sirit
vision beyond sight™

Sirit Guidelines for RFID Security in AVI Applications

Thomas J. Frederick and Scott McMillan

Sirit Guidelines for RFID Security in AVI Applications

By Thomas J. Frederick and Scott McMillan

May 4, 2009

This product is covered by one or more of the following patents: U.S. Patent No. 7,199,713, 7,209,040, 6,346,881, and 6,617,962.

Disclaimer and Limitation of Liability

The content of this paper is for information use only and is subject to change without notice. Sirit assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication. No part of this paper may be reproduced in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Sirit.

About Sirit

Sirit Technologies designs, develops, manufactures and sells Radio Frequency Identification (RFID) technology. Targeted at a diverse set of markets RFID technology has become a core technology for applications including: electronic toll collection, access control, cashless payment systems, product identification, and supply chain management systems including logistics, warehousing and manufacturing, and asset management.

Head Office - Canada
372 Bay Street, Suite 1100
Toronto, Ontario, M5H 2W9 Canada
Tel: 416.367.1897
Fax: 416.367.1435
Toll Free: 1.800.498.8760
Email: mail@sirit.com

Sirit Technologies - US
1321 Valwood Parkway, Suite 620
Carrollton, Texas 75006 United States
Tel: 972.243.7208
Fax: 972.243.8034
Toll Free: 1.866.338.9586

Web: www.sirit.com

Contents

This page intentionally left blank.

1 Introduction

Security is a common concern in today's AVI applications. As of this writing there are workgroups within ISO (JTC1/SC31/WG4) and EPCglobal (Data Protection Group) dealing exclusively with security, as well as numerous publications on the topic by experts in the field ([1-13]). While it is clear that ISO 18000-6C and Gen2 standards will keep moving forward the state-of-art in RFID security, present AVI deployments must provide reasonable levels of security now for potential threats faced.

The security risks faced by AVI include business risk such as cloning or counterfeiting and intelligence risk such as skimming license numbers, vehicle identification numbers, or other personally identifiable information off of tags [1]. By carefully developing tag and reader authentication algorithms, data protection layers, and key management systems, the AVI application can be assured of state of the art security.

This document provides guidelines and best practices for AVI security using Sirit RFID and introduces additionally available Sirit security services. Note all Sirit security technology described in this document require IDentity 5100 (ID5100) firmware version 2.1 or later.

2 Tag Authentication

The tag authentication algorithms provide a mechanism to detect cloned or counterfeit tags. Sirit provides three options for tag authentication. Each option will be presented in the following sections followed by a summary of the customer implementation requirements and issues with sharing tags among multiple vendors.

2.1. Unique TID Authentication

Each Sirit ISO18000-6C tag has a unique factory locked serial number in tag ID (TID) memory that can be authenticated using Sirit RFID equipment. Figure 1 provides an example that illustrates how Sirit equipment implements TID authentication using an ID5100 and an ISO 18000-6C tag. The reader can validate the TID memory to be from an authentic tag as well as take the extra step of validating the TID memory against a mask based upon the TID serial numbers ranges used in the customers system.

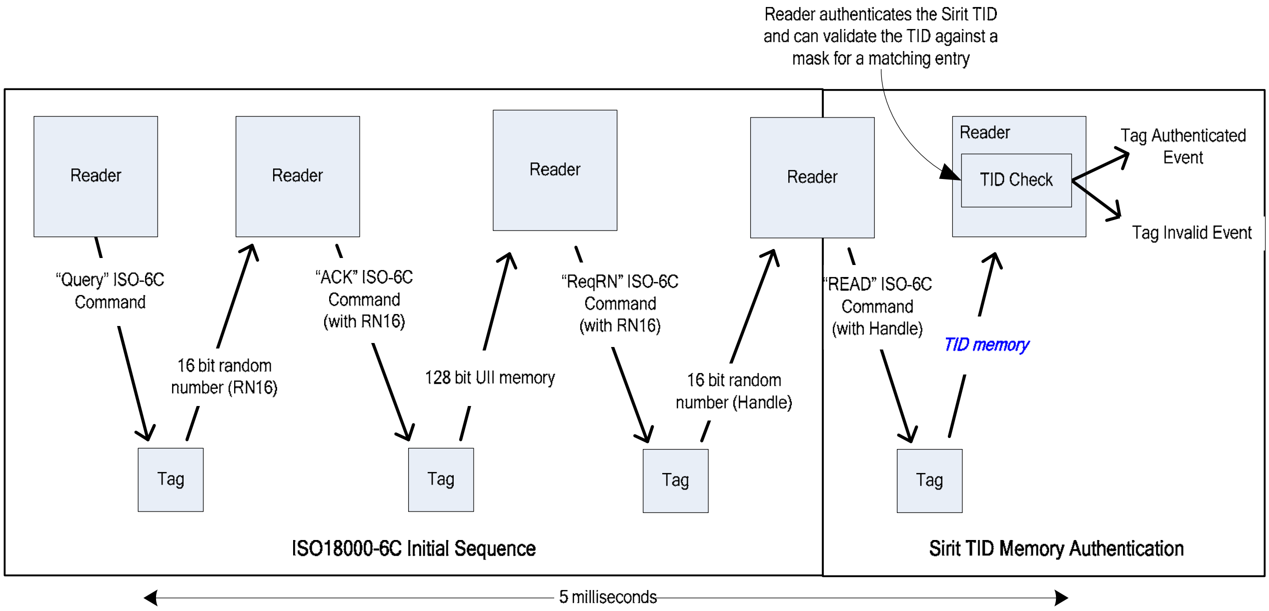
Reader authenticates the Sirit TID and can validate the TID against a mask for a matching entry
Reader
Reader
Reader
Reader
Reader
TID Check
Tag Authenticated Event
Tag Invalid Event
"Query" ISO-6C Command
16 bit random number (RN16)
"ACK" ISO-6C Command (with RN16)
128 bit UII memory
"ReqRN" ISO-6C Command (with RN16)
16 bit random number (Handle)
"READ" ISO-6C Command (with Handle)
TID memory
Tag
Tag
Tag
Tag
ISO18000-6C Initial Sequence
Sirit TID Memory Authentication
5 milliseconds

Figure 1 Communication sequence using ISO 18000-6C and validating unique TID

2.2. Challenge-Response Authentication

ISO18000-6C tags provide the ability to lock memory with a 32 bit password. This ability to lock memory can be used to authenticate by ensuring the tag "knows" the password. The ID5100 will access protected memory with a password challenge to the tag and will analyze the response to ensure the tag knows the correct password. This password will always be sent over the air in an encrypted form using the one time pad cover codes available via the ISO18000-6C protocol. Figure 2 provides an example of a communication sequence that would be used in a challenge-response authentication on Sirit's ID5100 and ISO 18000-6C tags.

The password used by each tag will be unique and generated using SHA-1 hash of the tag unique TID and a secret key. This will ensure that a compromised tag password will not expose the entire system. Section 5 provides information on the secret key used with the TID to generate the unique password for the tag. Note, for customers not using Sirit tags with serialized TIDs, there is an option to use the Unique Item Identifier (UII) instead of the TID to generate the tag unique ID via the SHA-1 hash.

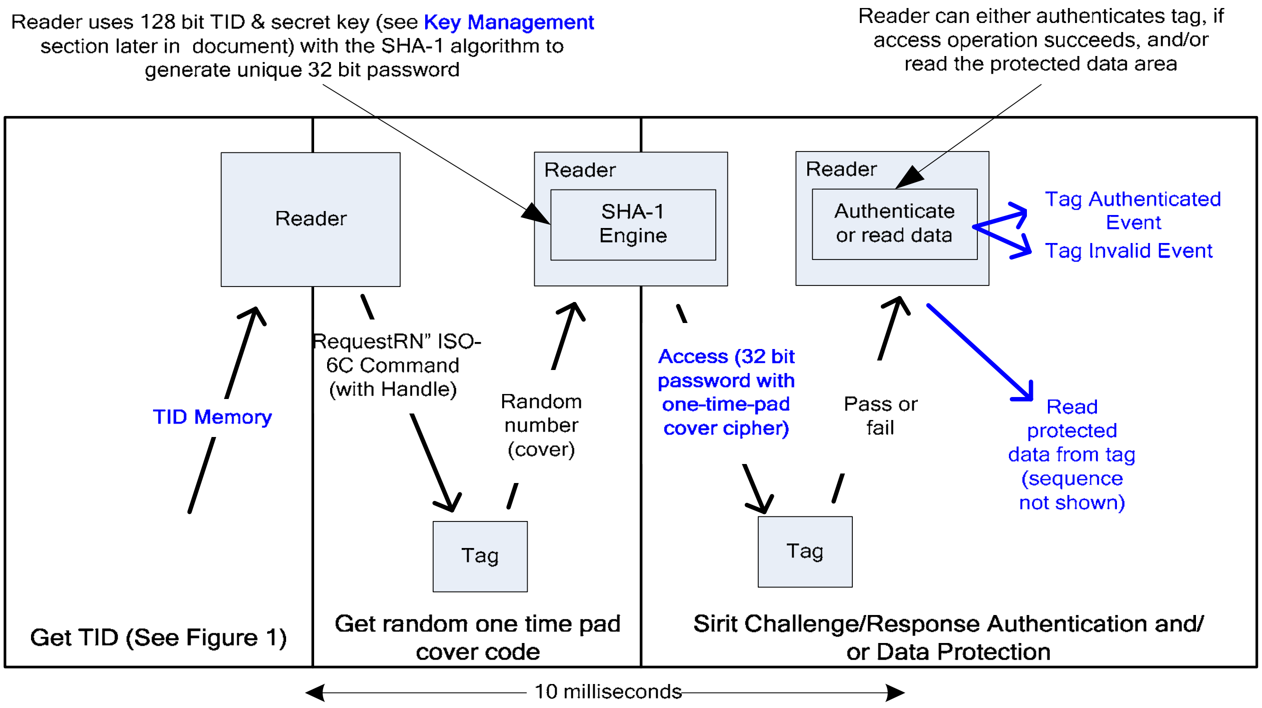
Reader uses 128 bit TID & secret key (see Key Management section later in document) with the SHA-1 algorithm to generate unique 32 bit password
Reader can either authenticates tag, if access operation succeeds, and/or read the protected data area
Reader
TID Memory
Get TID (See Figure 1)
Reader
SHA-1 Engine
RequestRN" ISO-6C Command (with Handle)
Random number (cover)
Tag
Get random one time pad cover code
Reader
Authenticate or read data
Tag Authenticated Event
Tag Invalid Event
Access (32 bit password with one-time-pad cover cipher)
Pass or fail
Read protected data from tag (sequence not shown)
Tag
Sirit Challenge/Response Authentication and/ or Data Protection
10 milliseconds

Figure 2 Communications sequence using 18000-6C tags for password challenge-response authentication and/or data protection

2.3. Packet Counters

Packet counters provide an effective mechanism for back end systems to audit tags and detect clones. A portion of user memory will be required to store the packet counter. The ID5100 will read the packet counter in tag user memory, increment it by one, and write it back out to the tag each time the tag passes through a read point. The packet counter, along with a timestamp and the tag data, will be reported to the back end server. The back end system can then validate that the reads of the tag are progressing sequentially to ensure presence of only one tag with a particular Unique Item Identifier (UII) in a system. Discontinuities or duplications in the packet counter and timestamps are an indication that this tag has been cloned.

2.4. Tag Authentication Implementation Summary

2.4.1. Unique TID Authentication

- **Reader Commissioning Requirements** – Setup tag TID authentication and/or TID serial number mask.
- **Tag Commissioning Requirements** – Serial numbers must be within the TID mask if TID serial number mask turned on.
- **Effectiveness** – Medium, very effective when used in conjunction with challenge-response.
- **Multiple Vendor Issues** – TID serial number ranges must be shared if serial number mask is turned on.

2.4.2. Challenge Response Authentication

- **Reader Commissioning Requirements** – Generate secret keys, install keys on reader in encrypted, hidden, and obfuscated form.
- **Tag Commissioning Requirements –** Configure lockable memory with passwords based upon TID and secret keys. Write key index into tag user memory (see Section 5 on key management).
- **Effectiveness** – High.
- **Multiple Vendor Issues** – Vendors must share the same set of secret keys.

2.4.3. Packet Counters

- **Reader Commissioning Requirements** – Setup location in memory for reader to use as packet counter.
- **Tag Commissioning Requirements** – Reserve and initialize user memory location for packet counters.
- **Effectiveness** – High, relies upon back end system to perform auditing of tag packet counters.
- **Multiple Vendor Issues** – Vendors will need to share the packet counter information along with the UII when accounts get paid.

3 Reader Authentication

Reader authentication provides a mechanism for tags to ensure that sensitive information on the tag will only be made available to the appropriate readers. Sirit ISO18000-6C tags can password lock user memory for read and/or write access to accomplish this task.

While not preventing the tags UII or TID memories from being read, this does provide a form of reader authentication before providing access to protected areas on the tag. These capabilities, combined with the tag authentication algorithms of Section 2, provide a means to ensure mutual authentication using Sirit ISO18000-6C tags.

Please see Section 4.1 for an example of reader authentication access to read locked memory.

4 Tag Data Protection

The data protection layer ensures that valuable information cannot be retrieved from the tag. Sirit provides data protection through a read lockable memory mechanism. This option will be discussed in more detail below followed by additional data protection approaches built upon and completely controlled by customer back end systems. A summary of implementation requirements and issues with sharing tags among multiple vendors will complete this section.

4.1. Read Lockable Memory

Sirit ISO18000-6C tags provide the ability to read lock memory with a 32 bit password. This ability can be used to prevent unauthorized access to a tags data to only those readers with the appropriate password. This password will always be sent over the air in an encrypted form using the one time pad cover codes available via the ISO18000-6C protocol. Figure 2 provides an example of the communication sequence used to access memory using a tag unique password.

The password used by each tag is unique and is generated using SHA-1 hash of the tag TID (or UII) and a secret key. This ensures that a compromised tag password will not expose the entire system. Section 5 provides information on the secret key used with the UII to generate the unique password for the tag. See Section 2.4.2 for a mechanism that utilizes this same lockable memory capability to provide tag authentication.

4.2. Customer Encrypted Tag Data

Customers with back end systems can provide their own mechanisms for encryption and decryption of stored tag data, completely controlling access to the data. Figure 3 provides a flow chart showing how this might be done. Using this method, the tag will only be a carrier of encrypted data and the customers back end systems will control the encryption and keys. Sirit products will never touch the plain text customer records.

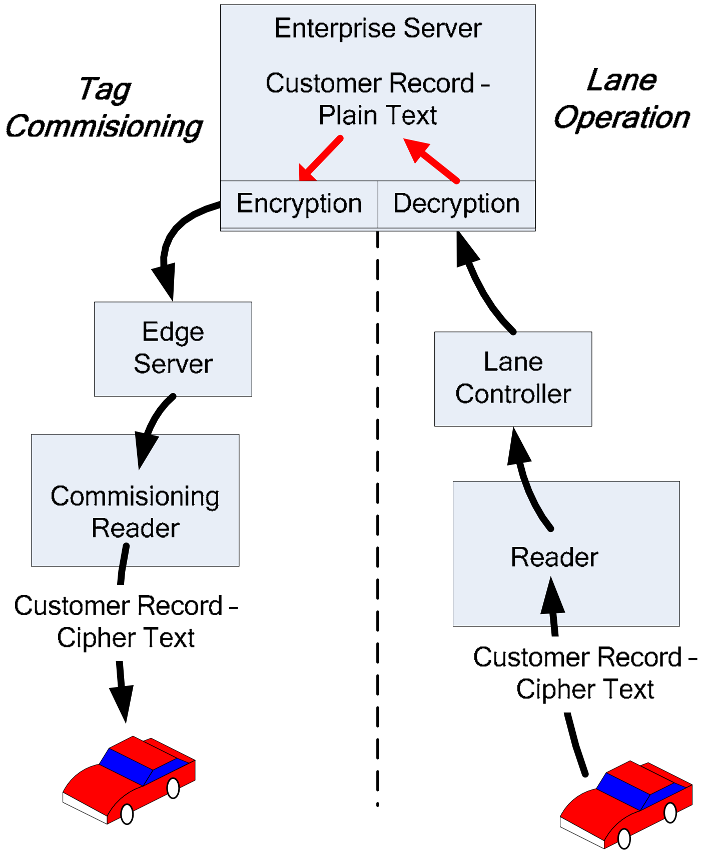

Figure 3 Storing encrypted data on tags

4.3. Data Protection Implementation Summary

4.3.1. Read Lockable Memory

- **Reader Commissioning Requirements** – Generate secret keys, install keys on reader in encrypted, hidden, and obfuscated form.
- **Tag Commissioning Requirements** – Configure read lockable memory with passwords based upon TID and secret keys. Write key index into tag user memory (see section on key management).
- **Effectiveness** – High.
- **Multiple Vendor Issues** – Vendors must share the same set of secret keys and will have to agree on the data organization and ownership of the password protected block.

4.3.2. Customer Encrypted Tag Data

- **Reader Commissioning Requirements**
  None, reader does not interpret data
- **Tag Commissioning Requirements**
  No extra requirements, data needs to be written to the tag with or without encryption
- **Effectiveness**
  High
- **Multiple Vendor Issues**
  Data will only be readable by the vendor writing data to tag and vendors will have to agree on organization and ownership of tag user memory

5 Password/Key Management

The use of challenge-response passwords for tag authentication and data protection requires a key management system [4]. Sirit employs a key indexing scheme for key management and a symmetric key and tag TID (or UII) based SHA-1 hash to generate a unique per tag password for authentication and data protection. As stated previously in Sections 2.4.2 and 4.3.1, the secret keys cannot be extracted from the reader thereby offering further system protection. The text below describes this key indexing scheme in more detail.

5.1. Key Indexing

Sirit will encode a plain text key index record in the tag user memory which indicates which key to use for that specific tag. Figure 4 provides an example of the key index in tag user memory. When a vehicle is brought in for scheduled renewal the key index can be updated. Note that the key index is simply a record number for a key database, but the keys themselves are never transmitted over the air.

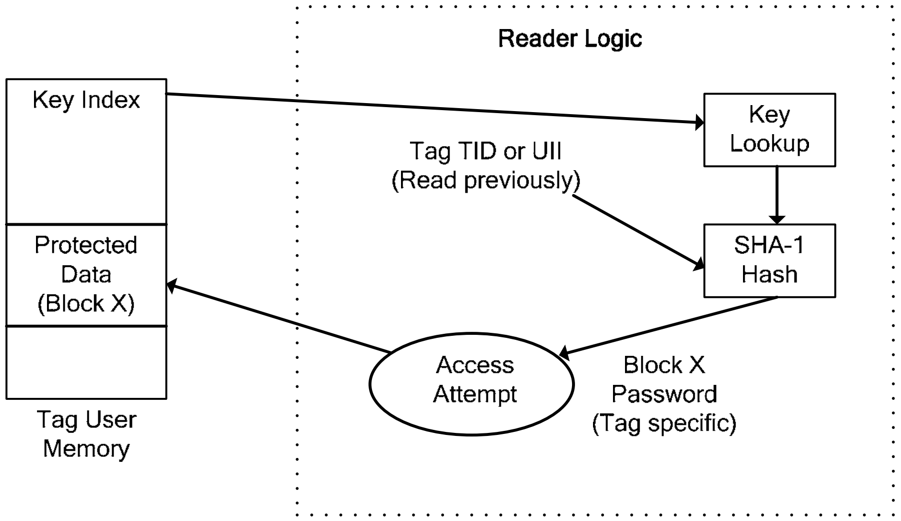

Figure 4 Key index, password generation, and block access

5.2. Password Generation

As shown in Figure 4, Sirit will generate a tag specific password utilizing both the secret key and the TID (or UII) read from the tag. A SHA-1 hash will generate the tag specific password that will be used to access the protected data block. This password will be written into the tag during commissioning and as discussed in Sections 2.2 and 4.1, the tag password will be sent over the air in an encrypted format when accessing the protected area of the tag.

6 Sirit Security Services

In order to provide optimal AVI security, Sirit can provide additional security services for tag commissioning and/or customized vendor security solutions.

6.1. Tag and Lane Reader Commissioning

Sirit can provide tag commissioning as an option for those customers requiring the utmost in cloning and data protection. Tags provided to customers will be enabled with TID and password authentication protection at time of delivery. Additionally, Sirit will commission lane readers with the information needed to read and authenticate tags only and will not allow the lane readers to write to the data areas or change the access passwords. This will:

- Prevent unauthorized access to commissioning readers outside of Sirit.
- Reduce chain of access to encrypted keys.

6.2. Customized Security

Additional security measures may be required on a case by case basis. For example, if multiple vendors require sharing of a tag in a seamless manner, Sirit can provide custom trusted third party solutions. Please contact a Sirit representative for more information.

7 Conclusion

Sirit provides the products, tools, services, and best practices for effective AVI tag security. With tag authentication, reader authentication, data protection, key management, and trusted third party services, customers can feel confident that Sirit provides the state of the art in ISO18000-6C security. Please contact a Sirit representative for more information.

A Transitioning Existing ISO18000-6C Tag Populations

Many customers will have an existing population of ISO18000-6C tags and will want to know how to integrate their current tag base into a new system with secure Sirit tags and readers. The simplest and quickest approach to handling the older tags would be to continue to utilize the previous tag handling algorithms for those tags marked as inauthentic or incompatible by the security algorithms of the new system. These older tag algorithms could exist as applications on either a lane controller or embedded directly on the Sirit reader.

Customers could also take the approach of transitioning the old ISO18000-6C tags to utilize the new security features. This can be done prior to commissioning the new system security features in order to avoid using the older tag handling algorithms. Unfortunately, this approach will require that all existing tags be serviced before starting up the secure system. More likely, this transition will be done slowly over time, necessitating the use of the old tag algorithms until all system tags contain the new security algorithms.

The sections to follow will consider both tag authentication and tag data protection in the context of transitioning existing ISO18000-6C tags to utilize the new security algorithms.

A.1 Tag Authentication

A.1.1 TID Authentication

If all the TID memories of the existing tag base have an easily maskable value, the TID authentication mask can be used to validate older tags. Otherwise, TID authentication will not be available on the reader for older tags. Of course, lane controllers can implement a TID database that provides a similar function outside of the Sirit reader.

A.1.2 Challenge-Response Authentication

Challenge-response authentication requires that existing tags have a mechanism to read or write lock user memory. Without this capability, this type of authentication may not be used with older tags. In addition, if the TID memories are not serialized, the UII must be used for generating the tag specific passwords (see Section 5.2).

If the existing tags do have the ability to provide an access password to user memory, the tags will have to be brought in for commissioning. At the time of commissioning, the appropriate tag specific passwords will be written in to the tag along with a key index (see Section 5.1).

A.1.3 Packet Counters

Packet counters will require that the existing tags have available user memory to utilize for packet counters. Without available user memory, packet counters may not be used on existing tags. If the tag does have available user memory and that memory location is the same as the packet counter memory used on the new tags, this algorithm can be used immediately on older tags.

A.2 Tag Data Protection

A.1.4 Read Lockable Memory

Read lockable memory requires that existing tags have a mechanism to read lock user memory. Without this capability, this type of tag data protection may not be used with older tags. If the existing tags do have this ability, the tags will need to be brought in for commissioning where the passwords will be programmed accordingly (see section A.1.2).

A.1.5 Customer Encrypted Tag Data

Existing tags with enough available memory can utilize the customer encrypted tag data feature. As discussed in Section 4.2, the tag acts as a carrier of data and any tag with user memory can be utilized. Of course, tags without enough memory cannot use this feature and tags that can support it must be commissioned accordingly.

References

[1] Guidelines for Securing Radio Frequency Identification (RFID) Systems, National Institute of Standards and Technology (NIST), Special Publication 800-98, April 2007

[2] Chun-Te Chen; Kun-Lin Lee; Ying-Chieh Wu; Kun-De Lin; "Construction of the Enterprise-level RFID Security and Privacy Management Using Role-Based Key Management", *Systems, Man and Cybernetics*, 2006, IEEE International Conference on Volume 4, Oct. 2006

[3] Namje Park; Jooyoung Lee; Howon Kim; Kyoil Chung; Sungwon Sohn, "A Layered Approach to Design of Light-Weight Middleware Systems for Mobile RFID Security", *Network Operations and Management Symposium*, 2006

[4] Hyun-Seok Kim; Jun-Hyun Oh; Ju-Bae Kim; Yeon-Oh Jeong; Jin-Young Choi; "Formal Verification of Cryptographic Protocol for Secure RFID System", *Networked Computing and Advanced Information Management*, 2008. NCM '08. Fourth International Conference Sept. 2008

[5] - Hyun-Seok Kim; Jeong-Hyun Oh; Jin-Young Choi; "Security Analysis of RFID Authentication for Pervasive Systems using Model Checking", *Computer Software and Applications Conference*, 2006. COMPSAC '06. 30th Annual International Volume 2, Sept. 2006

[6] Ari Juels, "RFID Security and Privacy: A Research Survey", *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, February 2006

[7] Ari Juels, "Strengthening EPC Tags Against Cloning", RSA Laboratories

[8] Daniel V. Bailey and Ari Juels, "Shoehorning Security into the EPC Standard", RSA Laboratories

[9] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, "The Evolution of RFID Security", *Pervasive Computing*, January-March, 2006

[10] R. Chandramouli, T. Grace, R. Kuhn, and S. Landau, "Security Standards for the RFID Market", *IEEE Computer Magazine*, November/December 2005

[11] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and Privacy in RFID and Application in Telemedicine", *IEEE Communications Magazine*, April 2006

[12] Bruce Schneier, *Applied Cryptography*, John Wiley and Sons, Inc, 1996

[13] Niels Ferguson and Bruce Schneier, *Practical Cryptography*, Wiley Publishing, 2003

vision beyond sight™

SIRIT - CANADA
372 Bay Street, Suite 1100
Toronto, ON M5H 2W9 Canada
Tel: 416.367.1897
Fax: 416.367.1435

SIRIT - USA
1321 Valwood Parkway, Suite 620
Carrolton, TX 75006 USA
Tel: 972.243.7208
Fax: 972.243.8034

For more Information
call toll free:

1.800.498.8760 (CA)
1.866.338.9586 (US)

www.sirit.com