ISO/IEC JTC 1 N 9198

2008-07-18

ISO/IEC JTC 1
Information Technology

Document Type:	**Text for DTR Ballot**
Document Title:	**ISO/IEC DTR 24729-4, "Information technology -- Radio frequency identification for item management -- Implementation guidelines -- Part 4: RFID guideline on tag data security"**
Document Source:	**SC 31 Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for DTR ballot. National Bodies are asked to vote and submit their comments via the on-line balloting system by the due date indicated.**
Action ID:	**VOTE**
Due Date:	**2008-10-19**
No. of Pages:	**30**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1/SC 31

Automatic Identification and Data Capture Techniques

Secretariat: ANSI (USA)

DOC TYPE:	**Text for DTR Ballot**
TITLE:	**ISO/IEC DTR 24729-4, "Information technology -- Radio frequency identification for item management -- Implementation guidelines -- Part 4: RFID guideline on tag data security"**
SOURCE:	**ISO/IEC JTC 1/SC 31/WG 4/SG 5**
PROJECT:	**24729-4**
STATUS:	**ISO/IEC 24729-4 BRM requests the convener of the BRM to forward the reviewed and updated document according to N2579 to the SC 31 Secretariat for a 3 month DTR ballot.** **JTC 1/SC 31 forwards the DTR to JTC 1 for DTR balloting.**
ACTION ID:	**JTC 1**
DUE DATE:	**2008-10-13**
DISTRIBUTION:	**ISO/IEC JTC 1/SC 31 members**
MEDIUM:	**ISO TC Portal (LiveLink)**
NO. OF PAGES:	**29 (including this cover)**

Reference number of working document: **ISO/IEC JTC 1/SC 31 N 2579**

Date: 2008-06-04

Reference number of document: **ISO/IEC DTR 24729-4**

Committee identification: ISO/IEC JTC 1/SC 31/WG 4/SG 5

Secretariat: JISC

Information technology — Radio frequency identification for item management — Implementation guidelines – Part 4: RFID guideline on tag data security

Technologie de l'information – a Identification de fréquence par radio directives de mise en place pour d'élément de gestion â- partie 4: L'indication de RFID sur étiquette la sécurité des données

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International standard
Document subtype: if applicable
Document stage: (30) Committee
Document language: E

\\192.168.4.16\NJ_Public\James C Info Folder\SC 31 - v1.0\Document Information\N2000 - N2999\N2579\SC031-N-2579 - DTR Text.doc Basic template BASICEN3 2002-06-01

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

Technical Committee ISO/IEC JTC 1/SC 31, *Automatic identification and data capture techniques*, Working Group 4, *Radio frequency identification* prepared ISO/IEC 24729-4.

ISO/IEC 24279 consists of the following parts, under the general title Information technology — Radio frequency identification for item management:

— *Part 1: RFID-enabled labels and packaging supporting ISO/IEC 18000-6C*

— *Part 2: Recycling and RF tags*

— *Part 3: Implementation and operation of UHF RFID Interrogator systems in logistics applications*

— *Part 4: RFID guideline on tag data security*

Introduction

This document looks at systemic solutions that prevent unauthorized or inadvertent access to data on an RFID tag and in an RFID system. It is intended to provide guidance to users and systems designers on potential threats to data security and countermeasures available to provide RFID data security.

Determining the appropriate approach to RFID data security is highly dependent on the type(s) of possible threat(s), the intended use of the tag, and the type of data on the tag for a particular application. Therefore, this document cannot provide specific recommendations but will, rather offer sufficient guidance to enable users or developers to assess potential risks and determine appropriate techniques to mitigate these risks.

An RFID system is divided into modules, each having their own security elements. These modules are tag, tag-to-reader, reader, reader-to-host, host (back-end enterprise) system, and data throughout the tag, reader, host and communications. This document addresses the RFID components of a system: tag and tag-to-reader (or tag-to-tag) communications. Other components of the system are more typical "system" security issues and are covered by a variety of other best practice documents.

This document is divided into three sections:

- Possible threats to data access security ranging from unauthorized access to data to denial of service.
- A methodology for assessing the various possible threats in order to determine the relative risk level of a specific application and whether security measures are required.
- Countermeasures to effectively address specific possible threats.

The thorough review of possible threats should not be construed to mean that RFID itself is inherently vulnerable but, rather, like any technology, it will be subject to attempts to exploit or subvert it by unscrupulous individuals or by those merely wishing to demonstrate their technical prowess. This information is provided to help technical personnel anticipate and prevent successful attacks on RFID systems.

Potential threats must also be taken in context. Technologies or methodologies currently being used for some of the applications discussed may have greater risk factors.

Implemented with appropriate countermeasures and forethought, RFID systems can be secure, beneficial and cost-effective.

Information technology — Radio frequency identification for item management — Implementation guidelines – Part 4: RFID guideline on tag data security

1 Scope

This document provides guidance on RFID Security. The RFID system is divided into modules, each having their own security elements. These modules are tag, tag to reader, reader, reader to host, and host (back-end enterprise) system. The scope of this document is restricted to the security aspects of the tag and tag-to-reader communication (identified as 1 through 2 in Figure 1). Although important, it is beyond the scope of this group to address security aspects of the reader-to-host and back-end enterprise modules (identified as 4 through 7 in Figure 1). [The Center for Democracy in Technology (CDT), as of the date of this publication, has released a draft "Privacy Best Practices for Deployment of RFID Technology" (http://www.cdt.org/privacy/20060501rfid-best-practices.php) that addresses elements 4 through 7. Readers are encouraged to reference the CDT document for further information.]

This document will provide some guidance to systems designers to help them determine potential threats and appropriate countermeasures for modules 1 through 2 in **Figure 1**. This document is not intended to specifically address consumer privacy concerns. However, since data and personal privacy depend on the use of appropriate security measures, privacy will be addressed in general terms. Data access security provides a measure of personal privacy protection by mitigating the potential for unauthorized reading of data on a tag. However, not all data access security countermeasures provide the same level of protection.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15963, *Information technology — Radio frequency identification for item management — Unique identification for RF tags*

ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

> Note: ISO/IEC 17799 is a comprehensive set of controls comprising best practices in information security. [http://www.iso-17799.com/]

ISO/IEC 19762-1, *Information technology — AIDC techniques — Harmonized vocabulary — Part 1: General terms relating to Automatic Identification and Data Capture (AIDC)*

ISO/IEC 19762-3, *Information technology — AIDC techniques — Harmonized vocabulary — Part 3: Radio-Frequency Identification (RFID)*

ISO/IEC 24791-6, Information technology – Automatic identification and data capture techniques – Radio frequency identification (RFID) for item management – software system infrastructure Part 6: Security

Guidance from AIM Global's RFID Expert Group, RFID — Guidelines on data access security

NIST-800-30 – Risk Management Guide for Information Technology Systems [http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf]

NIST Special Publication 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*

Federal Information Security Management Act (FISMA) [http://csrc.nist.gov/sec-cert/]

Open Web Application Security Project (OWASP) [http://www.owasp.org/index.php/Main_Page]

3 Terms and definitions

For the purposes of this document the terms and definitions, abbreviations, and symbols given in ISO/IEC 19762, Information Technology – AIDC techniques – Harmonized vocabulary and the following apply:

3.1
network
for the purpose of this document, network in this document is restricted to tag and tag-to-reader

3.2
ciphertext
encrypted text – the output of the encryption process that can be transformed back into a readable form, plaintext, with the appropriate decryption key

4 Background

4.1 System definition: tag, tag to reader, reader

An RFID end-to-end system architecture is comprised of the components shown in Figure 1. The components can be listed as:

1 Tags (transponders) (physical and information component),

2 Tag-to-Reader Interface and Tag-to-Tag Interface (air interface)

3 Readers (transceivers),

4 Reader-to-Enterprise (air /network interface), and

5-7 Back-end System (Enterprise-to-User).

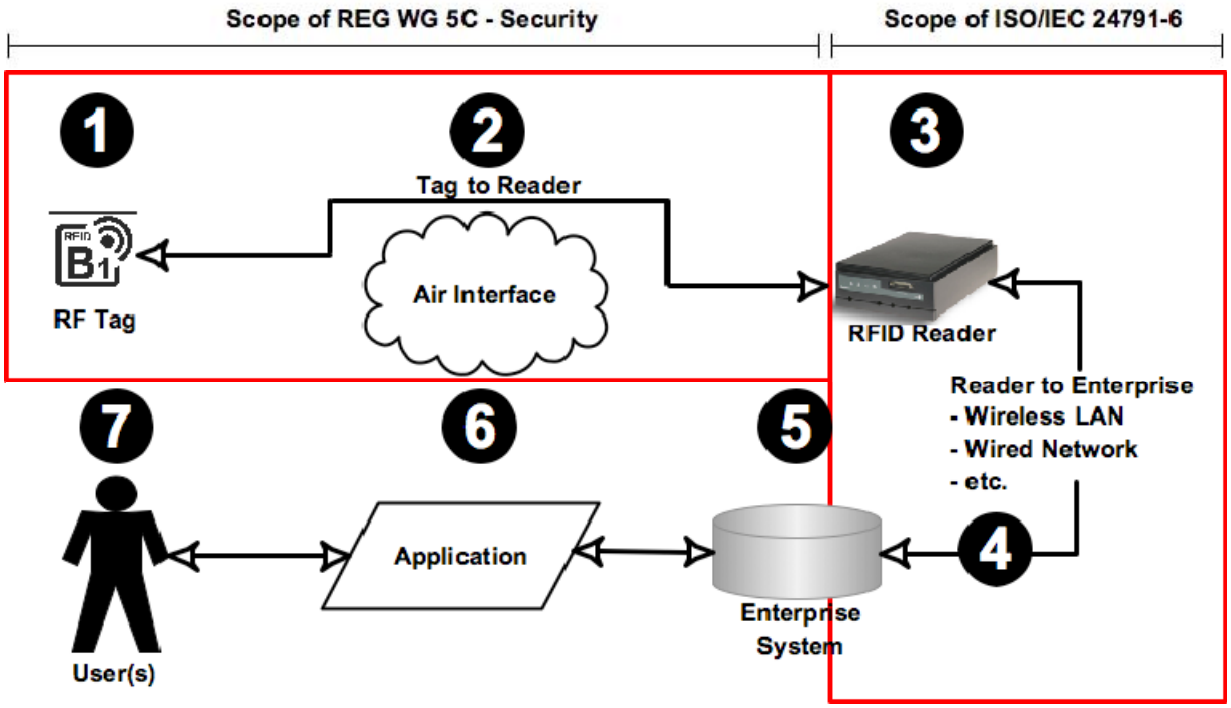

Figure 1 – RFID system top level architecture

The tags are affixed to objects and carry data. Some tag technologies can communicate with each other as data transfer nodes. The reader communicates with the tag to read or write data and interface to the back-end infrastructure. Both the tag-to-tag and tag-to-reader involve the air interface. Threats and countermeasures are similar for either air interface between tags or tag-to-reader. The back-end system includes the entire enterprise infrastructure such as middleware, database, and application interfaces that accept and process the tag data. The overall system should be analyzed for true end-to-end security assurance or risk mitigation. This document will only focus on items 1 through 2, the Tag and Tag-to-Reader data communications.

4.2 Definition of security

RFID security is the prevention of unauthorized reading and changing of RFID data. RFID data security means protecting the data on the tag and the data transmitted between the tag and reader (or tag to tag in more advanced systems) to ensure it is accurate and safe from unauthorized access. In addition, security includes unauthorized access to the reader from the air interface.

System security involves numerous components that ensure authorized entities (includes individuals and corporations) have access to RFID data (tag or reader) at all times. Many of these system security elements are outside the purview of this document because they are standard IT security issues. Confidentiality, integrity, and authenticity as defined by FISMA are key elements to RFID security. Expanding the FISMA security objectives, this document adds authentication.

4.3 Security objectives

The Federal Information Security Management Act (FISMA) defines three security objectives for information and information systems (6): confidentiality, integrity, and availability.

4.3.1 Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [FISMA, 44 U.S.C., Sec. 3542]

A loss of confidentiality is the unauthorized disclosure of information.

4.3.2 Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of integrity is the unauthorized modification or destruction of information.

4.3.3 Availability

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of availability is the disruption of access to or use of information or an information system.

4.3.4 Authentication

Ensuring that a tag's data can only be accessed by authorized individuals/systems.

5 RFID data access security risk assessment

The measures taken to ensure RFID data access security depend, in part, upon the perceived risks. For RFID data access security, risk is dependent on two variables: probability and impact upon the individual or organization.

Impact can be assessed in terms of Damage Potential and Affected Users, while thinking of Reproducibility, Exploitability, and Discoverability in terms of Probability. Impact vs Probability approach follows best practices such as defined in NIST-800-30.

Risks are also both application- and commodity-dependent. Not all types of data justify high levels of security nor are the costs justified. As security measures increase, cost increases. For pharmaceutical chain-of-custody, security breaches could lead to product tampering, counterfeiting, or theft. The impact on the individual could be life-threatening. For dispensing of pharmaceuticals, however, if a pharmacy order number is the only data on the tag, the risk is low because the number itself is non-significant and would not differentiate between Schedule drugs and non-Schedule drugs. Unauthorized access to the pharmacy's database would be required to understand the code's association.

5.1 Risk assessment

Open Web Application Security Project (OWASP) identifies other factors to security threat levels that include Damage Potential, Reproducibility, Exploitability, Affected users, and Discoverability (DREAD). DREAD modeling influences the thinking behind setting the risk rating, and is also used directly to sort the risks. Although the OWASP is targeted toward software security threats, the categories are applicable for this document on RFID security. The DREAD algorithm is

> **Risk_DREAD** = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5 ;

and is used to compute a risk value, which is an average of all five categories. The calculation always produces a number between 0 and 10; the higher the number, the more serious the risk.

Damage Potential: If a threat exploit occurs, how much damage will be caused?

FIPS Publication 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). This document added authenticity to the list of potential impacts and would fall into the damage category:

- 0 = The loss of confidentiality, integrity, availability, or authenticity could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- 5 = The loss of confidentiality, integrity, availability, or authenticity could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- 10 = The loss of confidentiality, integrity, availability, or authenticity could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Reproducibility: How easy is it to reproduce the threat exploit?

- 0 = Very difficult, requires extensive equipment and/or knowledge.
- 5 = One or two steps required.
- 10 = Just a reader, without authentication.

Exploitability: What is needed to exploit this threat?

- 0 = Advanced programming and equipment knowledge, with custom or advanced attack tools.
- 5 = An exploit is easily performed but requires additional resources
- 10 = Uses commercially available equipment (readers / tags)

Affected Users: How many users will be adversely affected? If unknown use 5.

- 0 = None
- 5 = Some users, but not all
- 10 = All users

Discoverability: How easy is it to discover this threat?

- 0 = System tools are available for monitoring and identifying threat
- 5 = Can figure it out by monitoring tag data and air interface, may require process change.
- 10 = Very hard to impossible – requires additional equipment and/or major process change

5.2 Probability

In many scenarios, it is theoretically or actually possible to adversely affect an RFID system's security but the probability of such an attack is low. That is, such breaches might depend on:

- Access to a remote, secure database
- Unusual or contrived circumstances to enable reading or data manipulation
- Expensive or sophisticated equipment (that exceeds the value gained from the security breach)

— Unusually specialized knowledge of the target system

In these scenarios, the probability is low and may not require significant security measures.

In other scenarios, the probability may be determined to be high because of the value of data accessed or action enabled by the breach. These scenarios may require more significant security measures.

6 Threats

Threats are categorized as normal, abnormal, or malevolent. Normal or abnormal threats are the result of physical or environmental effects, e.g., daily wear and tear on a tag or reader or accidental damage. This document will focus on malevolent threats (intentional user abuse - human factors). The physical destruction of the tag and/or reader is not considered in this document because there are no technical solutions to discriminate between an intentional or unintentional destruction of a tag and very few means (countermeasures) to address it. Some of the types of threats are listed in Sections 6.1 – 6.9.

The threats can be grouped into three primary categories labeled as Mimic, Gather, and Denial of Service (DOS). These categories are shown in Figure 2.

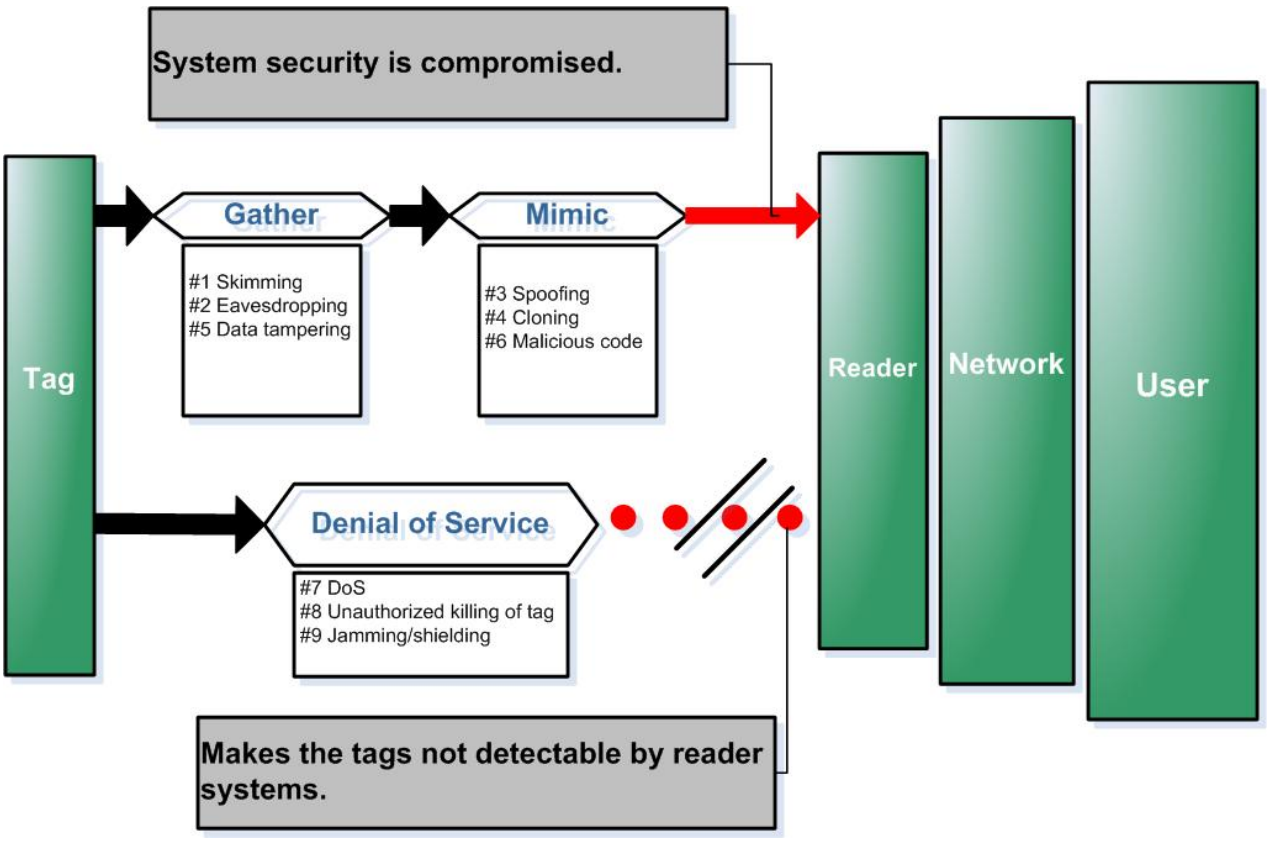

Figure 2 - Threat categories

For skimming, eavesdropping, spoofing, and cloning the read and write ranges may be very different especially for passive tags. Close proximity and higher power are required to write data to a tag. Listening to a tag can be done from comparatively much longer distances with highly sensitive receivers.

6.1 Skimming data

Skimming data is the unauthorized access of reading of tag data (skimming). Data is read directly from the tag without the knowledge or acknowledgement of the tag holder.

6.2 "Eavesdropping" or “sniffing” on transmission between tag and reader

Eavesdropping (also called "man-in-the-middle" reader) is unauthorized listening / intercepting, through the use of radio receiving equipment, of an authorized transmission to monitor or record data between the tag and reader for the purpose(s) of:

- collecting raw transmissions to determine communications protocols and/or encryption
- collecting the tag's data, or
- determining traffic patterns

6.3 Spoofing

Spoofing is defined as duplicating tag data and transmitting it to a reader. Data acquired from a tag, by whatever means, is transmitted to a reader to mimic a legitimate source. For example, for an electronic seal, a threat that defines spoofing is where the e-seal information is transmitted to the reader from some alternative source that is not the original e-seal.

6.4 Cloning

Cloning is defined as duplicating data of one tag to another tag. Data acquired from a tag, by whatever means, is written to an equivalent tag. For example, in contrast to spoofing, cloning an e-seal would be the duplication of the e-seal and replacement of the original with a duplicate/cloned version that would then communicate with the reader.

6.5 Data tampering

Data tampering is unauthorized erasing of data to render the tag useless or changing of the data. For example data tampering in the consumer goods market could involve changing the price of an item for sale to the detriment of the owner.

6.6 Malicious code

Insertion of a executable code / virus to corrupt the enterprise systems is hypothetically possible given a tag with sufficient memory and range.

6.7 Denial of access / service

Denial of service (DoS) occurs when multiple tags or specially-designed tags are used to overwhelm a reader's capacity to differentiate tags, rendering the system inoperative. A type of denial service is a blocker tag that confuses the interrogator so that they are unable to identify the individual tags. (Ref. NIST Special Publication 800-98, “Guidance for Securing Radio Frequency Identification (RFID) Systems)

6.8 Unauthorized killing the tag (electronic or mechanical)

Killing of a tag is an operational threat in that the physical or electronic destruction of the tag deprives downstream users of the tag of its data.

6.9 Jamming / Shielding

Jamming is the use of an electronic device to disrupt the reader's function. Shielding is the use of mechanical means to prevent reading of a tag.

7 Scenarios

The following sections show various applications and discussions of probability of a threat and the impact associated with the threat. These are only examples and not absolute cases.

7.1 Unsecured access control card, no PIN; No encryption or other security feature

Potential Risks:

- Data can be read remotely from card
- Data can be "spoofed"
- Card could be cloned
- Killing of tag
- Jamming

Potential Gain:

- Unauthorized access to "controlled" area

Impact:

- Varies from very low to very high depending on the area to which access is granted.
- If access granted only to "general" areas, impact is low.
- If access granted to secure/sensitive area, potential impact may be very high.

Likelihood of Attack

- High

7.2 Secured access control card, no PIN; Encrypted or other security features

Potential Risks:

- Data can be recorded via eavesdropping
- Cloning
- Killing of tag
- Jamming

Potential Gain:

- Unauthorized access to "controlled" area

Impact:

- Varies from very low to very high depending on the area to which access is granted.
- If access granted only to "general" areas, impact is low.
- If access granted to secure/sensitive area, potential impact may be very high.

Likelihood of Attack

- Low to moderate because of encryption or other security features.

7.3 Customer Loyalty Card

Potential Risks:

- Data can be read remotely from card
- Data can be "spoofed" or cloned
- Killing of tag
- Jamming

Potential Gain:

- Unknown

Impact:

- Very low due to limitation of benefit to be gained

Likelihood of Attack:

- Very low due to limited benefit to be gained

7.4 EPC Label (Batch TAG ID only)

(TAG ID section of EPC memory contains only a tag batch number and not a serial number.)

Potential Risks:

- Data can be read remotely from tag
- Tag can be duplicated
- Data can be tampered with
- Tag can be killed

Potential Gain:

- Identify high value items
- Change identity of high value items to low value items or vice versa

Impact:

— Potentially high (profit loss), depending on value of item

— Low for killing of tag; bar code or HRI backup of data available

Likelihood of Attack:

— Low to high depending on value of item

7.5 Contactless Payment, No PIN

Potential Risks:

— Data can be read remotely from tag

— Tag can be jammed

— Spoofing / cloning

Potential Gain:

— Unauthorized purchases

— Identity theft

Impact:

— Low due to back-end checks and/or limit on value of transactions

Likelihood of Attack:

— Low due to limited read range

7.6 Contactless Payment, PIN

Potential Risks:

— Data can be read remotely from tag

— Tag can be jammed

— Spoofing / cloning

Potential Gain:

— Unauthorized purchases

— Identity theft

Impact:

— Low due to back-end checks, limitation of liability

Likelihood of Attack:

— Very Low due to requirement for PIN

7.7 Contactless Payment, Biometric or other physical activation

Potential Risks:

— Tag can be jammed

Potential Gain:

— Unauthorized purchases

— Identity theft

Impact:

— Very Low due to back-end checks

Likelihood of Attack:

— Very low because physical activation enables only eavesdropping, limited read range

7.8 Pharmaceutical e-Pedigree

Potential Risks:

— Data tampering (change data)

— Killing of tag

Potential Gain:

— Change identity of controlled substance

— Divert or counterfeit controlled or high value drugs

Impact:

— High for changing identity

— Low for killing of tag, other back-up will be available

Likelihood of Attack:

— Low to moderate because of existing supply chain security measures

7.9 Example of Impact

Product ID impact depends on the product.

Example: salt

Table salt is a low value product. Salt used in healthcare grade saline solution is an extremely high value product. Changing the EPCglobal code of table salt to high value salt could have severe health and safety consequences.

Example: Replacement parts - fasteners

Fasteners sold for home use are low value items. Failure of fasteners offers some, but not great, potential for injury. Fasteners often require different grades depending on the application, such as commercial, automotive and aerospace. Fasteners that are intended for commercial or automotive applications, if used on aircraft requiring aviation grade fasteners can lead to catastrophic failure resulting in the loss of lives

7.10 Summary

There is no clear pathway or absolute approach to determining application and threat levels of probability or likelihood of attack and impact.

Table 2 illustrates varying probability and impact of the different threats for several representative scenarios discussed in Section 7. Table 2 shows the rankings used in Table 1 to determine: L = Likelihood of attack, P = Probability of success (ease of attack), I = Potential Impact from very low to very high.

Ease of attack is a relative evaluation of the level of technical skill or equipment required plus the application environment and other constraints. A very high level of relative ease means that little skill or specialized equipment is needed and that the application environment does not provide physical safeguards or constraints thus the higher the ease of attack the greater the probability of success.

Table 1 – Key for Table 2, Threat scenarios and potential impact levels

Key: L = likelihood of attack; P = probability of success (ease of attack); I = impact		
○ Low	⭘ Moderate	● High

Table 2 – Threat scenarios and potential impact levels

Application		Skimming	Eaves-dropping	Spoofing	Cloning	Data Tampering	Malicious Data	Denial of Service	Killing of Tag	Jamming
Contactless Payment, No PIN	L	⊙	○	○	○	○	○	○	○	○
	P	⊙	○	⊙	○	○	○	○	○	○
	I	○	○	○	○	○	○	○	○	○
Contactless Payment, Physical Activation	L	○	⊙	○	○	○	○	○	○	⊙
	P	○	○	○	○	○	○	⊙	○	⊙
	I	○	○	○	○	○	○	○	○	○
Contactless Payment, PIN	L	●	●	●	○	○	○	○	○	⊙
	P	⊙	⊙	⊙	○	○	○	⊙	○	⊙
	I	○	○	○	○	○	○	○	○	○
Customer Loyalty Card	L	○	⊙	●	●	○	○	○	●	○
	P	●	⊙	⊙	●	○	○	○	●	○
	I	○	○	○	○	○	○	○	○	○
EPC Shipping Container Label (Batch TAG ID only)	L	●	●	⊙	●	⊙	○	⊙	⊙	○
	P	●	●	○	●	●	○	○	●	⊙
	I	○/●	○/●	○/●	○/●	○/●	○/●	○	○	○
Pharmaceutical e-Pedigree	L	○	○	○	○	●	○	○	○	○
	P	○	○	○	○	○	○	○	●	⊙
	I	⊙	⊙	●	●	○	○	⊙	○	○
Shipping Container Label (Full TAG ID)	L	●	●	⊙	○	○	○	⊙	⊙	⊙
	P	●	●	○	○	⊙	○	⊙	⊙	⊙
	I	○/●	○/●	○/●	○/●	○/●	○/●	○	○	○
Secured Access Control Card, No PIN	L	○	●	●	○	○	○	⊙	⊙	⊙
	P	○	⊙	⊙	○	○	○	⊙	○	⊙
	I	○/●	○/●	○/●	○/●	○/●	○/●	○/●	○/●	○/●
Unsecured Access Control Card, No PIN	L	●	●	●	●	○	○	⊙	⊙	⊙
	P	⊙	⊙	○	⊙	○	○	⊙	○	⊙
	I	○/●	○/●	○/●	○/●	○/●	○/●	○/●	○/●	○/●

Note: ○/● indicates that impact is highly dependent on the type of data or access provided.

8 Types of security safeguarding countermeasures

Countermeasures can be categorized from basic to sophisticated. In general, the more sophisticated the countermeasures, the more expensive the tag. Furthermore, not all countermeasures are applicable to all threats.

In addition, some physical measures can be employed, such as shielding, to prevent unauthorized access to tag data. Technical approaches to countermeasures are listed below. The specific risks and countermeasures are identified in Table 5.

This list of countermeasures is not comprehensive and new methods are continuously being developed to provide for security. Some emerging solutions, which at the time of publication are not available for deployment, include chaff, and tag aliasing. Others are well documented.

No single countermeasure is 100% effective in all situations. Combinations of countermeasures can be used to increase RFID data access security.

8.1 Wafer programming (true WORM)

True Write-Once-Read-Many (WORM) tags are programmed at the fabrication facility with a unique code that cannot be changed. Since the data cannot be changed after manufacture, as an example, wafer programming of a WORM device at the IC foundry prevents data from being inadvertently or clandestinely altered later in the supply chain.

8.2 ISO Tag ID verification

ISO/IEC 15963 defines a unique tag identification (Tag ID) encoded by the I.C. manufacturer. For the purposes of this countermeasure a Tag ID shall be serialized in accordance with ISO/IEC 15963 to uniquely identify the chip and then locked by the I.C. manufacturer. The Tag ID can be used to authenticate that the chip is the original and not a copy. To provide I.C. traceability and tracking, the I.C. manufacturer has a vested interest in ensuring that the Tag ID cannot be altered. The TAG ID uniquely identifies the RFID chip and the Unique Item Identifier (UII) uniquely identifies the item to which the RFID tag is attached.

The combination of Tag ID and UII, with a secure chain of custody within the supply chain, provides an assurance of anti-counterfeiting. The supplier of a tagged item communicates both the UII and the Tag ID of that item being shipped to the recipient. This solution presumes that tag identification serialization is programmed by the manufacturer and locked before distribution. At the time of this publication, the effectiveness of this countermeasure is weakened because of the availability of field programmable Tag IDs and the ability to validate when the Tag ID was manufactured.

When the original EPC UHF Gen2 specification was developed, concerns existed that the Tag ID might potentially supplant the EPC (UII); consequently the Gen2 specification did not require Tag ID serialization. EPC compliance has continued to not require Tag ID serialization through Version 1.1.0.

8.3 License plate

A license plate is the use of a non-significant number that serves only as a pointer to a database. This can provide security by not representing any sensitive information in the open. The security of this method is at a level determined by the security of the enterprise systems as shown in Figure 1.

8.4 Memory lock

Memory lock is the disabling of the write/rewrite function on the tag or a given block of memory, preventing unauthorized users from deleting or changing data or inserting unexpected data.

8.5 Password protection

A password is used to unlock the tag's memory for either read or write operations, or both.

8.6 Authentication

There are three types of authentication, data, reader, and tag authentication. At the time of this document development, reader and tag authentication standards are still in development.

8.6.1 Data authentication

Data authentication is a comparison of known validated data with read tag data. Back end systems that anticipate data content and validate that 'what is received is what is expected' is a form of data authentication.

8.6.2 Reader authentication

A process by which a tag ensures a reader is authorized to access tag data.

8.6.3 Tag authentication

A process by which a reader ensures a tag is an authorized tag to send data.

8.7 Cloaking / Data security (obfuscated ID)

For the purposes of this document *cloaking* is the process of altering the transmitted UII code that is different than the UII encoded, thereby obfuscating the identity of the item to which the RF tag is attached. There are several methods by which cloaking could be accomplished, however, at the time of this writing, none are known to be available to public standards.

8.8 Encryption

RFID security at one level can be handled through data encryption. Encryption is the process of converting a plaintext message into an alternate ciphertext message. The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer. The inverse process, of extracting the original information, is called decryption and can only be accomplished using auxiliary information, called a key (a relatively small amount of information that is used by an algorithm to customize the transformation of plaintext into ciphertext, or vice versa (1).

The use of public or private encryption schemes when writing data to the tag is discussed in detail in Annex A. The primary issue and barrier to using encryption is key distribution. A communication channel with all involved in the chain of data custody is required for successful key distribution.

8.9 Limitation of read distance

8.9.1 Frequency selection

The choice of frequency defines the distance of which the tag can be read. Many systems rely on distance as a primary means of security. Table 3 illustrates representative frequencies and typical ranges as referenced in ISO 1736X.

Table 3 – Typical tag performance

Parameter	860 – 960 MHz Passive	13,56 MHz Passive	<135 kHz Passive	433.92 MHz Active
Distance	3 meters	0.7 meter	0.7 meter	30 meter

8.9.2 Physical activation

The ability to have a tag transmit only when the user activates the tag, e.g. using a momentary switch, electrical, or physical addition to alter the readability of a tag requiring close proximity to read during a prescribed time period. Direct electrical contact offers the most secure form of physical activation

8.10 Summary

Table 5 shows threats and potential countermeasures available for that threat with a level of effectiveness as depicted by the rankings ranging from none to high. The key for the table is shown in Table 4:

Table 4 – Key for Table 5 – Threat and Countermeasure effectiveness

- None	○ Low	⭘ Moderate	● High

Table 5 – Threat and Countermeasure effectiveness

Threat → ----- Counter-measure ↓	Skimming	Eaves-dropping	Spoofing	Cloning	Data Tampering	Malicious Code	Denial of Service	Jamming
WORM	-	-	-	-	●	●	-	-
ISO Tag ID	-	-	-	⭘	-	○	-	-
License Plate	-	-	-	-	-	⭘	-	-
Memory Lock	-	-	-	-	●	●	-	-
Password PIN	⭘	-	●	⭘	⭘	⭘	-	-
Authentication	⭘	⭘	⭘	⭘	⭘	⭘	-	-
Cloaking	-	-	⭘	-	-	-	-	-
Encryption	-	-	-	-	⭘	⭘	-	-
Obfuscation/Hash/ Randomization	-	-	-	-	⭘	⭘	-	-
Read Distance / Other Constraints	○	⭘	⭘	-	-	-	⭘	⭘
Physical Activation	●	-	-	○	-	-	⭘	⭘

9 Threat response "best practices"

It is not possible to define the best approach for every product type, application and threat potential. It is up to systems designers to assess the risk and choose appropriate countermeasure(s).

However, some general guidelines can be stated:

- Limit data on tag to non-significant database pointer
- Check Tag ID
- Employ database lookup for sensitive data or validation
- Employ checksums
- Employ secondary security measures in back-end systems
- Filtering

Annex A
(informative)

Encryption

Most encryption methods can be divided into symmetric key algorithms and asymmetric key algorithms. In a symmetric key algorithm (such as DES and AES) the sender and receiver must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption. In an asymmetric key algorithm there are two separate keys: a public key is published and enables any sender to perform encryption, while a private key is kept secret by the receiver and enables him to perform decryption (1).

Some of the common encryption schemes include:

RSA uses a private and a public key. RSA is the most popular method for public key encryption and digital signatures today.

The Data Encryption Standard (DES) was developed and endorsed by the U.S. government in 1977 as an official standard and forms the basis not only for the Automatic Teller Machines (ATM) PIN authentication but a variant is also utilized in UNIX password encryption. DES is a block cipher with 64-bit block size that uses 56-bit keys. Due to recent advances in computer technology, some experts no longer consider DES secure against all attacks; since then Triple-DES (3DES) has emerged as a stronger method. Using standard DES encryption, Triple-DES encrypts data three times and uses a different key for at least one of the three passes giving it a cumulative key size of 112 - 168 bits. (2)

Advanced Encryption Standard (AES) is a block cipher adopted as an encryption standard by the U.S. government, and with worldwide and analyzed extensively. After a five-year standardization process (1) the National Institute of Standards and Technology (NIST) adopted AES as US FIPS PUB 197 in November 2001.

International Data Encryption Algorithm (IDEA) is an algorithm that was developed in the early 1990s to replace the DES standard. It uses the same key for encryption and decryption. Unlike DES, though, it uses a 128-bit key. This key length makes it impossible to break by simply trying every key, and no other means of attack is known. It is a fast algorithm, and has also been implemented in hardware chipsets, making it even faster.

Blowfish is a symmetric block cipher just like DES or IDEA. It takes a variable-length key, from 32 to 448 bits, making it ideal for both domestic and exportable use. Blowfish has been analyzed considerably and is gaining acceptance as a strong encryption algorithm.

Software-optimized Encryption Algorithm (SEAL) was developed in 1993 and is a Stream-Cipher, i.e. data to be encrypted is continuously encrypted. Stream Ciphers are much faster than block ciphers (Blowfish, IDEA, DES) but have a longer initialization phase during which a large set of tables is done using the Secure Hash Algorithm. SEAL uses a 160 bit key for encryption and is considered very safe.

RC4 is a cipher that is used in a number of commercial systems like Lotus Notes and Netscape. It is a cipher with a key size of up to 2048 bits (256 bytes), which on the brief examination given it over the past year or so seems to be a relatively fast and strong cypher. It creates a stream of random bytes and 'XORing' those bytes with the text. It is useful in situations in which a new key can be chosen for each message.

Although data encryption has been well established and numerous schemes have been presented, they present a challenge for RFID and contactless card applications. Public Key Cryptography System (PKCS) for security is an option for RFID where multiple tags talk to a reader. The premise behind PKCS is the use of a public and private key where the public key is sent to the users. This is the general concept behind PGP.

Security Standards

FIPS 199 Standards

Overview (5):

A new Federal Information Processing Standard (FIPS), recently approved by the Secretary of Commerce, will help federal agencies protect the information and information systems that support their operations and assets. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, is an important component of a suite of standards and guidelines that NIST is developing to improve the security in federal information systems, including those systems that are part of the nation's critical infrastructure.

FIPS 199 will enable agencies to meet the requirements of the Federal Information Security Management Act (FISMA) and improve the security of federal information systems. The security standard will also make it possible for federal agencies to establish priorities for protecting their information systems, ranging from very sensitive, mission-critical operations to lower-priority systems performing less critical operations. Background information on NIST's efforts to provide the security standards, guidelines, and technical tools for implementing FISMA is available at: http://csrc.nist.gov/sec-cert/ca-background.html.

FIPS 199 is effective immediately and applies to:

— All information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and

— All federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2).

Why Security Categorization Standards Are Needed

FISMA, Title III of the E-Government Act of 2002 (Public Law 107-347), was passed in December 2002. This legislation recognizes the importance of information security to the economic and national security interests of the United States, and tasked NIST with responsibilities for standards and guidelines, including the development of:

— Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

— Guidelines recommending the types of information and information systems to be included in each category; and

— Minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each such category.

By providing a common framework and method for categorizing information and information systems, FIPS 199 responds to the first task assigned to NIST. Use of this standard will enable agencies to identify and prioritize their most important information and information systems by defining the maximum impact a breach in confidentiality, integrity, or availability could have on the agency's operations, assets, and/or individuals.

A FIPS 199 security categorization serves as the starting point for the selection of security controls for an agency's information system—controls that are commensurate with the importance of the information and information system to the agency. Additional NIST guidance will instruct agencies how to use FIPS 199 to select minimum security controls for an information system and subsequently assess the controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

Scope of FIPS 199:

1. The E-Government Act of 2002 (Public Law 107-347)

2. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with responsibilities for standards and guidelines, including the development of:

— Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels

— Guidelines recommending the types of information and information systems to be included in each category

— Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category.

FIPS 140-2

The National Institute of Standards and Technology (NIST) issued the 140 Publication Series to coordinate the requirements and standards for cryptography modules, which include both hardware and software components for use by departments and agencies of the United States federal government. FIPS 140 does not purport to provide sufficient conditions to guarantee that a module conforming to its requirements is secure, still less that a system built using such modules is secure. The requirements cover not only the cryptographic modules themselves but also their documentation and (at the highest security level) some aspects of the comments contained in the source code.

User agencies desiring to implement cryptographic modules should confirm that the module they are using is covered by an existing validation certificate. FIPS 140-1 and FIPS 140-2 validation certificates specify the exact module name, hardware, software, firmware, and/or applet version numbers. For Levels 2 and higher, the operating platform upon which the validation is applicable is also listed. Vendors do not always maintain their baseline validations.

Bibliography

[1] ISO/IEC Directives, Part 2, Rules for the structure and drafting of International Standards, 2001

[2] http://encyclopedia.thefreedictionary.com/Data%20encryption

[3] http://www.mycrypto.net/encryption/crypto_algorithms.html

[4] http://www.aimglobal.org/standards/rfidstds/RFIDStandard.asp

[5] http://www.ntru.com

[6] The Federal information Security Management Act (FISMA) - FIPS PUB 199

[7] Federal Information Processing Standard (FIPS) 199

[8] FIPS 140-2

[9] http://www.itl.nist.gov/lab/bulletns/bltnmar04.htm

[10] Chaff describes the creation of a noisy background with the ability to detect a signal of known characteristic. [For further information about chaff and rogue tags and receivers see NIST Special Publication 800-98, Guidance for Securing Radio Frequency Identification (RFID) Systems, [11], [12]]

[11] M.R. Rieback, B. Crispo, A.S. Tanenbaum. "The Evolution of RFID Security." IEEE Pervasive Computing, vol. 5(1):62-69, 2006

[12] Stephen Weis. ”Security and Privacy in Radio-Frequency Identification Devices”, Master’s Thesis, Massachusetts Institute of Technology, May 2003

Template for comments and secretariat observations

Date: 2008-05-17	Document: **31nXXXX_31n2508_DoC_24729-4**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
JP				Security function is needed for RFID system as same as IC card system. We agree the NP titled RFID guideline on tag data security but we found out some confusing expression of application naming in PDTR document table 1. Ex. Contactless payment This is one of the IC card applications (SC17).	We propose that this PDTR should distribute other security related SC's for comments to decrease these confusing expression and to avoid misunderstandings.	The Project Editor would like to draw the National Body's attention to 31n1154, the results of which were reported and approved unanimously by SC 31 in 31n1171, *only comments submitted on the adopted form (13B) will be accepted.* SC 17 is a liaison member to SC 31 and is copied on all SC 31 documents. The project editor requests the SC 31 Secretariat forward DTR 24729-4 to the SC 17 Secretariat for information
SE	2			Last part of description of "ISO/IEC 24791-6" should be changed from "Part 1: Device Management" to "Part 6: Security"	Last part of description of "ISO/IEC 24791-6" should be changed from "Part 1: Device Management" to "Part 6: Security"	The Project Editor would like to draw the National Body's attention to 31n1154, the results of which were reported and approved unanimously by SC 31 in 31n1171, *only comments submitted on the adopted form (13B) will be accepted.* Agreed – Clause 2 corrected
SE		Figure 1		In RFID contexts the term "Air interface" is used for the tag <-> reader interface. Due to this we propose the usage of the term is removed from the reader <-> enterprise interface. Possible replacements are, WLAN, Wireless Networks, etc.	In RFID contexts the term "Air interface" is used for the tag <-> reader interface. Due to this we propose the usage of the term is removed from the reader <-> enterprise interface. Possible replacements are, WLAN, Wireless Networks, etc.	Agreed – Figure 1 modified

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Resolutions of the Ballot Resolution Meeting
PDTR Ballot of ISO/IEC 24729-4
Toronto, Canada,

Date: 4 June 2008
Number: SG5n0064

RESOLUTION 1

The BRM committee for the PDTR of 24729-4 accepts the Disposition of Comments (SG5n0061_31n2508_DoC_24729-4_13B_format_20080517), and instructs the project editor to incorporate the comments into the revision of ISO/IEC DTR 24729-4 .
- Unanimous

RESOLUTION 2

The project editor is instructed to submit the revision document (SG5n0062) to the SC31 Secretariat for DTR ballot.
- Unanimous

APPRECIATION

1. The BRM committee thanks Don Ferguson, the National Body of Canada and the Standardization Council of Canada for their excellent organization and support in arranging the meetings in Toronto, Canada.
- Acclamation

2. The BRM committee also thanks the following companies for their sponsorship of this meeting, including: Lyngsoe Systems, Intermec, GS1 Canada, Sirit, International Post Corporation, iPico, Industry Canada and RFID Canada.
- Acclamation