ELATEC
RFID Systems

RFID JOURNAL

This article was published in August 30, 2020 Issue of RFID Journal

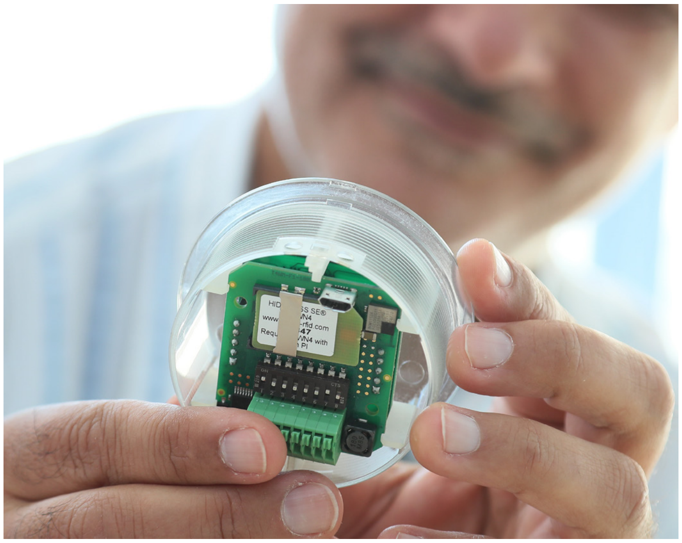
CUSTOMIZATION CONSIDERATIONS FOR EMBEDDED SYSTEM RFID READERS

By Kiran Vasishta, ELATEC, Inc.

With increasing security and public health concerns, contactless credentials are gaining more and more importance. Contactless credentials can be divided into two main categories: soft credentials that include mobile phone applications that tap into their BLE/NFC hardware and transmit the data, and hard credentials that typically include low frequency (125 kHz) and high frequency (13.56MHz) based passive RFID transponders. With the help of these credentials, organizations can tackle safety concerns related to other common user authentication and access control solutions such as biometric, password/PIN and magstripe.

Today, RFID readers can be found in numerous devices requiring user authentication, authorization and access control, from doors to multifunction printers to point of sale terminals to computers and more. As OEMs and system integrators increasingly consider adding a security aspect to their product, choosing an appropriate RFID reader becomes that much more important. One of the main goals of an OEM or a system integrator should be to select a reader that is "future proof" or built to sustain the advancement or shift in the market from a technical standpoint.

Furthermore, it should be kept in mind that customers have varied needs and requirements. This is especially true when dealing with customers that use contactless credentials. Depending on the type of customer even the type of hard or soft credential will vary. For example, a product deployed in a university will have different security needs compared to the one deployed in a federal office. Not only the credentials are different in the above scenario but the level of security is different as well.



This article covers some of the important customization considerations that can help satisfy an OEM's or integrator's goals of a future proof device and also a device that can accommodate the requirements of different customers.

THE CONSIDERATIONS ARE:

1. CAN THE READER'S OUTPUT FORMAT BE CHANGED OR ADJUSTED?

The reader is typically a small component of the product manufacturer's ecosystem. Usually, the embedded product has a host that runs its application that interacts with a backend system or a database. There are instances with a requirement to match credential ID’s that are already part of the end user’s database or active directory. In systems where the host application cannot manipulate the reader's data, it becomes very important that the reader can manipulate and adjust its output to help match the credential ID stored in a database.

2. CAN THE READER READ MULTIPLE TECHNOLOGIES WITH THE SAME HARDWARE?

There are numerous RF standards and technologies present in the market. Some examples of RF standards are ISO14443A/B, ISO 15693, etc., and some examples of RF technologies are NFC HCE, EM4x02, Prox, etc. The reader must be able to fully support these transponders.

This not only ensures that the RFID reader is capable of detecting the technology, but it ensures that it can support them to its full extent. For example, users may use a UID (unique identification number) as a credential ID and in some instances, users employ memory-based transponders that contain the credential ID stored in one of the memory sectors. So, it is critical that the reader not only supports reading the UID but also the memory segments of the transponder.

3. DOES THE READER HAVE RECONFIGURATION FLEXIBILITY POST INTEGRATION?

Having the flexibility to change the reader's firmware or configuration is necessary when considering an embedded product with a reader integrated as a subsystem. This allows the reader's software to be updated in the event a new credential is added to the customer's fleet or in a scenario where the customer decides to opt for a higher security-based credential. Although the feature to be able to reconfigure the reader is critical, it is even more important to have a reasonable way of updating the readers. Imagine an instance wherein the readers are embedded within your end products and the only method available to update the reader is by dismantling it from the enclosure. Now, compound this effort with a distributed fleet of hundreds of such devices with readers embedded in an enclosure. To avoid such a daunting task, look for the capabilities of remote and/or contactless reconfiguration, updates and upgrades such as over-the-air via NFC or BLE, or via contactless RFID configuration card or app.

4. HOW DOES THE READER INTEGRATE WITH THE HOST APPLICATION SOFTWARE?

When we refer to the host application, we are referring to the software component that directly interacts with the reader. Typically, the reader either communicates with the whole system as a keyboard device or as a serial device. There are also instances wherein the host application expects the reader to work as a PC/SC (personal computer / smart card) device. It is very important to understand the software specifications of the host application as it directly affects the functioning of the reader. One should evaluate if appropriate drivers are being made available to the embedded designers and whether the reader will be able to appropriately interact with the host via standard software communication protocols. Even though there is a certain amount of software development necessary for the communication to occur between embedded devices. Whether or not this effort can be reduced is a question one should evaluate when choosing the reader.

5. CAN THE COMMUNICATION PROTOCOL BE CUSTOMIZED?

In embedded design projects, one of the key aspects is the execution of embedded applications that are created for a very specific purpose. For example, the end goal of the embedded product could be to complete a secure transaction or exchange information under time constraints.

Any electronic device that interfaces with the host running an embedded application needs to work hand in hand with it to fulfill the end goal. In some situations, the task of the reader could be to simply send the data over a serial line. In other situations, the task would be to perform operations based on the input given by the embedded host application or hardware. An example of such a scenario would be when the host expects the reader to detect transponders only when a particular character is transmitted to the reader. Another example would be that the reader would execute a sequence of commands based on a GPIO output initiated by the host. It can be very beneficial if the reader can run a custom protocol under the embedded host.

6. CAN THE SECURITY ALGORITHM AND DATA INTEGRITY CHECK BE CUSTOMIZED?

Typically, it is desirable to have popular encryption standards such as AES, DES, 3DES, etc. to be part of the reader's firmware. This would help embedded designers to readily take advantage of these encryption methodologies. But there are cases wherein the host system is using a HashMap based algorithm. In such a scenario the reader should have the capability 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 custom algorithms so that the host can properly decrypt the data and also verify data integrity

7. DOES THE READER HAVE THE ABILITY TO CONTROL THE USE OF FEEDBACK?

One of the most important considerations is having the ability to modify the reader's user feedback or physical behavior per the customer's needs. Some customers expect the reader to blink a Green LED when an RFID card is presented, and some expect the reader to beep and transition its LED color state from red to green. Having the ability to control this basic feedback (and more) or response to an event initiated by the user is of prime importance.

Kiran Vasishta 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