolution Transactions

Traditional DNS	ONS	Discussion
User enters a text-based Uniform Resource Locator (URL) into a Web browser or an e-mail address into a messaging client. Examples: http://www.nist.gov/ john.doe@mail.nist.gov	EPC Uniform Resource Identifier (URI) is converted to a fully qualified domain name. Example: urn:epc:id:sgtin:0513347.004106.325 is converted to: 004106.0513347.sgtin.id.onsepc.com	The EPC is first translated into a form that DNS can interpret. The Root ONS is the domain onsepc.com. The Root ONS is built upon the Internet DNS.
The messaging client sends the query to a local DNS resolver, which queries a DNS server to resolve the domain name (e.g., www.nist.gov or mail.nist.gov). DNS contains host (A) records for Web servers and other Internet hosts. DNS contains mail exchanger (MX) records for mail servers.	The Root ONS forwards the query to a Local ONS resolver to resolve the converted URI. The Root ONS portion of DNS has Naming Authority Pointer (NAPTR) records for EPCs.	The transactions are identical, but they involve different types of records in DNS.
DNS returns an IP address for the relevant server. Example: 129.6.13.23	The Local ONS returns a service registration entry for the relevant EPCIS. Example: http://epcis.nist.gov/epc-wsdl.xml In this example, subsequent communication with epcis.nist.gov occurs using Web Services Description Language (WSDL).	An IP address alone is insufficient for the Web services on which most RFID applications rely. ONS supports several types of service registrations, which define how applications will interact with the EPCIS.
The Web browser or messaging client uses the IP address to contact the server at that address.	Where required, the Local ONS resolves the domain name in the response using traditional DNS methods and then directs the EPC query to the specified service to get information about the EPC.	ONS-based RFID applications require additional steps to resolve the service registration.

Much like the DNS, the Root ONS is accessible by any Internet user. Some organizations may choose to implement their own Local ONS that is not connected to the EPCglobal Root ONS. Using an independent ONS limits the applications and users that can access it. This characteristic is a beneficial feature for organizations that require their EPCs to remain confidential, but is overly restrictive for organizations that expect large numbers of external users or that cannot anticipate *a priori* who will have a legitimate need for the EPC records (e.g., individual retail consumers seeking support after purchase of a tagged object).

2.5.3 Discovery Service

The EPCglobal Discovery Services are still in the early phases of development and use cases are still being developed to better understand the needs and requirements for this service. The concept of the EPCglobal Discovery Services is similar to ONS in that it is envisioned to return network addresses where data related to an EPC can be found. However, the Root ONS only provides information regarding where a particular tag was commissioned. It does not provide information regarding the history of a particular tag's transactions. Multiple entities along the supply chain would benefit from having quick access to this information that ONS does not offer. Discovery services offer a potential mechanism to make this information available over an inter-enterprise subsystem.

The EPCglobal Discovery Services can be viewed as a search engine that provides a means to locate the network addresses of all EPCIS services that may have information about a specific EPC (not just the EPCIS service of the EPC Manager). For instance, it is envisioned that the EPCglobal Discovery Services will ultimately return multiple pointers from the multiple organizations that have collected information about the tagged object at some point in the object's life cycle. In addition, the EPCglobal Discovery Services may provide a cache for selected EPCIS data and may enforce authorization policies with respect to access of the aforementioned data. It is envisioned that more than one EPCglobal Discovery Service may operate in parallel, and may compete against each other and/or cater to particular audiences with specific information requirements.

2.6 Summary

RFID is an innovation in AIDC technology that provides significant advantages over earlier technology, such as optical scanning of bar codes. These advantages include the ability to identify objects without optical line of sight over significant distances and the ability to work reliably both indoors and outdoors.

The components of an RFID system can be categorized into three subsystems:

- The RF subsystem,
- The enterprise subsystem, and
- The inter-enterprise subsystem.

Every RFID system includes an RF subsystem, which is composed of (1) tags attached to or embedded in objects and (2) readers that query the tags. Important characteristics of tags include their identifier format, the source of their power, the radio frequencies over which they operate, their size and shape, and additional functionality they support, such as security features and connections to environmental sensors. Important characteristics of readers include their power output, duty cycle, antenna design, and interface to the enterprise subsystem, which can be either wireless or wired. A wireless enterprise interface enables the reader to be mobile. Important aspects of tag-reader communication include the singulation protocol, the encoding scheme, and the distance over which tag and reader signals can be reliably received.

In many RFID systems, the tags and readers are supported by an enterprise system that is composed of middleware, analytic systems, and networking services. The middleware filters data, aggregates data, and manages readers and other RFID devices. Analytic systems process and store this information to support business processes. Lastly, the networking services are used to provide the connections among the components of enterprise subsystem and between the enterprise subsystem and the RF subsystem.

RFID systems that share information across organizational boundaries, such as supply chain applications, also have an inter-enterprise subsystem. The RF, enterprise, and inter-enterprise subsystems together allow an RFID system to support business processes. The versatile components of these subsystems allow an RFID system to be tailored to the needs of a particular application. If an inter-enterprise subsystem is constructed to EPCglobal specifications, then it will have a local ONS and an EPCIS, and may utilize the EPCglobal Root ONS and Discovery Services. The Root ONS provides an authoritative lookup for an EPC identifier that returns pointers to the resources from the organization that created that identifier. Finally, EPCglobal Discovery Services are envisioned to serve as a type of search engine for an EPC identifier that can return pointers to multiple organizations that have information related to that EPC identifier (e.g., companies in the supply chain that have completed a transaction with a particular tag and registered information related to its EPC in their EPCIS).

3. RFID Applications and Application Requirements

RFID technologies are being deployed by many organizations because they have the potential to improve mission performance and reduce operational costs. To achieve these goals, RFID systems must be engineered to support the specific business processes that the organization is automating. Applications for RFID technologies are diverse because of the wide range of business processes that exist.

RFID security risks and the controls available to mitigate them are also highly varied. Typically, only a subset of the full range of technologies, risks, and controls is applicable to any given RFID implementation. Important business drivers that shape RFID application requirements and the resulting characteristics of RFID systems include:

- The general functional objective of the RFID technology (i.e., the application type),
- The nature of the information that the RFID system processes or generates,
- The physical and technical environment at the time RFID transactions occur,
- The physical and technical environment before and after RFID transactions take place, and
- The economics of the business process and RFID system.

This section discusses each of these characteristics in greater detail and provides an overview of common types of RFID applications.

3.1 RFID Application Types

There are many types of RFID applications, of which some of the most common are asset management, asset tracking, automated payment, and supply chain management. The key characteristic differentiating one RFID application from another is the purpose of identifying the tagged items. Table 3-1 lists reasons why an organization might want to identify an item and the general application type that best corresponds to those reasons.

Table 3-1. RFID Application Types

Purpose of Identification	Application Type
Determine the presence of an item	Asset management
Determine the location of an item	Tracking
Determine the source of an item	Authenticity verification
Ensure affiliated items are not separated	Matching
Correlate information with the item for decision-making	Process control
Authenticate a person (holding a tagged item)	Access control
Conduct a financial transaction	Automated payment

Application types are not mutually exclusive; an implementation can combine elements of several application types. For example, both access control systems and sophisticated asset management systems include tracking features. Supply chain management is a tracking application that spans organizational boundaries and often includes process control and payment transactions.

Personnel responsible for designing and implementing RFID systems should understand what application types apply to their implementation so that they can select appropriate security controls. For example, the

security controls needed to protect financial transactions in automated payment systems are different than those needed for tracking applications. The personnel should also understand that an adversary may leverage RFID technology for an unintended purpose. For example, a warehouse may use RFID technology to determine what items it has in its current inventory, but an adversary may use the same system to track an item's whereabouts after it leaves the warehouse. In this case, an asset management system is later used to enable an unauthorized tracking application, perhaps used by an adversary to locate high value targets.

The remainder of Section 3.1 examines each of the application types mentioned in Table 3-1, as well as supply chain management. The section uses hypothetical examples to illustrate the key characteristics of each application type and highlights how they differ from one another. The section also incorporates other examples of each application to provide additional information on current and potential applications of the technology.

3.1.1 Asset Management

RFID-based *asset management systems* are used to manage inventory of any item that can be tagged. Asset management systems using RFID technology offer significant advantages over paper-based or bar code systems, including the ability to read the identifiers of multiple items nearly simultaneously without optical line of sight or physical contact. These features increase the speed of common asset management tasks, which improves operational efficiency and effectiveness.

Perhaps the simplest form of asset management is Electronic Article Surveillance (EAS), which accounts for items in retail stores.[23] For example, EAS tags are placed on electronic equipment, clothing, books, and many other consumer goods at major retailers. After a customer purchases an item, the sales clerk deactivates the tag. If a person attempts to leave the shop with unpurchased goods, readers at the doors will detect the activated tag and trigger an alarm. In this case, the RFID technology determines only one thing: whether or not the EAS tag is still operating, indicating that the item has not been properly checked out.

Most RFID-based asset management systems provide additional functionality. For example, at a doctor's office, the medical records clerk can quickly scan the filing system on a monthly or quarterly basis to determine how many medical records are present or missing. The records clerk can also instantly compare the list of missing records with a list of those known to be checked out of the filing system. Without RFID technology, this task could take hours or days to complete by hand. Bar code technology, such as that found at a supermarket, would require physical handling of each medical record, which is labor-intensive.

RFID is also an enabling technology for smart shelves and smart cabinets, which automatically maintain continuous inventories of the items they hold by tracking items entering and leaving. Items are reordered automatically when inventory is low. The smart shelves and cabinets can also be used for theft prevention, alerting personnel when many high-value items are taken at the same time, and perhaps activating a camera to record the event.

3.1.2 Tracking

Tracking applications are used to identify the location of an item, or more accurately, the location of the last reader that detected the presence of the tag associated with the item. Many tracking applications are

[23] While EAS can be implemented using RFID technology, it can also be implemented using acoustomagnetic technology, which is not based on RFID. Source: K. Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, 2nd edition. Munich: John Wiley & Sons Ltd., 2003, pp. 29-40.

part of an asset management system. One difference between relatively simple asset management systems and tracking systems is that an asset management system can detect the presence of an item with readers at a single location. In contrast, tracking systems require more than one reader, as well as a network, so that a central system can aggregate and correlate information received from each of the readers.

At transportation hubs (such as ports or train stations), readers are placed throughout the facility. The security staff can track the location of its employees wearing RFID-equipped identification badges as they pass through doors or gates. In addition to restricting access to specific areas of the facility, these RFID-enabled identification badges help the security department locate specific staff members during emergency situations and to monitor building evacuations during fire alarms.

Tracking applications can also be used to measure sports performance. Some companies sell systems to track athletes during races. This application requires each racer to wear a unique tag that is registered with the tracking system. Such systems can be used for any mass start event, including bicycling, running, or triathlons. Different events may require the athletes to wear the tags in a certain way to be detected by the system. For example, runners may be required to put the tag in one of their shoes or cyclists may be required to mount the tag on their bicycles.

3.1.3 Authenticity Verification

In *authenticity verification* applications, the tag provides evidence of the source of a tagged item. Authenticity verification often is incorporated into a tracking application. The originating source of the tag creates a record of the initialization transaction, either on the tag or in an enterprise subsystem database. When readers subsequently query the tag, they can determine if it originated from a proper source. For authenticity verification systems to provide appropriate levels of assurance, they typically need to incorporate cryptography and mechanisms to prevent cloning.[24] Digital signatures use cryptography to provide the property of non-repudiation, which means the signatory cannot later deny creating the signature.[25] Authenticity verification applications can use digital signatures to establish evidence of authenticity and enable later verification. The pharmaceutical industry is using RFID for authenticity verification to reduce the prevalence of counterfeit drugs.

3.1.4 Matching

In a *matching application,* two tagged items are matched with each other and a signal (e.g., a light or tone) is triggered if one of the items is later matched with an incorrect tagged item. The most common matching application today occurs in hospitals and involves placing bracelets with tags on mothers and their newborn babies. If a new mother is accidentally given another woman's infant, the system issues an alert. Similar technology allows day care centers to match children to parents or guardians, and hospital patients to their medicines and designated visitors. In the future, RFID tags might match airline passengers with their checked luggage to prevent theft and inadvertent mistakes.

3.1.5 Process Control

Process control applications allow business processes to use information associated with a tag (or the item attached to the tag) to take a customized action. A common process control application is the facilitation of product design variations in manufacturing processes. For example, a tag might be affixed to the frame of a product on an assembly line in a manufacturing plant. The tag's identifier would be

[24] Section 5.3.3.4 provides more information on tamper protection. Anti-cloning measures also involve the use of non-modifiable identifiers.

[25] Section 5.3.1.3 contains additional information on digital signatures.

associated with desired features of the finished product. At each station in the assembly process, a reader would read the tag and take an appropriate action, such as adding a specialized component or using a particular color of paint. In another typical application, sensors are attached to tags to measure factors such as temperature, humidity, or shock. Information from the sensors can be used to make decisions regarding the tagged items. For example, a perishable product may be discarded if it has been exposed to room temperature for more than a threshold period of time.

In asset management, tracking, and matching applications, each reader only needed to capture the tag's identifier (a number permanently assigned to the tag) and apply a timestamp to the transaction. In process control applications, additional information beyond the tag's identifier is normally associated with each tag. That information could reside on the tag itself or in a networked database. In either case, the additional information introduces a level of complexity not found in the previously discussed applications. Implementing organizations have additional design issues to consider, such as exactly what information needs to be recorded, where it should be stored, how it should be protected, and their customers' expectation of privacy for that information.

3.1.6 Access Control

Access control systems use RFID to automatically check if an individual is authorized to physically access a facility (e.g., a gated campus or a specific building) or logically access an information technology system. Some systems are implemented using contactless RFID smart cards instead of mechanical keys. Every individual that is given access to specific areas must carry one of these cards. Locked doors or turnstiles typically protect the areas. To unlock them, authorized personnel must present their smart cards near the appropriate reader.[26] The door or turnstile will unlock once the reader has authenticated the smart card. The system can be configured such that only certain cards can be used to unlock certain doors or turnstiles. The possession of the cards may also be combined with a password, personal identification number (PIN), or biometric (e.g., fingerprint or retina scan) for additional security.

There are two general types of access control systems: online and offline. Online systems have readers that are networked to a central computer. In an online system, each card is linked to a specific person. Each reader is supplied by the central computer with a list of individuals that can access the corresponding area. Since this system is networked, the central computer can provide updated access lists to the readers. In contrast, offline systems are not networked. In offline systems, the card lists the rooms that the holder can access, perhaps also listing an expiration date. When someone attempts to access a room using the card, the reader checks that the card contains one of the permitted identifiers before allowing entry.

RFID technology is also used in automobile key applications, which is effectively a type of access control. There are two basic types: immobilizers and push-button keyless start. With immobilizers, a tag is embedded into a key similar to a traditional vehicle key; the tag in the key is read by a reader in the dashboard or steering column. For the key to start the vehicle, it must both have the right shape for the ignition system and contain the tag. Duplication of these keys is significantly more difficult and costly than traditional keys, which has helped to reduce vehicle thefts. The second automobile key application type is push-button keyless start, which allows a driver to start a vehicle without putting a physical key in the ignition. Instead, each driver simply carries a key fob into the vehicle. Once the key fob is detected, the vehicle is started by pushing a start button on the dashboard.

[26] Different standards for contactless smart cards have different read distances. For example, ISO/IEC 14443 proximity smart cards have an approximate operating range of between 7 and 15 centimeters and ISO/IEC 15693 vicinity smart cards have an approximate range of up to one meter.

3.1.7 Automated Payment[27]

RFID technology automates a variety of financial transactions, including fare collection on public transit systems,[28] toll collection on roads, fuel charges at gas station pumps, and retail payment using credit cards with embedded RFID tags. The US General Services Administration (GSA) Smart Card Program provides RFID-based cards that support financial transactions.[29] The main advantages over other payment forms are speed and convenience; RFID-based automated payment systems do not require users to physically exchange cash or cards with clerks or machines.

Automated payment systems are a specialized form of access control in which access is granted to credit or debit a financial account. Like other access control systems, they require additional security protections to prevent fraud and abuse. In the case of automated payment, integrity and confidentiality controls are needed as well as protection against duplicating or modifying tags; users should not be able to alter debit and credit amounts, and bystanders should not be able to record account numbers or other transaction details. For these reasons, the protocols and cryptography that support automated payment systems typically are considerably more complex than those that support physical access control systems.

Automated payment systems can be online or offline. Online systems, which are the most common, store and process the financial data in a central system networked with the readers. Offline systems require the smart card to store "electronic cash" and handle debit and credit transactions, which involve more sophisticated computing and increase the cost of each card. One advantage of offline systems is that they can support the same user anonymity achieved with cash, while centralized systems must link users to their accounts. However, because most users do not demand complete anonymity, the additional complexity and expense of offline systems make them relatively uncommon.

One example of an automated payment system is currently being used by large resorts and cruise ships. Guests are issued RFID-enabled identification cards upon check-in. These cards are linked to credit card accounts and enable passengers to pay for meals and gift shop items. They are also used for identification when guests disembark the ship or leave the resort grounds.

3.1.8 Supply Chain Management

Supply chain management involves the monitoring and control of products from manufacture to distribution to retail sale. Supply chain management typically bundles several application types, including asset management, tracking, process control, and payment systems. An important distinguishing feature of supply chain management systems is that they span multiple organizations, each of which uses RFID technology that interoperates with the others. When a system is not under one organization's control, it is referred to as an *open system*. The previously discussed systems are *closed systems* because a single organization manages them.[30] Open systems are inherently more vulnerable than closed systems because the network, application and operational interfaces between organizations provide an adversary with more potential avenues to attack the system.

---

[27] This document does not describe or discuss in detail the multi-layered security controls required for RFID-based automated payment systems. Automated payment systems, point-of-sale systems, and financial transaction systems typically have complex security systems with a variety of controls and safeguards.

[28] Chicago, San Francisco, and Washington, D.C. use RFID-based fare collection. For additional information see Permanent Citizens Advisory Committee to the Metropolitan Transportation Authority, "In your pocket: using smart cards for seamless travel," October 2004, http://www.pcac.org/reports/pdf/Smart%20Card%20Exec%C9ive%20Summary.pdf.

[29] For additional information on the program, see http://www.smart.gov/.

[30] Another common term is a closed *loop* system, which refers to RFID systems that recycle their tags for reuse. Open loop systems could refer to RFID systems that use disposable tags, which is the case in most supply chains.

Supply chain systems can record information about products at every stage in the supply chain. Ideally, tags are affixed to products during the manufacturing process or soon afterward. As a product moves through the supply chain, to the end customer, and later to post-sale service, the tag's identifier can be used by all supply chain participants to refer to a specific item. In addition, supply chain systems that use active tags can track larger objects such as cargo containers. Tags on these containers can store a manifest of the items shipped in each container. This manifest can be automatically updated when items are removed from the container.

The information collected by a supply chain RFID system offers many benefits. By more accurately tracking products throughout their life cycle, participants can realize improved speed and accuracy of ordering, automated invoicing and payment, fewer supply shortages with lower inventory levels, and reduced *shrinkage* (product loss or theft). Furthermore, RFID-based supply chain systems give management programs better visibility into the supply chain, which enables identification of bottlenecks, targeted recalls, and new forms of market research. Such systems also generate an electronic pedigree for each item. This feature gives buyers evidence of the item's freshness, so they can identify if its useful life has expired. It also provides buyers evidence of a product's authenticity, so buyers can determine if it is an unauthorized clone.

3.2 RFID Information Characteristics

Once an organization determines the general application type that corresponds to the business process it wants to enhance or enable with RFID technology, it should characterize the information that will be processed by the system. At the low end of the data requirement spectrum is the case of EAS. In EAS, systems, the necessary information is conveyed in a single bit: either the tag is functioning (the item has not yet been sold), or it is has been deactivated (the product has been sold). For this reason, EAS is referred to as a one-bit or single-bit application. Similarly, in the case of relatively simple asset management systems, the only data required is the identifier on the tag. The RFID system merely records which items are present or have been read by the reader. Matching applications also have relatively simple data requirements because they just link one identifier with another.

Data storage requirements increase in tracking applications. The system needs to record which of multiple readers last read the tag and at what time. As the tracking systems get more complex, more data is collected, such as changes in the possession of the item (e.g., someone signing for a package) or the particular contents of a container. Process control applications further increase data requirements because they use the recorded specifications of an item to customize actions in the business process.

Supply chain management systems are the most data-intensive RFID application. They not only process data, but they must also maintain information about the data, such as the formats the various organizations in the supply chain use to store and transmit data and the network addresses of database servers that contain data about tagged items.

When determining the appropriate RFID technology and security controls for a given RFID application, the personnel responsible should ask three questions regarding each data element in the RFID system:

- Is it considered sensitive or confidential?
- Could the data element be easily correlated or combined with other data to allow someone to infer sensitive or confidential information through indirect means?
- Does it change, and if so, how frequently?

In many cases, the data element is not sensitive. Organizations need to examine and invest in security controls to protect RFID data depending on the sensitivity level of that data. They also need to consider how data elements might be combined with other data to make inferences or build profiles, particularly if data elements are shared across organizations or stored for long periods of time.

Another important characteristic of the data is whether it changes over time. In general, tag identifiers never change, but the data associated with the identifier can change. For example, in asset management applications, the RFID system may maintain information about product features such as make, model, size, color, and serial number. These product features typically will be written once and then will not change while the item remains in the system. However, if the asset management application's primary focus is tracking containers rather than specific items, then the data changes frequently as the container is reused to store and transport new items. In access control applications, if a tag acts as a key for a particular item, such as an automobile, then nothing should change once the tag is linked with that item. If the access control application allows a security administrator to change someone's access to different areas and rooms based on changing business roles, then the system must store data related to the access rules.

In general, the implementation specifics rather than the application type determine the extent to which data must be modified. When data elements change, the supporting technology must support write transactions and must have an access control mechanism to protect the integrity of the data. Sections 5.3.1 and 5.3.3.1 provide information on authentication and access control methods. When an element does not change, it does not require this support. Organizations planning RFID implementations should analyze what data is required to support the business process and which elements must be modifiable. One important factor is whether tags and their identifiers will be used once and discarded, or reused. The results of this exercise will help organizations identify appropriate RFID technology and security mechanisms to meet their requirements.

3.3 RFID Transaction Environment

The conditions under which readers query tags are a significant determinant of an RFID system's technology requirements. The most important parameters regarding the RFID transaction environment include:

- The distance between the reader and the tag,
- The amount of time in which a transaction must be completed, and
- Whether or not the reader has access to a network and can use the network to store related data.

Sections 3.3.1 through 3.3.3 discuss these parameters.

3.3.1 Distance between Reader and Tag

Distance requirements often determine the type of tag that can be deployed. The distance between the reader and the tag also has security implications. In general, longer distances between the reader and the tag could make it easier for an adversary to eavesdrop on their communications. Longer distances also allow an adversary to use their own reader to perform unauthorized transactions more easily (as discussed in Section 2.3.3.3).

In some cases, the RFID system designer has considerable latitude in setting the distance between reader and tag. For example, an application controlling access to a garage might require drivers to place an RFID-enabled badge within inches of a reader or it might require a general proximity of several feet to a

RFID-enabled transponder within the vehicle. The choice is essentially an application design decision that may include such factors as cost and convenience.

In other cases, the distance between reader and tag is dictated by the environment in which the RFID system will be deployed. For example, a toll payment application that identifies vehicles on a highway may require that readers query tags from a distance of several meters. In this case, the minimum read distance is a requirement for the design of the RFID system.

3.3.2 Transaction Speed

Transaction speed can be measured in a variety of ways. A common metric is the number of tags read per second. The main reasons why an application has requirements related to the speed of transactions are:

- Readers are expected to communicate with multiple tags nearly simultaneously and cannot do so if each transaction takes longer than a certain period of time.
- Tagged items are in motion and only reside in a reader's operating range for a limited period of time.
- The system's users may perceive the application as a nuisance if transactions take longer than a short period of time to complete.

For example, in some inventory applications, operators may need to confirm the entire inventory at the end of each business day. In this case, each transaction must be completed within a small fraction of a second or the process may take too long to finish. Similar issues may arise when trying to read the tags of athletes in a tracking system designed to measure race times. In this case, if the transactions take too long, there is a chance that some participants in the race may go out of range before the reader identifies them.

Many security mechanisms introduce latency into RFID transactions. Additional steps are needed to perform authentication, encryption, cover-coding, and other security-related procedures. Each additional step takes time. When considering security controls, organizations need to balance the business impact of each security control's effect on transaction speed with the protection it provides.

3.3.3 Network Connectivity and Data Storage

Whether or not an RFID system's readers are networked with database applications has major implications for the architecture of the RFID system and its security. When an application needs to link data with tags, the data needs to be stored somewhere. If the readers are networked with databases, then the data can be stored in the databases. Otherwise, the data must be stored on the tags.

When data is stored centrally on database servers, the tag only needs to contain an identifier, which links the tag to its associated information. In this architecture, the vast majority of the data processing occurs on the supporting systems to which the reader is connected. On the other hand, when data is stored on tags, the tags must have some form of memory and support both write and read transactions.

Regardless of where data is stored, the data's integrity must be protected. If the data is sensitive, its confidentiality must also be protected. The methods for achieving this include authentication, access control, encryption, and physical security. However, database servers and tags implement these methods in different ways. Nearly all commercial database servers support a wide variety of configurable security controls, but most tags do not. In general, RFID systems that use networked readers to access database

servers are preferable to those that store data on tags, both in terms of cost and security. However, a system may require local storage of data on tags for several reasons, including:

- Extending the network to a remote RFID reader is not feasible or is more expensive than using tags that support the required functionality.
- Accessing the data from the network introduces unacceptable latency.
- Network availability is inherently poor, perhaps as a result of harsh operating conditions, which makes accessing data on tags a more reliable approach.
- The participants in an open system have determined that the risk of storing data on tags is less than the risk of opening their networks to external entities.
- Each tag must collect and store information from a sensor or other data source before it can communicate with a networked reader.
- Users want control over when personal data is shared and therefore prefer that it remain on the tag and not in an enterprise database.

3.4 The Tag Environment between Transactions

RFID system requirements depend on what happens between transactions, as well as during transactions. Relevant factors before and after reader communication include:

- Whether or not the business process requires that the tag collect data about its environment, and
- The human, technical, and environmental threats that pose risks to the tag's integrity.

These factors are discussed in Sections 3.4.1 and 3.4.2.

3.4.1 Data Collection Requirements

In some applications, each tag is attached to a sensor that stores data in memory that is accessible to the tag. The memory may belong to the sensor, to the tag, or to a combined device. In some cases, the application's core purpose is to capture this data, and RFID technology merely provides a vehicle to access it remotely. In other cases, the sensor data supports an asset management or tracking application, and the objective is to take measurements to ensure that storage or transport conditions are as expected.

3.4.2 Human and Environmental Threats to Tag Integrity

Tags are vulnerable to a variety of threats that could adversely impact the business processes that they support. Selecting appropriate RFID technology and security controls depends on the level of the threat in the environments in which the tags are expected to reside. Some human threats to tags include the ability of an adversary to:

- Damage or destroy a tag,
- Remove the tag from the item to which it was attached,
- Replace a tag with another one, or
- Clone a tag and use the clone for an unintended purpose.

For example, in an EAS application, someone might remove or disable a tag to steal an item from a store without triggering an alarm. Alternatively, someone could replace a tag with one from a lower-priced item before purchasing the tagged item. In an access control application, someone might replace a tag with one that has greater access. If the replaced tag were attached to a picture identification badge, an adversary might be able to effectively gain the privileges of another person while appearing legitimate to personnel who visually check the badge.[31]

Environmental threats to tags include extreme heat, cold, moisture, vibration, shock, and radiation (including sunlight). Any risk assessment of environmental threats should also consider the impact of these conditions to the material to which the tag is attached and the glue or other mechanism that attaches the tag to the item. Impacts of harsh environmental conditions include degradation of tag performance, destruction of the tag, and separation of the tag from its associated item.

Organizations need to assess the likelihood of these threats in their environment and set requirements for their RFID technology accordingly. In general, human threats are more likely to be realized if outsiders (e.g., customers or members of the general public) have physical access to the tags and therefore the means to engage in malicious behavior. Human threats are also more likely if people have an incentive to perform the attack, such as some form of financial gain or access to a restricted resource.

3.5 RFID Economics

Cost-benefit tests can be applied to any technology project, but the RF subsystem of an RFID system has differentiating characteristics, especially regarding security. Table 3-2 examines the key factors to consider.

Table 3-2. Economic Factors for Traditional IT Systems versus RFID Systems

Economic Factor	Traditional Systems	RFID	Discussion
Target of protection	Primarily, the information that the system stores and processes. Secondarily, the hardware and software components of the system.	In asset management and tracking systems, organizations typically are more concerned with protecting the item being tagged (especially against theft) than the information that the system processes. Similarly, in RFID-based access control systems, the ultimate objective typically is protecting physical assets rather than information.	The value of the information and physical assets is entirely dependent on the specific implementation. In general, it is easier to place a value on physical assets than information assets because physical assets have a known price and depreciation schedule.

[31] Smartcard standards (as distinguished from RFID standards) include specifications for tamper proofing, including lamination of the cards. Lamination is the application of a transparent material that, among other things, prevents the easy removal of a tag attached to the surface of the card.

Economic Factor	Traditional Systems	RFID	Discussion
Number of units	Systems can involve anything from a handful to several thousand users and components; only the very largest IT systems exceed this scale.	Small-scale RFID applications typically are not economical. RFID systems can involve from hundreds to millions of tags.	In implementations with many RFID tags, small changes in the unit cost of tags (e.g., several cents a tag) can have enormous impacts on the total cost of the system and, therefore, its economic feasibility. Small changes in the unit costs of traditional IT system components typically do not impact the economic viability of the implementation.
First (or upfront) cost of security functionality	Basic security functionality (e.g., authentication and encryption) usually is bundled into commercial-off-the-shelf operating systems, database software, and network components; it does not increase the upfront cost of the system from the consumer's perspective.	Incorporating basic security functionality significantly increases the cost of a tag. Encryption that is commonly supported on traditional IT systems is currently cost-prohibitive on tags for most applications.	The upfront cost associated with security functionality likely is a more significant factor in RFID procurement decisions than it is for traditional IT systems.
Operational complexity and cost of basic security controls	While costs can vary greatly, many controls such as passwords are commonplace and are not perceived as unnecessarily burdensome. Many enterprises require users to have complex unique passwords that change at least every 90 days.	Assigning unique tag passwords or periodically changing tag passwords may be administratively unmanageable in many RFID applications.	The operational costs of even basic security controls such as passwords need to be carefully considered when setting policy for and designing an RFID implementation.

3.6 Summary

RFID technology can support a wide range of applications—from asset management and tracking to access control and automated payment. The business requirements for these applications are as varied as the applications themselves. In particular, they are implementation-specific and depend on such factors as:

- The nature of the information that the RFID system manages, including its sensitivity and how it changes over time,
- The RFID transaction environment, including the distance between reader and tag, the required speed of the transactions, and the level of network connectivity during the transaction,
- The characteristics of the tag environment between transactions, such as whether tags collect data from sensors and the human and environmental threats that tags face, and
- The economics of RFID technology and security controls.

This page has been left blank intentionally.

4. RFID Risks

RFID technology enables an organization to significantly change its business processes to:

- Increase its efficiency, which results in lower costs,
- Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and
- Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk. For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics.

This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments. The risks are as follows:

- **Business Process Risk.** Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.
- **Business Intelligence Risk.** An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.
- **Privacy Risk.** Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.
- **Externality Risk.** RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users. In other AIDC and IT systems, it often is easier to identify when unauthorized behavior is occurring. This section characterizes the risks listed above in more detail. The security controls that mitigate these risks are discussed in Section 5.

4.1 Business Process Risk

RFID systems typically are implemented to replace or enhance a paper or partially automated process. Organizations implementing RFID systems could become reliant on those systems, which if not implemented properly with business continuity planning might be less resilient to disruptions than the systems they replace. For example, suppose that a warehouse replaces its paper-based inventory management system with an RFID-enabled system. The paper system involves storing completed forms at the warehouse and sending form duplicates to a central office, while the new RFID system locates its backend database servers at a single computing center. In this environment, the paper system might be more resilient to a local disaster than the RFID system, despite the increased efficiency, accuracy, or effectiveness of the RFID-enabled business process.

Failure in any component or subsystem of the RFID system could result in system wide failure. In the warehouse example, system wide failure might result from many causes, such as loss of the network connection between the warehouse and the computing facility, a software virus that disables critical middleware functionality, or a new source of radio interference that prevents readers from accurately reading tags. If an RFID system is rendered unavailable for any reason, then potential impacts can range from a deceleration of the business process to the loss of critical business or operational records. If the system is mission critical, then the consequences could be devastating to the organization's performance.

Table 4-1 reviews some of the factors that determine the level of business process risk.

Table 4-1. Factors Influencing Business Process Risk

Factor	Discussion
The importance of the RFID-supported business processes to the mission of the organization	The tighter the link between the RFID-supported business process and the mission of the organization, the greater the impact will be if the business process is degraded or disabled. Organizations whose core business is logistics or asset management stand the most to lose when their supporting RFID systems fail. If an organization's primary mission is outside these areas, it is less likely to be impacted. For example, a hospital whose primary mission is patient care could be significantly inconvenienced with the loss of an RFID system, but medical care is likely to continue regardless of the system's status.
The robustness of business continuity planning or fallback procedures that can be implemented when the RFID system is unavailable	In many applications, the fallback procedure is trivial to implement, in which case business process risk is relatively low. For example, a push-button keyless start automobile key could be designed to operate as a physical key when the RFID system is not functioning properly. If an RFID-based automated payment system is down, cash and credit cards are viable alternatives. In many cases, bar codes or visual inspection of tagged items may provide a workable interim solution until the RFID system returns to operation. In general, as the complexity of the system increases, so does the risk and, consequently, the need for business continuity planning. Plans should include the ability to use geographically distributed personnel and enterprise equipment so that timely recovery is possible in case of local disasters.
The environment in which the RFID technology is located	Important environment factors include the existence of radio frequency interference, electrostatic discharge, vibration, abrasion, extreme temperatures, or humidity. The presence of physical access controls also is a key determinant of the risk to business processes from human threats. Public and densely populated areas pose more risk than tightly controlled or remote areas.
The existence of adversaries with the motivation and the capability to perform RFID attacks	Individuals or groups with malicious intent are more likely to target organizations with a high public profile, such as government agencies, than less well-known entities. Individuals seeking financial gain are likely to target RFID systems that support financial transactions and systems that involve high-value assets. For example, individuals may try to replace the tag on a high value item in a retail store with a tag from a low value item to purchase the high value item at a reduced cost. The computer attacker seeking a challenge is also a threat for all systems.
The presence and effectiveness of RFID security controls	The stronger the controls and countermeasures, the lower the risk. These controls are discussed in more detail in Section 5.

Unlike most of the other risks, business process risk can occur as a result of both human action and natural causes. Moreover, human causes may be intentional or unintentional. For example, a tag might

fail to perform its intended function because someone removed it from its packaging, an employee accidentally damaged it with a box cutter, or a severe storm covered it in ice.

An example of an intentional attack on an RFID business process is cloning, which occurs when an adversary reads information from a legitimate RFID tag and then programs another tag or device to emulate the behavior of the legitimate tag. Documented examples of cloning have occurred in tags used for financial payment[32] and access control.[33] Another attack on an RFID business process would be removing a tag from the item it is intended to identify and attaching it to another unrelated item. Someone might, for example, perform such an attack to get a better price on an expensive item in a store.

Potential problems are not just limited to the RF subsystem. If the network supporting the RFID system is down, then the RFID system is likely down as well. In supply chain applications, network failures at any point in the chain have the potential to impact the business processes of any subsequent link in the chain. For example, if a supplier is unable to write manifest data to a tag, then the recipient cannot use that data in its operations even if its RFID readers and network infrastructure are fully functional. Servers hosting RFID middleware, databases, analytic systems, and authentication services are all points of failure. Any efforts to assess business process risk need to be comprehensive, because such a wide variety of potential threats exist. All of these threats have the potential to undermine the supported business process and therefore the mission of the implementing organization.

4.2 Business Intelligence Risk

RFID is a powerful technology, in part, because it supports wireless remote access to information about assets and people that either previously did not exist or was difficult to create or dynamically maintain. While this wireless remote access is a significant benefit, it also creates a risk that unauthorized parties could also have similar access to that information if proper controls are not in place. This risk is distinct from the business process risk because it can be realized even when business processes are functioning as intended.

A competitor or adversary can gain information from the RFID system in a number of ways, including eavesdropping on RF links between readers and tags, performing independent queries on tags to obtain relevant data, and obtaining unauthorized access to a back-end database storing information about tagged items. Supply chain applications may be particularly vulnerable to this risk because a variety of external entities may have read access to the tags or related databases. The risk of unauthorized access is realized when the entity engaging in the unauthorized behavior does something harmful with that information.

In some cases, the information may trigger an immediate response. For example, someone might use a reader to determine whether a shipping container holds expensive electronic equipment, and then break into the container when it gets a positive reading. This scenario is an example of *targeting*.

In other cases, data might also be aggregated over time to provide intelligence regarding an organization's operations, business strategy, or proprietary methods. For instance, an organization could monitor the number of tags entering a facility to provide a reasonable indication of its business growth or operating practices. In this case, if someone determined that a warehouse recently received a number of very large

[32] Researchers from the Johns Hopkins University and RSA Laboratories cloned tags used as vehicle immobilizers and electronic payment tokens. Source: S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in the *Fourteenth USENIX Security Symposium*, 2005, pp. 1-16.

[33] A University of Waterloo student cloned a proximity card used for access control. Source: S. Garfinkel, Ed., and B. Rosenberg, Ed., *RFID Applications, Security, and Privacy*. Upper Saddle River, New Jersey: Pearson Education, Inc., 2006, pp. 291-301.

orders, then that might trigger an action in financial markets or prompt a competitor to change its prices or production schedule.

Table 4-2 reviews some of the factors that determine the level of business intelligence risk.

Table 4-2. Factors Influencing Business Intelligence Risk

Factor	Discussion
The existence of adversaries with the motivation and the capability to perform RFID attacks	For an attack to be successful, the attacker must have the knowledge and tools necessary to perform the attack and a motive for engaging in malicious behavior. Many organizations have known adversaries and consequently need to implement countermeasures against that threat. Other organizations may not have identifiable adversaries with the required characteristics. However, organizations should proceed with caution because they may not be able to anticipate who may be an adversary in the future. For example, disgruntled employees always represent an insider threat even if the organization has not experienced attacks to date.
The usefulness or relevance of information available to the adversary	The most critical item is what information is stored on tags. With the exception of some access control applications, if tags contain only identifiers, then the risk is substantially lower than it would be if tags store data about the tagged item. Information potentially stored on tags that could be of great value to an adversary includes personal records, location history, container manifests, and sensor measurements. Some adversaries might obtain valuable intelligence from the mere existence of a tag or knowledge of the number of tags at a particular location. For example, if the tagged item is associated with an individual, then it could reveal the presence of that person at a specific location. Similarly, the number of tags at a location provides information about inventory levels. Accordingly, organizations need to consider how an adversary might use information about the presence of a tag as well as data stored on the tag.
The location of RFID components	If tagged items are located in public areas, business intelligence risk is considerably higher than it would be if tags stay within access-controlled facilities. Another consideration is the ability of radio communication to occur beyond the physical perimeter. For example, if an adversary can read tags outside of a facility's fence, then the business intelligence risk is higher than it would be if signals were limited to a few feet and could not easily penetrate walls. The physical location of supporting IT infrastructure can also play a role in risk determination.
The presence and effectiveness of RFID security controls	The use of controls such as database access controls, password-protection, and cryptography can significantly mitigate business intelligence risk if applied properly. Section 5 discusses these controls in more detail.

4.3 Privacy Risk

RFID technology raises several important privacy concerns. One concern is that organizations may collect personal information for a particular purpose, such as to complete a financial transaction or grant an individual access to a facility, and then later use that information for a different purpose that the individual finds undesirable, such as to conduct a direct marketing campaign. Another concern is that organizations that are implementing RFID systems to serve a particular business process might not be aware of how the RFID information could be used for unintended purposes, such as the targeting or tracking of individuals, or the potential disclosure of personal practices or preferences to unauthorized third parties.

There are privacy risks from the perspective of the individual and from the perspective of the organization implementing RFID technology. The privacy risk from the perspective of the individual is the unauthorized revelation of personal information and the personal consequences of that breach. The privacy risk from the perspective of the implementing organization might include:

- Penalties if the organization does not comply with privacy laws and regulations,
- Customer avoidance or boycott of the organization because of real or perceived privacy concerns about RFID technology,
- Being held legally liable for any consequences of the weak privacy protections, and
- Employees, shareholders and other stakeholders might disassociate with the organization due to concerns about corporate social responsibility.

Business objectives often conflict with privacy objectives. Organizations can benefit from the analysis and sharing of personal information obtained with RFID technology. At the same time, these activities may potentially violate the privacy rights or expectations of citizens and consumers. Similarly, methods to protect personal privacy may pose a business process risk. For example, consumers may want tags to be disabled at point-of-sale so that they cannot be used for tracking purposes afterwards. However, if it is easy to disable a tag at point-of-sale, then it may also be easier for adversaries to disable tags prior to point-of-sale, thereby disrupting the business process. Moreover, organizations may want to use tags after point-of-sale for post-sale support, recalls, and other purposes.

Privacy risk may increase when an individual possesses tags from multiple organizations because someone reading the tags can now combine and correlate information to profile individuals in ways that none of the organizations alone might have anticipated. For example, if a consumer purchases a tagged item and the tag is not disabled or removed, then the seller or someone else could subsequently use the tag to reveal the presence of that person at a another location and time. The consumer may have purchased the item with cash, presuming to remain anonymous in the transaction. However, if she also carries another tag that reveals her identity, such as an RFID-enabled identification card, then someone may be able to surreptitiously read both tags to establish an association between the purchased item and her identity that had not previously existed. As people possess more tagged items and readers become more prevalent in everyday life, the potential for more complex associations and inferences increases.

Other factors that impact the level of privacy risk include:

- Whether personal information is stored on tags,
- Whether the tagged items are considered personal (e.g., pharmaceuticals or devices that would reveal a medical condition, or a book that might reveal a political or religious affiliation),
- The likelihood that the tag will be in the proximity of compatible readers,
- The length of time records are retained in analytic or archival systems, and
- The effectiveness of RFID security controls, in particular:
  - The efficacy of tag memory access control and authentication mechanisms,
  - The ability of tags to be disabled after their use in a business process has been completed, and
  - The ability of users to effectively shield tags to prevent unauthorized read transactions.

For additional information on privacy considerations, see Section 6.

4.4 Externality Risk

RFID systems typically are not isolated from other systems and assets in the enterprise. Every connection point between the RFID system and something outside the RFID system represents a potential vulnerability for the entity on the other side of the connection, whether that is an application process, a valued asset, or a person. Externality risks are present for both the RF and enterprise subsystems of an RFID system. The main externality risk for the RF subsystem is hazards resulting from electromagnetic radiation, which could possibly range from adverse human health effects to ignition of combustible material, such as fuel or ordnance. The main externality risk for the enterprise subsystem is successful computer network attacks on networked devices and applications. Computer network attacks can involve malware (e.g., worms and viruses) or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage. The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application.

Because the externality risk by definition involves risks outside of the RFID system, it is distinct from both the business process and business intelligence risks; externality risks can be realized without having any effect on RFID-supported business processes or without revealing any information to adversaries.

4.4.1 Hazards of Electromagnetic Radiation

RFID technology, like any other radio technology, relies on the use of electromagnetic radiation to communicate information. The potential risk of electromagnetic radiation includes:

- Hazards of electromagnetic radiation to people (HERP),
- Hazards of electromagnetic radiation to ordnance (HERO),
- Hazards of electromagnetic radiation to fuel (HERF), and
- Hazards of electromagnetic radiation to other materials, including medical supplies such as blood products, vaccines, and pharmaceuticals.

As of the publication of this document, no documented examples have been identified that any of these hazards have been realized with respect to RFID technology, which typically operates at power levels below those that would cause a concern. Moreover, no research has suggested the realization of these risks with respect to RFID technology is likely, although interaction with some medical devices has been the subject of research studies.[34] The US Federal Communications Commission (FCC) promulgates regulations to protect citizens against unsafe radio transmissions by requiring equipment testing and certification. The FCC limits for general population/uncontrolled exposure are tabulated in Appendix E.

[34] US Food and Drug Administration has identified the potential for human implanted RFID chips to be incompatible with magnetic resonance imaging (MRI). Source: D. Tillman, "Re: K033440; evaluation of automatic class III designation; VeriChip™ health information microtransponder system; regulation number: 21 Code of Federal Regulations (CFR) § 880.6300; classification: class II; product code: NRV," October 12, 2004, http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt. While RF interference with pacemakers is a concern, it does not appear to pose a serious problem in practice. Source: R. Cleveland Jr. and J. Ulcek, "Questions and answers about biological effects and potential hazards of radiofrequency electromagnetic fields," Federal Communications Commission Office of Engineering and Technology (OET), Washington, D.C., OET Bulletin 56, Fourth Edition, August 1999, pp. 26.

In addition, DoD regulations require HERO and HERF evaluation of RF systems.[35] It is important to note that RFID systems may be within exposure limits when initially installed, but later exceed limits if operators increase the emitted power of readers, perhaps to improve the performance and reliability of the system.

Nevertheless, the critical consequences that would result from any realization of the risk suggest that organizations exercise prudence when fielding RFID technology, especially in complex electromagnetic environments. Electromagnetic signals and waves can reflect, interfere, and resonate in unintended ways in complex electromagnetic environments that include metal objects such as metal doors, window frames, and metal enclosures. This can result in unexpected or unintended signal and field cancellation, interference, summation, or resonance. This makes it difficult to accurately predict specific localized field levels from radiated power alone. Some factors that may warrant additional examination of electromagnetic radiation hazards include:

- The use of RFID equipment that has not been certified by the FCC or that has been modified to operate outside of FCC mandated limits[36] (both of which are illegal in the US but may be legal in other countries), and
- Operating RFID equipment in environments in which signal reflections and other electromagnetic effects can focus radiation in unintended ways.[37]

4.4.2 Computer Network Attacks

RFID technology represents a new attack vector on an enterprise network. Once RFID systems are implemented, a possibility exists that attackers could reach non-RFID and enterprise subsystem computers through a reader, although no such attack is known to have successfully occurred to date. If the system involves wireless handheld readers, then the wireless link between the reader and the networked middleware servers is another point of entry. Once RFID servers are compromised, they can be used to launch attacks on other networked systems. Attack possibilities include the introduction of malware (e.g., a worm or virus) or the exploits of a single adversary compromising one computer at a time. Once additional systems are compromised, all types of adverse consequences to the IT infrastructure are possible, including loss of confidentiality, integrity, and availability.

While the risk of network compromise through an RFID interface is considered low, it is possible, especially as the number of RFID reader, middleware, and enterprise applications increases. RFID air-interface protocols do not support the execution of remote commands on the RFID interface, but if the reader accepts data formats outside those expected by the protocol, then conceivably an adversary could exploit a buffer overflow vulnerability on a reader by sending it non-compliant data. If the system is poorly designed, the adversary may be able to insert code or commands in memory buffers read by processes that can execute administrative functions such as disabling security controls. The potential consequence is that the adversary could gain full control of the device and use that control to attack other systems.

Although no known instance of this type of attack has occurred in a real-world application, RFID security specialists have demonstrated RFID viruses in a controlled laboratory environment.[38] An RFID virus is a

---

[35] Department of Defense, "Directive 3222.3: DoD electromagnetic environmental effects (E3) program," September 8, 2004, http://www.dtic.mil/whs/directives/corres/pdf/d32223_090804/d32223p.pdf.

[36] Under US FCC regulation, the antennas of RFID readers operating in the 902–928 MHz band may output radiated power up to 4 watts. Source: 47 CFR § 15.247.

[37] An example might be the hull of a steel ship, in which there are numerous reflective metal surfaces with a variety of curvatures. While everyday objects such as metal furniture or vehicle bodies can reflect and focus RF signals in ways difficult to predict, they are unlikely to cause electromagnetic hazards.

small program encoded on a tag that becomes active once it has been read and is then passed to the middleware or database of an IT system. If the system is poorly designed, the virus could possibly take advantage of internal software weaknesses in middleware or database products to replicate itself to other tags. This distinguishes the risk from AIDC technologies such as bar codes that cannot be changed after manufacture because they do not contain modifiable memory.

Some factors influencing the magnitude of the risk to the IT infrastructure and the applications they support are presented in Table 4-3.

Table 4-3. Factors Influencing Cyber Attack Risk

Factor	Discussion
The characteristics of connected hosts and networks	The greatest factor determining the risk from an RFID system is the number and value of the systems with which it interconnects. Each host represents both a potential source of and target of attacks. If external network access is limited, risk is limited as well.
Vulnerability of RFID software	The ability of RFID components to be breached largely depends on the assurance of the implementing software (e.g., reader drivers, middleware, and analytic systems). Poorly developed software might be more easily compromised.
Physical proximity to RF subsystem	The likelihood that an adversary with both the skills and motivation to compromise RF subsystem components depends heavily on whether the adversary is able to get within reasonable proximity to the components so that RF communication is possible. When tags and readers are in public or easily accessible spaces, greater risk exists than when they are not in these areas. However, RFID enterprise servers can still be breached from network-based attacks even if the attacker has no access to RF subsystem components.
Presence and effectiveness of security controls	Known, effective, and widely available strategies exist for preventing or limiting the impact of most computer network attacks. Professionals designing RFID products can mitigate and even eliminate these risks through secure development practices, including simple steps such as data validation. However, these strategies are only effective if they are implemented properly.

4.5 Summary

For RFID implementations to be successful, organizations should effectively manage their risk. The major categories of risk are as follows:

- **Business Process Risk.** This encompasses threats and vulnerabilities that could cause part or all of the RFID system to fail. Potential impacts range from a deceleration of the business process to the loss of critical business or operational records. Business process risk can occur for many reasons, including human action (either benign or malicious) and natural causes. Factors influencing business process risk include the importance of the RFID-supported business processes to the mission of the organization, the robustness of business continuity planning, and the environment in which the RFID technology is located. The cloning of tags and attacks on enterprise subsystem networks are examples of threats to business processes.
- **Business Intelligence Risk.** This involves threats and vulnerabilities that could permit unauthorized parties to gain access to sensitive or proprietary information. A competitor or adversary can gain

[38] M. Rieback, B. Crispo, and A. Tanenbaum, "Is your cat infected with a computer virus?" in the *Fourth IEEE International Conference on Pervasive Computing and Communications*, 2006, pp. 169-179.

information from the RFID system in a number of ways, including eavesdropping on RFID transactions, reading tags, and gaining access to RFID-related databases. The risk of unauthorized access is realized when the entity engaging in the unauthorized behavior does something harmful with that information. In some cases, the information may trigger an immediate response, such as breaking into a container holding valuable goods. In other cases, data may also be aggregated over time to provide intelligence related to an organization's customers, operations, business strategy, or proprietary methods.

- **Privacy Risk.** Privacy rights or expectations may be compromised if an RFID system uses what is considered personal information for a purpose other than originally intended or if a third party uses the presence of tagged items to profile individuals. In the case of the latter, the primary privacy risk is likely borne by the consumer, not the organization that implemented the RFID system. Nevertheless, the RFID implementing organization still has privacy-related risks, including penalties from non-compliance with existing privacy regulations, legal liability, and the reaction of consumers, employees, public interest groups, and other stakeholders.

- **Externality Risk.** Every connection point between an RFID system and other systems represents a potential vulnerability. One externality risk for an RF subsystem is hazards resulting from electromagnetic radiation, which could possible range from adverse human health effects to ignition of combustible material, such as fuel or ordnance. The main externality risk for an enterprise subsystem is successful attacks on networked hosts and applications. Computer network attacks can involve malware or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage. The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application.

This page has been left blank intentionally.

5. RFID Security Controls

This section discusses security controls that can potentially mitigate the business risks associated with RFID systems. As previously discussed, RFID implementations are highly customized. As a result, the security controls listed are not all applicable or effective for all RFID applications. Organizations need to assess the risks they face and choose an appropriate mix of controls for their environments, taking into account factors such as regulatory requirements, the magnitude of the threat, cost and performance.

Federal agencies should refer to Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* and NIST Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*, when developing or revising policies related to an RFID system. NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers* may also be helpful as it provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.

This section covers security controls applicable to most RFID implementations. It does not address the security of RFID-enabled smart cards and payment systems. This section also does not discuss security controls related to general IT systems, such as network infrastructure, databases, and Web servers because these are already covered by other security requirements and guidelines. For example, EPCIS servers, which can be accessed by trading partners through the Internet, should be protected by the same types of controls that would be used for any other Internet-facing system (e.g., encryption of sensitive communications, access control to prevent unauthorized access to data and systems) to ensure the security of the data collected by the RFID system. Guidelines on topics such as IT server, application, database, and network security are available from many sources, including NIST's Computer Security Resource Center (CSRC).[39]

RFID security is a rapidly evolving discipline. Although promising research is noted when applicable, this section focuses on controls that are presently commercially available.

The RFID security controls discussed in this section are divided into three groups:[40]

- **Management.** A management control involves oversight of the security of the RFID system. For example, the management of an organization might need to update existing policies to address RFID implementations, such as security controls needed for an RF subsystem.
- **Operational.** An operational control involves the actions performed on a daily basis by the system's administrators and users. For example, RFID systems need operational controls that ensure the physical security of the systems and their correct use.
- **Technical.** A technical control uses technology to monitor or restrict the actions that can be performed within the system. RFID systems need technical controls for several reasons such as protecting data on tags, causing tags to self-destruct, and protecting wireless communications.

The information provided for each control includes:

---

[39] The CSRC is located at http://csrc.nist.gov/publications/nistpubs/index.html. Appendix D contains a list of NIST publications that address general security issues and provide guidelines for the configuration of specific technologies that might be of use when securing an RFID system, including the computing devices in the enterprise subsystem.

[40] For more information on security controls see R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, and G. Rogers, *Recommended Security Controls for Federal Information Systems*. NIST Special Publication 800-53 (as amended), December 2006.

- A description of the control and how it works,
- The types of implementations or applications where the control might be helpful,
- The benefits that the control provides, such as which risks it mitigates, and
- The weaknesses of the control, including why it might not be effective in some environments, and what residual risks and other concerns remain even if the control is implemented.

The summary at the end of Section 5 summarizes the controls and maps them to the risk categories discussed in Section 4.

5.1 Management Controls

Management controls are typically involved in risk assessment, system planning, and system acquisition, as well as security certifications, accreditations, and assessments. The sub-sections below discuss management controls for RFID systems in more detail.

5.1.1 RFID Usage Policy

Control: An RFID usage policy describes the authorized and unauthorized uses of RFID technology in an organization and the personnel roles assigned to particular RFID system tasks. Federal agencies should follow FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, when developing the RFID usage policy.

The usage policy also should be consistent or integrated with the organization's privacy policy, which addresses topics such as how personal information is stored and shared. The RFID usage policy should also address privacy issues associated with the tag identifier formats and the potential disclosure of information based on solely on the tag identifier format selected. Additional information resources are found in the privacy guidelines in Section 6.

Applicability: All organizations that use RFID technologies or are considering using them.

Benefits: The policy establishes the framework for many other security controls. It provides a vehicle for management to communicate its expectations regarding the RFID system and its security. It enables management to take legal or disciplinary action against individuals or entities that do not comply with the policy.

Weaknesses: The existence of a policy does not ensure compliance with the policy. A policy needs to be coupled with the implementation and enforcement of appropriate operational and technical controls to be effective.

5.1.2 IT Security Policies

Control: IT security policies describe the approach to achieve high-level security objectives of the usage policy. The IT security policies related to RFID should cover each RFID subsystem, including network, database and application security in the enterprise and inter-enterprise subsystems; they should not just be limited to security of tags and readers in the RF subsystem.

IT security policies for RFID systems should address:

- Access control to RFID information, especially records contained in RFID analytic system databases,

- Perimeter protection, including port and protocol restrictions for network traffic between the RF and enterprise subsystems and between the enterprise subsystem and a public network or extranet,
- Password management, particularly with respect to the generation, distribution, and storage of tags' access, *lock*, and *kill* passwords,
- Management system security for readers and middleware, including the use and protection of SNMP read and write community strings,[41]
- RFID security training for system administrators and operators, and
- Management of associated cryptographic systems, including certification authorities and key management.

Applicability: All RFID implementations, particularly those with enterprise subsystems or inter-enterprise subsystems.

Benefits: Well-crafted security policies govern the mitigation of business risks associated with the use of RFID technologies. The policies provide requirements and guidelines for the individuals designing, implementing, using, and maintaining RFID systems. For example, IT policies help the personnel designing RFID systems or procuring system components to make appropriate decisions. Similarly, they help system administrators correctly implement and configure software and related network components.

Weaknesses: The existence of a policy does not ensure compliance with the policy. A policy needs to be coupled with the implementation and enforcement of appropriate operational and technical controls to be effective.

5.1.3 Agreements with External Organizations

Control: When data associated with an RFID system needs to be shared across organizational boundaries, formal agreements among the participating organizations can codify the roles and responsibilities, and in some cases the legal liability, of each organization. These formal agreements are usually documented as a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU). The MOU or MOA specifies the network connections and authentication mechanisms to be used, the data to be shared, and the manner in which data should be protected both in transit and at rest. It may also address controls on vendors, subcontractors, and other third parties to the extent they have access to the system.[42]

If the inter-enterprise application requires tag passwords to be shared across organizations, then the MOU or MOA should specify how these passwords will be generated, stored, and shared. The memorandum may specify IT security controls such as methods of authentication, access control, or encryption that participating organizations shall implement to protect the passwords.

Applicability: Any RFID system involving more than one organization, which is most common in supply chain applications.

---

[41] *SNMP community strings* are passwords that provide anyone with an SNMP management client and network access the ability to manage the associated systems. Knowledge of the *read community string* provides the holder the ability to view the system configuration and track system behavior. Knowledge of the *write community string* provides the holder the ability to reconfigure system components.

[42] For additional information on agreements with external organizations, see NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, which can be found at http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf.

Benefits: Having an MOA or MOU significantly reduces the potential for subsequent misunderstandings and security breaches. They enable signatories to communicate their respective security requirements while also realizing the benefits of the business partnership that led them to collaborate in the development and use of the RFID system.

Weaknesses: Monitoring an external organization's enforcement of an agreement is difficult without full access to its systems and personnel, which is unlikely. As a result, violations may occur without detection. This risk can be mitigated with independent audits if signatories agree to hire third-parties to conduct such audits.

5.1.4 Minimizing Sensitive Data Stored on Tags

Control: Instead of placing sensitive data on tags, the data could be stored in a secure enterprise subsystem and retrieved using the tag's unique identifier.

Applicability: Applications that use tags with on-board memory and process data that is either considered sensitive or that could be combined with other data to infer sensitive information.

Benefits:

- Adversaries cannot obtain information from the tag through rogue scanning or eavesdropping.
- Data encryption and access control is often more cost-effectively performed in the enterprise subsystem than in the RF subsystem.

Weaknesses:

- Adversaries can often obtain valuable information from the identifier alone. For example, knowledge of the EPC manager ID and object class bits in certain EPC formats may reveal the make and model of a tagged object concealed in a container. An adversary might target containers based on the perceived worth of their contents.
- Placing data in the enterprise subsystem makes the availability of that data contingent on the availability of the network. Retrieving data over a network also introduces a small delay, which could be unacceptable for some applications. Section 3.3.3 discusses why organizations might choose to store data on tags even after taking into consideration the risks of doing so.

5.2 Operational Controls

There are several types of operational controls:

- Physical access controls restrict access to authorized personnel where the RFID systems are deployed.
- Proper placement of RF equipment helps avoid interference and reduce hazards from electromagnetic radiation.
- Organizations can destroy tags after they are no longer useful to prevent adversaries from gaining access to their data.
- Operator training can help ensure that personnel using the system follow appropriate guidelines and policies.

- Information labels and notice can inform users of the intended purposes of the RFID system and simple methods users can employ to mitigate risk.

The sub-sections below discuss operational controls for RFID systems in more detail.

5.2.1 Physical Access Control

Control: Physical access controls include fences, gates, walls, locked doors, turnstiles, surveillance cameras, and security guards. When the objective is to limit radio communication over a short distance, room walls or partitioned stalls might provide adequate protection if they are opaque to the relevant radio frequencies that the RF subsystem uses.

Applicability: All RFID implementations except those in which RFID tags or other system components are in public areas.

Benefits: Physical access controls limit the ability of an adversary to get close enough to RFID system components to compromise RFID data security or to modify, damage, or steal RFID system components. Physical security applies to all RFID subsystems. In the RF subsystem, the primary objective of the control is to prevent unauthorized radio communications. In the enterprise and inter-enterprise subsystems, the primary objective is to prevent physical access to system components.

Examples of risks that are mitigated by physical access controls include:

- Unauthorized reading and writing of tag data,
- Rogue and cloned tags,
- Reader spoofing,
- Denial of service resulting from radio interference or unauthorized commands,
- Targeting,
- Physical destruction of RFID equipment, and
- HERF/HERO/HERP.

Weaknesses:

- Physical access controls are not a countermeasure for radio interference from legitimate radios located within a perimeter designed to block external emissions,
- The effective range of RF signals may be much longer than stated operating ranges, thereby allowing many attacks to occur using customized directional antennas and other technologies (see Section 2.3.3.3 for additional information on relevant operating ranges),
- Physical access controls do not protect against attacks by insiders (i.e., those granted access to the area),
- HERF/HERO/HERP still exists with respect to radiation emitted within the physical perimeter, and
- Physical controls may fail to contain radio signals as expected if ductwork or other openings allow radio signals to escape.

5.2.2 Appropriate Placement of Tags and Readers

Control: RFID system equipment can be placed to minimize unnecessary electromagnetic radiation. Tags and readers can be kept away from:

- Fuel, ordnance, and other materials that could *cause harm* if exposed to electromagnetic radiation,
- Humans and sensitive products (e.g., blood, medicine) that *might be harmed by* sustained exposure to RF subsystem radiation,
- Metal and reflective objects that can modify and amplify signals in unintended and potentially harmful ways, and
- Legitimate radios with which the RF subsystem communication will cause interference.

Applicability: All environments in which the organization deploying RFID systems determines the location of the RF equipment (which excludes many consumer and supply chain applications).

Benefits:

- Reduced risk of interference with legitimate radios
- Reduced risk of eavesdropping and unauthorized RF subsystem transactions
- Mitigation of HERF/HERO/HERP

Weaknesses:

- Tag location cannot always be controlled, such as when tags are used to track mobile items (e.g., hospital cart) or items in transit (e.g., pallet on a truck).
- Radio interference may persist even if the tags or readers are placed in a new location that is still sufficiently close to other radios.[43]

5.2.3 Secure Disposal of Tags

Control: Secure disposal involves physically or electronically destroying tags, as opposed to just discarding them, when they are no longer needed to perform their intended function. Physical destruction may involve manual tearing or shredding using a paper shredder. Electronic destruction can be accomplished by using a tag's kill feature or using a strong electromagnetic field to render a tag's circuitry permanently inoperable. When a tag supports an electronic disabling mechanism, it usually is the preferred way to disable a tag before it is disposed because it can be accomplished without touching each tag, thereby reducing the cost of the effort. The kill feature is also discussed in Section 5.3.3.3.

Applicability: RFID applications in which the continued operating presence of a tag after it has performed its intended function poses a business intelligence or privacy risk (e.g., an adversary can subsequently use the presence of the tag to track items or people).

Benefits: Destroying or disabling tags:

- Eliminates the possibility that they could be used later for tracking or targeting, and

[43] In this situation, a panel or wall of grounded wire fencing between the two RF sources is a possible alternative means to reduce interference.

- Prevents access to sensitive data stored on tags.

These benefits apply to both business intelligence and privacy risks.

Weaknesses:

- Even if minimal, the effort it takes to destroy a tag increases the tag's life cycle cost, which is a concern if very low costs are required to justify an RFID-enabled business process.
- Destruction of a tag precludes the ability to use it for future value-added applications such as post-sale product support, targeted recalls, receipt-free returns, expiration date monitoring, and sorting assistance for recycling.

5.2.4 Operator and Administrator Training

Control: Operator and administrator training provides personnel with the skills and knowledge necessary to comply with RFID usage, IT security, and privacy policies, as well as agreements with external organizations. In most RFID implementations, personnel will perform various roles, which might require different training materials for each role. For example, an administrator of middleware might need different information than an operator of a mobile reader. Appropriate security and privacy training addresses at least three points:

- What constitutes unauthorized use,
- How to detect that unauthorized use might be occurring, and
- To whom to report violations.

If HERF/HERO/HERP risks are present, appropriate security training covers mitigation techniques, such as safe handling distances.

If tags are destroyed or recycled, training should cover how to perform these functions. For example, operators might be trained how to clear tag memory before reuse.

Applicability: All RFID implementations.

Benefits: Operator training helps ensure that the system is used and maintained properly. Training also helps operators identify security violations and take appropriate actions to prevent their reoccurrence.

Weaknesses: Training alone cannot ensure proper operation of the system or compliance with policy.

5.2.5 Information Labels / Notice

Control: A written message is affixed to or distributed with each tag or is posted near readers. The notice may inform users of the purposes of the RFID system or advise users on how to minimize privacy or other risks (e.g., place an RFID-enabled access card or transponder in metal foil or a sleeve that shields RF radiation when the card or transponder is not in use).

Applicability: All applications in which there is a risk that could be mitigated with simple informational messages. The control is particularly relevant to consumer applications in which privacy is a concern.

Benefits: Information labels or notices can communicate basic information about risks that might otherwise be left unknown by users that are able to take simple steps to mitigate the risk (e.g., remove a tag or place it in a shielded sleeve).

Weaknesses: Distributing a notice is no guarantee that it will be read or understood. Notice is not an appropriate communications medium for complex concepts or instructions that may require formal training.

5.2.6 Separation of Duties

Control: RFID system duties are distributed among various personnel roles to minimize the damage resulting from an inadvertent or malicious activity of a single person. The general principle of the control is that malicious collusion between two or more authorized users is much less likely than one person engaging alone in inappropriate behavior.

One example of separation of duties is having different personnel (1) attach tags to objects and (2) read the tags. If an individual performed both functions, the individual could intentionally put the wrong tag on an object to circumvent the objectives of the business process. For example, a store clerk could affix tags intended for low-priced items on high-priced items, and then later work the checkout scanner while the clerk's accomplice purchased the items. The system would not know that the tags had been switched, but if another person performed the checkout, he or she might be suspicious of the checkout total, which could uncover the plot.

Applicability: RFID applications in which an insider might have a motive to perform unauthorized RFID transactions. This scenario is most likely to occur when tags support commercial transactions, especially those related to high-value objects.

Benefits: Separation of duties helps to reduce fraud and malicious damage, because any user attempting to engage in such activities would be forced to collude with at least one other user. Separation of duties also reduces errors, because a second operator will often catch mistakes made or missed by the first.

Weaknesses: Multiple employees still could collude to commit fraud or violate the RFID usage policy. Also, organizations with a limited staff may not be able to perform complete separation of duties.

5.2.7 Non-revealing Identifier Formats

Control: RFID tags are assigned identifiers using identifier formats that do not reveal any information about tagged items or the organization operating the RFID system. Non-revealing identifier format options include serially assigning identifiers and randomly assigning identifiers.[44]

In contrast, if an adversary reads an identifier that is encoded with a standardized format, such as the EPC format, that adversary may be able to discern the manufacturer or issuer of the item, as well as the type of item. For example, all cans of a soft drink from a certain manufacturer will have the same EPC manager

[44] A related control is rotating identifiers. Auto-rotating tags store a list of identifiers and cycle through the list when queried. To support multiple identifiers, databases in the enterprise subsystem must associate each identifier in the list to the particular item. The benefit of rotating identifiers is that organizations can make it more difficult to identity and track particular items as well as hide the type of item. Random and serialized identifiers, on the other hand, may not reveal information about the type of item, but since these identifiers are fixed, once they are revealed that particular item can be tracked. One weakness to rotating identifiers is that a rogue reader can easily obtain the complete list of identifiers through repeated queries. Therefore, this control is more appropriate when the primary threat is eavesdropping. While research is being conducted on the concept of rotating identifiers, it is not specified in any RFID standard and proprietary designs are not widely commercially available.

ID and object class bits if their identifiers are encoded in an EPC identifier format. Figure 5-1 shows an example 96-bit EPC and how it can be parsed into the four aforementioned, individual fields.

Figure 5-1. Example 96-bit EPC

Tags must have programmable identifiers to support the control. Even tags that are designed to support standard tag formats can still be assigned non-standard identifiers in the field. However, some tags have factory-initialized identifiers that cannot be modified after manufacture.

Applicability: Any applications in which the implementing organization determines that the revelation of a tag's identifier is a business intelligence risk.

Benefits: Adversaries cannot obtain information about tagged items from the identifier alone.

Weaknesses:

- The use of non-revealing identifier precludes an organization from realizing benefits that come from standard identifier formats that reveal organization and item type information. For example, standard identifier formats are particularly advantageous when designing and maintaining distributed databases in inter-enterprise systems. Lookup and query functions are much easier in such databases when the identifiers provide information on where item data is located.
- If identifiers are assigned randomly, then a potential exists that two tags may be assigned the same identifier. The likelihood of such an event is very small, but it could lead to errors in the supported business process.[45]
- If there is logic in how the identifiers are assigned, an adversary may uncover the method that is used, which would defeat the control. For example, an adversary knows that an identifier was assigned to a certain item and that all items of that type were assigned sequentially, then the adversary may be able to deduce the approximate range of identifiers that correspond to items of that type. Similarly, when identifiers are serialized, the adversary may be able to deduce the approximate time of the assignment based on the identifier.

5.2.8 Fallback Identification System

Control: A fallback identification system provides an alternative means to identify, authenticate, or verify an object when the RFID system is unavailable or an individual tag is inoperable. Options include text labels and AIDC technology such as bar codes.[46] The fallback may consist of just an identifier, or it may also include additional data about the tagged object. The fallback system is accompanied by standard operating procedures and operator training to ensure that personnel know when and how to use it.

---

[45] When two tags are assigned the same identifier, the event is called a collision. If identifiers are randomly assigned, a collision is expected after approximately the square root of the total number of possible identifiers. Therefore, in the case of a 96-bit EPC, a collision is expected after approximately 2^{48} tags, which is an enormous number not likely to be encountered in most RFID applications.

[46] If the RFID application's objective is to provide security or authentication, then a fallback technology such as holograms or other optical security features may be used.

Applicability: All RFID applications.

Benefits: Duplicating tag identifiers and data on a label provides a fallback in case of malicious or accidental tag damage, reader malfunction, or enterprise subsystem network outage. The redundant data can also be used to verify that tag data has not been altered improperly.

Weaknesses: This control has several potential weaknesses, including:

- Damage to the tag could render both the stored data and the printed data unusable. Similarly, many enterprise subsystem outages that would affect the RFID system would also affect its fallback alternative.
- The data stored on the label is visible, so it may be easier for unauthorized parties to gain access to it than it would be to read the data from the tag.
- The text label or bar code might not provide the same data capacity as RFID memory, although two-dimensional bar codes can encode at least as many bits as standards-based tag identifiers.
- Text labels and AIDC technologies are static, so they do not provide a complete fallback solution for applications in which tag data changes over time. However, some identification information is still likely to be better than none in most applications.

5.3 Technical Controls

There are a number of technical controls currently available for RFID systems, and many others are under development in industrial and university research labs. This section focuses on technical controls that are commercially available as of the publication date of this document. Supplementary information on selected emerging security technologies is provided in footnotes. Many of the technical controls listed are specified in standards, while others are available only in proprietary systems.

Many technical controls related to a tag require the tag to perform additional computations and to have additional volatile memory. Accordingly, a tag that uses such technical controls requires a more sophisticated microchip than those that do not use such controls. In the case of passive tags, the tags may also need to be closer to readers to obtain the required power to perform these computations. Alternatively, readers may need to operate at greater power levels, although this may not be feasible or permitted in many cases. These inherent characteristics of passive tags can limit the use of certain technical controls in some environments.

Technical controls exist for all components of RFID systems, including the RF, enterprise, and inter-enterprise subsystems. This section focuses on technical controls for the RF subsystem. Many controls also exist for the enterprise and inter-enterprise subsystems, but these typically apply to IT systems in general rather than to RFID systems in particular. Readers are encouraged to read other NIST IT system and network security guidelines, many of which are listed in Appendix D.

The general types of RF subsystem controls include controls to:

- Provide authentication and integrity services to RFID components and transactions,
- Protect RF communication between reader and tag, and
- Protect the data stored on tags.

Examples of each of these types of controls are discussed in depth in Sections 5.3.1 through 5.3.3, respectively.

5.3.1 Authentication and Data Integrity

While a wide variety of authentication methods exists for IT systems, the most common techniques for the RF subsystem of RFID systems are passwords, keyed-hash message authentication codes (HMAC), and digital signatures. In some cases, the primary objective of the authentication technology is to prevent unauthorized reading from or writing to tags. In other cases, the objective is to detect cloning of tags. Authentication techniques based on cryptography often provide integrity services for data included in the authentication transaction; in other words, an adversary cannot modify data in the transaction without the reader or tag detecting the change.

5.3.1.1 Password Authentication

Control: A tag does not permit password-protected commands to be executed unless they are accompanied by the correct password. Protected commands may include those that support reading and writing of tag data, memory access control (Section 5.3.3.1), and the kill feature (Section 5.3.3.3).

Organizations properly implementing this control will develop a password management system to support it. The password management system addresses all stages of the password, including generation, conveyance, and storage. From a security perspective, effective password generation involves random selection of each password.[47] Whenever possible, the passwords are assigned to each tag in a physically secure environment to reduce the likelihood of eavesdropping. Tags should not share passwords, although this may not be administratively feasible in some environments, such as those in which the reader is not expected to have access to a networked database of tag passwords. In inter-enterprise applications such as supply chains, multiple organizations may need to access databases that contain tag identifiers and passwords. Authenticating external entities likely will require additional security systems. While in traditional IT systems, passwords are often changed on a periodic basis (e.g., every 90 days); in RFID systems, such changes may be infeasible, especially if the tags are not always accessible to the organization assigning the passwords.

Applicability: Any application where authorized execution of a particular command represents a business process, business intelligence, privacy, or externality risk.

Benefits: The likelihood that tags will be used for unauthorized purposes is greatly reduced.

Weaknesses:

- Password management for RFID systems is complex, particularly if the application deploys large number of tags or if passwords must be shared across organizational boundaries as might be the case in supply chains.
- Adversaries can intercept passwords transmitted over the air and then use them at a later time to perform unauthorized transactions.[48]

---

[47] For additional information on proper random number generation, see E. Barker and J. Kelsey, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, NIST Special Publication 800-90, June 2006.

[48] RFID passwords are often transmitted "in the clear" (i.e., without cryptography to hide them), which makes them particularly vulnerable to eavesdropping. The cover-coding technique described in Section 5.3.2.1 mitigates this risk for tags that support cover coding, but this technique is not without its own limitations.

- If the application environment precludes access to an on-line tag password database (e.g., mobile readers in remote locations), then the implementing organization may need to take simplifying measures, such as assigning the same password to multiple tags. In cases such as these, the compromise of a single password could compromise the integrity of the entire system.
- RFID passwords can be obtained through brute force methods (i.e., cycling through all possible passwords) when the tag technology is limited to short passwords.[49]
- RFID passwords can be revealed through power analysis attacks on some types of passive tags.[50]

5.3.1.2 Keyed-Hash Message Authentication Code (HMAC)

Control: Both the reader and the tag share a common secret key that can be used in combination with a hash algorithm to provide one-way or mutual authentication between tag and reader. When HMAC is applied to messages, it also ensures the integrity of data in the messages. HMAC is specified in FIPS Publication 198.[51] HMAC supports any cryptographic hash algorithm, but Federal agencies must use one of the secure hash algorithms (SHA) specified in FIPS Publication 180-2.[52] HMAC is not specified in any RFID standard, but it is available in proprietary designs.

Applicability: Applications in which passwords are considered to offer an inadequate authentication mechanism, perhaps because the risk of eavesdropping is high. Applications that require evidence of a tag's authenticity.

Benefits: The advantages of HMAC relative to password authentication include that HMAC:

- Provides evidence of tag's authenticity,[53]

---

49 For example, EPC Class-1 Generation-1 UHF tags support a maximum password length of 8-bits, which enables only 256 possible passwords. An adversary can cycle through 256 passwords in a matter of seconds. EPC Class-1 Generation-2 tags support 32-bit passwords and, therefore, 2^{32} possible passwords, which is sufficient if the passwords are randomly generated. However, if the binary password is based on American Standard Code for Information Interchange (ASCII) characters, then the actual number of possible passwords may be much smaller. For example, the ASCII representation of a 4-digit decimal number (a common length for personal identification numbers) is 32-bits, but results in only 10,000 possible combinations, a number certainly vulnerable to brute force attacks. Tags typically do not lock-out readers after a certain number of incorrect guesses, which means a determined adversary can continue to guess the password as long as the tag remains within the operating range of the adversary's reader.

50 The power analysis attack (also called a side channel attack) is based on the fact some passive tags use different levels of power depending on how close the password provided is to the actual password. For instance, if the first bit in a password is incorrect, the tag uses less energy than it would if the eighth bit is incorrect, given how the algorithm is hard-coded into the tag's circuitry. These power differences are detected in the backscatter to the reader, but it requires that the adversary be reasonably close to the tag to get effective measurements. If such measurements are possible, an adversary can determine the password much more quickly than by using a brute force method. Lab experiments proved that someone could crack the 8-bit password protection found on EPC Class-1 Generation-1 tags in one minute. For more information, see Y. Oren and A. Shamir, "Power Analysis of RFID Tags," discussed at the *Cryptographers Panel of the Fifteenth RSA Conference*, San Jose, 2006.

51 The FIPS HMAC is a generalization of HMAC described in H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: keyed-hashing for message authentication," Internet Engineering Task Force, Request for Comments (RFC) 2104, February 1997 and American Bankers Association, "Keyed Hash Message Authentication Code," American National Standards Institute (ANSI) X9.71, Washington, D.C., 2000.

52 The specified algorithms are SHA-1, SHA-256, SHA-384, and SHA-512. While SHA-1 offers the lowest level of assurance and is not recommended for use in digital signatures beyond 2010, it is likely most applicable to RFID systems due to its greater computational efficiency relative to the other algorithms. See NIST Special Publication 800-57, *Recommendation on Key Management*, Part 1 for additional information.

53 The evidence of tag or item authenticity is provided by authenticating a tag to a reader, which can be accomplished when the tag computes and returns an HMAC using a random challenge provided by the reader. Mutual authentication is also possible if both tag and reader provide challenges to each other. Passwords, on the other hand, typically only are used to authenticate readers to tags, thereby protecting the tag against rogue commands. If the tag were to authenticate itself to a

- Provides integrity protection,[54] and
- Does not transmit secrets over-the-air, which eliminates the risk of eavesdropping inherent with clear text passwords.

Weaknesses:

- The management of HMAC keys provides similar challenges to those of password management and may not be practical if mobile readers do not have reliable access to an HMAC key management system.
- The authenticity claims associated with HMAC authentication only hold when the HMAC key remains secret. If an adversary has physical access to a tag and can obtain its HMAC key, then the adversary can clone the tag. This attack, however, assumes that that the adversary has some level of expertise, both in reverse engineering the HMAC-capable tag and in producing a reasonable facsimile.
- When HMAC keys are shared across organizations, authenticity claims rely on an implicit trust between the organizations that may not be present in practice.
- HMAC requires greater computing power than password comparisons, and therefore requires more complex tag designs to support it.

5.3.1.3 Digital Signatures

Control: Readers digitally sign tag identifiers, time stamps, and related event data to provide for non-repudiation of tag transactions. The resulting signatures are stored on tags for subsequent verification, although recording signatures in enterprise subsystem databases provides additional assurance of the tag's chain of custody.

Digital signatures are based on *asymmetric cryptography*, also commonly referred to as *public key cryptography*. Federal agencies implementing digital signature technology must comply with FIPS Publication 196, *Entity Authentication Using Public Key Cryptography*. The use of digital signature technology in the context of RFID systems is also referred to as *authenticated RFID*. It typically works as follows:

1. The tag has a permanent unique identifier than cannot be modified after manufacture.
2. The reader generates a public/private key pair and obtains a corresponding public key certificate.
3. The reader uses a specified hash algorithm to compute a message digest of the tag's identifier and possibly other transaction-related data, encrypts the message digest with its private key to create a digital signature for the transaction, and stores the resulting signature on the tag.
4. Other readers read the signature, decrypt it with the first reader's public key, and compute the identical message digest to determine if a match exists. If the message digests match, then verification procedure provides assurance of the authenticity of the earlier transaction. If the message

---

reader using a password, an adversary could simply use a rogue reader to obtain the password and then re-use with a legitimate reader. HMAC provides an effective countermeasure to this attack because it never reveals the secret key during any of its transactions.

[54] Integrity protection is when either tag or reader computes an HMAC using as input the data for which integrity protection is desired. Any change in the data results in a different value of the HMAC, which would be detected by the receiving entity.

digests do not match, then either the transaction data has been altered or an unauthorized device created the digital signature.

5. The other readers can store their own event transactions on the tag or record them in enterprise subsystem databases for later queries regarding the tag's chain of custody.

Applicability: Applications that require more robust evidence of authenticity than provided by HMAC technology, including authentication of multiple chain of custody events. Applications that require verification of authenticity without network connectivity.

Benefits: Digital signatures offer several advantages relative to HMAC authentication, including:

- Digital signature systems do not require tags to store cryptographic secrets. Instead, readers maintain private keys. In password and HMAC authentication, both the tag and the reader must share a secret for the system to function, but there are no shared secrets in the public key cryptosystems that support digital signatures. Tags are typically much more vulnerable to compromise than readers, so eliminating the need to store secrets on tags enhances overall system security. One private key and one or more public key certificates are on the reader. Integrity is needed for the certificates, but not confidentiality.
- In many cases, digital signatures do not require network connectivity to successfully perform the authentication function. In password and HMAC authentication, a reader is unlikely to have the memory to store the passwords or keys for large numbers of tags. With digital signatures, a reader may only need to store the public key certificate of the entity that initialized the tags or perhaps a relatively small number of readers. In inter-enterprise systems, each participating organization only has to share the public keys of its readers rather than provide its partners reliable network access to a password or secret key database.
- Digital signatures are compatible with existing RFID tag standards. HMAC requires tags to support hash algorithms and to implement a challenge-response protocol, neither of which are included in existing RFID standards. On the other hand, in authenticated RFID systems, tags can receive, store, and transmit digital signatures with existing read and write commands because the complexity resides in readers or middleware.

Weaknesses:

- A system of digital signatures requires a public key infrastructure (PKI), including registration and certification authorities, revocation functions, and associated policies and practice statements. Successfully implementing and operating a PKI requires careful planning and considerable expertise. In addition, readers or middleware need to support digital signature and other PKI functionality that is not commonly found in current RFID technology.
- Digital signatures systems require more memory than found on many current tags. For example, NIST recommends that RSA signatures have a length of 1024 bits, and a length of 2048 bits after 2010.[55] Additional memory is required to store identifying information related to the transaction. Providing chain of custody evidence requires storing a digital signature and related identifying information for each transaction.

[55] Elliptic curve cryptography can reduce the size of signatures. Elliptic curve methods provide comparable assurance to 1024-bit RSA signatures with 163 bits, and to 2048-bit RSA signatures with 224 bits. This approach combined with greater memory on tags may alleviate storage concerns over time.

- Digital signatures that are not generated by the tag are subject to replay attacks. An adversary could query a tag to obtain its evidence of authenticity (i.e., the digital signature created by a previous reader) and then replicate that data on a cloned tag.
- The use of digital signatures to support authentication of readers to tags would require tags to support relatively complex cryptographic functions beyond the capacity of most common tag designs. Consequently, password or symmetric key authentication systems likely will support tag access control, as opposed to tag authenticity verification, for the foreseeable future.

5.3.2 RF Interface Protection

Several types of technical controls focus on the RF interface to tags, including:

- Cover-coding can be used to obscure the content of messages from readers to tags.
- Data can be encrypted prior to its transmission.
- Shielding can be installed to limit eavesdropping and rogue scanning.
- The selection of an operating radio frequency can be used to avoid interference from other sources or achieve certain operating characteristics such as the ability to propagate through metals, liquids, and other materials that are opaque to many frequencies.
- Reader and active tag transmission characteristics can be tuned to reduce the likelihood of eavesdropping and help mitigate interference and the hazards from electromagnetic radiation.
- The RF interface for tags can be temporarily shut off to prevent unauthorized access when the tag is not expected to be used for authorized purposes.
- The RF interface may be turned off by default until a user takes an action to activate it.
- Readers may periodically poll tags to determine the presence of the tags, assess system health, and acquire environmental data.

These controls are discussed further in Sections 5.3.2.1 through 5.3.2.8.

5.3.2.1 Cover-Coding

Control: Cover-coding is a method for hiding information on the forward channel from eavesdroppers.

In the EPCglobal Class-1 Generation-2 standard, cover-coding is used to obscure passwords and information written to a tag using the *write* command. The EPCglobal Class-1 Generation-2 cover-coding protocol works as follows:

1. The reader sends a message to the tag requesting a key.
2. The tag generates a random 16-bit number (i.e., the key) and returns it to the reader.
3. The reader produces ciphertext (i.e., a message unintelligible to an eavesdropper who cannot intercept the key) by applying an exclusive-or (XOR) operation[56] to the key and the plain text.

[56] The XOR operation is a binary operation denoted with the symbol "⊕" that works as follows: $1 \oplus 1 = 0$; $1 \oplus 0 = 1$; $0 \oplus 1 = 1$; $0 \oplus 0 = 0$. When the XOR operation is applied to two multi-bit strings, the XOR operation is applied to the first bit of the each string to produce the first bit of the result, the second bit of each string to produce the second bit of the result, and so

4. The reader sends the ciphertext to the tag.

5. The tag applies the XOR operation using the ciphertext and the key it generated to recover the plain text.[57]

Cover coding is an example of *minimalist cryptography* because it operates within the challenging power and memory constraints of passive RFID tags.[58] By itself, the XOR operation would be considered a trivial encryption algorithm in traditional cryptography, but it nonetheless mitigates risk to an acceptable level in many RFID environments.

Figure 5-2 illustrates how cover-coding works. As shown in the figure, the passive tag's back channel signal is weaker than the reader's forward channel signal. This will always be the case for a passive tag, which must use the forward channel to power both its computations and the backscattered signal. In the figure, the adversary is able to eavesdrop on the forward channel but not the back channel. So long as this condition holds, the adversary will not be able to learn the random number sent from the tag and therefore will be unable to decipher cover coded information.

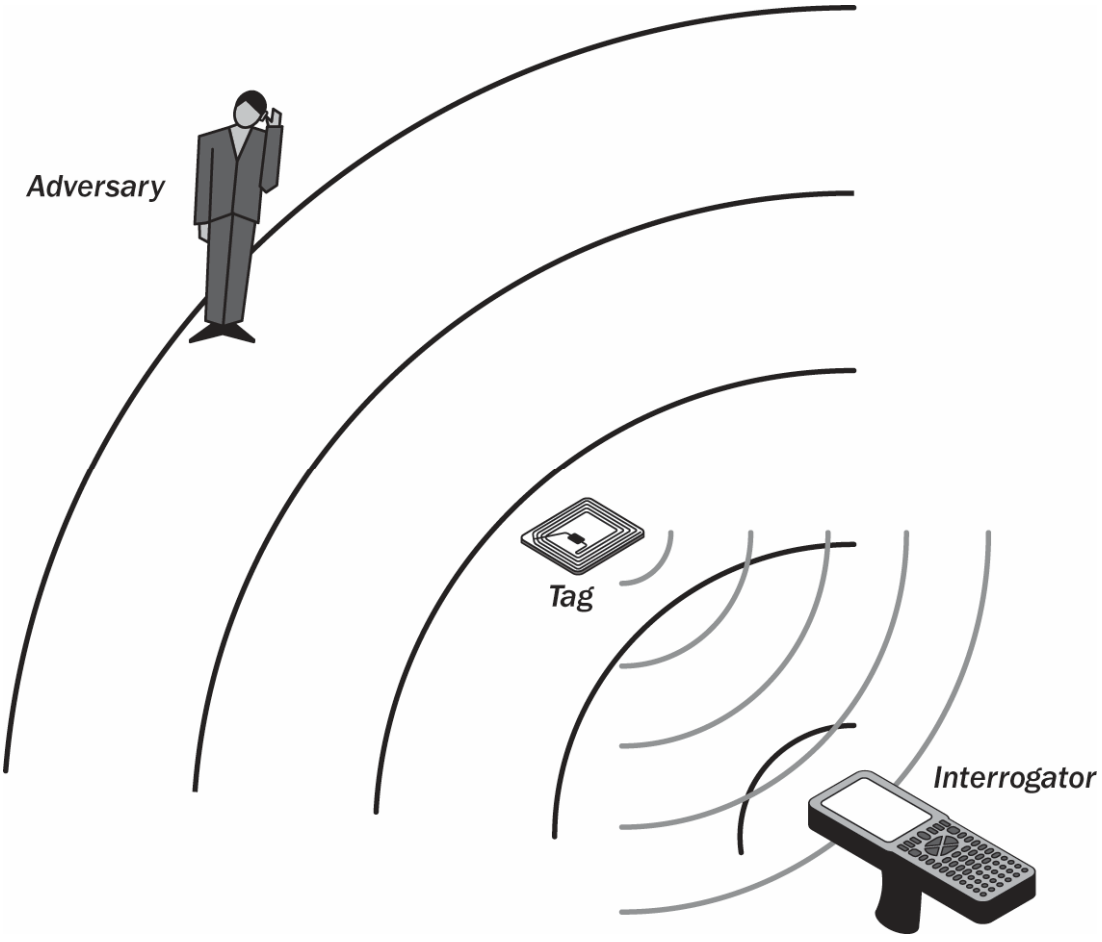

Figure 5-2. Cover-Coding

on. To work properly, the inputs to the XOR operation must be of equivalent length, and the output is also of the same length.

[57] The XOR operation is symmetric. For instance, given key K, plaintext P, and ciphertext C, if $P \oplus K = C$, then $C \oplus K = P$.

[58] For more information on minimalist cryptography, see A. Juels, "Minimalist cryptography for low-cost RFID tags," in the *Fourth Conference on Security in Communication Networks*, 2004, pp. 149-164.

Applicability: Cover coding is useful when eavesdropping is a risk that requires mitigation, but adversaries are expected to be at a greater distance from the tags than readers. Intelligible reception of back channel signals from a passive tag requires proximity of less than four meters in most applications. In many applications, an adversary's reception equipment would be conspicuous if it were located within this range. In contrast, reader signals can be detected at distances of a kilometer or more under ideal conditions.

Cover-coding is designed for RF subsystems in which the forward channel carries stronger signals than the back channel, which essentially limits the control to passive tags. EPCglobal Class-1 Generation-2 technologies support cover-coding. Proprietary technologies support similar features.

Benefits: Cover-coding helps prevent the execution of unauthorized commands that could disable a tag or modify the tag's data. Consequently, cover-coding mitigates business process, business intelligence, and privacy risks.

Weaknesses:

- If an adversary can intercept a key distributed on the back channel, the adversary could decrypt any ciphertext message generated with that key.
- The effectiveness of cover-coding depends on the performance of the tag's random number generator. If the random number is predictable due to a flaw in the tag's design or cryptanalysis, then an adversary can learn the key and decrypt subsequent communication.

5.3.2.2 Encryption of Data in Transit

Control: Data collected or processed by the tag is encrypted prior to over-the-air transmission.

Applicability: Applications that require an effective countermeasure to the threat of eavesdropping and for which cover coding offers inadequate protections. Tags typically only require on-board encryption capabilities to protect the confidentiality of data in transit if they collect or process data from sensors or other directly connected sources. In these cases, no alternative exists to hide the content of the data over-the-air because the data originates on the tag.

On-board cryptography for confidentiality is not required for applications in which readers are the only source of data. In these cases, the data can be encrypted in the enterprise subsystem or by a reader before it is written to the tag and then retrieved in its encrypted form from the tag when needed. If the tag never has to perform computations on the data, then it never has to decrypt it, but merely store it. Encryption of data at rest is also discussed in Section 5.3.3.2.

Proprietary tag designs support encryption for over-the-air confidentiality, but EPCglobal and ISO/IEC 18000 standards do not as of the date of this publication.

Benefits: Encryption of data in transit prevents successful eavesdropping of over-the-air RFID transactions.

Weaknesses:

- Data encryption requires a key management system, which can be complex to manage and operate.
- Cryptographic functions may introduce an unacceptable delay in RFID systems that require very fast read or write transactions.

- Cryptographic functions require additional power to complete, which could impact applications that use passive tags.
- Tags that support onboard encryption currently are more costly than those that do not. One reason for the increased cost is that onboard encryption requires additional logic gates to perform the necessary computations. Most low-cost passive tags do not have enough logic gates to perform complex encryption algorithms.[59]

5.3.2.3 Electromagnetic Shielding

Control: RF shielding encloses an area with a conducting material that limits the propagation of RF signals outside of the shielded area. Shielding can vary in size and form depending on the application.

For example, some RFID-enabled travel documents are protected by a metallic anti-skimming material. This material helps to prevent adversaries from reading the embedded tag when the passport cover is closed. Shipping containers are sometimes shielded to prevent the reading of tags during transit. Shielding is also placed in walls, partitions, or stalls to prevent RF emissions from leaving a confined area. When readers are placed in tunnels on industrial production conveyor belts, the tunnels may be shielded to reduce radio interference. Wrapping a tag in aluminum foil is also an effective means of shielding.

Figure 5-3 shows how shielded partitions can separate collocated readers to prevent interference. The readers near forklift A can operate without inadvertently reading tags on boxes on forklift B due to the shielding in the partition that separates the portals. Shielding may be necessary when middleware is unable to correctly filter duplicate read events from the two portals.

[59] Low cost tags currently have about 10,000 logic gates. The most efficient implementations of AES require 3,400 gates, which suggests that cryptographic support on low cost tags may be more feasible in the future. Source: M. Feldhofer, J. Wolkerstorfer and V. Rijmen, "AES implementation on a grain of sand," *IEEE Proceedings, Information Security*, vol. 152, issue 1, pp. 13-20, October 2005.

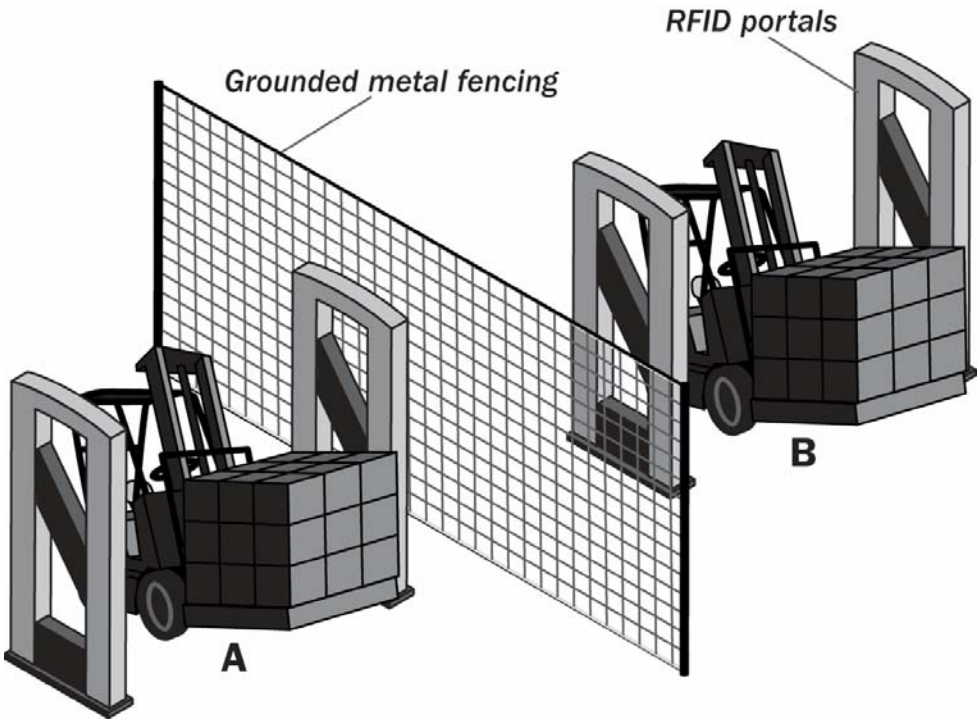

Figure 5-3. Grounded Metal Fencing as Shielding

Applicability: Shielding is applicable for contexts in which eavesdropping or RF radiation is a concern, and the use of temporary shielding would not stop valid transactions.

Benefits: Shielding can limit the ability of eavesdroppers or unauthorized readers to collect data from an RFID system.

Weaknesses:

- Shielding can prevent or hinder legitimate transactions. For example, shielded containers require objects to be physically removed from the shielding material. This prevents an implementing organization from realizing one of the key benefits of RFID technology, which is to read tags remotely without optical line of sight and additional handling.
- It may still be possible for an adversary to place a radio inside the shielded area. The radio could be used for malicious purposes, such as eavesdropping on RFID transactions or causing interference.

5.3.2.4 Radio Frequency Selection

Control: RFID technology can communicate over various radio frequencies, including those in the LF, HF, UHF, and microwave bands. Particular fixed frequencies can be assigned to an RFID application to avoid or reduce the effects of radio interference. Some tag technologies can perform frequency hopping within a limited frequency range, but in these cases, the technique is used primarily to avoid collisions with other tag transactions, not radio interference with different types of radio systems.[60] In some cases,

[60] For example, EPCglobal Class-1 Generation-2 915 MHz UHF systems use frequency hopping techniques. This capability is built into tags complying with the standard. Therefore, organizations implementing RFID systems using EPCglobal Class-1 Generation-2 compliant equipment do not have to configure this capability.

the implementing organization may need to obtain a license to use a particular desired frequency. Table 2-2 in Section 2.3.1.3 lists potential sources of interference on common RFID frequencies.

Ideally, an RF site survey will be performed before an RFID system is installed to determine what frequencies are already in use. After the RFID system is installed, site surveys can be conducted to determine if the RF characteristics of the site have changed (e.g., new sources of interference).

Applicability: All implementations whose radio frequency is not determined by other application requirements. Organizations that implement a closed RFID system have more freedom to select an operating frequency because they do not have to interoperate with other organizations. However, if tags are based on a particular air interface standard, the range of potential frequencies will be limited to those supported by the standard.

Benefits: Radio frequency selection permits the avoidance of RF interference with other radio systems that could disrupt the RFID system or other technologies. A particular frequency might be desirable because of radio interference on other frequency bands. Some frequencies also have desirable propagation characteristics, such as the ability to penetrate certain materials.

Weaknesses:

- It may be difficult to identify sources of interference. For example, bug zappers have been found to create interference in passive RFID trials.[61] Interference can be caused by poorly grounded motors, noisy relays, old fluorescent light ballasts, and other devices that generate unintended RF noise in nearby environments. Each RFID technology deployment should be tested in its intended environment prior to production use to identify these sources of interference.
- New sources of interference can be later introduced at the site.
- When implementing an inter-enterprise RFID system, all organizations involved in the system will have to agree on a tag type that supports all the frequencies that the organizations collectively intend to use.

5.3.2.5 Adjustment of Transmission Characteristics Other than Frequency

Control: Operators adjust the level of transmitted RF energy from a reader or active tag. The use of particular antenna types and configurations can also determine the direction of transmitted RF energy. Additionally, the duty cycle of a reader can be controlled.

Applicability: All applications for which eavesdropping, radio interference, or hazards of electromagnetic radiation are a concern.

Benefits: Reducing transmitted power can:

- Reduce the likelihood that an adversary can intercept communication,
- Limit radio interference with other legitimate radios, and
- Lessen hazards of electromagnetic radiation.

[61] L. Sullivan, "IBM Shares Lessons Learned From Wal-Mart RFID Deployment," October 15, 2004, http://informationweek.com/story/showArticle.jhtml?articleID=49901908.

Weaknesses: The drawback of reducing transmission power or the duty cycle is performance degradation, especially with respect to back channel communication from a passive tag. For instance, readers might fail to detect the presence of valid tags. Also, changes in the physical environment or the introduction of new radio equipment can impact the power levels required for consistently successful transactions. Consequently, the benefits of power adjustments based on a site survey can be negated by changes to the environment.

5.3.2.6 Temporary Deactivation of Tags

Control: The RF interface on some proprietary tags can be turned off temporarily. Tag manufacturers have different methods of turning their tags on and off. For example, some tags are designed so that the tag is on or off depending upon which end is inserted into a mounting clip. Other tags have replaceable batteries that can be removed to deactivate them.

If the control is implemented, tags would be turned on inside a designated area where the RF subsystem operates. When the tags leave that area, they would be turned off. For example, in a supply chain application, tags may be turned off to prevent unauthorized transactions during shipment. When the tags arrive at their destination, they would be powered on again and managed. Conversely, tags used for in-transit visibility may be turned on for their trip and turned off when they reach their destination.

Applicability: This control is most useful when communication between readers and a tag is infrequent and predictable. For example, a warehouse might store items for an annual event, such as a holiday celebration or parade. In this case, the RFID confers a benefit only for a short period each year, but could remain vulnerable to rogue transactions if left operational for the rest of the year.

Benefits: Deactivating tags temporarily:

- Prevents unauthorized tag transactions during periods of inactivity, and
- Extends the battery life of active tags.

Weaknesses:

- If operators or system software fail to reactivate the tag when it is needed, then the missing transactions resulting from the tag's RF silence could adversely impact the supported business process.
- If turning a tag on or off requires human intervention, then this control would result in additional labor expense, which could be significant for systems that process large numbers of tags. The potential increased labor required to operate the system could negatively affect the business case for RFID relative to other AIDC technologies.
- Even if the activation and deactivation process is automated, it introduces a delay that might not be acceptable for many time-sensitive applications.

5.3.2.7 Tag Press-to-Activate Switch

Control: The tag remains deactivated by default unless a user or operator takes a positive action, such as holding a press-to-activate switch on the tag to turn it on. When the switch is on, the tag is capable of RF communication, but when pressure on the switch is released, the tag returns to its default deactivated status so that tag transactions can no longer occur.

Applicability: Primarily access control or automated payment applications in which the holder of the tag desires or requires control over when tag transactions occur.

Benefits: A press-to-activate switch provides a user with physical control over when and where the tag can respond to a reader. Consequently, this control mitigates privacy and business intelligence risks by providing a countermeasure to the threat of eavesdropping and the execution of unauthorized tag commands. Eavesdropping would be limited to the immediate vicinity of authorized readers and tracking beyond the immediate vicinity of the authorized readers would not be possible.

This control also provides assurance that a person is knowingly in possession of the tag, and that it has not been intentionally or inadvertently separated from that person. For example, this control could be useful in ticketing or access control applications in which the objective is to get an accurate count of the number of individuals present, and to prevent spare tags in pockets or bags from interfering with the accuracy of the count.

Weaknesses:

- Requiring the user to activate the tag would require some level of instruction, however minimal, which might add a cost or delay in the business process. For example, the user would need to know when and for how long they would need to activate the tag.
- Some users may consider activating a switch to be an inconvenience, which could hinder user acceptance of the technology.
- A press-to-activate switch could distract the user from other functions that the user is performing. For example, a press-to-activate switch is not an appropriate control for an automated toll-payment system because the user needs to have both hands available for driving the vehicle.

5.3.2.8 Tag Polling

Control: A reader periodically queries the tag to determine its continued presence and operating status.

Applicability: Process control or asset management applications in which a design objective is periodic or near continuous monitoring. Examples include medical facilities that require real-time inventory of certain medical supplies or systems that collect sensor data. Tag polling also is applicable for high-value business processes that require early indications of system failures or performance problems. This control is most effective in applications in which those with access to the tags are trusted or when detaching the tag is not feasible (e.g., when a tag is embedded in another item such as a poker chip).

Benefits: Operators obtain timely information about system failures, item theft, or unusual environmental conditions that enables them to proactively address problems.

Weaknesses: Tag polling:

- Reduces the battery life of active and semi-active tags,
- May not detect critical events in a timely manner if the polling frequency is too low,
- Is a business intelligence risk if the tag polling enables an adversary to perform traffic analysis, or track or target tags that might have otherwise remained silent, and.
- Could be circumvented in some cases by detaching the tag, taking the item, and leaving the tag behind so that it continues to signal its presence to readers.

5.3.3 Tag Data Protection

Technical controls currently available for protecting tag data include:

- Tag memory access control, which can restrict use of tag commands and protect data stored in a tag's memory,
- Encrypting the data on tags,
- The kill feature, which can prevent subsequent unauthorized use of a tag, and
- Tamper protection.

These controls are described in more detail in Sections 5.3.3.1 through 5.3.3.4.

5.3.3.1 Tag Memory Access Control

Control: Many tags support a password-protected lock feature which provides read or write protection to memory. In some RFID technologies, the lock feature is permanent and in others it is reversible. For example, the EPCglobal Class-1 Generation-2 has five areas of memory, each of which can be protected using the *lock* command. [62] The memory is either both read- and write-protected, or only write-protected, depending on the parameters issued with the command. The EPCglobal Class-1 Generation-2 UHF standard also has a *permalock* feature. If engaged, permalock will make the lock status (locked or unlocked) permanent for all or part of a tag's memory. ISO/IEC 18000-3 Mode 2 supports both read and write protecting all areas of memory with a 48-bit memory access password. Finally, Mode 2 of the ISO/IEC 18000-3 standard describes a *lock pointer*, which is a memory address. All areas of memory with a lower address than the lock pointer are write-protected, while those areas of memory above the pointer address are not.

The effectiveness of tag memory access controls depend on proper management of passwords. Section 5.3.1.1 provides additional information on password authentication.

Applicability: All applications that store data on tags.

Benefits: A write-protect *lock* command will prevent the contents of a tag's memory from being altered. A read-protect *lock* command will prevent unauthorized users from reading or accessing the data on tags.

Weaknesses:

- The password length on many tags is too short to provide meaningful memory access protection. Even when the technology supports longer passwords, password management is challenging (see Section 5.3.1.1 on password authentication for additional information).
- Locking a tag's memory does not prevent data loss from electromagnetic interference or physical tag destruction.

[62] The five areas of memory are registers for the kill password, access password, EPC memory, TID memory, and User memory. When locked, the kill password and access password become both read and write protected. If they are locked, the EPC memory, TID memory, and User memory are only write protected.

5.3.3.2 Encryption of Data at Rest

Control: Data stored on a tag is encrypted before it is written to the tag. The control does not require that the tag encrypt or decrypt data. Instead, the encryption is performed by either the reader, middleware, or other enterprise subsystem components.

Applicability: All applications that store additional data beyond an identifier on the tag that needs to be kept confidential on the tag. If the encryption and decryption functions are performed in the enterprise subsystem, then network access is required to read the content of data stored on the tag, which makes the control unsuitable for mobile readers that do not always have real-time network access.

Benefits: Data encryption protects sensitive tag data from being read by individuals with unauthorized access to the tags.

Weaknesses:

- Data encryption requires a key management system, which can be complex to manage and operate.
- Sending tag data to network components for encryption or decryption is a source of network latency, when in conjunction with the time to complete cryptographic functions may introduce an unacceptable delay in RFID systems that require very fast read or write transactions.

5.3.3.3 Kill Feature

Control: The kill feature permanently disables a tag's functionality using a remote command. The most common implementation of the kill feature is the EPCglobal *kill* command. The EPCglobal Class-1 Generation-2 *kill* command is password-protected using a 32-bit password different from the access password.[63]

Applicability: RFID applications that encounter business intelligence and privacy risks after a tag has moved beyond its intended functional environment (e.g., after a tag moves beyond the supply chain in which it served inventory and checkout functions). EPCglobal tags are the only standards-based tags that support a kill feature.

Benefits: Using the kill feature prevents a tag from being reused improperly. The kill feature was designed and implemented in EPCglobal tags primarily to protect consumer privacy. It also protects improper access to tag data used in business processes. For example, discarded tags that have not been disabled may be read by adversaries to gain access to data, such as which products an organization or individual is purchasing or using.

Weaknesses:

[63] Several alternative technical controls to the kill feature are under development, but have not yet been fully commercialized. One approach is to disable the tag's antenna in such a way that it can still perform transactions over short distances (e.g., 10 cm or less) but not longer than that. The objective is to greatly reduce the probability that an adversary could track or target someone in possession of the tag after the tag longer serves its primary purpose, but still enable the tag to perform some additional functions, albeit with additional effort. For example, the primary purpose of the tag might be to facilitate a point-of-sale transaction, but using the approach described, the tag could also facilitate a receipt-less return, although the item would need to be placed closer to the reader to complete this post-sale transaction. Another approach is to use multiple control domains as described in the immediately preceding footnote. The objective of both of these approaches is to extend the life of a tag to support some residual functionality that would otherwise be eliminated as a result of the kill feature.

- The existence of a kill feature represents a significant business process threat to an RFID system. If an adversary who learns the kill password improperly disables tags that should remain in operation, the supported application will not function properly because it will not be able to perform transactions on the disabled tags. This risk is particularly salient for organizations that assign the same password to multiple tags because doing so could enable an adversary to disable large numbers of tags with a single compromised password.
- Once killed, a tag cannot be used for any further application involving the asset (e.g., recalls, receipt-less product returns).
- If an organization assigns a weak (e.g., short or easily guessed) password for the *kill* command, unauthorized parties can kill the tag at will.[64] Moreover, the longer a tag maintains the same password, the more likely it is that the password will be compromised.
- Data stored on the tag is still present in the tag's memory after it is killed (although it can no longer be accessed wirelessly), and therefore still may be accessible to someone with physical access to the tag.[65]
- Although the *kill* command was added to tags as a potential solution for privacy concerns, consumers cannot easily detect whether a tag has been deactivated.[66] Moreover, typical consumers cannot easily kill tags on their own because this action requires a reader and knowledge of the *kill* password.

5.3.3.4 Tamper Resistance

Control: Certain RFID tags have tamper resistant or tamper-evident features that help prevent an adversary from altering the tags or removing them from the objects to which they are attached. One simple type of tamper resistance is the use of a frangible, or easily broken, antenna; if a tag of this type is removed, the electric connection with the antenna is severed, rendering the tag inoperable. Other, more complex types of RFID systems monitor the integrity of objects associated with the tags to ensure that the objects have not been compromised, altered, or subjected to extreme conditions.

Applicability: Applications in which tags are frequently outside of the direct control of the implementing organization and therefore vulnerable to tampering. Tamper resistance and tamper-evident features are currently only available on specialty RFID tags that are designed for tamper resistance to support specific buyer requirements.

Benefits: This control helps to prevent adversaries from breaking the association between a tag and its corresponding object. The more complex tamper-resistant / tamper-evident tags provide health and status monitoring of the attached objects to ensure that they have not been opened, manipulated, damaged, or subjected to extreme temperature, humidity, or shock.

Weaknesses: Sophisticated adversaries may be able to defeat the tamper resistance mechanisms. This is dependent upon the implementation of the tamper resistance feature. For example, a sophisticated adversary may be able to repair a frangible antenna. In addition, tamper-resistance / tamper-evidence technologies do not prevent the theft or destruction of the tag or its associated items.

---

[64] An EPCglobal Class-1 Generation-2 tag cannot be killed if it has a null password (i.e., one whose bits are all zeros). Source: EPCglobal, "EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9," January 2005, pg. 58.

[65] Obtaining data from the tag in this circumstance would require an attacker to have specialized equipment and expertise.

[66] This may open a door for future consumer products to test for the presence of passive RFID tags and probe their characteristics. It is hypothesized that cellular phones may be able to provide this service for EPC passive tags since cellular phones already operate in the 860 to 960 MHz band.

5.4 Summary

Organizations should use a combination of management, operational, and technical controls to mitigate the business risks of implementing RFID systems. Table 5-1 maps the presented controls to the categories of risks that they mitigate. Because each RFID implementation is highly customized and each organization's requirements are different, the security controls discussed in this section are not all applicable or effective for all RFID applications. Organizations need to assess the risks their RFID implementations face and choose the appropriate controls, taking into account factors such as regulatory requirements, the magnitude of threats, and cost and performance implications of the controls. For example, a remote warehouse may have little need to protect against eavesdropping, but it may require redundant processes in case of system failure. Traditional security controls are often preferable to RFID-specific controls. For example, if RFID data can be stored in an enterprise database rather than on tags, then physical and network security controls for the database server probably are more practical than using tags with cryptographic capabilities.

Table 5-1. RFID Controls Summary

	Control	Risk Mitigated by Control				
					4.4 Externality Risk	
		4.1 Business Process Risk	4.2 Business Intelligence Risk	4.3 Privacy Risk	4.4.1 Hazards of Electro-magnetic Radiation	4.4.2 Computer Network Attacks
Management	5.1.1 RFID Usage Policy	X	X	X	X	X
	5.1.2 IT Security Policies	X	X	X		X
	5.1.3 Agreements with External Organizations	X	X	X		X
	5.1.4 Minimizing Data Stored on Tags	X	X	X		
Operational	5.2.1 Physical Access Control	X	X	X	X	X
	5.2.2 Appropriate Placement of Tags and Readers	X	X			X
	5.2.3 Secure Disposal of Tags	X	X	X		
	5.2.4 Operator and Administrator Training	X	X	X	X	X
	5.2.5 Information Labels / Notice	X	X	X	X	
	5.2.6 Separation of Duties	X		X		
	5.2.7 Non-revealing Identifier Formats		X	X		
	5.2.8 Fallback Identification Systems	X				
Technical	5.3.1.1 Password Authentication	X	X	X		X
	5.3.1.2 HMAC	X	X	X		X
	5.3.1.3 Digital Signatures	X	X			

Control		Risk Mitigated by Control				
					4.4 Externality Risk	
		4.1 Business Process Risk	4.2 Business Intelligence Risk	4.3 Privacy Risk	4.4.1 Hazards of Electro-magnetic Radiation	4.4.2 Computer Network Attacks
	5.3.2.1 Cover-Coding	X	X	X		
	5.3.2.2 Encryption of Data in Transit		X	X		
	5.3.2.3 Electromagnetic Shielding		X	X	X	
	5.3.2.4 Radio Frequency Selection	X			X	
	5.3.2.5 Adjustment of Transmission Characteristics		X	X	X	
	5.3.2.6 Temporary Deactivation of Tags	X	X	X		
	5.3.2.7 Tag Press-to-Activate Switch		X	X		
	5.3.2.8 Tag Polling	X				
	5.3.3.1 Tag Access Controls	X	X	X		X
	5.3.3.2 Encryption of Data at Rest	X	X	X		
	5.3.3.3 Kill Feature		X	X		
	5.3.3.4 Tamper Resistance	X	X			

This page has been left blank intentionally.

6. RFID Privacy Considerations

While this document is primarily about securing RFID systems, privacy issues are often interrelated with security considerations in a manner that one cannot be discussed without the other. For example, protecting privacy often requires technical security controls related to data confidentiality. This section explains what types of information are considered personal, reviews a number of privacy considerations that impact the life cycle of RFID systems, explains general privacy controls, and lists privacy guidance with which US Federal agencies are required to comply.

Privacy regulations and guidance are often complex and change over time. Organizations planning, implementing, or managing an RFID system should always consult with the organization's privacy officer, legal counsel, and chief information officer when developing and enforcing privacy policy related to the system.

6.1 Types of Personal Information

Federal privacy laws predominantly address the requirements for assessing, managing and safeguarding data defined as personal information. Figure 7-1 provides a taxonomy of personal information that is useful in describing privacy considerations for RFID systems.

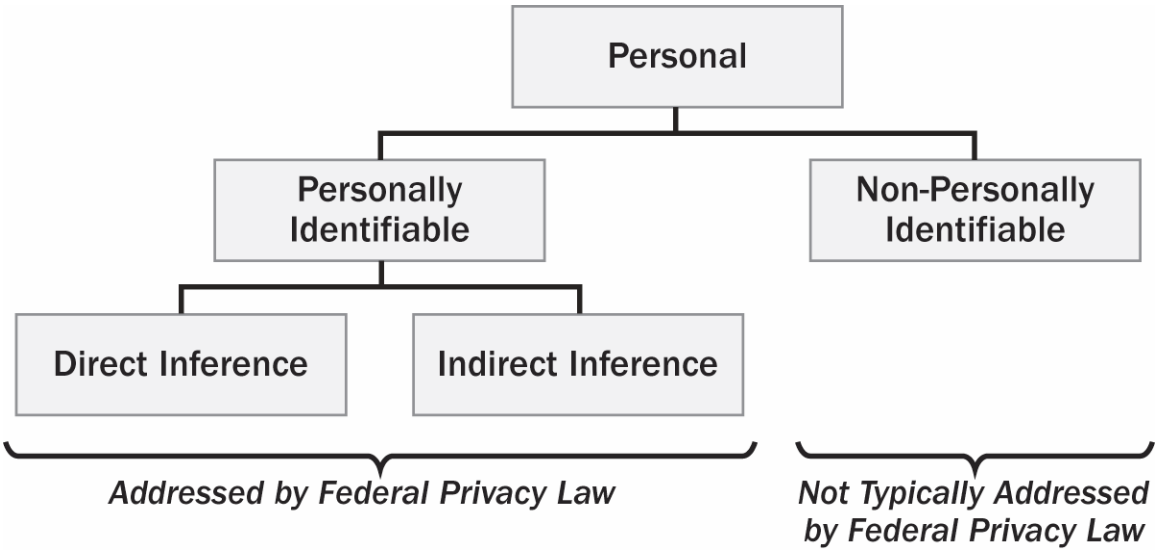

Figure 6-1. Taxonomy of Personal Information

For the purposes of current privacy regulation, the most important distinction about the information being addressed is whether personal information is personally identifiable information (PII) or non-personally identifiable information. PII is information that can be used to uniquely identify, locate, or contact an individual.[67] Examples of data elements that typically are considered PII include, but are not limited to, an individual's full name, social security number, passport number, financial account or credit card numbers, and biometric data such as fingerprints. Individual data elements associated with characteristics

[67] PII is also referred to as personally *identifying* information or "information in identifiable form," which is defined in the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2923, as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form."

that many people share are generally not considered PII. Examples include age, gender, city of residence, religious affiliation, and medical conditions.

Sometimes multiple pieces of information, none of which alone is considered PII, might still uniquely identify a person when combined. For example, NIST may employ only one 39-year old female with a residence in Roanoke, Virginia. In this case, the employer, age, gender, and city of residence are not PII elements by themselves, but become PII when they are presented together. This scenario is an example of PII established through *indirect inference*, while data elements such as a driver's license number constitute PII through *direct inference*.

As a general rule, privacy laws govern the management of PII inferred through both direct and indirect means. The same laws, however, usually do not address data elements that individuals perceive as personal information but do not meet the criteria of PII as defined by the E-Government Act of 2002. For example, people anonymously walking down the street may perceive a loss of privacy if someone with a reader can ascertain the books they are reading or the medicine they are taking, but not their identities, by remotely scanning various tagged items in a bag, purse or on one's person. In this case, the individuals remain anonymous but may perceive a compromise of privacy because they do not have control over the personal information they reveal to others. To address these concerns, organizations implementing RFID systems may choose to mitigate the risk associated with these scenarios. In these cases, the range of privacy considerations is not limited to those required by law.

6.2 The Applicability of Privacy Considerations to RFID Systems

RFID systems support a large variety of business processes, not all of which involve personal privacy. Examples of RFID systems that likely do not have privacy considerations include those supporting industrial processes, animal tracking, and asset management systems in which the assets are never associated with individuals during their life cycle. Privacy considerations exist when the system uses, collects, stores, or discloses personal information. An RFID system might use or disclose personal information in one of several ways:

- Personal information such as a name or account number may be stored on the tag or in a database in the enterprise subsystem.
- A tag may be associated with a personal item such as a blood sample, a bottle of prescription medicine, or a folder of legal documents that might be outside of the individual's possession.
- A tag may be associated with an item that often travels with an individual, such as a tagged box or a vehicle part in an automobile or truck the individual often drives.

The RFID system does not have to store personal information to have privacy implications. For example, the tag on a bottle of prescription medicine may identify the drug in the bottle, but not the identity of the person for whom the prescription was written. Nonetheless, the individual taking the medicine may still perceive the possession of the drug as personal information if scanned and read by another, as it might reveal information about a medical condition that the individual considers private.

Similarly, the individual does not have to own a tagged item for the RFID system to have privacy implications. For example, if an employee carries an employer-tagged computer or tools, then RFID technology potentially could be used to track the employee's whereabouts. The employee may agree to be on-call after business hours but could consider his or her location during those times as personal information.

While the concepts of privacy and PII are not new, RFID technology is an example of a technology that introduces new complexity to the landscape of privacy considerations for several reasons. For example, RFID technology increases the likelihood that someone can create PII through indirect means. RFID technology creates opportunities to record, store, and process item-specific information related to business transactions more easily than ever before. In addition, the breadth of items in everyday life that will be incorporated into RFID systems is expected to increase in the coming years. The increase in the coverage of information systems in our daily life combined with the increase of the level of detail of information in those systems will likely create new opportunities for combining data elements to generate PII. Advances in Internet search and data mining software also will facilitate the ability to capture PII from large volumes of what previously might have been considered uncorrelated data. All of these trends can occur even if PII is not recorded on tags themselves.

Several inherent features of RFID tags make enforcement of privacy controls more difficult than traditional information technology systems. Organizations may face challenges enforcing privacy policies when they cannot be coupled with effective security controls. RFID uses wireless communication, which is more vulnerable to eavesdropping and other attacks than the wired systems on which most traditional IT systems reside. In many applications, RFID tags will travel between organizations and often will be found in public areas, which means they cannot benefit from physical security commonly provided to most traditional IT systems. In general, RFID computing resources are limited and are not capable of implementing sophisticated technical controls. As this document describes, many techniques exist to mitigate these security and privacy risks, and these are expected to improve over time. However, the economics of many RFID applications will require low cost tags with limited functionality, which has significant implications for privacy protections. Finally, in many applications, especially those involving passive tags, identifiers can live beyond the usefulness of the application for which they were intended, but still may store PII or be used to generate PII when combined with other data. While traditional IT systems have well-established policies and procedures for the retention and destruction of data, destroying or disabling tags may be infeasible once they are outside the control of the organization managing the RFID system.

RFID technology may introduce new privacy considerations that are not fully understood today. Privacy regulation and principles evolve to meet the demands of new IT systems. For instance, technical advances such as the Internet, electronic databases, and analytic system software have made the collection and sharing of PII easier than it was in a world of paper files. RFID technology further extends the reach of IT systems and the collection and sharing of information that might be considered personal. While today RFID readers typically are located in designated locations to support a particular business process, in the future readers may be ubiquitous and capable of supporting multiple objectives. For example, today an RFID system might be implemented to provide access control to a facility using RFID-enabled badges. Badge holders are unlikely to possess other tagged items. In the future, badge holders may routinely carry a number of tagged items, and the badge reader may be used to scan them and create a profile as well as authenticate the badge. The data collected might be shared with third parties for justifiable business needs and with legitimate data sharing agreements. The systems might be implemented with disclosure and consent, but may not be effective because individuals and organizations cannot reasonably understand all the potential uses of the data or predict what type of transactions might create PII through indirect inference. For these reasons, new privacy tools and concepts may need to be developed to address the complexity introduced by RFID technology.

6.3 Privacy Principles

An organization's privacy policy is most effective when it is based on principles that reflect a thorough understanding of privacy-related risks. Well-formulated principles lead to a baseline set of privacy requirements that can be further tailored to address organization-specific or application-specific

considerations. In 1973, the US Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services) issued a report entitled *Records, Computers, and the Rights of Citizens*. This report recommended that Congress enact legislation adopting a "Code of Fair Information Practice" for automated personal data systems and many of its ideas were eventually incorporated into the Privacy Act of 1974.[68] The HEW Fair Information Practices listed five main privacy objectives:

- There must be no personal data record-keeping systems whose very existence is secret;
- There must be a way for an individual to find out what information is in his or her file and how the information is being used;
- There must be a way for an individual to correct information in his or her records;
- Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and
- There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

In 1980, the Organisation for Economic Co-operation and Development (OECD) adopted *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which provide a framework for privacy policy that has been referenced in US Federal guidance and internationally.[69] Table 6-1 lists the OECD basic principles for privacy and data protection, their definitions, and discusses how each might be addressed in the context of an RFID system.

Table 6-1. OECD Basic Principles: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

#	OECD Privacy Principle	Definition	RFID Considerations
1	Collection Limitation	There should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	Organizations can enforce this principle on their own information systems but may not be able to prevent others from surreptitiously collecting PII through indirect means, such as correlation of tag data with other data sources, including other tagged items in the individual's possession and databases maintained by organizations other than the one issuing the tag.
2	Data Quality	Personal data should be relevant to the purposes for which they are to be used. The data should be accurate, complete, and be kept up-to-date.	Organizations may establish procedures for data quality, but strict enforcement could be challenging given the volume of data processed in many RFID systems. Independent audits and sampling techniques may mitigate this risk. The data stored on tags or in enterprise subsystem databases may not be up-to-date or accurate if there is an extensive period of time between read transactions that would synchronize information. Managing data quality may be challenging for RFID applications involving multiple enterprises, such as supply chains. Audit records that can identify which

[68] 5 USC § 552(a).

[69] The OECD privacy principles and their associated definitions are offered neither as an endorsement of OECD's privacy program, nor an endorsement of the privacy policies of any of its members.

#	OECD Privacy Principle	Definition	RFID Considerations
			entities were responsible for which data elements at which time are critical to the success of data quality efforts.
3	Purpose Specification	The purposes for which personal data are collected should be specified not later than at the time of the data collection. Subsequent use should be limited to the fulfillment of those purposes. In the event subsequent purposes arise, they should be specified on each occasion of change and compatible with the original purposes.	Organizations should be able to specify their own purposes for collecting personal data but may not be able to determine the potential purposes of those engaged in surreptitious reading of tags. In some cases, even the existence of a tag could be used for tracking or targeting purposes for which there are few practical countermeasures. RFID applications involving multiple enterprises should be accompanied by an MOU or MOA clearly delineating the purposes for which RFID data may be used, as each party to the agreement may be unfamiliar with the potential purposes of other parties.
4	Use Limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.	Similar to the collection limitation, organizations can enforce this principle on their own information systems but may find it challenging to prevent authorized parties from surreptitiously reading tags for other purposes.
5	Security Safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.	This document describes several security mechanisms for safeguarding personal data. The adequacy of any given set of safeguards needs to be evaluated in the context of a particular RFID system.
6	Openness	There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller.	No characteristic of RFID technology prevents a general policy of openness although this principle may not be consistent with RFID applications supporting intelligence or law enforcement missions because of the secrecy required for their effectiveness.
7	Individual Participation	An individual should have the right to learn whether a data controller has data relating to the individual, and, if so, to obtain that data within a reasonable time period, at a charge that is not excessive, and in a readily intelligible form. If a request is denied for some reason, the individual should be given reasons for the denial and be able to challenge the denial. The individual should also be able to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended as appropriate.	Organizations should be able to design RFID systems consistent with this principle in most cases, especially when the system manages sensitive PII data elements, such as a Social Security Number or financial account number. The individual participation principle, however, was created at a time when the amount of data stored was relatively limited. In some applications, the nature of the data and the large number of transactions may determine what level of individual participation is realistic. For example, many casinos now have RFID-enabled poker chips to prevent fraud and improve the accuracy of bets. The casino may establish a procedure to enable an individual to challenge specific pay outs, but not dispute precisely which chip was used for which bet even if this information is stored in the system for some period of time.
8	Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.	In general, nothing about RFID technology prevents accountability with the caveat that organizations may not be able to limit access to tags when they are outside of their control. In this case, proper

#	OECD Privacy Principle	Definition	RFID Considerations
			disclosure of the risk is appropriate. RFID applications involving multiple parties should be accompanied by an MOU or MOA that specifies which entity is accountable for which privacy principle at which time.

6.4 Privacy Requirements for Federal Agencies

This section provides an overview of the following Federal privacy statutes and guidance that pertain to Federal agencies and, in many cases, other organizations that handle, process, or share data with Federal agencies:

- Privacy Act of 1974,
- Section 208 of the E-Government Act of 2002,
- Section 522 of the Consolidated Appropriations Act of 2005,[70]
- Federal Information Security Management Act (FISMA),[71] and
- OMB memoranda on the implementation of privacy requirements.

This section is not intended as an interpretation of law, legal advice, or a mandate for any organization. Federal officials responsible for RFID systems should consult with the senior agency official for privacy[72], legal counsel, and other privacy compliance-related officials to appropriately identify and integrate privacy controls into RFID systems. RFID privacy stakeholders also may include the Office of the Chief Information Officer, the organizational components that the RFID system supports, and the office implementing the Freedom of Information Act (FOIA).

Collaboration among RFID project managers and privacy officials will help ensure greater understanding of privacy initiatives currently in place, provide for greater efficiencies in the use and sharing of agency resources, and lower the risk of RFID projects. Additionally, collaboration can better ensure privacy controls are considered early in the system development life cycle and avoid costly retrofitting of solutions.

While Federal agencies must meet certain privacy requirements as a matter of legal compliance, organizations not covered by the mandates may implement privacy controls for other purposes, such as to maintain the trust and confidence of their customers and business partners, or to protect or enhance their reputation. These organizations may still find it useful to review requirements for Federal agencies to determine what might be appropriate for their environment.

6.4.1 Privacy Act of 1974

For over 30 years, the cornerstone of federal information privacy law has been the Privacy Act of 1974 ("the Privacy Act"), (5 USC § 552a), which was written before the widespread adoption of IT as the primary means of managing data. The Privacy Act regulates the collection, use, maintenance, and

[70] Consolidated Appropriations Act, 2005, Pub. L. No. 108-447.

[71] Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946.

[72] The senior agency official for privacy may also be known as the Chief Privacy Officer or Privacy Advocate. In some cases, the role may be filled by the agency's Chief Information Officer. The senior agency official privacy may also head an office responsible for Privacy Act implementation or other privacy-related law(s), but not hold one of these titles.

dissemination of personal information about US citizens or aliens lawfully admitted for permanent residence. The Privacy Act applies only to records about individuals maintained by agencies in the executive branch of the government. It also only covers information filed within a *system of records*, which is a group of files that:

- Contain an individual's name, Social Security Number (SSN), or some other unique personal identifier (such as employee number) AND at least one other element of personal information about the individual (such as date of birth); and
- Are retrieved by an individual's name, SSN, or personal identifier.

6.4.2 E-Government Act of 2002

Title II, Section 208 of the E-Government Act of 2002 ("Section 208") prescribes the establishment of a privacy framework for agencies to manage compliance with privacy mandates passed since 1974. The Act contains several provisions likely to apply to RFID systems, including requirements to:

- Perform a privacy impact assessment (PIA),[73]
- Ensure employees, business partners and contractors are informed and educated of their responsibility to protect PII (if the RFID system manages or generates PII),
- Evaluate IT system and business model privacy risks for program activities and their information systems, and
- If the RFID system contains an inter-enterprise subsystem that enables external parties to access RFID information through a Web site, then the RFID system manager may also be required to:
  - Ensure Web site privacy policies and notices adhere to Federal requirements,
  - Comply with Web site tracking technology requirements, and
  - Develop and implement a machine-readable privacy policy plan.

The Act also requires that agencies designate a point of contact for privacy compliance and related matters. This official should be consulted throughout the life cycle of the RFID system.

[73] The PIA requirement applies to systems involving data collection from 10 or more members of the general public when one or more of the following "PIA triggers" occurs: (1) conversions - when converting paper-based records to electronic systems; (2) anonymous to non-anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form; (3) significant system management changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system: (4) significant merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated: (5) new public access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public; (6) commercial sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis does not trigger the PIA requirement); (7) new interagency uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA; (8) internal flow or collection - when alteration of a business process results in new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form; and (9) alteration in character of data - when new information in identifiable form is added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

6.4.3 Federal Information Security Management Act (FISMA)

Title III of the E-Government Act of 2002 provides for FISMA provisions. The purpose of FISMA is to provide a comprehensive framework for the management of federal information security, including the establishment of a minimum level of controls to protect information and information systems, the improved oversight of agency information security programs, and the use of commercially developed information security products. For the past two years, OMB has required that in addition to the quarterly reporting on compliance with FISMA security requirements, agencies must now report on their privacy compliance posture with federal laws (for instance, the Privacy Act of 1974 and Section 208 of the E-Government Act of 2002). In Fiscal Year (FY) 2006, OMB's *Instructions for Preparing the FISMA and Privacy Management Report*[74] prescribed that information and information systems must be categorized and have an appropriate number of security controls and privacy considerations given to each. In addition, OMB stated that there must be a mechanism in place to monitor the security controls and privacy risks, as well as to determine the security and privacy deficiencies of the system.

6.4.4 Consolidated Appropriations Act of 2005

Section 522 of the Consolidated Appropriations Act ("Section 522") prescribes privacy rules for the Departments of Treasury and Transportation, as well as Independent Agencies, but does not currently apply to agencies outside this group. Section 522 extends the mandates in Section 208 of the E-Government Act of 2002 to include requirements that agencies:

- Assure that the use of technologies sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in an identifiable form,
- Assure that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program,
- Assure that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974,
- Evaluate legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government,
- Conduct privacy impact assessment of proposed department rules on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected,
- Prepare a report to Congress on an annual basis on activities of the department that affect privacy,
- Ensure that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction,
- Train and educate employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies,
- Establish privacy and data protection procedures and policies,
- Ensure compliance with the departments' established privacy and data protection policies,

[74] Office of Management and Budget, "Instructions for Preparing the FISMA Report and Privacy Management Report," Executive Office of the President, Washington, D.C., OMB Memorandum 05-15, June 13, 2005.

- Record with each agency's Inspector General a written report of the agency's use of information in identifiable form, along with its privacy and data protection policies, and
- Ensure each agency performs an independent, third party review of the use of information in identifiable form.

6.4.5 Office of Management and Budget (OMB) Privacy Memoranda

OMB has issued several memoranda that provide policy guidance and instructions for the implementation of privacy laws, including:[75]

- OMB Memorandum 03-22, Guidance for Implementing Section 208 of the E-Government Act of 2002, provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002.
- OMB Memorandum 05-08, Designation of Senior Agency Officials for Privacy, was issued in support of the Administration's commitment to protecting information privacy, and required each executive Department and agency to identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues. The senior agency official should have authority within the agency to consider information privacy policy issues at a national and agency-wide level.
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, reemphasizes agencies' responsibilities to appropriately safeguard sensitive personally identifiable information and to train its employees on their responsibilities in this area. It explains how Senior Agency Officials for Privacy should conduct FISMA reporting, review their policies and processes, and take corrective action as appropriate to ensure adequate safeguards prevent the intentional or negligent misuse of, or unauthorized access to PII.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, provides a checklist for safeguarding information removed from or accessed outside of an agency's physical location.
- OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, provides updated guidance on the reporting of security incidents involving PII. It explains new requirements related to security and privacy with which agencies must comply beginning with fiscal year (FY) 2008 budget submissions for IT.
- OMB Memorandum M-06-20, FY 2006 Reporting Instructions for FISMA and Agency Privacy Management, provides FISMA security quarterly reporting instructions that will apply annually beyond FY 2006 unless amended. It also includes quarterly reporting instructions for agencies' privacy compliance management activities.

6.5 Health Insurance Portability and Accountability Act (HIPAA) of 1996

The HIPAA privacy and security rules represent a national effort to protect individuals' personal health information (PHI)[76] from unwarranted access and disclosure. The covered entities include *all* health care providers, insurers, third-party administrators, and the business partners of these entities.

The privacy rule defines PHI as health information that can be associated with a specific individual. It describes the policies, procedures, and business service agreements required to control the access to and

[75] Additional OMB privacy policies and policy updates can found at http://www.whitehouse.gov/omb/inforeg/infopoltech.html.

[76] PHI is also termed *protected* health information in some documents.

use of PHI. In all but a few circumstances, disclosure of PHI is only permitted if the organization has obtained the individual's consent in advance. The security rule addresses an organization's infrastructure requirements to assure secure and private communication, as well as the confidentiality of patient information.

To comply with HIPAA, organizations must identify how RFID-enabled business processes create, collect, store, monitor, transmit, or share PHI. In particular, organizations should explore how PHI may be established through indirect means, including scenarios in which information obtained from RFID tags may be combined with other data to infer someone's identity or link it with health information. One example mentioned previously is the possibility that, without implementation of appropriate controls, someone may be able to identify that an individual is consuming prescription drugs or a particular type of drug by surreptitiously reading information on a tagged label. Scenarios involving medical devices may present similar risks. Perhaps the greatest HIPAA privacy compliance challenges occur when RFID-tagged medical services and products are delivered or purchased outside the boundaries of hospitals or doctor offices because it is more difficult to enforce controls in these circumstances.

6.6 Federal CIO Council Privacy Control Families

Organizations may be required to implement privacy controls to comply with the laws and regulations discussed earlier in this section or they may do so voluntarily to protect and improve relationships with customers, business partners, and employees. To assist agencies with their privacy programs, the Federal Chief Information Officers (CIO) Council ("CIO Council") developed a reference model that describes 17 privacy control families. Many of the privacy control families are closely related to the security controls discussed in detail in Section 5. How controls within these families will be implemented for RFID systems will vary depending on the characteristics of the business process the RFID system supports. For RFID technology supporting transportation initiatives will likely have a different set of privacy controls those involving delivery of healthcare. However, both would likely involve privacy controls within the notice and consent family. The control families and related considerations for RFID systems are presented in Table 6-2.

Table 6-2. Federal CIO Council Privacy Control Families

#	Federal CIO Council Control Family	Definition	RFID Considerations
1	Policies and Procedures	Creating policies and procedures governing the appropriate use of personal information and implementing privacy controls	RFID systems should be supported by appropriate policies and procedures. Privacy policies should be consistent or integrated with an RFID usage policy that describes the authorized and unauthorized uses of RFID technology.
2	Privacy as Part of the Development Life Cycle	Implementing privacy reviews and controls throughout the information system development life cycle	RFID systems that have potential privacy implications should include privacy considerations throughout the development life cycle. Federal agencies will likely have to conduct a PIA prior to implementing an RFID system and subsequent major changes. Section 7 (Recommended Practices) provides additional information on the appropriate actions at each stage in the development life cycle. One of the most significant privacy challenges for RFID systems is the end of the life cycle, when tags are no longer required to support the intended business purpose. At this point, the tags may no longer be in the possession of the organization that issued them, but they may still store identifiers or other data that could reveal PII

#	Federal CIO Council Control Family	Definition	RFID Considerations
			though either direct or indirect means. In many cases, collection or destruction of the tags is infeasible or cost prohibitive.
3	Assigned Roles, Responsibilities, and Accountability	Identifying general and specific roles and responsibilities for managing and using personal information and ensuring accountability for meeting these responsibilities	The policies and procedures governing the RFID system should assign roles and responsibilities. As mentioned previously, accountability can be difficult when tags are outside of the control of the implementing organization or when the RFID application involves an inter-enterprise subsystem. Audit records of RFID transactions can help mitigate this risk.
4	Monitoring and Measuring	Monitoring the implementation of privacy controls and measuring their efficacy	The organization's privacy officer and legal counsel should be consulted during the design, execution, and reporting of monitoring and measuring activities. Privacy monitoring may be conducted in conjunction with RFID security assessments, which are recommended to be performed at regular and/or random intervals.
5	Education and Awareness	Ensuring managers and users of personal information are made aware of the privacy risks associated with their activities and of applicable laws, policies, and procedures related to privacy	If an RFID system has potential privacy implications, privacy training should include a broad range of personnel extending beyond those that manage and operate the system. Some members of the public have significant concerns about the ability of RFID technology to compromise their privacy and may contact the organization to express those concerns or ask detailed questions about how the RFID and technology is used. Accordingly, any personnel routinely interacting with the public should be prepared for such interactions and be able to direct concerns and questions to appropriate staff in the organization. The staff to which inquiries are referred should receive comprehensive privacy training and know how the organization uses RFID technology and information systems to support business processes and protect PII.
6	Public Disclosure	Publicly disclosing privacy policies and procedures for a program or system	Privacy policies related to RFID systems should be publicly disclosed. In some intelligence and law enforcement applications, public disclosure may not be consistent with the need to maintain program secrecy, but this does not obviate the need to maintain such policies and procedures even if not disclosed.
7	Notice	Providing notice of the information practices to the individual before collecting personal information	Notice related to the RFID system is likely to be provided in the context of information disseminated about the business process it supports. Notice may take different forms, such as a mass mailing, a sign posted near readers, or a statement on a Web site. Notice should describe the purposes for which data might be used. For example, in consumer applications, customers might be contacted for post-sale activities such as a customer satisfaction survey.
8	Consent	Gaining consent from the individual to use their personal information	Whenever an organization collects data elements considered PII, it should obtain the individuals' consent prior to using the information. For some intelligence and law enforcement applications, consent may be inconsistent with program secrecy.

#	Federal CIO Council Control Family	Definition	RFID Considerations
			In addition, consent may not be possible during medical emergencies. The scope of the consent is a key issue; holders of tagged items may not fully appreciate all the potential ways in which data may be correlated with other sources, especially as data sharing and search technologies evolve. In these circumstances, some may argue that it is difficult to achieve *informed* consent, even if the potential for data sharing is disclosed. Moreover, some consent requirements may become either impractical or unenforceable as readers become more ubiquitous in everyday life, especially if they are imbedded in consumer devices such as mobile phones or personal digital assistants.
9	Minimum Necessary	Collecting the minimum amount of personal information necessary to accomplish the business purpose	Organizations should collect only PII data elements necessary for business purposes. Moreover, in RFID systems, PII should be stored in enterprise subsystem databases rather than on tags whenever possible. However, the value of RFID technology is its ability to support rapid collection of highly specific data without optical line of sight. Inevitably more data is collected than is necessary. A major challenge for RFID systems is how to filter and discard unnecessary data so as to not overwhelm computing resources. While these processes are primarily designed to achieve cost and performance objectives, they may also incorporate privacy principles.
10	Acceptable Use	Ensuring that personal information is used only in the manner provided on the notice, to which the individual consented, and in accordance with the publicly disclosed practices	Organizations should implement controls to enforce its RFID usage policy. Depending on the environment, controls related to notice, consent and disclosure may not be appropriate or effective due to the factors discussed above.
11	Accuracy of Data	Ensuring that personal information is accurate, particularly if harm or denial of benefits may result	RFID systems can employ recommended practices for user forms and IT database controls to ensure data accuracy.
12	Individual Rights	Providing individuals an opportunity to access and correct their personal information and to seek redress for privacy violations	Organizations should establish an appeal process to correct inaccurate data, particularly if an individual has been harmed or denied benefits due to the error. The volume and level of detail of data collection made possible through RFID technology may preclude individual access to *all* information linked to that individual, particularly if the information is distributed across multiple enterprises. Determining the appropriate balance between individual rights and the benefits that RFID technology conveys likely will generate considerable discussion which is beyond the scope of this document.
13	Authorization	Ensuring that the individual authorizes all new and secondary uses of personal information not previously identified on the original	Organizations should notify and seek authorization from users whenever there are significant changes in the planned use of personal data. However, as mentioned in the consent family above, the potential ways in which data collected using RFID technology

#	Federal CIO Council Control Family	Definition	RFID Considerations
		collection notice	can be combined to make inferences about an individual may not be readily understood by those individuals, which can complicate informed consent or authorization. Furthermore, it must be recognized that third parties may be able to surreptitiously read or recognize the presence of tags, and may use any information obtained for unknown purposes without authorization. Organizations that implement authorization systems to mitigate risks within their control should determine how authorizations will be obtained, authenticated, and stored prior to new uses of data.
14	Chain of Trust	Establishing and monitoring third-party agreements for the handling of personal information	If an organization contracts with a third-party to handle personal information, the third-party should be contractually obligated to comply with the organization's RFID usage, privacy, and IT security policies. In inter-enterprise RFID applications, such as those supporting supply chains, the MOU or MOA between participating organizations should include provisions for monitoring the agreements. These agreements are critical because in many cases the parties of the agreements may be unaware of how the other parties could potentially use the RFID system to manage PII. For example, a pharmaceutical company tags its products without any PII, but a pharmacy may later use the tag to associate the product with an individual account, thereby entering PII into the RFID system unknown to the manufacturer.
15	Risk Management	Assessing and managing risks to operations, assets, and individuals resulting from the collection, sharing, storing, transmitting, and use of personal information	Section 4 of this document describes the risks that arise with RFID systems, including privacy risk. Methods for the management of these risks are discussed in Sections 5, 6, and 7.
16	Reporting and Response	Providing senior managers and oversight officials the results of the monitoring and measuring of privacy controls and responding to privacy violations	The organization's privacy officer, legal counsel, and the operational managers of RFID systems should be included in the reporting of results and involved in responses to privacy violations.
17	Security Measures	Implementing the appropriate safeguards to assure confidentiality, integrity and availability of personal information	This document lists a number of potential security measures that can be employed to safeguard personal information. The appropriateness of these measures depends on the characteristics of the RFID technology and the nature of the business process it supports.

6.7 Industry Resources Addressing RFID Privacy

The EPCglobal *Guidelines on EPC for Consumer Products* are a set of principles that are intended to address the need for privacy and consumer trust (i.e., Consumer Notice, Consumer Choice, Consumer Education, and Record Use, Retention and Security). The Guidelines were created to provide a responsible basis for the use of EPC technology for consumer items. It is anticipated that these principles will continue to evolve with advances in EPCglobal technology and its applications. Additional

information on the *EPCglobal Guidelines on EPC for Consumer Products* and a *Frequently Asked Questions* document is provided on the EPCglobal Inc Web site at http://www.epcglobalinc.org/public/ppsc_guide/.

The Center for Democracy and Technology drafted *Privacy Best Practices for Deployment of RFID Technology*[77] as a stakeholder response to privacy challenges posed when personally identifiable information is involved.

6.8 Summary

Privacy considerations are interrelated with security considerations. A key objective of any RFID security program is to identify risks and controls for safeguarding PII. An organization implementing a security and privacy program for an RFID system should consult its privacy officer and legal counsel throughout the information system development life cycle.

A privacy program may protect different types of personal information. Some information is personally identifiable, meaning that someone can use it to identify a particular individual. Other information may not be personally identifiable, but individuals may still consider it private even in settings where they are anonymous. For example, an individual anonymously traveling on a public bus may not want other passengers to know what items are in her handbag.

Information that is not PII typically is not subject to legal requirements, but many people may still consider this information personal and worthy of safeguards. Therefore, organizations may still choose to implement privacy controls voluntarily to safeguard information its customers, business partners, employees, and other stakeholders consider personal.

Federal law governs Federal government agencies' collection and handling of PII. Relevant statutes include the Privacy Act of 1974, the E-Government Act of 2002, FISMA, and the Consolidated Appropriations Act of 2005. OMB memoranda provide policy guidance and instructions for agencies' implementation of these laws. The privacy of health information is covered by HIPAA, which applies to non-Federal as well as Federal entities.

The Federal CIO Council developed a list of privacy control families that provide a reference framework for those integrating privacy principles into RFID systems. In some cases, controls can serve to enhance both security and privacy. In other cases, the privacy controls complement security controls. Since RFID implementations are typically highly customized, the privacy controls listed are not always applicable or may not be effective for all RFID systems.

[77] Center for Democracy and Technology, "CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology," Interim Draft, May 1, 2006, http://www.cdt.org/privacy/20060501rfid-best-practices.php.

7. Recommended Practices

As explained in Sections 2 through 5, there are numerous ways to implement and configure RFID systems to support a wide variety of applications. RFID systems typically must be highly customized to support the business processes they automate; no one-size-fits-all approach will work across implementations. Nevertheless, organizations can benefit from following some general principles when using RFID technology. This section describes a set of recommended security practices that can help organizations manage RFID risks to an acceptable level.

To be most effective, RFID security controls should be incorporated throughout the entire life cycle – from policy development to operations. This section references a five-phase life cycle to help organizations determine the most appropriate actions to take at each point in the development of the RFID system. The life cycle is based on a model introduced in NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*. Organizations may follow a project management methodology or life cycle model that does not directly map to the phases presented here, but the types of tasks and their sequencing are probably similar. The phases of the life cycle are as follows:

- **Phase 1: Initiation**. This phase covers the tasks that an organization should perform before it starts to design its RFID system. These tasks include conducting a risk assessment and developing policy and requirements with which the RFID system must comply.
- **Phase 2: Acquisition/Development**. For the purposes of this guide, the acquisition/development phase is split into two sub-phases:
  - **Phase 2a: Planning and Design**. In this phase, RFID network architects specify the standards with which the RFID system must comply, the network infrastructure that will support the system, and the technical characteristics of the RFID system, including the types of tag and readers that will be deployed. This phase should also include site surveys of the facilities and relevant IT infrastructure.
  - **Phase 2b: Procurement**. In this phase, the organization specifies the RFID components that must be purchased, the feature sets and protocols they must support, and any standards on which they must be based.
- **Phase 3: Implementation**. In this phase, procured equipment is configured to meet operational and security requirements, RFID data is integrated with legacy enterprise systems, and staff are trained in the proper use and maintenance of the system.
- **Phase 4: Operations/Maintenance**. This phase includes security-related tasks that an organization should perform on an ongoing basis once the RFID system is operational, including conducting periodic security assessments, applying security-related software patches, and reviewing RFID event logs.
- **Phase 5**: **Disposition**. This phase encompasses tasks that occur when a system or its components have been retired, perhaps as a result of a significant upgrade. These tasks include preserving information to meet legal requirements and disabling or destroying tags and other components when they are taken out of service.

The practices presented in this section are provided in tables corresponding to the life cycle phases. Each practice is accompanied by a brief explanation of the rationale for its inclusion and is rated as "recommended" or "should consider." Organizations are strongly encouraged to adopt the "recommended" practices. Failure to implement them significantly increases the risk of an RFID security

failure. Organizations should also examine each of the "should consider" practices to determine their applicability to the target environment. A "should consider" practice should be rejected only if it is infeasible or if the reduction in risk from its implementation does not justify its cost.

Organizations should develop their RFID security controls based not only on the practices in the tables, but also using other guidelines on security controls. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, establishes three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system. NIST Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*, provides minimum management, operational, and technical security controls for information systems based on the FIPS Publication 199 impact categories. The information in NIST Special Publication 800-53 should be helpful to organizations in identifying controls that are needed to protect networks and systems, which should be used in addition to the specific practices for RFID systems listed in this document. Federal agencies should also use NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, to evaluate their RFID system and select appropriate security controls.

The RFID policies that an organization develops should be consistent with existing IT and operations policies. However, in some cases, the organization may need to modify the existing policies to accommodate the introduction of an RFID system.

Some large organizations may divide RFID-related duties among various teams. For example, one group may be responsible for the RF subsystem, while another might focus on the enterprise subsystem. To assist with this division of labor, the tables in this section identify the affected subsystem or components (e.g., tag or reader) for each of the listed practices.

The tables can also serve as checklists. In particular, the status column on the right is blank so that RFID support staff or auditors can use it to measure progress toward implementation of the practices.

Table 7-1. RFID Security Checklist: Initiation Phase

Initiation Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
1	Perform a risk assessment to understand RFID threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of the organization's assets.[78]	All risks should be considered, including the risk of RFID systems to other enterprise information systems and the risk that the existence of RFID will enable adversaries to collect information about an organization's activities that could adversely impact its ability to perform its mission. For supply chain applications, the risk assessment should consider threats that occur when the RFID tags are located outside the organization's control, such as when tagged items are in transit. The risk assessment is an important input to the development of the RFID usage policy because it identifies which RFID activities pose an acceptable risk to the organization's information resources and which do not. In particular, it can help determine which type of RFID technology may be appropriate for the desired application (e.g., active versus passive tags). The risk assessment should also determine whether the RFID system will collect, store, process or share PII or enable PII to be inferred through direct or indirect means. A complete privacy impact assessment should be conducted for any RFID systems involving PII.	ALL	Recommended	

[78] For more information on performing risk assessments, see G. Stoneburner, A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems.* NIST Special Publication 800-30, July 2002.

Initiation Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
2	Establish an RFID usage policy that specifies what assets should be tagged, who is authorized to use RFID technology, and for what business purposes this authorization applies.	An RFID usage policy is the foundation on which subsequent security controls are based. The policy should cover all components of the RFID system, including tags, readers, and support systems (e.g., middleware and analytic systems). The policy should distinguish between the levels of access provided to those that use the system, those that administer it, and those that need access to its data, including external business partners. For instance, logistics administrators may be granted the ability to modify a reader's configuration (duty cycle, power output, network settings, RF frequency settings, Transmission Control Protocol (TCP) ports, etc.) while operations personnel may only be able to scan tags. External parties should almost never get access to an organization's readers, but they might need read access to certain database elements. The policy should also address the collection and handling of sensor data that might be transmitted over the RFID system. The RFID usage policy should also integrate privacy policies and practices. All statements made in privacy compliance documentation should be reflected in and supported by the RFID usage policy.	ALL	Recommended	
3	Establish an RFID privacy policy.	Federal government agencies are required to create a Privacy Impact Assessment (PIA) if the RFID system will store or manage personal information. While privacy policy is not within the scope of this publication, the technical security controls that result from the policy are within the scope of the publication. For example, implementation of the privacy policy might require the use of the *kill* command or an alternative means to disable tags. Requirements related to data sharing limitations may need to be supported by certain authentication and access control methods. A privacy policy should be in place before RFID system architects determine the appropriate security controls.	ALL	Recommended	

Initiation Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
4	Establish HERF/HERO/HERP policies if applicable.	If the risk assessment identifies risks related to human health, fuel, ordnance, or other sensitive materials (e.g., pharmaceuticals) that are not fully mitigated by the RFID usage policy, then the organization should require additional controls to prevent the associated hazard from being realized. A separate policy is needed for each hazard type (HERF/HERO/HERP/other sensitive materials) because each one has distinct issues. Organizations facing these hazards should also consult safety and regulatory experts in this area to ensure their approaches are valid and comply with legally-mandated FCC exposure limits.[79]	RF Subsystem	Recommended	
5	Enhance the organization's information security policy to account for the presence of RFID systems.	The introduction of RFID technology represents a new challenge to the security of the enterprise network that should be mitigated by policy and associated technical, operational, and management controls. Elements of the network security policy that might require revision include (a) perimeter security (i.e., firewalls and extranets), (b) database security, (c) application security, and (d) wireless connections (i.e., between readers and the enterprise network). Typically a firewall separates readers from the enterprise network that hosts RFID database and application servers. Policies related to database and application security should cover authentication, access control, and development practices to reduce the likelihood of malicious code insertion, exploitation of buffer overflow vulnerabilities, and other attacks. In addition, if readers are connected to the enterprise infrastructure via a wireless link, then the policy should require mutual authentication between the reader and its network access point. It should also provide for data confidentiality and integrity services for wireless traffic, if needed.	ALL	Recommended	

[79] R. Cleveland Jr. and J. Ulcek," Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields," Federal Communications Commission Office of Engineering and Technology (OET), Washington, D.C., OET Bulletin 56, Fourth Edition, August 1999, pp. 11-16.

Initiation Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
6	Establish an RFID security and privacy training program for operators of the RFID system.	Many RFID risks are best mitigated when the personnel operating the system are aware of the risks and the associated countermeasures. The training program should cover the RFID usage policy and teach administrators and operators how to identify and report violations of the policy. If the system involves PII, operator training should explain how individuals and PII should be handled to sustain privacy protections. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, contains detailed guidelines on designing, developing, implementing, and monitoring an IT security awareness and training program.[80]	ALL	Should Consider	

Table 7-2. RFID Security Checklist: Planning and Design Phase

Planning and Design Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
7	Identify the RFID standards with which the RFID system will comply.	The selected RFID standards in effect determine the types of tags that will be deployed and the operating frequencies on which RF subsystem communication will occur. The standards also specify the available technical security mechanisms. For instance, some tags support passwords while others do not. An organization may also choose a standard to support a particular operating frequency to avoid unwanted RF interference, improve performance, and reduce technical problems. The choice of operating frequency is often closely associated with relevant regulations and the application area (e.g., healthcare, supply chain, security access control, and animal tracking).	RF Subsystem	Recommended	
8	Include security and privacy considerations in RFID system investment and budget requests.	Including security and privacy planning in funding plans ensures that adequate resources are available for implementation of appropriate controls. Including these considerations in budget planning and analysis also increases the likelihood that cost-effective approaches will be selected to mitigate risk. Budget requests should also demonstrate that plans for the RFID system are consistent with the information technology architecture of the implementing organization.	ALL	Recommended	

[80] M. Wilson and J. Hash, *Building an Information Technology Security Awareness and Training Program*. NIST Special Publication 800-50, October 2003.

Planning and Design Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
9	Conduct a site survey to determine the proper location of readers and other devices given a desired coverage area.	The estimated usable range of readers and tags should not extend beyond the physical boundaries of the facility whenever possible. The survey should note the location of metal or reflective objects and RF absorbing materials such as water that have the potential to adversely affect the operation of the RFID system. The site survey should also identify potential radio interference between the RFID system and other RF sources at the site or in neighboring facilities.	RF Subsystem	Recommended	
10	Determine approach to RF emissions control.	The approach should be based on the risk assessment and site survey. In many cases, physical security may offer the best mechanism to protect against unauthorized use of RFID technology, including attacks involving reader spoofing and jamming, modification of tag data, and eavesdropping. When this is not possible, countermeasures such as shielding and adjusting the power level of the reader may be employed. The selected approach might involve the location of readers and tagged assets, the placement of blocker devices, the power levels at which RF components operate, and the potential need for additional perimeter security (e.g., fences around warehouses).	RF Subsystem	Recommended	
11	Identify an approach to securing network management traffic, using dedicated networks and encryption when feasible.	If network management traffic is left unprotected, adversaries might be able to breach the RFID system, enabling a number of subsequent attacks, including those that could disable the system or compromise confidential data. The approach to securing network management traffic depends largely on the technical architecture. If network management occurs over Web interfaces, then Secure Sockets Layer (SSL) or Transport Layer Security (TLS) should be employed. In some cases, devices such as readers will be managed using SNMP. In these cases, SNMP version 3 is the preferred protocol, and community strings should be changed from defaults to complex character strings (i.e., mix of upper and lower case, both alphabetic and numeric characters).	Enterprise Subsystem and Readers	Recommended	

Planning and Design Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
12	Design a network firewall between the RF subsystem and the enterprise network.[81]	A firewall can enforce a security policy on the information flow between the RF subsystem and any attached network, allowing only authorized protocols and services to traverse this boundary, such as those needed for readers to communicate with middleware servers and for management consoles to monitor and configure readers. This configuration limits the ability of an adversary that compromises RFID equipment to exploit vulnerabilities on non-RFID systems that also reside on the network. Appropriate firewall placement depends on the network architecture. For example, if middleware is integrated into the switches to which the readers connect, the firewall may be included in the switch or may reside between the middleware and the enterprise network. On the other hand, if middleware servers are located inside an enterprise network (e.g., at a remote data center), then the firewall may reside between the readers and the middleware.	Enterprise Subsystem	Should Consider	
13	Develop RFID audit processes and procedures that identify the types of security relevant events that should be captured, and determine how audit records will be securely stored for subsequent analysis.	Audit records are necessary for forensic analysis of security and privacy incidents and also support real-time intrusion detection capabilities in many cases. The audit procedures should be reviewed for privacy protection considerations to determine if audit records contain or could be used to create PII. Ideally, audit data should be forwarded to a dedicated audit server that can preserve the integrity of event logs even when other RFID system components have been compromised. To facilitate implementation and compliance, existing audit processes and procedures for other enterprise information systems should be leveraged whenever appropriate. Events to be captured should include, at a minimum, unsuccessful authentication attempts.	Enterprise Subsystem and Readers	Recommended	
14	Develop a password management system for tags that support password-protected features.	The password management system should specify how passwords are generated, assigned, stored, shared, and discarded. Passwords should be randomly generated. When passwords are written to tags using over-the-air mechanisms, additional care should be taken to avoid eavesdropping. When passwords are stored in enterprise databases, the databases have authentication and access control mechanisms to prevent unauthorized reading of the passwords. MOUs and MOAs with external organizations should cover roles and responsibilities related to the handling of passwords.	Tags	Recommended	

[81] For more information on network firewalls, see J. Wack, K. Cutler, and J. Pole, *Guidelines on Firewalls and Firewall Policy*. NIST Special Publication 800-41, January 2002.

Planning and Design Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
15	Determine approach to tag memory protection, if applicable.	Important considerations include what data elements require read or write protection and whether write protection for certain elements must be permanent. In some applications, the tag identifier may be modifiable while in others it must be permanently fixed.	Tags	Recommended	

Table 7-3. RFID Security Checklist: Procurement Phase

Procurement Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
16	Procure products that use FIPS-validated cryptographic modules.[82]	Federal agencies are required to use FIPS-validated cryptographic modules. Cryptographic modules that are not FIPS-validated cannot be assured of providing the level of cryptographic protection intended. Identify all expected uses of cryptography, including those that will be used to secure data traffic in the enterprise subsystem. Significant resource constraints on tags preclude the use of cryptography for many applications, but if an organization decides that the additional expense of cryptography is required to protect sensitive information, then the corresponding cryptographic modules must be FIPS-validated.	ALL	Recommended	
17	Procure products that are functionally capable of supporting the organization's security and privacy policy.	If a product that does not support the security and privacy policy is deployed, non-compliance is guaranteed. For example, if the RFID usage policy requires data confidentiality between the reader and the enterprise subsystem, then the readers need to support appropriate cryptographic services on their enterprise interface. In general, tags do not have cryptographic data functionality, but data encrypted elsewhere can be stored on a tag if it has sufficient capacity, which typically is the case for active tags only. If a requirement exists to read or write protect certain data elements on a tag, then the organization should procure tags that support the desired memory access protections.	ALL	Recommended	

[82] The following reference provides a list of FIPS-validated cryptographic modules: National Institute of Standards and Technology, "Cryptographic Standards and Validation Programs at NIST," December 19, 2006, http://csrc.nist.gov/cryptval/.

Procurement Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
18	Procure readers, middleware, and analytic systems that log security relevant events and forward them to a remote audit server.	Audit technology helps ensure that the organization can detect unauthorized behavior and take actions to prevent or limit the extent of a security breach. If software components do not support audit event forwarding, then the organization should ensure that the supporting operating systems do so. At a minimum, the events should contain the tag ID, reader ID, and the reader timestamp for security relevant events.	Readers and Enterprise Subsystem	Recommended	
19	Procure readers and server platforms that support the selected approach to securing network management traffic.	The network management architecture only can be implemented if the selected products support it. Potential protocols include SNMP version 3 or the encapsulation of management traffic within SSL/TLS or Internet Protocol Security (IPsec) tunnels.	Readers and Enterprise Subsystem	Recommended	
20	Procure readers and server platforms that support Network Time Protocol (NTP).	NTP allows distributed devices to synchronize timestamps, which is critical to effective log analysis because it allows audit personnel to establish accurate event sequences across multiple devices. Many applications also need to obtain very accurate measurements of the time elapsed between transactions.	Readers and Enterprise Subsystem	Recommended	
21	Procure an auditing tool to automate the review of RFID audit data.	Audit tools often are more effective than humans at distilling relevant information from multiple sources. In large enterprise RFID deployments, reviewing the amount of data generated could overwhelm technical support staff if they do not have appropriate tools to assist them with this task.	Enterprise Subsystem	Should Consider	
22	Procure readers that can be upgraded easily in software or firmware.	This capability enables the readers to receive security patches and enhancements released after product shipment.	Readers	Recommended	

Table 7-4. RFID Security Checklist: Implementation Phase

Implementation Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
23	Harden all platforms supporting RFID components (e.g., middleware, analytic systems and database servers).	Organizations should apply secure operating system and database configurations to all relevant hosts. See other NIST guidelines for recommended configuration information.[83]	Enterprise Subsystem	Recommended	
24	Ensure that readers that support user authentication have strong, unique administrative passwords.	To protect against dictionary attacks, administrator passwords on readers should not be easy to guess.	Readers	Recommended	
25	Secure wireless interfaces on readers.	If the reader is mobile, it likely will have a second wireless interface to connect to the enterprise subsystem. In this case, the second interface should have a secure configuration.[84]	Readers	Recommended	
26	Assign unique passwords to tags.	When tags support passwords, organizations should not use a common password for multiple tags. Otherwise, a compromised password on one tag could have much wider consequences. Managing unique passwords requires the implementing organization to maintain a password database and support remote queries of the database, which might not be feasible in all environments.	Tags	Should Consider	
27	Lock tag memory.	The organization should lock tag memory to meet business and security requirements as determined in the planning and design phase.	Tags	Recommended	

[83] The NIST Security Configuration Checklists Program for IT Products contains a repository of checklists for securing various operating systems and applications. Additional information may be obtained at http://checklists.nist.gov/.

[84] For more information on how to secure common wireless protocols, see T. Karygiannis and L. Owens, *Wireless Network Security: 802.11, Bluetooth and handheld devices*. NIST Special Publication 800-48, November 2002) and S. Frankel, B. Eydt, L. Owens, and K. Scarfone, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST Special Publication 800-97, February 2007).

Implementation Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
28	Disable all insecure and unused management protocols on readers and enterprise subsystem components. Configure remaining management protocols for least privilege.	Disabling all insecure and nonessential management protocols eliminates potential methods that an adversary can use when attempting to compromise a host. Examples of insecure management protocols include SNMP version 1 and SNMP version 2. If SNMP version 3 is used, configure it for least privilege (i.e., read only) unless write access is required (e.g., to change configuration settings as part of an automated incident response procedure).	ALL	Recommended	
29	Activate logging and direct log entries to a remote audit server.	Logs enable security and support staff to identify potential security issues and respond accordingly. Using a remote central logging server facilitates reviews of logs across the enterprise and ensures the integrity of log data when RFID components are compromised.	Readers and Enterprise Subsystem	Should Consider	
30	If applicable, initiate a HERF/HERO/HERP compliance program to include operator training, posting of notices, and application of labels to sensitive materials.	If personnel are reminded of risks to their safety, they are more likely to engage in behavior that will prevent the realization of those risks. The compliance program should comply with Occupational Health and Safety Administration (OSHA) regulations regarding workplace safety.[85] Notices should appear in the same or comparable locations as other OSHA notices.	RF Subsystem	Recommended	

Table 7-5. RFID Security Checklist: Operations/Maintenance Phase

Operations/Maintenance Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
31	Test and deploy software patches and upgrades on a regular basis.[86]	Newly discovered security vulnerabilities of vendor products should be patched to prevent inadvertent and malicious exploits. Patches should also be tested before implementation to ensure that they work properly.	ALL	Recommended	

[85] 29 CFR § 1910.97. Nonionizing radiation.

[86] For more information on patching, see P. Mell, T. Bergeron, and D. Henning, *Creating a Patch and Vulnerability Management Program*. NIST Special Publication 800-40, Version 2.0, November 2005.

Operations/Maintenance Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
32	Review audit logs frequently.	Frequent reviews of audit logs allow security and support personnel to identify security issues and take corrective or preventative measures quickly. All components of the RFID system should generate event logs. Automated logging tools can assist with log review and send real time alerts in response to critical events, such as repeated failed authentication attempts during a short time period. RFID middleware products often provide advanced audit capabilities, including "dashboards" that allow administrators to monitor the activities of readers in real time.[87]	ALL	Recommended	
33	Perform comprehensive RFID security assessments at regular and/or random intervals.	Security assessments, or audits, are an essential tool for checking the security posture of an RFID system and identifying corrective actions necessary to maintain acceptable levels of security. The assessments should include monitoring of the RF spectrum to determine potential sources of RF interference and to identify ongoing surveillance or attacks. The assessment should also verify configuration settings on all RFID components.	ALL	Recommended	
34	Designate an individual or group to track RFID product vulnerabilities and wireless security trends.	Assigning responsibility to an individual for tracking wireless security issues helps ensure continued secure implementation of the organization's RFID systems.	ALL	Should Consider	

[87] For additional information on log management, see K. Kent and M. Souppaya, *Guide to Computer Security Log Management*. NIST Special Publication 800-92, September 2006.

Table 7-6. RFID Security Checklist: Disposition Phase

Disposition Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
35	When disposing of tags, disable or destroy them.	The appropriate disposal or destruction mechanism depends on the type of tag, the level of assurance required, and the cost of the destruction. When tags contain memory, this memory should be rendered inaccessible. Options include the *kill* command and physical destruction. Many tags can be rendered inoperable by cutting them with a box knife, scissors, or other sharp object. The antenna on some tags can be separated from their transmitters by tearing them by hand, although accessing the tag data is still possible through physical analysis. Even if a tag contains nothing but an identifier, destruction may be advisable if there is the potential for an adversary with knowledge of the tag encoding protocol to correlate the identifier with other information, such as tag ownership. This attack is particularly salient for EPCglobal tags, because of the potential to discern the identity of the EPC Manager from the pointers returned by the Root ONS. In many cases, the tag identifier also reveals the serial number of the asset. On the other hand, many organizations may determine that that this risk is acceptable, especially if database records corresponding to a particular identifier are erased or disabled when the tag is no longer needed.	Tags	Should Consider	
36	When disposing of an RFID component, ensure that its audit records are retained or destroyed as needed to meet legal or other requirements.	Information contained in the audit records may be needed even after an RFID component is discarded (e.g., for an investigation of a subsequently discovered security breach). Organizations should identify the legal requirements for data retention that apply to their operations.[88] When log events are forwarded to a central audit server, regular backup of the server facilitates the retention of records. When a log server does not exist, the disposal process may include capturing the existing log data and storing it on alternative media, such as CD-ROM or tape. On the other hand, retention of audit records may raise a privacy concern in some applications. For example, records may reveal sensitive personal information or associate a person with particular items or transactions in a manner that violates privacy laws or policy. In these cases, the requirement may be to destroy the records after a certain period of time or after they are no longer needed.	ALL	Recommended	

[88] For an example of a requirements document, see National Archives and Records Administration, "General Records Schedule 24, Information Technology Operations and Management Records," April 2003, http://www.archives.gov/records-mgmt/ardor/grs24.html.

Disposition Phase					
#	Security Practice	Rationale / Discussion	Affected Components	Recommended or Should Consider	Checklist Status
37	Recycle retired tags.	In some cases, recycling may involve putting the tags back into service. This type of recycling is not recommended when tag memory contains confidential data, but may be cost effective otherwise. Recycling may also involve using discarded tag material for other purposes in a similar manner to recycling programs for household plastics and metals. Both forms of recycling address a concern about the environmental impact of large scale consumer and industrial uses of tags.	Tags	Should Consider	

This page has been left blank intentionally.

8. Case Studies

This section presents two hypothetical case studies to illustrate how RFID security might be implemented in practice. Although the case studies are fictional, they are intended to resemble real-world activities, including how decision makers address common and expected RFID security problems and their solutions. The case studies do not cover *all* of the aspects of RFID system engineering or operations that an organization may encounter in its RFID implementation, but rather a representative sample of salient issues. The two case studies are as follows:

- Case Study #1: Personnel and asset tracking in a health care environment, and
- Case Study #2: Supply chain management of hazardous materials.

In each case study, the fictional organization followed the information system development life cycle introduced in NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, and the practices discussed in Section 7.

8.1 Case Study #1: Personnel and Asset Tracking in a Health Care Environment

The Contagion Research Center (CRC) is a health care facility dedicated to the study of highly contagious diseases—those transmitted through casual human contact. The Center has 40 beds for patient care, a radiology unit with two rooms of sophisticated imaging equipment, and four laboratories with various diagnostic and research capabilities. The Center confronts the same management issues as many hospitals, including locating portable diagnostic equipment when needed and accounting for missing assets. Another important concern is the ability to quickly locate patients and staff as they move about the facility. Poor asset management results in higher costs, reduced efficiency, and lower quality of care.

The mission of the CRC also leads to specialized requirements. To prevent unnecessary outbreaks of disease and to understand how transmission occurs, CRC needs to track the interactions among its staff, patients, and visitors. These tracked interactions provide useful information to researchers about who came into contact with whom and at what time. Additionally, CRC must alert caregivers of disease-specific protocols when they are in close proximity to particular patients, including prohibiting staff contact in some cases. It must track blood, urine, and stool samples from patient to laboratory. Finally, CRC would like to track the history of in-house diagnostic equipment and trace how the equipment is used to support patients throughout each day. Currently, paper processes are used to achieve these objectives, but they are very labor-intensive and error-prone, sometimes with fatal consequences.

CRC executives tasked the CRC's Chief Information Officer (CIO) to use RFID technology to improve the CRC's traditional asset management function, as well as meet its specialized requirements. Working with the CRC executives, the CIO commissioned a project to reengineer CRC business practices using RFID technology as a primary tool to improve organizational performance.

8.1.1 Phase 1: Initiation

The first step in the project was to conduct a risk assessment to help shape the final scope of the project and identify the most appropriate uses of the RFID technology, as well as potential controls to mitigate the accompanying risk. Some risks identified during the assessment were as follows:

- RFID systems could open a "backdoor" to the CRC computer network, which could result in the compromise of mission-critical systems and research archives.

- Anyone eavesdropping on RFID transactions could compromise the privacy of patient medical records.
- The CRC could be held liable for violations of the privacy provisions of Health Insurance Portability and Accountability Act (HIPAA).
- The radio frequencies used by the RFID system could interfere with wireless patient sensors and medical telemetry devices, which could impact quality of care and research results.
- Dermal contact with RFID tags might be a potential vector for the transmission of some highly contagious diseases.

The risk assessment also concluded that some RFID risks were minimal or nonexistent in the CRC environment. The worst case for expected patient and staff exposure to RF radiation was forecasted to be significantly below any level that might adversely affect their health. CRC already had a well-enforced policy that prohibits the storage of fuel or ordnance at the facility, and the use of potentially explosive material such as ether and oxygen tanks was tightly controlled. The likelihood that an adversary would attempt to use the CRC RFID system to gather intelligence or target personnel was deemed negligible.

As a result of the risk assessment, the CRC enhanced its network security policy to require that the RFID system be separated from other network systems using a firewall that permits only required data and management traffic to traverse the network boundary. The network security policy also was amended to require user authentication to all non-stationary RFID readers and encryption of wireless traffic between mobile readers and access points. Existing policy regarding secure server configurations and least privilege[89] data access would extend to the RFID systems without requiring any modifications. The CRC also decided that it would not institute a new requirement for wireless intrusion detection, but it would revisit this decision during the following fiscal year.

The CRC also conducted a privacy assessment based on information collected during the risk assessment. As a result, the CRC privacy policy was revised to account for the introduction of RFID technology. The revision noted that any patient data collected by the RFID system would be subject to the CRC's internal procedures implementing HIPAA regulations. A final determination was made to update patient release forms to include a statement that inherent risks exist with wireless communications and that network security controls were implemented to help mitigate these risks.

Based on the project charter and the updated security and privacy policies, the CIO led an interdisciplinary team of medical practitioners and information technology professionals to develop the business and functional requirements for the RFID system. These requirements formed the basis for the phases of the project that followed.

8.1.2 Phase 2: Acquisition/Development

The acquisition and design phase of the project involved planning the RFID system. One design decision was to select the tag type for each application. Many of the items to be tracked, including laboratory samples and disposable supplies, were numerous and would be scanned at very close ranges (within 10 centimeters). For these items, passive tags made the most sense, given their low cost. People, high-value assets, and mobile equipment such as carts, gurneys, and wheelchairs needed to be tracked as they moved around the facility. The readable range for these applications needed to be at least a few meters. The team considered active tags, but worried that they could cause interference problems when located in the radiology unit. Accordingly, they selected semi-active tags, which are less likely to emit radiation

[89] The principle of least privilege in computer security refers to the concept of granting each user and each module of a system only the necessary resources to perform authorized actions.

inadvertently and which have a considerably longer battery life than active tags, but which still have effective operating ranges within CRC's requirements.

The next step was to plan the location of the stationary readers and the frequencies at which they would operate. In preparation for this exercise, CRC had qualified individuals perform a site survey, which recommended locations for the readers and identified existing spectrum utilization within the facility. They found that patient sensors and medical telemetry devices were operating at low frequencies (125 kHz) and at ultra high frequency ranges (915 MHz). Frequencies throughout and above the radio spectrum were identified in the radiology unit. Based on this information, the design team determined that the passive RFID system would operate in the high frequency range (13.56 MHz), and the semi-active RFID system would operate at microwave frequencies (2.45 GHz).

While the risk of eavesdropping from locations outside the facility was considered to be very low, the design team still thought it would be of value to mitigate the risk to the greatest extent feasible. Therefore, they ensured that design drawings placed readers away from windows and exterior walls. Preferred locations were over doorways in rooms and on ceiling mounts in hallways. The devices would be prohibited in the radiology unit, but would be placed at entries to the unit. Previously installed shielding in the walls would prevent emissions from impacting the operation of the imaging equipment inside the unit.

The design team determined that stationary readers would be connected to the RFID middleware infrastructure using Ethernet, which is also used to network the desktop computers and servers in the building. To accomplish this, the plan called for the installation of additional network cabling and drops, and use of the existing Ethernet switches, which had considerable excess capacity. Having the RFID systems, desktops, and servers all cabled into the same switches created a risk that the RFID system could be used as a platform to launch an attack on the rest of the network. To mitigate this risk, the design called for a dedicated VLAN to host the RFID-related network hosts. Traffic could only pass from the RFID VLAN to other network segments if it traversed the network firewall required by policy in the initiation phase.

Once the architecture was completed, the CIO assigned two members of the design team to the job of procuring the system with her review and approval. They paid particular attention to the products' audit and management capabilities. Four vendors provided demonstrations of their products and submitted bids.

8.1.3 Phase 3: Implementation

The various components of the system arrived over a three-week period following the procurement effort. The implementation team followed the CRC secure configuration guidelines when building all the servers hosting RFID enterprise software and databases. The implementation team configured all the audit events and alerts on the RFID systems to be directed to a CRC audit server cluster that supports all of the CRC IT infrastructure. They also ran a vulnerability scan on all hosts after the installation to identify remaining weaknesses. Approximately a dozen minor issues were discovered and quickly resolved, mostly through the application of software patches. The last step in preparing the infrastructure was to configure the firewall traffic filters and VLAN architecture specified during the acquisition/development phase.

Applying tags to all the items within the scope of the project was a challenging and time-consuming task. When possible, tags were positioned on items in such a way as to minimize the probability of tampering, destruction, or removal. They were also placed where patients are unlikely to experience dermal or respiratory contact, therefore reducing the probability that a tag's surface could ever be a mechanism for

the spread of disease. Tags on patients were embedded in hospital admission wrist bracelets. Tags for staff and hospital personnel were embedded in their hospital identification cards, which are typically worn around the neck on a lanyard or on a retractable leash attached to the belt.

8.1.4 Phase 4: Operations/Maintenance

The operation of the new systems proceeded as expected. CRC experienced a reduction in asset losses resulting from better tracking and some personnel mentioned that the system significantly reduced paperwork. The system also provided benefits to CRC research. In one case, patients in separate rooms under the supervision of different medical teams contracted a particular illness. These facts initially led the CRC epidemiologists to believe that an airborne pathogen caused the disease. Subsequent analysis of the RFID data showed that a medicine cart handled by several nurses' aides was the likely infection vector by transferring the disease from patient to patient through dermal contact.

The operations phase also included the management of the RFID system. Hospital IT personnel received pages when systems were malfunctioning and took corrective actions as necessary. Recently, audit records showing excessive numbers of malformed read transactions led to the detection of an unauthorized radio in the proximity of one of the readers.

8.1.5 Phase 5: Disposition

The new RFID system has not been in operation long enough to encounter significant disposition issues, but the CRC has instituted procedures for the disposal of RFID tags. The passive tags on disposable items are discarded along with the item. In the case of tags on blood, urine, and stool samples, the tags are disposed as hazardous medical waste. Semi-active tags on patients are disposed of as medical waste upon death or discharge. Data did not need to be removed from the tags prior to disposal because the tags only stored an identifier. Semi-active tags on physical assets are reassigned when the asset is retired. If a tag is malfunctioning, it is physically disabled to ensure inoperability and discarded with office waste.

8.1.6 Summary and Evaluation

The system involving read-only passive and semi-active tags is helping reduce costs and improve research. Security risks were identified early, and risks were managed to an acceptable level. Table 8-1 presents a summary of how each risk identified in the risk assessment was subsequently addressed.

Table 8-1. CRC Risk Management Strategy

Risk	Mitigation Approach
Exploitation of "backdoor" to IT network	• Stationary readers kept away from windows and exterior walls • VLAN isolates RFID network from other network segments • Network firewall restricts traffic to/from RFID network • Servers hosting RFID middleware, analytic systems, and databases are built with secure configurations • RFID audit events are sent to centralized audit server that is continuously monitored by operations personnel
Compromise of patient information confidentiality	• Stationary readers kept away from windows and exterior walls
Radio interference with diagnostic sensors and equipment	• 13.56 MHz frequency selected to minimize interference with other devices

Risk	Mitigation Approach
Spread of disease	• Tag placement minimizes chances of dermal or respiratory contact • Tags in contact with patient or lab samples are discarded as medical waste

8.2 Case Study #2: Supply Chain Management of Hazardous Materials

The Radionuclide Transportation Agency (RTA) oversees the movement of radioactive research materials between production facilities, national laboratories, military installations, and other relevant locations. The RTA oversight of the supply chain for these materials involves many of the same issues as in most any other supply chain. The agency wants to know who is in possession of what quantity of materials at any given time. It also wants to locate materials at a site quickly, without having to search through numerous containers to find them. Bar code technology does not provide that capability.

Some of RTA's requirements are more unique. For instance, much of the transported radionuclide material must be closely monitored because extreme temperatures or excessive vibration can make it useless for its intended applications. Consequently, RTA wants temperature and vibration sensors to continuously measure environmental conditions and record readings on the tag. Additionally, the handling of RTA-regulated materials is a homeland and national security issue. If the materials were to fall into unauthorized hands, they could endanger the public welfare.

8.2.1 Phase 1: Initiation

The project team began with a risk assessment, which identified a number of concerns, the most significant of which were as follows:

- An adversary could identify and target a vehicle containing RTA-regulated material.
- An adversary could eavesdrop on tag transactions to learn the characteristics of the material, which could help determine whether it is worth stealing.
- An adversary could damage or disable a tag, making it easier to steal material without detection.
- An adversary could alter sensor or manifest data stored on the tag in an effort to undermine the business processes for which the material is being used.
- The radiation from readers could accidentally cause combustion of collocated volatile materials when several of them are operating concurrently in close proximity.

To help address the risks, RTA established a policy that required that tagged items only be identifiable during embarkation, debarkation, and storage, but not during transport. The policy further stated that tag-reader communication should be authenticated whenever technically feasible with commercial-off-the-shelf systems. The RTA conducted a privacy assessment that identified that the system would handle PII due to the need to associate materials with particular individuals, although most such information was already contained in existing logs. The agency updated its privacy disclosure statement for employees and contractors to account for the new technology. Finally, it required that all personnel involved in handling of the tagged materials be provided RFID security and privacy awareness training. The agency already had a HERF policy, but everyone agreed the introduction of the RFID system would require the agency to revisit the efficacy of these HERF-related controls.

8.2.2 Phase 2: Acquisition/Development

The acquisition/development phase focused on the planning and design of the RFID system. The nature of the supply chain was such that tagged items would be located at numerous facilities, including future facilities not yet known at time the design was created. However, some general parameters were known. For instance, readers would need to read tags from distances up to 10 meters, and this capability is typically only found in active tags.

The design team spent a significant amount of time on how to mitigate risks associated with the RF link between the readers and the tags. It determined that the risk of eavesdropping and rogue RFID transactions could be within acceptable levels if adversaries were located at least 100 meters from the storage area.[90] The few facilities that could not maintain a perimeter of that distance would rely on bar code technology, which RTA understood would significantly increase labor costs at these sites relative to those using RFID because people would need to be hired to scan items and open containers to inventory their contents.

To address the requirement of preventing readings during transport, the design team specified mechanisms for shielding containers and vehicles. The shielding would prevent adversaries from determining that items inside a vehicle were tagged, thereby reducing the risk of targeting. In the case of shielded transport vehicles, tags could be read when they were removed from the vehicle at debarkation. Many vehicles were shielded prior to the RFID program to prevent harmful radiation from escaping the vehicle. When vehicles were not shielded, tarp-like shielding could be placed around containers within the vehicle and then easily removed when they leave the vehicle. While some users would benefit from the convenience of reading tags from outside the vehicle, the risk this introduced outweighed any potential advantage it offered. Indeed, the primary objectives of the RFID system were to identify the facility at which a radionuclide sample was located and to quickly find items once stored, neither of which necessitated readings when the item was in transport.

The tags were also password-protected using a proprietary technology to prevent unauthorized parties from reading or writing to the tags. Because custody of the tags moved from one organization to another, the RTA decided to host a central password database that could be remotely accessed by the RFID middleware of each participating organization. To limit access to the central database to business partners, it was placed on a VPN called RTAnet to which each of the partner organizations connected. The VPN isolates the RFID activity from public networks, thereby making it difficult for an outside adversary to perform a successful attack.

The team also had to tackle the HERF risk. Although the probability was small that readers would cause combustion of volatile materials stored near radionuclide material, the devastating consequences of its realization still made it a significant concern. The primary mechanism was to use an HF system because it would be less likely to cause combustion than higher frequency UHF and microwave technology. New guidelines also required a separation of five meters between fuel and tagged items unless the volatile materials were shielded.

8.2.3 Phase 3: Implementation

The implementation phase was straightforward, given the extensive planning in the previous phase. The first task was to conduct a pilot test of the system to identify potential problems before they adversely impacted the full supply chain. The test exercise uncovered several interoperability issues with RTAnet

[90] The risk was determined by field tests to be acceptable because the 100 meter distance was shown to prevent eavesdropping of tag to reader communications.

devices. In particular, some of the readers did not work properly with the middleware because an undocumented feature conflicted with the settings RTA selected for its equipment. The vendor issued a patch to its software that solved the problem.

8.2.4 Phase 4: Operations/Maintenance

Once the system was fully operational, the RTA was able to obtain regulatory information more quickly than before, which reduced the labor time required to support the program. Suppliers and consumers of the regulated materials also decreased their paperwork. They also were able to better match supply of materials with demand for them, since authorized organizations could retrieve information about the quantities present at each site.

The operations phase also included security monitoring. All participating organizations signed a MOU that covered sharing of information pertaining to possible intrusions or security exploits and proper management of PII. The MOU also included a provision that prohibited participating organizations from using PII for any purpose not explicitly stated in the MOU. This close cooperation enabled one of the suppliers and a national laboratory to recognize a recurring attack pattern across facilities that might otherwise have been ignored.

8.2.5 Phase 5: Disposition

As a new program, RTA has not actively confronted disposition issues. It plans to instruct participating organizations to retire their RFID systems as they would any other system holding data that RTA deems sensitive. In most cases this involves using disk wiping utilities to delete sensitive files. With regard to tag disposition, RTA's position is that organizations are free to recycle tags so long as they clear sensor and manifest data before affixing a tag to a new item.

8.2.6 Summary and Evaluation

The RTA RFID initiative allowed the agency to exercise more effective oversight of the transportation of radionuclide material while also reducing the regulatory compliance cost of impacted organizations. Some important security concerns had been raised, particularly with regards to the possibility that an adversary might use the RFID tags as targeting devices. Early identification of these risks allowed them to be managed during each stage of the systems. A listing of the main risks and the corresponding mitigation approach is presented in Table 8-2.

Table 8-2. RTA Risk Management Strategy

Risk	Mitigation Approach
Targeting of transport vehicles	• Shielding of vehicles and containers to prevent electromagnetic emissions
Eavesdropping to gather intelligence	• Physical facility perimeter at least 100 meters from storage locations
Disabling tags to allow material movement to go undetected	• Shielding during transport • Physical access controls
Altering sensor or manifest data stored on the tag to undermine mission	• Shielding during transport • Physical access controls • Password-based authentication for write transactions

Risk	Mitigation Approach
Combustion of collocated volatile materials	• Use of less risk-prone radio frequency (i.e., HF) • Five meter separation between tags and volatile materials

Appendix A—RFID Standards and Security Mechanisms

RFID readers and tags must conform to the same standards and designs to be interoperable. These standards and designs also can be used to coordinate the use of certain tags across multiple enterprises and in the supply chain. Common standards and designs may facilitate training, future equipment procurement, and equipment upgrades. Some readers and some tags can operate using multiple standards. This appendix describes international and industrial standards for RFID systems, as well as security mechanisms used in those standards. It also discusses regulations for frequencies used by various RFID standards and non-standard implementations. For the updates on the status of any particular standard, readers should refer to the standard body's official Web site.

A.1 International Standards

RFID standards have been developed by national and international standards groups such as the ISO and the IEC. There are separate standards for contactless smart cards and for item management.

ISO/IEC 14443 and ISO/IEC 15693 are the most popular smart card standards.

- ISO/IEC 14443 describes proximity smart cards which have an intermediate range up to 10 cm and operate at 13.56 MHz. The standard contains four parts: (1) physical characteristics, (2) radio frequency power and signaling, (3) initialization and anti-collision, and (4) transmission protocols. ISO/IEC 14443 has two variants known as ISO/IEC 14443A and ISO/IEC 14443B which have different communications interfaces. Readers that are ISO/IEC 14443 compliant must be able to communicate using ISO/IEC 14443A and ISO/IEC 14443B. ISO/IEC 14443A parts 1 through 4 are used in the DoD Common Access Card (CAC), which serves as an identification card. The CAC has a FIPS-approved algorithm.
- ISO/IEC 15693 operates at 13.56 MHz and describes vicinity smart cards which can be read from a farther distance than proximity cards. Such cards have a range of up to approximately 1 meter.

ISO/IEC 18000 is an RFID standard for item management and describes the air interface for various frequencies. Each standard within the ISO/IEC 18000 family defines communications parameters and applies to a specific electromagnetic frequency. ISO/IEC 18000-1 covers general parameters, and ISO/IEC 18000-2 through 18000-7 cover specifics for particular frequency ranges.

- ISO/IEC 18000-2 covers frequencies below 135 kHz. It has two types, A (Full Duplex) and B (Half Duplex). These types are different on the physical layer. A full duplex tag can communicate with a reader while the reader is simultaneously communicating with the tag. A half duplex tag supports bi-directional communication with a reader but only one device, the tag or the reader, can communicate at the same time.
- ISO/IEC 18000-3 covers frequencies operating at 13.56 MHz and describes two non-interfering and not interoperable modes of operation. Users are recommended to use just one mode for any single application. Both modes use a 64-bit identifier.
  - Mode 1 has a locking feature that is not protected by a password. If the tag receives the *lock* command, it locks the corresponding area of memory permanently. *Lock* can be applied selectively to different blocks of memory.
  - Mode 2 has a 48-bit password used to protect memory access. The tag can be configured to require or not require this password. If required, then *read* and *write* commands will require the reader to issue the correct 48-bit password. The lock command can be used to

permanently write protect a block of memory. Mode 2 also has a 16-bit lock pointer which is located in unaddressable memory. The lock pointer points to a word in memory. All complete blocks of memory at addresses less than the number stored in the lock pointer cannot be overwritten.

- ISO/IEC 18000-4 covers systems operating at 2.45 GHz. This standard has two modes: a passive tag reader-talks-first mode and a battery assisted tag-talks-first mode.
- ISO/IEC 18000-5 was developed for 5.8 GHz operation but this standard was withdrawn.
- ISO/IEC 18000-6 defines three types of tags. Types A and B operate at 860 to 930 MHz, but they use different encoding and anti-collision methods on the forward channel. Type C is equivalent to the EPCglobal Class-1 Generation-2 standard.
- ISO/IEC 18000-7 is an RTF protocol for an RFID system that operates at 433 MHz. Tags have a 32-bit tag ID and a 16-bit manufacturer ID. Readers are given a 16-bit identifier as well. A 32-bit password can be set on the tags. A bit, referred to as the "secure bit" in the standard, is set to determine if the tag is password protected or not. If protected, read/write of the User ID, User ID Length, Routing Code, and memory are password protected. ISO/IEC 18000-7 supports optional command database query commands that are transmitted to all tags. The queries are sent in multiple steps and can use logical operators such as clear, and, and-or, and relational operators such as equal, less than, greater than, and not. Tags that receive all steps of the query will do an internal database search and readers can retrieve the results of these queries.

There are also a number of item management-related standards for the application of livestock tracking.[91]

A.2 Industry Standards

The most prominent industry standards for RFID are the EPCglobal specifications and standards for supply chain and patient safety applications. All EPCglobal specifications developed to date are for passive, RTF RFID systems. Four specifications have been developed by EPCglobal: Class-0 UHF, the Class-1 Generation-1 HF, the Class-1 Generation-1 UHF, and the Class-1 Generation-2 UHF specifications. Of these specifications, the Class-1 Generation-2 specification has been approved by EPCglobal as a standard.

The first specification developed by EPCglobal was the EPCglobal Class-0 specification for 900 MHz UHF operation. The intent of this specification was to establish a low cost identification tag. The Class-0 specification provides three main features: an EPC, a 16-bit cyclic redundancy check (CRC),[92] and a self-destruct feature. The self-destruct feature is also known as the kill feature. When a reader issues the *kill* command and the appropriate 24-bit password, the tag no longer responds to any commands. [93] The Four EPC identifiers described in the standard are shown in Table A-1.

---

[91] Livestock tracking standards include ISO 11784, ISO 11785, and ISO 14223. ISO 11784 covers the data format for such tags. ISO 11785 defines the technical details of such a tag, and ISO 14223 is an updated standard for livestock tracking tags.

[92] A cyclic redundancy check is used to detect errors such as those introduced by noise in a communication channel.

[93] Auto-ID Center, "Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag," February 23, 2003, http://www.epcglobalinc.org/standards/specs/900_MHz_Class_0_RFIDTag_Specification.pdf.

Table A-1. EPC Identifier Formats

EPC Type	Header Size	First Bits	EPC Manager ID	Object Class	Serial Number	Total
64 bit Type I	2	01	21	17	24	64
64 bit Type II	2	10	15	13	34	64
64 bit Type III	2	11	26	13	23	64
96 bit and more	8	00	28	24	36	96

Next, two EPCglobal Class-1 Generation-1 specifications were developed: one for HF operation and one for UHF operation. The HF specification defines a tag that operates at 13.56 MHz and has three main features: an EPC, a 16-bit cyclic redundancy check, and a self-destruct feature. Its *kill* code is 24 bits.[94] There currently are no commercial products based on the EPCglobal Class-1 Generation-1 specification for 13.56 MHz and nearly all references to EPC Class-1 Generation-1 tags refer to the UHF specification. This is because 13.56 MHz offers operating ranges of up to one meter, which is not as useful in item management as UHF, which can offer operating ranges of several meters. The UHF specification defines a tag that operates at 860 MHz – 960 MHz and has an EPC identifier, an error detection code, and a *kill* command. The EPC shall be a valid EPC that contains four subfields: a header, an EPC manager ID, an object class, and a serial number. The error detection is performed using a 16-bit CRC. The *kill* password is 8 bits.[95]

The EPCglobal Class-1 Generation-2 standard is the only specification that became a standard ratified by EPCglobal.[96] The previous Class-0 and Class-1 Generation-1 tags are expected to be phased out and replaced by Class-1 Generation-2 tags. It describes tags with five major features: an EPC, a tag identifier (TID), a *kill* command, an optional password-protected access control, and an optional user memory. The tag identifier is used to identify the design and features of the individual tag. This is necessary since tags may have optional or custom commands and features. CRCs are used in some communications and for the EPC. There is a 32-bit *kill* password and a 32-bit access password. The standard also implements a *lock* command which can temporarily or permanently make an area of memory write-protected or read-and-write protected.[97] EPCglobal Class-1 Generation-2 tags also use a cover-coding method to obscure information that is sent from a reader to a tag. Cover-coding is explained in Section 5.3.2.1.

A.3 Security Mechanisms in RFID Standards

Table A-2 provides an overview of the security mechanisms offered by several RFID standards.

---

94 Auto-ID Center, "Technical Report, 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0," February 1, 2003, http://www.epcglobalinc.org/standards/specs/13.56_MHz_ISM_Band_Class_1_RFID_Tag_Interface_Specification.pdf.

95 Auto-ID Center, "Technical Report, 860 MHz - 930 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1," November 14, 2002, http://www.epcglobalinc.org/standards/specs/860MHz_930_MHz_Class_1_RFID_Tag_Radio_Frequency_Logical_Communication_Interface_Specification.pdf.

96 This EPCglobal standard, with minor changes, has been standardized as the ISO/IEC 18000-6C.

97 EPCglobal, "EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9," January 2005.

Table A-2. Security Mechanisms in RFID Standards[98]

RFID Standard (application)	Technical Features			Security Mechanisms	
	Band	Range (m)	Data	Confidentiality/Anonymity	Integrity
EPCglobal Class-0 (supply chain)	UHF	3	64 or 96-bit identifier that is factory programmed	Readers singulate tags using static and/or dynamically generated random numbers	Parity bits and CRCs are used for error detection
EPCglobal Class-1 Generation-1 (supply chain)	UHF	3	64 or 96-bit identifier that is factory programmed or WORM	None in standard	Lock command that permanently write protects all memory CRC error detection Commands are sent with 5 parity bits
EPCglobal Class-1 Generation-2 / ISO/IEC 18000-6C (supply chain)	UHF	3	Supports identifiers up to 496 bits, user defined memory, and R/W memory	Cover-coding masks reader-to-tag communications Readers address tags using 16-bit random numbers	Areas of memory can be locked, which write protects those areas Areas of memory can also be permanently locked CRC error detection
ISO/IEC 18000-2 (item management)	LF	< 0.010	64 bit identifier, and up to 1 kbyte of R/W memory	None in standard	Memory blocks can be permanently locked CRC error detection
ISO/IEC 18000-3 (item management)	HF	< 2	64 bit identifier, R/W memory	Mode 2 has 48-bit password protection on *read* commands	Memory blocks can be permanently locked Mode 2 has a lock pointer that stores a memory address. This feature write protects all areas of memory below that stored address Mode 2 has 48-bit password on *write* commands CRC error detection
ISO 11784/11785 (animal tracking)	LF	< 0.010	64-bit identifier	None in standard	CRC error detection
ISO/IEC 14443 (contactless smart cards)	HF	≈ 0.07 to 0.15	Type A: 32, 56, or 80 bit identifier Type B: 32 bit identifier	None in standard[99]	CRC error detection

[98] T. Phillips, T. Karygiannis, and R. Kuhn, "Security standards for the RFID market," *IEEE Security and Privacy*, vol. 3, issue 6, pp. 85-89.

[99] While the ISO/IEC 14443 itself does not provide confidentiality services, these services are available in many applications that use ISO/IEC 14443 for wireless communications.

RFID Standard (application)	Technical Features			Security Mechanisms	
	Band	Range (m)	Data	Confidentiality/Anonymity	Integrity
ISO/IEC 15693 (vicinity smart cards)	HF	1	64 bit identifier, and up to 8 kbytes R/W memory	No protection on the *read* command No onboard encryption or authentication	Lock feature permanently write-protects memory CRC error detection

A.4 Proprietary Designs

Numerous companies have created their own proprietary RFID tag designs, many of which are based on open standards. In the case of proprietary designs, readers of this document are encouraged to seek information from the vendors about these products.

Two prominent examples of proprietary tags that are, in effect, proprietary extensions of open standards, but offer extended features are item management tags and contactless smart cards. Item management tags that are based on the air interface defined by ISO/IEC 18000-7 are widely used to monitor shipments of cargo containers. US DoD uses these tags to track military cargo. Proprietary tags based on ISO/IEC 18000-7 operate at 433 MHz, can have a range of 100 meters, and can have user memory up to 128 kilobytes. Contactless smart cards are often based on ISO/IEC 14443 and are widely used in public transportation and can also be used in access control, financial payment, gaming, loyalty card programs, and toll road payment. Many contactless smart cards are enhanced with proprietary extensions and security features.

This page has been left blank intentionally.

Appendix B—Glossary

Selected terms used in *Guidelines for Securing Radio Frequency Identification (RFID) Systems* are defined below.

Active Tag: A tag that relies on a battery for power.

Analytic Systems: IT systems that process the information outputs produced by middleware. Analytic systems may be comprised of databases, data processing software, and Web services.

Authenticated RFID: The use of digital signature technology to provide evidence of the authenticity of a tag and possibly chain of custody events.

Back Channel: The channel on which a tag transmits its signals.

Backscatter Channel: The type of back channel used by passive tags. Since passive tags do not have a local power source, they communicate by reflecting or backscattering electromagnetic signals received from a reader.

Cloned Tag: A tag that is made to be a duplicate of a legitimate tag. A cloned tag can be created by reading data such as an identifier from a legitimate tag and writing that data to a different tag.

Closed System: A system that is self-contained within an enterprise. Closed systems do not have an inter-enterprise subsystem.

Cover-Coding: A technique to reduce the risks of eavesdropping by obscuring the information that is transmitted. The EPCglobal Class-1 Generation-2 and ISO/IEC 18000-6C standards use cover-coding to obscure certain transmissions from readers to tags. A more detailed description of how cover-coding is used in these two standards can be found in Section 5.3.2.1 on cover-coding.

Duty Cycle: The percentage of time that a device is operating over a specified period. For example, a reader that is emitting energy to communicate with tags for 15 seconds every minute has a duty cycle of 25%.

Eavesdropper: A party that secretly receives communications intended for others.

Electronic Product Code (EPC) Identifier: One of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain. This number may be used to identify a container, pallet, case or individual unit.

Electronic Product Code Information Services (EPCIS): An inter-enterprise subsystem that facilitates information sharing using the EPCglobal network. EPCISs provide information services necessary for the storage, communication and dissemination of EPC data in a secure environment.

Enterprise Subsystem: The portion of the RFID system that analyzes, processes, and stores information collected by the RF subsystem. The primary role of the enterprise subsystem is to make the data collected by the RF subsystem useful for a supporting business process. An enterprise subsystem is made up of middleware, analytic systems, and network infrastructure.

Form Factor: The physical characteristics of a device or object including its size, shape, packaging, handling, and weight.

Forward Channel: The channel on which a reader transmits its signals.

Inter-Enterprise Subsystem: The portion of the RFID system that connects multiple enterprise subsystems together. The inter-enterprise subsystem consists of network infrastructure, a naming service, and possibly a discovery service. Inter-enterprise subsystems are most commonly associated with supply chain applications.

Jamming: A deliberate communications disruption meant to degrade the operational performance of the RF subsystem. Jamming is achieved by interjecting electromagnetic waves on the same frequency that the reader to tag uses for communication.

***Kill* Command:** A command that readers can send to tags that uses electronic disabling mechanisms to prevent tags from responding to any additional commands.

***Lock* Command:** A command that readers can send to a tag to block access to certain information on the tag.

Lock Pointer: A memory pointer that points to a target area of memory and write protects all memory locations less than the target location. This form of access control is implemented in ISO/IEC 18000-3.

Middleware: Software that aggregates and filters data collected by RFID readers and possibly passes the information to an enterprise subsystem database. Middleware may also responsible for monitoring and managing readers.

Minimalist Cryptography: Cryptography that can be implemented on devices with very limited memory and computing capabilities, such as RFID tags.

Object Naming Service: An inter-enterprise subsystem for the EPCglobal Network that provides network resolution services that direct EPC queries to the location where information associated with that EPC can be accessed by authorized users.

Open System: A system that allows entities from different enterprises to access information related to tags used in the system. Open systems use an inter-enterprise subsystem to share information between entities.

Passive Tag: A tag that does not have its own power supply. Instead, it uses RF energy from the reader for power. Due to the lower power, passive tags have shorter ranges than other tags, but are generally smaller, lighter, and cheaper than other tags.

Permalock: A security feature that makes the lock status of an area of memory permanent. If the area of memory is locked and permalocked, then that area is permanently locked. If the area of memory is unlocked and permalocked, then that area is permanently unlocked.

Reader: A device that can wirelessly communicate with tags. Readers can detect the presence of tags as well as send and receive data and commands from the tags.

Reader Spoofing: The act of impersonating a legitimate reader of an RFID system to read tags.

Reader Talks First: An RF transaction in which the reader transmits a signal that is received by tags in its vicinity. The tags may be commanded to respond to the reader and continue with further transactions.

Reverse Channel: See back channel

RF Subsystem: The portion of the RFID system that uses radio frequencies to perform identification and related transactions. The RF subsystem consists of two components: a reader and a tag.

Semi-Active Tag: A tag that uses a battery to communicate but remains dormant until a reader sends an energizing signal. Semi-active tags have a longer range than passive tags and a longer battery life than active tags.

Semi-Passive Tag: A passive tag that uses a battery to power on-board circuitry or sensors but not to produce back channel signals.

Shrinkage: Product loss or theft that results in declining revenue.

Singulation: A function performed by a reader to individually identify any tags in the reader's operating range.

Skimming: The unauthorized use of a reader to read tags without the authorization or knowledge of tag's owner or the individual in possession of the tag.

Smart Card: A plastic card containing a computer chip that enables the holder to purchase goods and services, enter restricted areas, access medical, financial, or other records, or perform other operations requiring data stored on the chip.[100]

Supply Chain: The network of retailers, distributors, transporters, storage facilities, and suppliers that participate in the sale, delivery, and production of a particular product.[101]

Tag: An electronic device that communicates with RFID readers. A tag can function as a beacon or it can be used to convey information such as an identifier.

Tag Talks First: An RF transaction in which the tag communicates its presence to a reader. The reader may then send commands to the tag.

Traffic Analysis: The analysis of patterns in communications for the purpose of gaining intelligence about a system or its users. Traffic analysis does not require examination of the content of the communications, which may or may not be decipherable. For example, an adversary may be able to detect a signal from a reader that could enable it to infer that a particular activity is occurring (e.g., a shipment has arrived, someone is entering a facility) without necessarily learning an identifier or associated data.

Transponder: See Tag

---

[100] The American Heritage® Dictionary of the English Language, Fourth Edition. Houghton Mifflin Company, 2004. http://dictionary.reference.com/browse/smart card (accessed: February 06, 2007).

[101] Webster's New Millennium™ Dictionary of English, Preview Edition, v 0.9.6, , http://dictionary.reference.com/browse/supply%20chain (accessed: January 22, 2007).

This page has been left blank intentionally.

Appendix C—Acronyms and Abbreviations

Selected acronyms and abbreviations used in *Guidelines for Securing Radio Frequency Identification (RFID) Systems* are defined below.

AIDC Automatic Identification and Data Capture
AIT Automatic Identification Technology
ANSI American National Standards Institute
ASCII American Standard Code for Information Interchange

CAC Common Access Card
CD-ROM Compact Disc Read Only Memory
CFR Code of Federal Regulations
CIO Chief Information Officer
cm Centimeter
CRC (fictional) Contagion Research Center
CRC Cyclic Redundancy Check
CSRC Computer Security Resource Center

DNS Domain Name System
DoD Department of Defense

E3 Electromagnetic Environmental Effects
EAN European Article Number
EAS Electronic Article Surveillance
EPC Electronic Product Code
EPCIS Electronic Product Code Information Services

FCC Federal Communications Commission
FIPS Federal Information Processing Standard
FISMA Federal Information Security Management Act
FOIA Freedom of Information Act
FY Fiscal Year

GHz Gigahertz
GRS General Records Schedule
GS1 Global Standards One
GSA General Services Administration

HERF Hazards of Electromagnetic Radiation to Fuel
HERO Hazards of Electromagnetic Radiation to Ordnance
HERP Hazards of Electromagnetic Radiation to People
HEW Health, Education and Welfare
HF High Frequency
HIPAA Health Insurance Portability and Accountability Act
Hz Hertz

ID Identifier
IEC International Electrotechnical Commission
IEEE Institute of Electrical and Electronics Engineers
IP Internet Protocol

IPsec	Internet Protocol Security
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
ITU	International Telecommunication Union
kHz	Kilohertz
LAN	Local Area Network
LF	Low Frequency
m	Meter
MHz	Megahertz
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MRI	Magnetic Resonance Imaging
MX	Mail Exchanger
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCIO	Office of the Chief Information Officer
OECD	Organisation for Economic Co-operation and Development
OET	Office of Engineering and Technology
OMB	Office of Management and Budget
ONS	Object Naming Service
OSHA	Occupation Safety and Health Administration
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RSA	Rivest Shamir Adelman
RTA	(fictional) Radionuclide Transportation Agency
RTF	Reader Talks First
RTLS	Real-Time Location System
R/W	Read/Write
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SP	Special Publication
SSL	Secure Sockets Layer
SSN	Social Security Number
TCP	Transmission Control Protocol
TID	Tag Identifier

TLS	Transport Layer Security
TTF	Tag Talks First
UCC	Uniform Code Council
UHF	Ultra High Frequency
URI	Uniform Resource Identifier
URL	Universal Resource Locator
US	United States
USC	United States Code
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WORM	Write Once, Read Many
WPA	Wi-Fi Protected Access
WSDL	Web Services Description Language
XOR	Exclusive-or

This page has been left blank intentionally.

Appendix D— Information Resources

The lists below contain information resources that may be helpful for organizations planning or operating RFID systems.

Print Publications and Books

K. Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, 2nd edition. Munich: John Wiley & Sons Ltd., 2003.

S. Garfinkel, Ed., and B. Rosenberg, Ed., *RFID Applications, Security, and Privacy*. Upper Saddle River, New Jersey: Pearson Education, Inc., 2006.

S. Lahiri, *RFID Sourcebook*. Pearson Education, 2005.

Articles and Other Published Materials

29 CFR § 1910.97. Nonionizing radiation.

47 CFR § 15.247. Operation within the bands 902 - 928 MHz, 2400 - 2483.5 MHz, and 5725 - 5850 MHz.

American Bankers Association, "Keyed Hash Message Authentication Code," American National Standards Institute (ANSI) X9.71, Washington, D.C., 2000.

Auto-ID Center, "Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag," February 23, 2003, http://www.epcglobalinc.org/standards/specs/900_MHz_Class_0_RFIDTag_Specification.pdf.

Auto-ID Center, "Technical Report, 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0," February 1, 2003, http://www.epcglobalinc.org/standards/specs/13.56_MHz_ISM_Band_Class_1_RFID_Tag_Interface_Specification.pdf.

Auto-ID Center, "Technical Report, 860 MHz - 930 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1," November 14, 2002, http://www.epcglobalinc.org/standards/specs/860MHz_930_MHz_Class_1_RFID_Tag_Radio_Frequency_Logical_Communication_Interface_Specification.pdf.

J. Blau, "FIFA boots chip ball from 2006 soccer World Cup," December 6, 2005, http://www.infoworld.com/article/05/12/06/HNfifaboots_1.html.

Center for Democracy and Technology, "CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology," Interim Draft, May 1, 2006, http://www.cdt.org/privacy/20060501rfid-best-practices.php.

R. Cleveland Jr. and J. Ulcek, "Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields," Federal Communications Commission

Consolidated Appropriations Act, 2005, Public Law No. 108-447.

Department of Defense, "Directive 3222.3: DoD Electromagnetic Environmental Effects (E3) Program," September 8, 2004, http://www.dtic.mil/whs/directives/corres/pdf/d32223_090804/d32223p.pdf.

E-Government Act of 2002, Public Law No. 107-347, 116 Stat. 2923.

EPCglobal, "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9," January 2005.

EPCglobal, "Guidelines on EPC for Consumer Products," September 2005, http://www.epcglobalinc.org/public/ppsc_guide/.

Federal Information Security Management Act of 2002, Public Law No. 107-347, 116 Stat. 2946.

M. Feldhofer, J. Wolkerstorfer and V. Rijmen, "AES implementation on a grain of sand," *IEE Proceedings, Information Security*, vol. 152, issue 1, pp. 13-20, October 2005.

S. Garfinkel, "Adopting Fair Information Practices to Low Cost RFID Systems," presented at the *Fourth International Conference on Ubiquitous Computing*, Göteberg, Sweden, 2002.

"Generation 2 Security," ThingMagic, Cambridge, Massachusetts, White Paper, 2005.

J. Guerrieri and D. Novotny, "HF RFID Eavesdropping and Jamming Tests," Electromagnetics Division, Electronics and Electrical Engineering Laboratory, National Institute of Standards and Technology, Boulder, Colorado, Report Number 818-7-71, 2006.

"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Organisation for Economic Co-operation and Development (OECD), Paris, France, 1980.

Intelligent Transportation Systems, US Department of Transportation, "What is ITS?," November 7, 2006, http://www.its.dot.gov/its_overview.htm.

"ITU Internet Reports 2005: The Internet of Things," International Telecommunications Union, Geneva, Switzerland, 2005.

A. Juels, "Minimalist cryptography for low-cost RFID tags," in the *Fourth Conference on Security in Communication Networks*, 2004, pp. 149-164.

A. Juels, R. L. Rivest, and M. Szydlo, "The Blocker Tag: Selective blocking of RFID tags for consumer privacy," in *Eighth ACM Conference on Computer and Communications Security*, 2003, pp. 103-111.

A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, February 2006.

I. Kirschenbaum and A. Wool, "How to build a low-cost, extended-range RFID skimmer," in *Fifteenth USENIX Security Symposium*, 2006, pp. 43-57.

H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: keyed-hashing for message authentication," Internet Engineering Task Force, Request for Comments (RFC) 2104, February 1997.

Office of Management and Budget, "Designation of Senior Agency Officials for Privacy," Executive Office of the President, Washington, D.C., OMB Memorandum 05-08, February 11, 2005.

Office of Management and Budget, "FY 2006 Reporting Instructions for FISMA and Agency Privacy Management," Executive Office of the President, Washington, D.C., OMB Memorandum 06-20, July 17, 2006.

Office of Management and Budget, "Incorporating and Funding Security in Information Systems Investments," Executive Office of the President, Washington, D.C., M-00-07, 2000.

Office of Management and Budget, "Instructions for Preparing the FISMA Report and Privacy Management Report," Executive Office of the President, Washington, D.C., OMB Memorandum 05-15, June 13, 2005.

Office of Management and Budget, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Executive Office of the President, Washington, D.C., OMB Memorandum 03-22, September 26, 2003.

Office of Management and Budget, "Protection of Sensitive Agency Information," Executive Office of the President, Washington, D.C., OMB Memorandum 06-16, June 23, 2006.

Office of Management and Budget, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," Executive Office of the President, Washington, D.C., OMB Memorandum 06-19, July 12, 2006.

Office of Management and Budget, "Safeguarding Personally Identifiable Information," Executive Office of the President, Washington, D.C., OMB Memorandum 06-15, May 22, 2006.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Radio Frequency Identification (RFID) Policy," July 2004, http://www.acq.osd.mil/log/rfid/Policy/RFID%20Policy%2007-30-2004.pdf

Y. Oren and A. Shamir, "Power Analysis of RFID Tags," discussed at the *Cryptographers Panel of the Fifteenth RSA Conference*, San Jose, 2006.

Permanent Citizens Advisory Committee to the Metropolitan Transportation Authority, "In your pocket: using smart cards for seamless travel," October 2004, http://www.pcac.org/reports/pdf/Smart%20Card%20Exec%C9ive%20Summary.pdf.

T. Phillips, T. Karygiannis, and R. Kuhn, "Security standards for the RFID market," *IEEE Security and Privacy*, vol. 3, issue 6, pp. 85-89.

Privacy Rights Clearinghouse, "RFID Position Statement of Consumer Privacy and Civil Liberties Organizations," November 20, 2003, http://www.privacyrights.org/ar/RFIDposition.htm.

M. Rieback, B. Crispo, and A. Tanenbaum, "Is Your Cat Infected with a Computer Virus?" in the *Fourth IEEE International Conference on Pervasive Computing and Communications*, 2006, pp. 10.

L. Sullivan, "IBM Shares Lessons Learned From Wal-Mart RFID Deployment," October 15, 2004, http://informationweek.com/story/showArticle.jhtml?articleID=49901908.

US Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens*, Washington, D.C.: US Department of Health, Education, and Welfare, 1973.

Internet Resources

Organization	URL
Auto-ID Labs	http://www.autoidlabs.org/
Automatic Identification Technology Office	http://www.dodait.com/
EPCglobal	http://www.epcglobalinc.org/
FCC OET Bulletins	http://www.fcc.gov/oet/info/documents/bulletins/
GSA Smart Card Web Site	http://www.smart.gov/
International Organization for Standardization	http://www.iso.org/
NIST Computer Security Guideline Publications	http://csrc.nist.gov/publications/
OMB Information Policy	http://www.whitehouse.gov/omb/inforeg/infopoltech.html
RFID Journal	http://www.rfidjournal.com/

General NIST Security Resources

Document	URL
FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*	http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS Publication 180-2, *Secure Hash Standard (SHS)*	http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
FIPS Publication 196, *Entity Authentication Using Public Key Cryptography*	http://csrc.nist.gov/publications/fips/fips196/fips196.pdf
FIPS Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*	http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf
FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*	http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
SP 800-12, *An Introduction to Computer Security: The NIST Handbook*	http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
SP 800-30, *Risk Management Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
SP 800-31, *Intrusion Detection Systems*	http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf
SP 800-34, *Contingency Planning Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
SP 800-35, *Guide to Information Technology Security Services*	http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf

Document	URL
SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf
SP 800-40v2, *Creating a Patch and Vulnerability Management Program*	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
SP 800-41, *Guide to Firewall Selection and Policy Recommendations*	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
SP 800-44, *Guidelines on Securing Public Web Servers*	http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf
SP 800-47, *Security Guide for Interconnecting Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf
SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*	http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
SP 800-50, *Building an Information Technology Security Awareness and Training Program*	http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf
SP 800-57, *Recommendation on Key Management*	http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf
SP 800-64, *Security Considerations in the Information System Development Life Cycle*	http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf
SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*	http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf
SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals*	http://csrc.nist.gov/itsec/download_WinXP.html
SP 800-70, *The NIST Security Configuration Checklists Program*	http://csrc.nist.gov/checklists/download_sp800-70.html
SP 800-77, *Guide to IPsec VPNs*	http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf
SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*	http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90_DRBG-June2006-final.pdf
SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
SP 800-100, *Information Security Handbook: A Guide for Managers*	http://csrc.nist.gov/publications/nistpubs/800-100/sp800-100.pdf

This page has been left blank intentionally.

Appendix E—FCC Exposure Limits

FCC Maximum Permissible Exposure Limits for General Population/Uncontrolled Exposure[102]

Frequency Range (MHz)	Electric Field Strength (E) (V/m)	Magnetic Field Strength (H) (A/m)	Power Density (S) (mW/cm^2)	Averaging Time $\|E\|^2$, $\|H\|^2$, or S (minutes)
0.3-1.34	614	1.63	(100)	30
1.34-30	824/f	2.19/f	($180/f^2$)	30
30-300	27.5	0.073	0.2	30
300-1,500	-	-	f/1,500	30
1,500-100,000	-	-	1.0	30

These general population / uncontrolled exposure limits are applicable in two situations. The first situation is general public exposure. The second situation is when employees are exposed and are either not fully aware of the potential for exposure or cannot control the exposure. The FCC also has published maximum permissible exposure limits for occupational or controlled exposure.

[102] The letter f represents the frequency of the electromagnetic waves in MHz. The power density for the 0.3 – 1.34 MHz range and the 1.34 – 30 MHz range is a plane-wave equivalent power density. For more information, see FCC OET Bulletin 56, "Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields," Table 1, p. 15.

This page has been left blank intentionally.

Appendix F—Index