securityinformed.com
Making The World A Safer Place

Technology Report:

5 Ways RFID Readers Can Secure Your Marketplace

Technology Report: 5 Ways RFID Readers Can Secure Your Marketplace

About the author

An experienced journalist and long-time presence in the U.S. technology marketplace, Larry Anderson is the Editor of leading digital publications SecurityInformed.com and SourceSecurity.com. Mr. Anderson is the websites' eyes and ears in the fast-changing security sector, attending industry and corporate events, interviewing leaders and contributing original editorial content to the two sites. He leads a team of dedicated editorial and content professionals, guiding the editorial roadmap to ensure that SecurityInformed.com and SourceSecurity.com provide the most relevant content for industry professionals. From 1996 to 2008, Mr. Anderson was editor of Access Control & Security Systems magazine and its affiliated websites. He has written numerous articles for and about some of the largest companies in the security industry and has received numerous awards for editorial excellence. He earned a Bachelor of Arts in journalism from Georgia State University with a minor in marketing.

ELATEC commissioned SecurityInformed.com to produce this document.

Technology Report: 5 Ways RFID Readers Can Secure Your Marketplace

Each component of a security system, including an RFID reader, serves a vital role in the security of any workplace. A chain of protection is only as strong as its weakest link. Therefore, choosing the right RFID reader for any application is a basic consideration to ensure that reader functionality promotes overall security.

Radio frequency identification (RFID) is a simple, secure and convenient access control solution for end users and original equipment manufacturers.

RFID readers are available today in numerous devices requiring user authentication, authorization and access control – from doors to multifunction printers to point-of-sale terminals to computers and more. RFID readers/writers come with a broad range of form factors, capabilities and configurations.

This Technology Report will focus on applications related to facility security and physical access control. We will highlight five ways that choosing the right RFID reader technology can promote greater security in any workplace, based on information provided by ELATEC.

Choosing the right RFID reader for any application is a basic consideration to ensure that reader functionality promotes overall security.

A device's compliance to certifications and standards must align with those required in the target market.

1. Choose a configuration that matches the needs of the application.

When choosing a reader for a system, it is important to make sure it meets all the design specifications. Some of the variables when choosing an RFID reader include transponder technologies, hardware communication interface, customization capabilities, power and consumption requirements and encryption/security. Choosing the appropriate combination of variables ensures optimal security.

One factor to consider is whether to use an RFID engine, or module, or to deploy a fully finished reader. RFID modules are electronic boards that require hardware integration and are not plug-and-play devices. They contain the pin configuration or connectors necessary to interact with the host board and to interface with antennas. Fully finished card readers on the other hand are ready to interface with the host, requiring little or no hardware integration, and they already have integrated antennas.

Does a card reader support all the card technologies a customer needs? Given the diversity in card technologies on the market, many end users have to support multiple technologies across their organization.

Not every finished product may meet a specific end user's technical specification. Shortcomings may include the size of the antenna (read range), voltage requirement, form factor, communication interface, etc. Users should consider how much voltage is required for a device, and how much power it consumes when in use and when inactive.

Size is another consideration. As electronic hardware continues to shrink in size, end users should evaluate performance thoroughly. A smaller form factor might mean a smaller diameter or circumference of the RF antenna, which can affect read range.

A device's compliance to certifications and standards must align with those required in the target market.

2. Ensure the system is adaptable and can evolve over time.

One important consideration when choosing a reader is to select equipment that is "future-proof," or built to sustain the advancement and/or shift in the market from a technology standpoint. Customers have varied needs and requirements. Customization options can help an OEM or integrator "future-proof" a device and accommodate the requirements of various customers.

A reader runs applications that interact with a backend system or a database. There are instances that require matching of credential IDs that are already part of the end user's database or active directory. A reader needs to be able to manipulate and adjust its output to help match the credential ID stored in a database.

Currently, there are numerous RF standards and technologies present in the market. Some examples of RF standards are ISO 14443A/B and ISO 15693, and RF technologies include NFC HCE, EM4x02, prox, etc. The reader must be able to fully support these transponders. The RFID reader should be capable of detecting the technology and to support it to the full extent.

Having the flexibility to change the reader's firmware or configuration enables the reader's software to be updated to accommodate if the customer adds a new credential to the fleet or decides to opt for a higher-security-based credential.

An element of "future proofing" is the ability to add new transponder technologies in coming years. Does the reader support addition of new transponder technologies after installation?

End users should also consider how easy it is to reconfigure a reader after installation. Does the reader support remote configuration? Can communication or security protocols be customized? Does the reader control user feedback (e.g., lights or sounds)?

3. Embrace the transition to mobile credentialing.

Card readers should support smartphone authentication for users wanting mobile device access. More and more users will be shifting to smartphone authentication in the future. Mobile solutions are now available for Bluetooth Low Energy (BLE) on iOS and Android mobile devices and for near field communication (NFC) on the Android platform. Multi-frequency contactless readers incorporate NFC and BLE for authentication and access control using mobile credentials.

Mobile credentials and access solutions merge security with convenience by storing secure identities on smartphones for unlocking doors, releasing print jobs, signing onto a computer network, dispensing product and more. These solutions enable iOS and Android phones to communicate with readers.

RFID readers are connected via USB/serial host to a computer system with an authentication infrastructure. When a mobile credential app is presented, it communicates with the reader using BLE or NFC. The mobile

Mobile credentials and access solutions merge security with convenience by storing secure identities on smartphones.

Sourcing the reader and transponder from the same developer makes it easier to build modern systems and/or extend existing systems.

credential also has a wireless connection to credential management in the cloud, which provides IDs based on authentication with the main system. The mobile credential solution is basically an app on a smartphone.

For example, ELATEC offers its own mobile solution app with essential functions, free of charge. There are also more complex apps including access and authorization management provided by ELATEC's partners.

In the case of mobile solutions, sourcing the reader and credentials from the same developer makes it easier to build modern systems and/or extend existing systems.

4. Utilize encryption and match the level to the application.

If an application requires encryption, the reader should be able to execute cryptographic algorithms. It should be able to support encrypted data exchange, if required.

Card readers should offer popular encryption standards such as AES, DES, Triple DES, etc., as part of their firmware. There is a need to assess whether encryption is required and, if so, the exact channel where this needs to be enforced, whether the host interface requires the exchange of encrypted data or the air interface needs to transfer protected data.

Flexibility is also key. If a host system uses a HashMap based algorithm, the reader should be able to implement the algorithm and produce an output that can be correctly processed. There are scenarios wherein the host system is also expecting CRCs (Cyclic Redundancy Checks) to be part of the data stream to verify the integrity of the data. It is extremely helpful if the reader can run applications and implement customer algorithms so that the host can properly encrypt the data and also verify data integrity.

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. The choice of RFID media can also impact security. For example, low-frequency (125kHz) contactless transponder types can be easily cloned and used to grant access.

The Wiegand interface also has vulnerabilities, so a card reader should offer other communication interfaces such as RS485 or RS232. Some older RFID transponders and communication interfaces have been subject to vulnerability hacks and are now considered fundamentally compromised.

5. Provide tamper detection.

The need for tamper detection varies from one application to another. For example, high security environments such as data centers need the most protection against tampering. Users should thoroughly evaluate the consequences of any attempts to compromise the device integrity or data associated with the device.

According to the application, tampering can impact 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 on the market such as mechanical and optical tamper detectors that can be embedded directly on the card reader for superior protection against threats.

Designing for Optimal Security

The RFID products deployed in various scenarios are determined by the diverse security needs of each end user. For example, a product deployed in a university will have very different security needs compared to one that might be deployed in a federal office. Credentials are different, as is the level of security, and both can help guide the correct choice of equipment. Considering the factors we have listed is a good starting point in the search for RFID readers that can ensure optimal security for any workplace.

RFID products deployed in various scenarios are determined by the diverse security needs of each end user.

About ELATEC

ELATEC is a global provider of solutions related to short-range wireless readers/writers. As a reliable partner, ELATEC offers the best products, processes and services for customer businesses. ELATEC, combines experience, technology leadership and comprehensive service.

securityinformed.com

Making The World A Safer Place

ELATEC

RFID Systems