Building **R**adio frequency **ID**entification for the **G**lobal **E**nvironment

Secure Semi-Passive RFID Tags – Prototype and Analysis

Authors: **Manfred Aigner (TU Graz), Thomas Plos (TU Graz), Antti Ruhanen (Confidex), Stefano Coluccini (CAEN)**

November 2008

This work has been partly funded by the European Commission contract No: IST-2005-033546

About the BRIDGE Project:

BRIDGE (**B**uilding **R**adio frequency **ID**entification for the **G**lobal **E**nvironment) is a 13 million Euro RFID project running over 3 years and partly funded (€7,5 million) by the European Union. The objective of the BRIDGE project is to research, develop and implement tools to enable the deployment of EPCglobal applications in Europe. Thirty interdisciplinary partners from 12 countries (Europe and Asia) are working together on : Hardware development, Serial Look-up Service, Serial-Level Supply Chain Control, Security; Anti-counterfeiting, Drug Pedigree, Supply Chain Management, Manufacturing Process, Reusable Asset Management, Products in Service, Item Level Tagging for non-food items as well as Dissemination tools, Education material and Policy recommendations.

For more information on the BRIDGE project: www.bridge-project.eu

This document results from work being done in the framework of the BRIDGE project. It does not represent an official deliverable formally approved by the European Commission.

This document:

This report documents the results of task 4.2.2 "Secure Semi-Passive RFID Tags". After a brief motivation for development of semi-passive tags in WP4 as prototype platform, the report shortly describes the three different platforms. A more detailed report about the development of the tags is available in D4.2.1. The following analysis section presents the results of the tests that were performed with the prototypes. All three prototypes are working according the defined specification and are available to serve as demonstrators of passive RFID tags with extended tag functionality.

Disclaimer:

Authors and Contributors

Work package leader Andrea Soppera (BT Research)

Task Leader: Manfred Aigner (TU Graz)

Authors : Manfred Aigner (TU Graz)
Thomas Plos (TU Graz)
Antti Ruhanen (Confidex)
Stefano Coluccini (CAEN)

Semi-Passive Tag Prototypes

Abstract:
This report documents the results of task 4.2.2 “Secure Semi-Passive RFID Tags”. After a brief motivation for development of semi-passive tags in WP4 as prototype platform, the report shortly describes the three different platforms. A more detailed report about the development of the tags is available in D4.2.1. The following analysis section presents the results of the tests that were performed with the prototypes. All three prototypes are working according the defined specification and are available to serve as demonstrators of passive RFID tags with extended tag functionality.

Contents:

Description of Semi-Passive Tag Prototypes

1.1 Introduction and Motivation

Workpackage 4 (WP4) of the BRIDGE is dedicated to research towards secure RFID systems. The research performed in the context of this workpackage covers several aspects. Activities range from the analysis of threats and definition of the security requirements or secure access and trust on RFID network infrastructure to protection of tags and readers against known attacks. WP4 Task 2 deals with research and development of secure RFID tags, covering also the protection of the wireless tag to reader link. Protecting that tag and the wireless link between the reader and the tag is not trivial due to the demanding operational and cost requirements of the passive RFID tags. To avoid security bottlenecks from a system's perspective, the protection level of the tags should not be lower than in other parts of the system. Goal of WP4.2 is to protect the tag and the wireless link with cryptographic measures. The protection measures must not prevent standardization; therefore it was decided to focus on open and standardized cryptographic primitives. To demonstrate the developed protection concepts a proper platform for a prototype implementation had to be developed. Due to the limited budget and the limited time for prototype development we were looking for a solution to demonstrate the protection of the wireless interface without the necessity of implementing the full approach in passive tag prototypes. Semi-passive tags using microcontrollers instead of hard-wired logic gates to execute the tags operations are a good choice as prototype platforms. Semi-passive means that those tags behave like fully passive tags, they send their responses to the readers exactly in the same way as normal passive tags do. As power supply semi-passive tags use a battery or any other power supply instead of pulling the necessary energy from the RF-field. This allows to use programmable microcontrollers or any other additional functionality on such tags, without reducing the operation range of the tags. Using a microcontroller allows changing or extending the functionality of the tag with minimal effort by simply extending the controllers firmware. The concept of semi-passive tags comes originally from the idea to extend the tags functionality by sensors; we use the same concept to provide a prototype platform for security extensions of passive tags. It is important to mention that the implementation of the cryptographic primitive on a microcontroller is very different from a dedicated implementation for a passive tag. It is not the purpose of the prototype platform to demonstrate that the cryptographic primitives fulfil the requirements of passive tags (this can be done more accurately with power simulations on chip level), but to show that the secure tags work and provide protection in real-live RFID demo setup, together with real RFID readers. WP4 Task 2 focused on solutions which stay compatible with unprotected infrastructure (means that secure readers still can communicate with unprotected tags[1] and vice versa) it is therefore also necessary to demonstrate how the protected tags communicate with unprotected readers.
First discussion about the prototype platforms between the participants was very fruitful and different solutions were exploited. It turned out during discussions that three different platforms were already available but they were operating on different standards and in different stages of development. Starting from these three platforms a concept for the semi-passive prototypes for semi-passive prototype operating on EPC Gen2 was developed.

Demonstration of WP4 results is only one use-case for the semi-passive RFID tags. Although they are not planned as high volume products, like passive RFID tags there are use cases which allow commercial exploitation of these semi-passive tags. Following is a short list of application scenarios where such tags are meaningful:

- Temperature monitoring of pallets
- Evaluation of security holes of RFID systems (especially access control systems)
- Combination with other sensors to observe the environment of the tag

[1] standard RFID tags without security support

- System development of RFID application with extended tag functionality (to be able to develop and test applications before tags with extended functionality are finally available as products.
- Reader development for trying readers conformity to new and future standards before tags are available
- Reader-to-tag communication eavesdropping to observe the commands an (unknown) reader sends to tags.
- RFID teaching and student project's
- Evaluation of protocol extensions

1.2 Different versions of prototypes

1.2.1 The IAIK – TU Graz Demotag

This semi-passive tag has been developed as a prototyping platform for development of secure RFID systems. The tag is battery-powered, but behaves like a fully-passive tag in the reader field. It is fully compatible to ISO 18000-6c and EPC class 1 generation 2 standards. The tag is optimized for easy adaptability to allow easy and fast development of prototypes. It features a ATMega128 microcontroller with JTAG and ISP interface for programming. An RS232 interface is available for configuration and logging. The front-end consist of discrete devices on a PCB, with a PCB antenna that is tuned to 868MhZ. The design allows connection of an FPGA to extend it also by functionality implemented in HW.

The firmware of the demo tag is designed for easy extension of functionality. Custom commands and additional functionality[2] can easily be integrated into the firmware by programming the tag's ATMega microcontroller. Figure 1 shows the final version of TU Graz' UHF demotag.
It is planned to exploit the demotag as development platform for systems that require additional tag requirements and to promote tit for use in academic teaching activities.

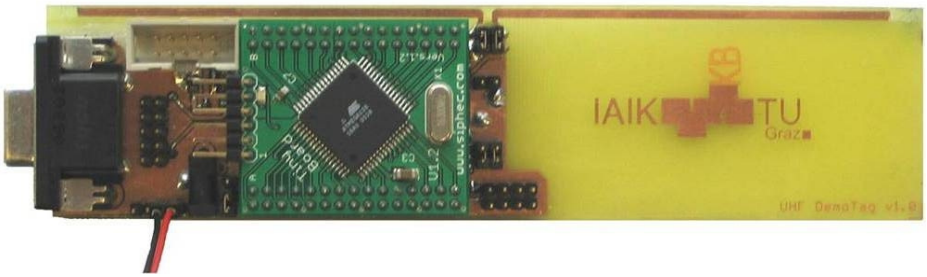

Figure 1: TU Graz Demotag

1.2.2 The semi-passive CAEN Tag

CAEN's development towards their semi-passive tag started from an available product (A927 demonstrator). The design was changed in several ways for the new version:

- A new controller platform was used with higher clk-rate and flash memory size (TI MSP430S2370).
- The implemented protocol was changed from ISO18000B to EPC Gen2 (ISO-18000C). To comply with Gen2 a new modulation and bit-encoding was implemented (PR-ASK & Miller encoding)
- A batter monitoring was included
- The bit-rate for Receive and Transmit was improved
- The (expected) battery life was improved from 2 years to 5 years
- Cryptographic authentication using AES was included (a SW AES library for TU Graz was used)

[2] as e.g. the security commands defined in Deliverable 4.2.1

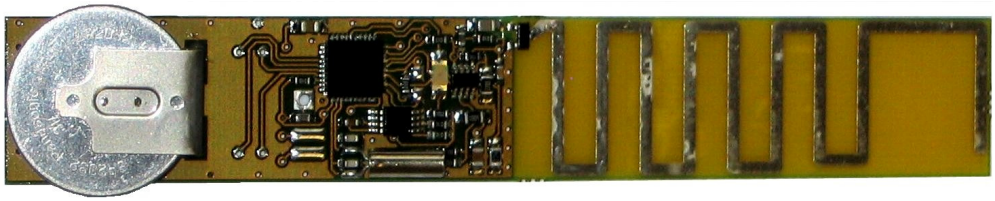

Figure 2: CAEN Tag

Particular attention way paid on engineering aspects, like reliability, energy consumption and reproducibility. The semi-passive tag prototype for BRIDGE is pre-production pilot for a new product of CAEN's product portfolio. The semi-passive tag from CAEN additionally includes a temperature sensor, which is not used for the demonstrator application in WP4. See Figure 2 for a picture of the new CAEN semi-passive tag platform

1.2.3 The Confidex Tag

Confidex' motivation of developing their own semi-passive platform are demonstration and validation purposes on one hand, but also exploitation of the result as a product that should be manufactured in low volumes. The design principles are therefore quite different, although the overall architecture is similar. Lifetime and production costs were a critical issue for development of this semi-passive tag. It is compatible with EPC Gen2 and the first prototypes were extended also by the authentication functionality based on AES (using AES cores from TU Graz). One of these prototypes is shown inFigure 3.

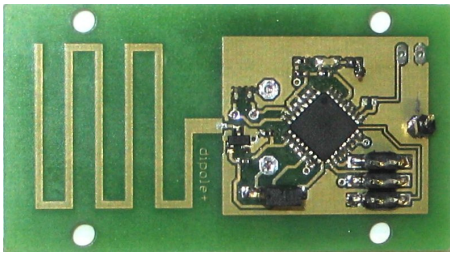

Figure 3: Confidex semi-passive Tag

1.3 Architecture of the semi-passive tags

Although the tags differ in the selection of controllers and the design and implementation of the analogue front-end, they are based on a similar architecture (Figure 4).
A discrete analogue front-end provides the bit-serial input and output of the contact-less channel for the microcontroller. A difference to passive tags is the generation of the clock signal. While fully passive tags derive the clock signal form the RF-field carrier, the semi passive tags use an own oscillator for the generation of the board. The reason is simple, since semi passive tags operate also when no RF field is available; they need an independent clock signal for operation. Synchronization of the received signal and the tag's clock needs to be considered in design of these tags.

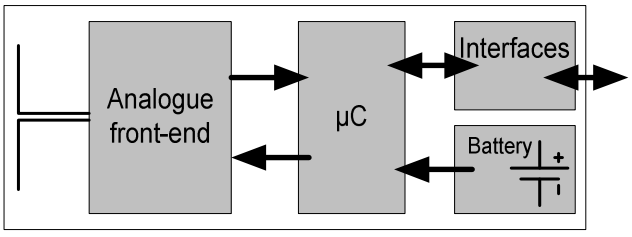

Figure 4: Architecture of semi-passive tags

The whole protocol-layer is implemented as firmware on the microcontroller. The bit-serial input signal is converted into frames, the CRC is checked and then the commands are interpreted. The tag's output is also sent as bit-serial signal to the analogue front-end, where the signals is used to control the backscatter circuitry.

The programmable approach allows inexpensive extension of the functionality. Sensors can be attached, complex computations can be performed, or information can be exchanges via external interfaces (RS-232) while the tag is in operation. Modern microcontrollers allow reconfiguration (re-programming of their firmware) therefore the systems functionality can be updated as long as the respective control bit-setting allows it.

1.3.1 The anti-cloning tag prototype

To use the semi-passive tags as a prototype tag for a simple anti-cloning demonstration. The standard functionality is extended by cryptographic authentication. The authentication operation is performed via a standard challenge response protocol. In an anti-cloning application secure authentication can be used to avoid cloning of tags. Each tag (or a group of tags) possesses a secret key, which is used only during the cryptographic operation, but cannot be read (and therefore not be copied to a clone). The key is written to the tag in a secure environment ("personalization"), where it can be assured that attackers cannot listen to the communication (due to e.g. proper protection of the room/building where the personalization takes place). The challenge response protocol provides a proof about knowledge of this secret key. Since only correctly personalized tags know the secret key, a verifier can be sure that only original tags are able to provide a correct response to a random challenge as long as the values for the challenge are not re-used (an attacker could record all used challenges and the respective response from previous authentications and re-use this value).

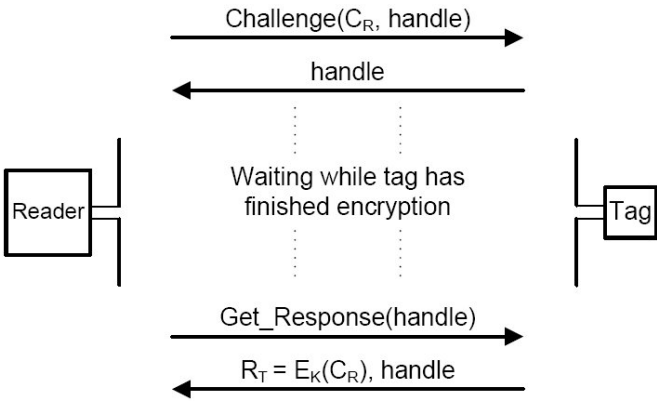

Figure 5: Protocol for Tag Authentication

Analysis of the semi-passive tags

1.3.2 Functional test:

- Inventory:
  - TU Graz Tag: OK
  - CAEN: OK
  - Confidex: OK
- Anti-colission:
  - TU Graz Tag: OK
  - CAEN: OK
  - Confidex: OK
- Authentication (challenge-response with AES):

- TU Graz Tag: OK
- CAEN: OK
- Confidex: OK

1.3.3 Test of operation characteristics

- Size
  - TU Graz Tag: 160mm x 38mm x 15mm
  - CAEN: 108mm x 17mm x 6mm
  - Confidex: 60mm x 33mm x 15mm

- Battery Supply / Livetime per battery (estimated):
  - TU Graz Tag: 9V battery block / estimated life time: 25h
  - CAEN: 3V lithium cell / estimated life time: 3-5 years
  - Confidex: 3V lithium cell / estimated life time: 17h

- Power/energy consumption
  - TU Graz Tag: 350mW
  - CAEN: 30uW enabled / 21uW standby
  - Confidex: 12mW

- Maximum reading Distance (CAEN A828EU compact reader @57mW ERP):
  - TU Graz Tag: 110cm
  - CAEN: 180cm
  - Confidex: 110cm

- Execution time for one AES-128 encryption:
  - TU Graz Tag: 235us (3760 cycles @ 16MHz)
  - CAEN: 679us (5432 cycles @ 8MHz)
  - Confidex: 470us (3760 cycles @ 8MHz)

1.3.4 Test of Air-Interface Parameters:

Using a CAEN A828-EU compact reader, two air-interface parameters of the semi-passive tags have been evaluated. The observed parameters are the time from reader transmission to tag response (T_1), and the link pulse-repetition interval (T_{pri}). Table 1 contains an overview of the determined parameters during the tests. For comparison, tow commercial passive tags have been evaluated as well. All tags that have been tested stayed within the tolerances provided by the EPC Gen2 standard.

Parameter	**T_1[µs]**	**T_{pri}[µs]**
Standard	250 +/-12s	25 +/-1
CAEN	246	25,8
Confidex	239	24,8
Tu Graz	260	26,0
Passive Tag 1	244	24,8
Passive Tag 2	251	25,0

Table 1: Interface Parameters

1.3.5 Susceptibility to SCA

Test Resutls
TU Graz Tag: successful
CAEN Tag: not yet performed
Confidex Tag: successful

Conclusions from SCA tests:

The result that the tags are susceptible to SCA attacks was not a surprise. The tags were not designed for avoidance of SCA attacks. Comparing more detailed results of the attacks on different tags is not meaningful due to rather different test-setups that were applied to achieve the best measurements. Anyway for a security point of view a conclusion that the attack was performed successfully with rather low effort is already enough.

SW countermeasures exist to protect the AES implementation. They would have added considerable effort to the implementation of the firmware, but the outcome would not be directly usable for development of passive tags, since in such designs the crypto algorithm would be implemented as hardware block. Countermeasures for HW and SW solutions differ significantly. Since the focus of the prototype was to demonstrate the security functionality, SCA protection was not defined as necessary requirement. The tests were performed mainly to test and improve the SCA setup and to learn about the differences of the used controller is respect to SCA susceptibility.

Conclusions

Three different semi-passive tag platforms have been developed and completed. While one platform (TU Graz) was developed as development tool to allow easy adaptation and extension (FPGA connector, framework for easy integration of additional commands & functionality) the other two platforms (CAEN, CONFIDEX) were designed for exploitation as products produced small series. One semi-passive tag (CAEN) features additionally a temperature sensor, which could also be combined with the security functionality (encrypted/protected storage of the monitored temperature on the tag). While the basic architecture of the three tags is similar, they differ in the respective implementation of the antennae, analogue front-ends, controllers and firmware. Nevertheless, interfaces have been agreed on during the specification phase to allow easy integration of the security features (AES encryption).

The presented results of the testing phase clearly show that all three prototypes were implemented successfully. All three of them can be used (and have been used already) in demonstration sessions to show the feasibility of proper security measures on RFID tags in a setup that may include readers and backend network elements. The choice, which one of the three prototypes is the most convenient, depends on the final application. While the TU Graz tag provides easy adaptability and extension, the other two tags show better characteristics when more tags are needed (they can be produced with less effort).
This report concludes the activities in Task 4.2.2, the semi-passive tags will be used in other subtasks of WP4. Internal (BRIDGE) and external exploitation activities have been started to provide also access to this platform for other BRIDGE members and also external parties.

Abbreviations:

AES	Advanced Encryption Standard
ASK	Amplitude Shift Key (Modulation)
CRC	Cyclic redundancy code (for error detection & correction)
EPC	Electronic Product Code
FPGA	Field programmable Gate Array
HW	Hardware
ISO	International Organization for Standardization
ISP	In System Programming
JTAG	Joint Test Action Group, IEEE 1149.1 standard
PCB	Printed Circuit Board
RF	Radio Frequency
RFID	Radio frequency Identification
RS-232	Serial Interface
SCA	Side-Channel Analysis
SW	Software
UHF	Ultra High Frequency

Filename: BRIDGE_WP04_Secure_semi-passive_RFID_Tags
Directory: \\gs1november\personal$\emilie.danel\My Documents\BRIDGE\Deliverables
Template: \\gs1november\personal$\sophie.schiettecatte\My Documents\BRIDGE\Templates\BRIDGE - general doc.dot
Title:
Subject:
Author: BRIDGE
Keywords:
Comments:
Creation Date: 1/19/2009 10:45:00 AM
Change Number: 2
Last Saved On: 1/19/2009 10:45:00 AM
Last Saved By: emilie.danel
Total Editing Time: 3 Minutes
Last Printed On: 1/19/2009 10:45:00 AM
As of Last Complete Printing
Number of Pages: 11
Number of Words: 3.317 (approx.)
Number of Characters: 18.913 (approx.)