From the need to the solution - Crypto in passive UHF RFID – in Brazil and Worldwide

Klagenfurt, 28.03.2014

Josef Preishuber-Pflügl, CTO of CISC Semiconductor GmbH, Austria

Passive UHF RFID started around 2000. Initial standards were ANSI 256 and ISO/IEC 18000-6 Type A and Type B. In parallel UCC (now GS1) initiated the initiative at the MIT Auto ID Center, which later became GS1 EPCglobal and developed the EPC Generation 1 Class 0 and Class 1. Having de-facto 4 competing UHF RFID standards meant that there was no standard. The industry was clever enough to recognize that this will not fly and under the umbrella of the MIT Auto ID Center (later EPCglobal) the EPCglobal Class 1 Gen 2 standard was developed and later also transferred into ISO and published as ISO/IEC 18000-6 Type C.

When the UHF RFID and EPC applications significantly increased, the European Commission recognized that RFID will be with the consumer and due to privacy concerns the EC asked the industry for a so-called silent tag. A silent tag should be a tag that can be put in a restricted mode of communication that it does not return any information or at least does not return a unique number that would allow tracking or identification.

Having been project reviewer for the EC in the project BRIDGE[1] and having had TU Graz[2] in the BRIDGE consortium who worked on AES-based (Advanced Encryption Standard) cryptology for UHF RFID, Austria started a new work item in ISO on privacy and security. Privacy and security were initiated together as it was clear that enabling and disabling of privacy protection requires secure communication in order to avoid that hackers could trace communication and therefore easily break the privacy by e.g. re-play attacks.

When this work item was initiated in 2008, there had been considerable scepticism on its technical feasibility. TU Graz reported a prototype of an ISO/IEC 18000-6 Type C / Gen 2 tag with battery support in the BRIDGE project. ETRI reported about research work with a passive UHF RFID product with rather high power consumption of 217 µW[3], which was around 5 times more than the state of the art passive UHF RFID tags available at that time an meant a communication distance below 3 m. As the feasibility maintaining fast identification speed and low power consumption was questioned for a long while the standardization efforts were moving slowly. In 2010 ISO and EPCglobal gained some momentum and the ISO/IEC 29167 for crypto suites and the new foundations for EPCglobal Gen 2 V2 have been done.

In parallel to these initial efforts driven by European privacy concerns, in Brazil, since 2008, CPA Wernher von Braun[4], in collaboration with government agencies, had actively promoted secure protocol extensions to EPCglobal Gen 2 for their national vehicle registration and identification systems SINIAV. As part of these efforts, CPA Wernher von Braun spearheaded the national development activities in passive UHF RFID with data encryption and authentication features.

After first getting in touch with ISO and later EPCglobal efforts, in June 2012, as a major achievement, Von Braun publicly announced the development of Brazil's first fully passive RFID chip with high-performance AES crypto engine, and a working prototype was demonstrated in high-speed

[1] BRIDGE (Building Radio Frequency IDentification for the Global Environment), http://www.bridge-project.eu/
[2] Technische Universität Graz (Graz University of Technology), www.tugraz.at/
[3] ISO/IEC JTC1 SC31 WG4/SG3 document N691
[4] Centro de Pesquisas Avançadas Wernher von Braun, Campinas-SP, Brazil, www.vonbraunlabs.org

automated vehicle identification field-tests in the presence of government and industry representatives at a test track in the State of Sao Paulo.[5]

Late 2012 stable working drafts for standards on passive UHF RFID crypto suites and EPCglobal Gen 2 V2 have been generated, integrating valuable experience obtained in the Korean research work and the Brazilian reference projects, through active participation of the respective national standardization bodies.

EPCglobal Gen2 V2 has been published in November 2013, and the upcoming ISO/IEC 18000-63 maintaining the same content is expected to become available later in 2014 together with the compatible crypto suites standardized in ISO/IEC 29167. Those standards together form the basis for passive UHF RFID tag supporting advanced privacy features and secure communication, utilizing crypto methodologies like AES-128, PRESENT-80, ECC, GRAIN-128, and others. First products supporting these standards are expected on the market in 2014.

As a significant milestone, prototypes that demonstrated the feasibility of advanced crypto on passive tags have already been shown by NXP and CPA Wernher von Braun in 2013 at the GS1 EPCglobal UHFAI Gen 2 V2 Prototype Demonstration[6] held on April 30, 2013, in Orlando, FL, USA. Among other displays, CPA Wernher von Braun demonstrated the fastest AES-128 implementation in silicon on a fully passive Gen2 tag with an encryption performance of below 1 ms per 128-bit data block.[7]

The recent statements of vendors that significantly changed the implementation concepts for advanced crypto, such as AES, for low power, say that the communication range loss can be neglected still maintaining a calculation time below 20 ms for crypto command execution on passive tags. In this context, to the best of my knowledge, at the date of this publication, the Von Braun implementation is the only existing and publicly field-tested AES implementation for fully passive Gen 2 tags in Brazil, and one of few publicly known AES implementations in the world, with other known reference implementations being provided by NXP (2012) and ETRI in Korea (2013)[8], for instance. The Von Braun implementation for a passive AES UHF RFID tag also exceeds the application expectations with 1 ms AES calculation time and 10 m communication range.

Based on the functionality and performance of the passive UHF RFID devices and their novel crypto functionality, new applications have been identified. While the original driver in the retail and consumer area still has not resolved the issue of key management for symmetric crypto algorithms and currently focuses on asymmetric methods like ECC, AES128 plays a more and more important role in vehicle management, where key handling aspects have been addressed already in earlier non-RFID implementations in practice in Europe, North America, and other places. In Brazil in 2012, an open, multi-operator infrastructure has been put into operation in combination with a novel 915 MHz based AVI and ETC system purely on UHF RFID including passive AES128 UHF RFID tags.

---

[5] CPA Wernher von Braun: *915 MHz passive tag with embedded AES128 secure custom commands over ISO 18000-6C.* Press Release, June 10th, 2012

[6] GS1 EPCglobal UHF AI WG 1&2: *GS1 UHF AI WG Meeting Notes for F2F at RFID Journal Live on April 30th 2013.*

[7] CPA Wernher von Braun: *GS1 UHFAI Prototype Demo: GS1 EPCglobol Gen2 v2.0 UHF RFID Reader & Transponders with ISO CD 29167-10 AES-128 Crypto Suite & Brasil-ID P63 Protocol.* Presentation and Live Demonstration at GS1 EPCglobal UHF AI WG 1&2 Prototype Demonstration on April 30th, 2013, Orlando, FL, USA

[8] CMOS Security-Enhanced Passive (SEP) Tag Supporting to Mutual Authentication, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6651806&queryText%3D6651806

While Europe and parts of North America have already established technologies based on active, battery supported technologies, passive UHF RFID systems with security have very high attention in South and Latin America, non-European countries around the Mediterranean Sea and South East Asia. In the latter case, the new security-enhanced Gen 2 based solutions typically either replace insecure Gen 2 / ISO/IEC 18000-6 legacy applications, or have become technically feasible and economically interesting by fulfilling the performance requirements for AVI and ETC with regard to speed and security.

About the author:

Josef Preishuber-Pflügl is an Austrian RFID and IoT expert who is convener of several ISO/IEC JTC1 and GS1 EPCglobal standardization groups and project editor of various international RFID standards.

Josef Preishuber-Pflügl was a design engineer, project manager and product manager at Phllips Semiconductors (now NXP), where he started to get involved in RFID with his diploma thesis. His work led him through the development of LF (<135 kHz), HF (13.56 MHz) and UHF (860-960 MHz) RFID products and systems.

Changing to CISC Semiconductor GmbH in 2003, Preishuber-Pflügl set up the company's RFID activities and expanded the international standardizatlon work on RFID. Today, in the role of Chief Technology Officer, he is responsible for CISC's state of the art protocol emulation and conformance and performance testing products, covering international ISO and EPCglobal standards on the one hand, and providing reference test frameworks for the Brazilian national RFID custom extensions to Gen 2 for secure AVI, ETC, and logistics applicatlons.

In 2011 he received the IEC 1906 Award by the International Electrotechnical Commission (IEC) as Expert of ISO/IEC JTC 1, Information Technology.

In 2012 he became co-author of the RFID Handbook of Klaus Finkenzeller.

Currently, he holds the following positions in respect to RFID standardization:

Convenor ISO/IEC JTC1 SC31 WG4/SG6 - Performance and Conformance Tests for RFID Devices

Convenor ISO/IEC JTC1 SC31 WG7 - Security for item management

Rapporteur ISO/IEC JTC1 SC31 WG4/SG4 – Regulatory

Co-chair GS1 EPCglobal T&C (UHF Gen 2 Testing & Certification Working Group)

Vice-chairman ERM TG34 Radio Frequency Identification (RFID) Devices

Convenor Austrian ASI K001 - Information technologies

Convenor Austrian ASI AG 001.31 - RFID for Item Management

Project Editor ISO/IEC 18000-4: RFID air interface 2.45 GHz

Project Editor ISO/IEC 18000-6: RFID air interface 860-960 MHz (UHF)

Project Editor ISO/IEC 18000-63: RFID air interface 860-960 MHz (UHF) Type C / EPC Gen 2 V2

Project Editor ISO/IEC 18000-7: Active RFID air interface 433 MHz

Project Editor ISO/IEC 29143: Air interface Mobile Item Identification