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

Trusted Reader's Hardware Description

Authors: Fabrizio Bertuccelli (CAEN RFID S.r.L), Stefano Coluccini (CAEN RFID S.r.L), Andrea Soppera (BT), Jeff Farr (BT), Trevor Burbridge (BT)

October 2009

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 describes the hardware specification of a near product implementation for the RFID Trusted Reader.

Disclaimer:

This document contains preliminary information and is not subject to any license agreement or any other agreement as between with respect to the above referenced consortium members. This document contains only intended strategies, developments, and/or functionalities and is not intended to be binding on any of the above referenced consortium members (either jointly or severally) with respect to any particular course of business, product strategy, and/or development of the above referenced consortium members. To the maximum extent allowed under applicable law, the above referenced consortium members assume no responsibility for errors or omissions in this document. The above referenced consortium members do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, or non-infringement. No licence to any underlying IPR is granted or to be implied from any use or reliance on the information contained within or accessed through this document. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intentional or gross negligence. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you. The statutory liability for personal injury and defective products is not affected. The above referenced consortium members have no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.

Executive Summary

This report describes the hardware specification of a near product implementation for the RFID Trusted Reader.

It is a companion to the report D4.2.2B which describes various processes associated with RFID-based Product Authentication that may be implemented and improved through the use of the Trusted Reader. Readers should also see D4.4.1 which describes the overall design of the Trusted Reader and presents the software stack. The complete set of deliverable documents represents the culmination of several years' research into the use of Trusted Computing technology in providing innovative security solutions for RFID.

The RFID Trusted Reader has been designed has a generic purpose platform. The hardware and the firmware have been designed with specific focus to flexibility and modularity. Each class of reader's functionality is implemented by a specific module. This approach enables user to design their application out of the different services provided. This architecture enables expert users to link, sequence and design different services to meet the requirements of new applications.

The main part of the report covers the general design of the different modules implemented in the RFID Trusted Reader:

- The radiofrequency module provides the low level physical communication interface to tags following the specification of the EPC gen 2 standard.
- The protocol module takes care of the digital implementation of the RFID UHF communication protocols such as the ISO18000-6B and the EPCC1G2.
- The control module acts like an interface between the reader and the outside world.
- The TPM Module of the trusted reader is based upon the SLB9635 component, a trusted platform module from Infineon. The TPM module is the core of the RFID Trusted Reader and it prevents the reader from being surreptitiously modified by unauthorised users.
- The firmware running on the Control Module is based on the same modularity of the hardware architecture and supports both synchronous and asynchronous data flow models.

Aside from the standard RFID functionalities a driver has also been developed to allow the communication between the *Control* module and the TPM chip. In particular, the driver has been developed to hide the hardware structure to the software stack while enabling the access to the whole set of RFID services.

In this report, we also discuss the problem faced during the integration of the TPM module devices. The specific component provided by Infineon uses high speed bus specification that is not compatible with the slow hardware modules used in the reader. The problem has been solved with a PLL block running inside the reader FPGA.

In summary, this task has demonstrated that is possible to integrate trusted computing technology to the domain of RFID reading. This approach could open a market for more flexible RFID reader devices that can support a different range of service specifications.

Contents

1 The Design of the Secure Reader

The design of the Secure Reader is based on modularity and flexibility both in hardware and in firmware. Modularity means that each class of reader's functional task is carried out by a specific hardware or firmware module, a solution that allow to optimise the performances of each task class and to add features and communication interfaces with a small impact on the overall system.

From a hardware point of view the reader is made up of four main modules: the radiofrequency module, the protocol module, the control module and the TPM module (the core of the trusted reader engine).

Each block will be extensively analyzed in the next paragraphs.

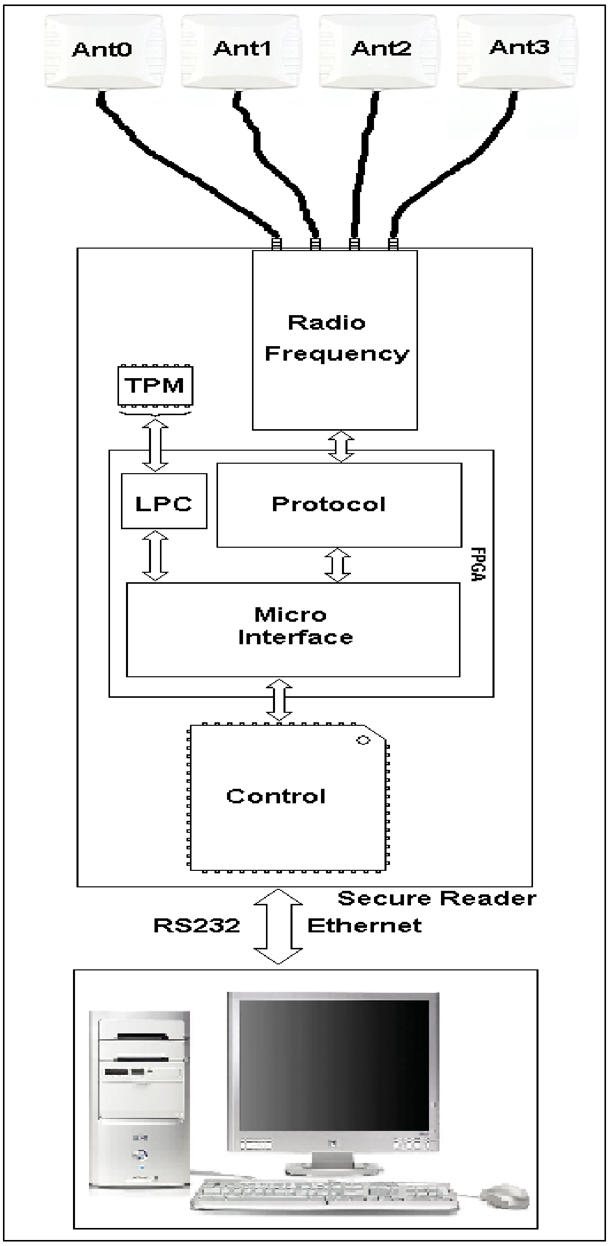


Figure 1. The Hardware Modules of a Trusted Reader

The Radiofrequency module

The radiofrequency module provides the low level physical communication interface to tags by means of generation and modulation of the radiofrequency field. All the analog functions placed here (PLL, Power Amplifier, RF Transmitter and Receiver) are controlled directly by the protocol section providing to it a first level of abstraction.

The Radiofrequency module's main characteristics are reported in the table below.

Frequency range	865.6 ÷ 867.6 MHz (ETSI EN 302 208) 869.525 MHz (ETSI EN 300 220)
Output Power	SW programmable Max.: 1.2 W (31 dBm) (RF Power up to 3.2 W ERP with 8dBi antenna)
Connectors' Number and Type	Nr. 4 TNC type female
Stability	±10 ppm over the entire temperature range
Number of RF Channels	10 channels, compliant to ETSI EN 302 208 1 channel, compliant to ETSI EN 300 220
Forward Modulation	DSB-ASK 40 KBit
Return link Modulation	FM0 40 KBit
Protocols Supported	ISO 18000-6B Philips UCODE EPC 1.19 EPC C1G2

The protocol Module

The protocol module takes care of the digital implementation of the RFID UHF communication protocols such as the ISO18000-6B and the EPCC1G2 and drives the *Radiofrequency module* providing the input digital signals to the RF Modulation block.

The module is realized around an FPGA (Field Programmable Gate Array), a component that allows incomparable performances in protocol implementation due to its great level of parallelism and speed in signal's handling. Despite this, the FPGA is based on RAM technology permitting an easy reprogrammability and upgradability for protocols additions or bug fixes. It has the flexibility of microcontrollers or DSPs but with better performances in digital signal handling.

The Control Module

The control module acts like an interface between the reader and the outside world; its main duty is the communication with remote hosts using a wide range of standard interfaces. The module is based on the Intel IXP465 microcontroller, a powerful 400 MHz processor with a large number of embedded communication peripherals and huge RAM memory on board.

The module uses services provided by the *Protocol module* to realize the "reader to tags" communication and services provided by the Linux OS to communicate with remote hosts; in this way the separation between real-time tasks (carried out by the *Protocol module* embedded in the FPGA) and high level communication tasks (running on the IXP465 processor of the control module) is obtained in a simple and natural way.

The TPM Module

The trusted reader is based upon the SLB9635 component, a trusted platform module from Infinenon.

Developed to comply with version 1.2 of the TPM specification defined by the Trusted Computer Group, this module provides an excellent ‘up to date’ cryptographic engine which quite easily fits into the UHF reader architecture.

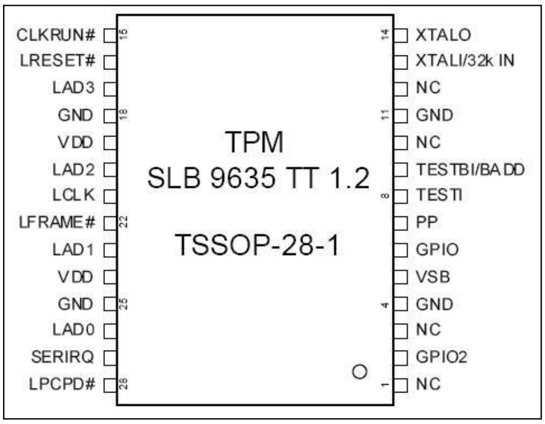


Fig. 1 SLB9635 pin out

Among the main characteristics, the device includes the following hardware blocks:

- ACE : Cryptographic engine for fast RSA computation in hardware with certified crypto Library providing security against all known physical side channel attacks
- HACO : Hardware accelerator for the SHA-1 hash algorithm
- DES : Data Encryption Standard accelerator:
  - Dual Key Triple DES in Hardware.
  - DES & 3DES.
  - Flexible key management.
  - Security against all known physical side channel attacks.
- RNG : Random number generator (AIS-31 compliant).
- CRC : Cyclic Redundancy Code module according to ISO 3309.

As the chip communicates with the reader through the LPC interface using both I/O and Memory access, an LPC block has been included in the FPGA in order to allow proper communication between the microcontroller and the SLB9635 device.

Trusted Reader Firmware

The firmware running on the Control Module is based on the same modularity of the hardware architecture; the main result of this approach is to show the remote host an abstract representation of the reader that hides the implementation details.

This abstract model is designed to cover all the actual and future CAEN RFID readers and it is centred on data flow; that is the propagation of data read from RFID tags up to the abstracted information layer provided to the remote host.

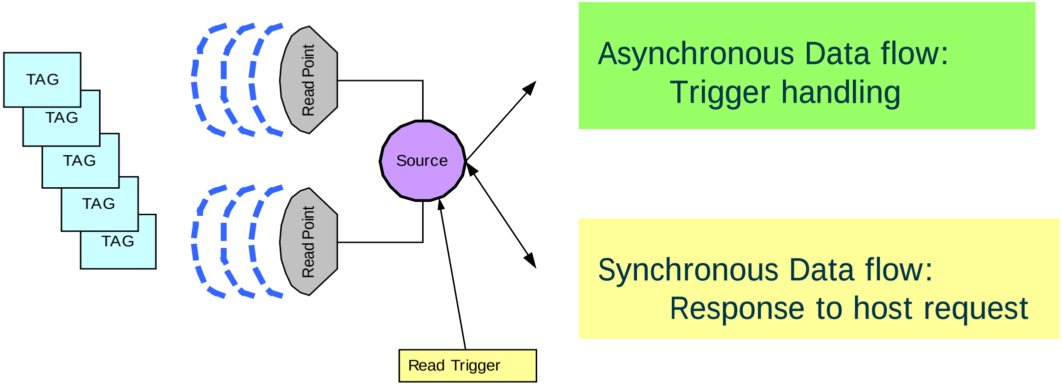


Figure 2. Data Communication Modes

Data coming from the protocol module follows two independent data flows:

- *Synchronous data* flow is implemented by a command handler task which parses commands coming from the communication interfaces (RS232 or Ethernet), performs the desired action and replies to the host the command's result.

  Command handler is responsible also to accept and handle configuration commands and all commands useful to access special tags features such as lock, kill, read memory and so on.

- *Asynchronous data* flow is handled by means of triggers, software objects with the ability to start read cycles automatically and notify asynchronously the incoming data to the remote host.

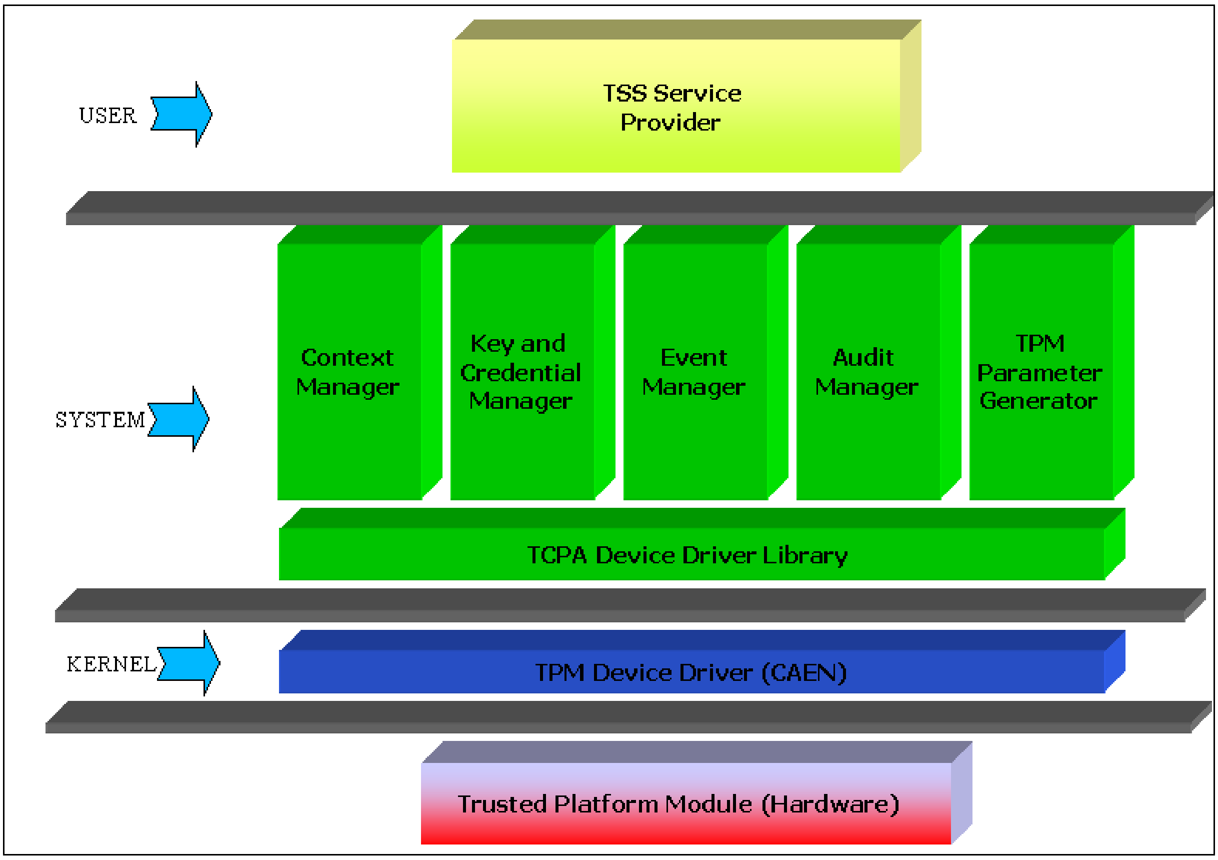
Some notification information are sent to the host to signal specific tag's events:

- Tag glimpsed when a tag is seen for the first time,
- Tag observed when a tag is confirmed to be in the field.
- Tag lost when a tag leaves the field

Trigger types available in the reader are:

- Continuous: data acquisitions/ notifications performed at maximum rate.
- Timer: data acquisitions / notifications are performed periodically.
- I/O: data acquisitions / notifications are driven by some equipment (like buttons, electronic eyes …) connected to the reader 's digital I/Os.

Beside standard RFID functionalities, a driver has been developed to allow communication between the *Control* module and the TPM chip. The driver has been developed in such a way that the underneath hardware structure has been hidden to the higher software stack.



Services offered by this driver are the same of the original tpm driver released by Infineon :

- tpm_open
- tpm_read
- tpm_write
- tpm_ioctl
- tpm_release

These services allow any software working with original Infinenon driver to run, without modification, on the Trusted Reader. A standard Trusted Software Stack can thus be included within the reader withouth requiring any modification.

2 Main problems and future developments

One of the main problems we have faced when using the Infineon TPM module was the introduction of the LPC bus, now available in almost all the recent desktop and laptop computers, in a classical reader architecture where this bus is usually unavailable. In particular the 33 MHz clock, needed by the LCLK signal, has required the synthesis of a PLL block running at 66 MHz inside the FPGA, a quite hard speed for the device used in the reader.

In addition to this, as the communication between the reader and the TPM module is controlled by the FPGA block, some extra time is required in order to instruct the FPGA to send commands to the TPM each time a secure operation is needed. Moreover, as the bus between the microcontroller and the FPGA is the same for both secure operations and RFID operations, the execution of any of the two will delay to some extent the execution of the other.

From the software side, a translation from the original TPM driver to a custom driver was required to hide the details of the hardware implementation. The new driver needs to allow developers to implement secure services and applications running on board the reader. This translation will be required every time new patches or improvements for the original drivers will be released.

These points will become more critical in the future when more demanding performance will be required from a Trusted Reader.

All the problems we have encountered and analysed are related to the different hardware architecture used in the current reader when compared to the intended controller for the TPM board. Future secure readers, based on some recent microprocessors like the ATOM family from INTEL, will probably benefit from a hardware design that, even if thought for the embedded world, is nevertheless quite similar to the one used in a standard PC.

These new devices generally implement an LPC bus (used specifically by the trusted modules as required by the Trusted Computing Group specification) and are able to run the most common OS like Windows and Linux. The main advantage of this approach is that the TPM board can, from the electrical side, be interfaced directly with the microprocessor and from the software side it can use exactly the same software stack (starting from the driver level) used in the PC environment.

The result will be a quite easy inclusion, without any extra cost in the design and implementation phase, of the TPM philosophy in the RFID world, with relevant benefits in terms of security.

3 Conclusions

In this report we have presented our pioneering work to implement a Trusted Reader. Due to the relative immaturity of the TPM boards, we have experienced considerable problems in interfacing the TPM module into the current generation of RFID readers. We expect that in future these problems will be alleviated.

Our experience with the hardware development of the Trusted Reader matches our experience of implementing a software stack as detailed in D4.4.1. Here we found that the maturity of the TPM drivers, support stack and secure operating system kernel implementations were all low. Although a software stack was implemented on a PC with a TPM module, we have no plans to port this software to the hardware of the Trusted Reader detailed in this report during the final 6 months of the project. In part this decision was made because some elements of the original software design are now unsupported (such as the Enforcer operating system kernel), and suitable new alternatives are not yet available. Also the implementation of the TCG software stack (TSS) is not yet supported for the architecture of the reader controller board, and secure BIOS and boot loaders are not available. Thus any early prototype would have not been truly secure, and any demonstrator would have provided little advantage to the one currently implemented on a PC architecture.

The valuable contribution of our work to date has been to motivate and design a Trusted Reader, to implement a hardware prototype to demonstrate such a possibility and to implement a software suite separately on a PC architecture to enable the concept to be elaborated and demonstrated.