

SECURITY CONSIDERATIONS FOR EMBEDDED SYSTEM RFID READERS

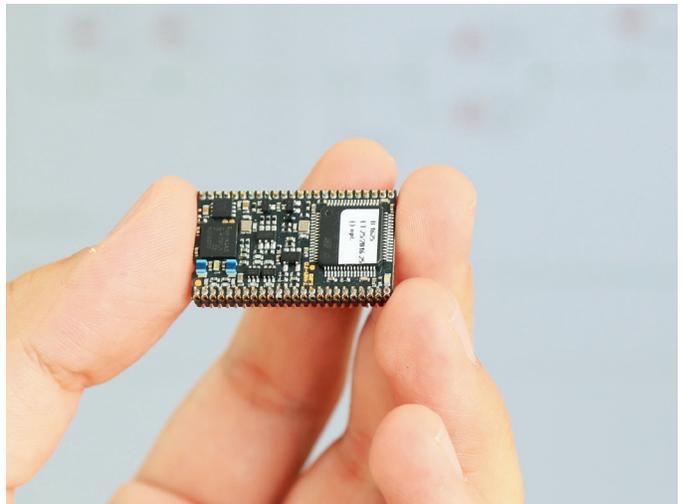
By Kiran Vasishtha, ELATEC, Inc.

This article is the third in a series on considerations for embedded system RFID readers for embedded engineers, solution architects and product managers.

In recent years, multinational corporations such as Cathay Pacific, Facebook, Uber and numerous others have been heavily fined due to security and data protection violations. This period has seen data protection laws increase as more and more information is gathered and shared online. As such, it becomes crucial to account for security capabilities when choosing an embedded device that touches potentially sensitive data.

RFID readers very much belong to the ecosystem wherein personal or user identification data is transmitted either to a host system such as a PC or to an endpoint such as a Human Machine Interface (HMI). A passive RFID transponder, soft credential such as a mobile phone app using BLE/NFC or smart cards and other contact-based credentials all can carry sensitive data or personal information. In the case of smart card or contact-based credentials, the storage of personal information such as name, address or date of birth is more prevalent compared to contactless credential where an identification number may be used.

In general, security as a concept is always related to the entire system that includes RFID media (contact/contactless credentials), RFID reader, the host system



and any database or cloud server. While accounting for security across a system is needed it is more important to consider the application or use case that is in question. One should carefully evaluate the consequences of any security breaches and if there is any sensitive information being exchanged from the RFID media to the host. As an example, the simple choice of RFID media may directly lead to a compromise in your intended application's security. There are numerous references on security vulnerabilities related to Low Frequency (125KHz) contactless transponder types. The references focus on using interceptors to access unprotected static card information. The adversaries may then clone this credential that may be used for triggering action such as granting access to a

facility or unlocking a computer. Some references also highlight vulnerabilities in the Wiegand interface about intercepting the data signals to capture card value.

Therefore, some older RFID transponders and communication interfaces that may be based on the aforementioned technology or have been subject to vulnerability hacks are now considered fundamentally compromised.

As mentioned previously, the overall security depends on every component of the system that includes the RFID reader. This article will mainly focus on some of the basic security considerations that need to be accounted for when choosing an RFID reader but also whether or not your application requires these abilities. Some of the key security considerations are as follows:

THE CONSIDERATIONS ARE:

1. DOES YOUR APPLICATION REQUIRE ENCRYPTION CAPABILITIES? IF SO, DOES THE READER HAVE THE CAPABILITY TO EXECUTE CRYPTOGRAPHIC ALGORITHMS?

In every application where RFID technologies are involved there is a need to first assess whether encryption is required and if so, determine the exact channel where this needs to be enforced. It could be that the host interface requires the exchange of encrypted data or the air interface needs to transfer protected data. Once the requirements are established, one may then evaluate the strength of this security.

Furthermore, many types of contactless transponders can store data within their memory segments and encrypt or lock these segments with cryptographic keys. An apt card reader is one that can not only decrypt the memory segments and access the data but also provides an easy means for the end-user to carry out this operation. In many instances, the end-users have their own customized cryptographic keys for their credentials and are unwilling to share these keys with the card reader provider. Therefore, having the capability to load custom keys by someone other than the card reader manufacturer becomes essential. This can be facilitated in multiple ways, such as implementing high-level APIs and allowing the user to write applications for the card reader, or it could be enabling the customer with a graphical user interface to enter keys used to access data sectors.

2. DO YOU REQUIRE ENCRYPTED DATA EXCHANGE? IF SO, WHERE AND CAN THE CARD READER SUPPORT THIS?

In a typical scenario, the card reader behaves as a medium to facilitate data collection and transfer between the contactless or contact-based transponder and the host system. The host system can either be an endpoint that locally validates the credential presented to it or it can be a microcontroller that sends data over the network to the cloud or a database for validation and authentication. As mentioned previously, assessing whether the need for encryption is between the RFID media and the reader or from the reader to the host is important. If the former, the appropriate credentials are required. Depending on this factor you may then consider choosing an appropriate RFID reader.

There are use cases wherein personal information such as name, address, date of birth or biometric data can be stored within the credential, eg: smart cards or passports as credentials. Therefore, encrypting the exchange of such data both between the credential and the reader as well as the reader and the host becomes critical. Moreover, encryption algorithm engines such as AES, DES, 3DES, or the capability to implement custom algorithms, need to be present on the card reader as this enables ease of integration. In cases where smartcards or contact-based credentials are used, the host system typically drives the communication in its entirety. So, the card reader must also have:

- + **Software capabilities** such as Personal Computer Smart Card (PCSC) or Chip Card Interface Device (CCID) mode of communication. The availability of drivers to facilitate communication with the host also enables easy software integration.
- + **Hardware support for communication standards** such as ISO7816 and the presence of Secure Access Modules (SAM) slots and other contact-based interfaces.

3. DOES YOUR APPLICATION REQUIRE MUTUAL AUTHENTICATION WITH SECURE ACCESS MODULES (SAM) AND RFID MEDIA? IF SO, DOES THE READER SUPPORT THIS?

A Secure Access Module is a type of smart card that follows a contact-based communication standard to interact with a card reader. These modules ensure the protection of security keys as well as facilitate cryptographic operations. Typically, SAMs are used to generate application keys based on a specific master key or to generate session keys. They also enable secure messaging between the RFID media, the reader and the host system.

Many contactless credentials hold memory segments/applications that are encrypted with cryptographic keys. These keys are often stored in SAMs and supplied to card reader manufacturers. This not only ensures the security of the keys but adds a step in the authentication process. The card reader in this case should first perform authentication operations with the SAM and then carry out a series of cryptographic and bit manipulation operations between the contactless card and the SAM. This can be further secured by adding a key diversification step. The card reader must be able to support such a scenario both in the hardware as well as in the software. Many end-users require the card reader to natively support such a scenario and have the ability to provide high-level API's to help in their implementation. In addition to this, high-security applications demand the transfer of data in an encrypted format. One can ensure end-to-end encryption/security with the help of SAMs. In such an architecture, the reader facilitates mutual authentication with the RFID media and the SAM, thus transferring protected data over a Radio-Link and also ensuring the security of encryption keys. The reader can also transfer data encrypted by the SAM to the host system maintaining a high level of security across the system.

Note that the safety of distributing SAMs as well as administering the installation process within the reader should be treated as a separate issue and tackled accordingly. There is also an issue of the readers being

stolen or the SAM modules being dismantled from the reader. The security considerations here do not indulge in these topics and appropriate precautions are to be put in place to improve the overall security of the system.

4. DOES THE CARD READER HAVE COMMUNICATION INTERFACES OTHER THAN WIEGAND SUCH AS RS485 OR RS232?

The Wiegand card as well as the Wiegand interface for data transmission is a 40-year old technology that originates from the Wiegand effect discovered by John R. Wiegand in the early 1970s. While the Wiegand cards are still in production, they have been largely replaced by newer and cheaper forms of access cards. However, these cards are still based on the Wiegand data format that is susceptible to interception as the data are available in plain text. Also, the Wiegand interface introduced in the 1980s remains prevalent across the logical access as well as the physical access control industry despite various security vulnerabilities. This technology no longer conforms to the current security standards. It is therefore important for integrators to choose a communication interface that can offer higher security from interception and support encrypted data exchange.

5. DO YOU REQUIRE TAMPER DETECTION TECHNOLOGIES? IF SO, CAN THE READER MEET THIS REQUIREMENT?

The need for tamper detection largely varies from one application to another so it is more important to consider whether this level of security is suitable for your respective use case. As an example, card readers attached to multi-function printers (MFPs) for releasing print jobs in an enterprise environment can be considered less critical since tampering with the reader can ultimately lead to the downtime of the printers but will not compromise the safety of your documents. Typically, in such scenarios, the card reader works hand in hand with the MFP and a print management solution that ensures the release of print jobs. Therefore, if the card reader is sabotaged

or tampered with, the MFP or the solution simply prevents the release of any information. On the other hand, high-security environments such as data centers certainly need greater protection. One must thoroughly evaluate the consequences of any attempts directed towards compromising the device integrity or the data associated with the device. These topics need to be considered separately and are outside the scope of this article. In conclusion, depending on the application, the credentials involved as well as the data that is being exchanged with the card reader and eventually the host, tamper detection technologies can improve the security of the device. There are several technologies in the market such as mechanical and optical tamper detectors that can be embedded directly on the card reader for superior protection against threats.

6. DO YOU REQUIRE THE READER'S CONFIGURATION OR FIRMWARE TO BE SECURELY SHARED OR LOADED ON THE CARD READER? IF SO, CAN THE READER MEET THIS REQUIREMENT?

We're all aware of system and application software updates as at some point our phones have received security patches or app upgrades over the network. In the case of card readers, the process is quite similar except here the software or configuration updates might require encryption based on your use case. For example, if an end customer is reading static card numbers from an RFID media or isn't using data protected by encryption keys this does not require the firmware or the configuration to be encryption for a simple reason that these files do not carry any sensitive information. The need to encrypt configuration/

firmware files arises if the data that is being read by the reader contains any personal information or is part of a proprietary corporate format that is confidential, or should a customer wish to move to a higher security credential encrypted with keys. This means that either their existing card readers or new card readers must have a configuration that holds these keys. In such a scenario the configuration or firmware must also be encrypted since it holds sensitive information. If the configuration or the firmware is encrypted, the file will no longer pose a security risk and can be shared with customers to perform updates to the existing readers or with the card reader manufacturers to load new readers with the configuration of firmware updates. This not only secures the sharing process but also the update process since the reader is now receiving an already encrypted file.

After all, it is essential to choose a card reader that can carry out the aforementioned security considerations but more importantly the security features that are chosen need to be appropriate to the requirement of the customer. Any integrator first and foremost should thoroughly evaluate the respective application. They should work with subject matter experts in the field and establish requirements and objectives. After developing the concept, system architecture, data flow as well as various secure channels, only then can one begin to account for the security features needed. This process not only helps cement the end system's overall security view but also elucidates the exact security requirements that correspond to the resulting application.

In conclusion, choosing an RFID product that not only has the above security features but also has a flexible system design capable of accommodating future adaptations will prove to be the right choice for OEM's and system integrators.

Kiran Vasishtha is a Field Application Engineer for ELATEC Inc responsible for engineering, applications and technical customer support from the Palm City, Florida headquarters. He and the team of technical specialists provide consultation and support to OEMs, software developers, and integrators. Kiran has a Master of Science degree in Electrical and Computer Engineering from the University of California, Riverside, and a Bachelor of Engineering, Electronics and Communications degree from the RNS Institute of Technology in Bangalore, India.



For more information contact our Application Specialists at the locations below:

elatec.com

EMEA

Puchheim, Germany
+49 89 552 9961 0
sales-rfid@elatec.com

AMERICAS

Palm City, Florida, USA
+1 772 210 2263
americas-info@elatec.com

ASIA

Shenzhen, China
+86 158 1759 1668
apac-info@elatec.com

AUSTRALIA

Sydney, Australia
+61 449 692 277
apac-info@elatec.com

JAPAN

Tokyo, Japan
+81 355 799 276
japan-info@elatec.com