Securing the Backbone of Connected Industry

OPC UA enabled RFID Readers use Secure Elements for Protected Communication

RFID in Industrie 4.0

Radio Frequency Identification (RFID) technology has long established itself as one of the crucial underpinnings of modern industry. Unobtrusive and ubiquitous, RFID tags have become the currency by which goods and information are navigated through the industrial production process. From their original domain of internal and external logistics, where small RFID tags help move shipments from A to B with full transparency and easy tracking, the technology has expanded into other areas, like access controls or manufacturing execution systems. Within the scope of Industrie 4.0, manufacturing becomes even more dependent on automatic tracking and reliable identification of items. In order to ensure high flexibility in increasingly complex, often very heterogeneous, but closely connected environments, RFID technology has become even more important. With its low costs and almost universal installed base, RFID is set to be the ideal solution for organizing the industrial applications of the future: Evolving from the ability to reliably track supply chains to helping coordinate customer-specific, custom production of small batches or single products, the new prospects for industrial application depend on communication and the secure flow of data and identities. Tiny RFID tags are the enablers for these scenarios, with RFID readers acting as the eyes and ears of the supply chain, the automated factory environment, and the later shipment and distribution of the finished products to their intended customers.

Challenges

Traditional RFID systems, however, represent a potential weak point in the new IIoT landscape. Without additional safeguards, the communication between RFID tags and readers is a target to be exploited by cloning, reverse engineering, snooping, replay, man-in-the-middle, or denial of service attacks or other malicious attempts to either sniff data or manipulate it for harm or illicit profit. With a well-established technology as ubiquitous as RFID, any attempts at closing these loopholes would have to work within the given parameters and within the limited capabilities of the technology. Replacing the entire concept seems a commercially untenable option. The new safeguards therefore need to fit seamlessly into the given standards while accommodating as strong and as versatile security capabilities as possible.

Solution

Balluff and Wibu-Systems teamed up as part of the German IUNO (IT Security in the Industrie 4.0) project under the leadership of the wood-processing specialist Homag to develop a solution that would successfully reconcile both challenges.

Their answer: an "OPC UA RFID Reader with Integrated Secure Elements", based on Balluff's intelligent UHF reader platform, supercharged with a CmASIC by Wibu-Systems as the security powerhouse based on Infineon's SLE97 crypto-controller.

The system uses the security functions of the OPC UA implementation of Unified Automation built around Open-SSL to secure M2M communication at both ends: the tag reader and the computer processing the data on the one end, and the manufacturing execution system using it to steer production operations at the other end.

Security for Industrie 4.0

RFID Readers with Secure Elements:

- Secure key and certificate storage
- Reliable tag identity
- Standard OPC UA communication
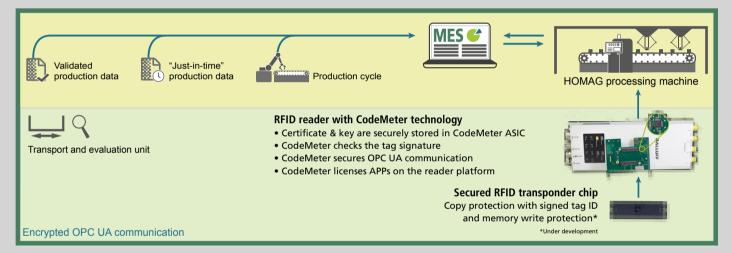- Greater security with CodeMeter

IUNO
Nationales Referenzprojekt
IT-Sicherheit in Industrie 4.0

OPC UA Background

For Wibu-Systems' and Balluff's solution, the security features of OPC UA offered the required versatility to add the necessary protections into the established RFID communication chain: with the CodeMeter ASIC as secure element, the required cryptographic keys can be stored securely and help enforce the strong protection accommodated by the OPC UA protocol for M2M communication. This adds three essential qualities to the formerly low-security RFID communication: secure identities for the devices involved, integrity for the tag reading process, and data communication protected from theft and manipulation. Specially protected memory is available for adding software with

model regarding data, operational commands, and diagnostics. With the aid of Unified Automation's development tools and code generator, the standard model can quickly be integrated into the implementation of any RFID Reader application. Easily upscaled with the special OPC UA security extensions made by Wibu-Systems, the security has been pushed to the next level. Based on OpenSSL, the security features of OPC UA are perfectly integrated with the CmASIC secure element. As another important gatekeeper, the CodeMeter stack controls access to the secure element and the communication between the OpenSSL and the protected key storage on board. With this, the integrity of all components in the communication chain is guaranteed.

Validated production data

"Just-in-time" production data

Production cycle

MES

HOMAG processing machine

Transport and evaluation unit

RFID reader with CodeMeter technology
• Certificate & key are securely stored in CodeMeter ASIC
• CodeMeter checks the tag signature
• CodeMeter secures OPC UA communication
• CodeMeter licenses APPs on the reader platform

Secured RFID transponder chip
Copy protection with signed tag ID
and memory write protection*

*Under development

Encrypted OPC UA communication

full licensing capabilities and secure updates, making it possible to upscale the reader's functionality in the field. At the same time, all communication can be encrypted end-to-end, putting an end to the most easily disrupted part of the communication process, i.e. the radio transmission between tag and reader.

Used Products of Unified Automation

The OPC UA communication protocol and information model was chosen for RFID reader and machine communication because of the versatility of the Unified Automation Software Development Kit (SDK). The information modeling capabilities of OPC UA are fully available in the Unified Automation Toolkits, and their use has been simplified to the max. The Companion Specification for Automatic Identification (AutoID) initiated by the AIM-D e.V. has standardized the semantics of RFID Readers and the information

About IUNO

Germany's flagship IT security project IUNO hosts the initiative of Balluff, one of the world's leading makers of sensor technology, and Wibu-Systems, the long-standing champion of licensing and IT security, under the leadership of Homag, a pioneering maker of wood processing technology, in its mission to protect the RFID landscape with secure identities and protected communication.

Together, the three partners have developed a viable demonstration of the new system as the underpinnings of custom manufacturing – one of the star capabilities of Industrie 4.0, but inherently dependent on trustworthy communication and secure identities in the increasingly complex and heterogeneous landscapes of intelligent factories and connected industry.