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

Interim Security Deliverable
Report on the First 18 Months of the BRIDGE WP4 Security Work (D4.X)

Authors: BT Research

December 2007

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 document introduces a set of reports that compose the BRIDGE deliverable D4.X and report on the work performed within WP4 Security within the 18 months of the project. The content of this deliverable represents our answer to the critical research challenge that BRIDGE addresses – how to overcome the technical and business barriers to the adoption of RFID for collaborative supply chains.

Disclaimer:

1 Introduction

The WP4 "Security" Work Package of BRIDGE is examining ways to ensure that RFID tags, readers and networked RFID services are developed in harmony with security features to enable effective and safe deployment of applications in various business sectors. RFID technology and serialised information services are essential tools to enable organizations to share item level information. As businesses begin to collaborate and share supply chain information, it is essential that solutions are in place to guarantee the integrity, confidentiality and accountability of this critical data.

This document introduces a set of reports that compose the BRIDGE deliverable D4.X and report on the work performed within WP4 Security within the 18 months of the project. The content of this deliverable represents our answer to the critical research challenge that BRIDGE addresses – how to overcome the technical and business barriers to the adoption of RFID for collaborative supply chains. To this end we focus our security efforts on the architectural layers where interaction and conflict between multiple parties occurs. Tag and reader devices must be available to meet the requirements of security sensitive applications. Such concerns become paramount in complex open supply chain situations where many parties have access to, or ownership of, the tags and rely on the information from limited reader deployments which are not operated by them. Since many application areas will have unique demands we concentrate our efforts into providing a secure base for both tag and reader development. Beyond each organisation's security perimeters we must also establish a framework that allows supply chain data to be shared without compromising business operations. Here we utilised existing Internet and Web Service security technology wherever possible and focus our resources on attacking the supply chain specific problems of fine-grained access control, security management, the establishment of trusted relationships and the integrity analysis of supply chain information.

The technical work presented in these reports build on a formal list of requirements that have been extracted from the questionnaire and interview processes in both WP2 and WP4. Our initial work, D-4.1.1 identified the requirements and research challenges for enabling open and collaborative RFID environments. Our second deliverable D-4.1.2 provided an insight into the problem of inter-dependent security between supply chain operators, and some mechanisms to enable businesses to start to analyse their risks and related security investment beyond their own domain. We demonstrated that only a collective approach to security can achieve the lowest threat for all partners for the same investment in security. In these reports we go into the technical details of our approach by presenting technology solutions that enable collective integrity, confidentiality and accountability.

When discussing about the security of the RFID-based information systems, it is perhaps more useful to talk about what such networked services seek to achieve - the automation of collaborative supply chains and the introduction of new applications for industries and end users. Early examples of RFID applications have been dominated by closed applications, with controlled feedback often through human processes. Future applications will see more tags and sensors in the environment that can be directly read and controlled. The EPCglobal architecture with components such as EPCIS and Discovery Services will enable processes to work in distributed environment without requiring the support of centralised

applications. To make this future a success we will need both monitoring and control capabilities embedded within the architecture.

Our layered approach does not claim completeness but provides a major step forward to address current security and risk exposure of individual parties, along with the potential to introduction new services such as product authentication and secure track-and-trace. To conclude, we aim to make supply chain entities aware of future RFID security capabilities and guide technology providers towards the development of secure solutions. It is essential to understand that RFID security is not a painful risk assessment process but it is critical capability in the architecture framework to enable both the automation of existing supply chain processes and the creation of new collaborative services.

In the remainder of this overview document we reproduce the descriptions of the motivation, scope and technical delivery detailed by the individual Deliverable reports:

D4.1.3 The Economic Relevance of Secure RFID Solutions: a Qualitative Perspective
D4.2.1 Tag Security
D4.3.1 Anti-Cloning Tag
D4.4.1 Trusted Networks: Design of an RFID Trusted Reader
D4.5.1 RFID Network Confidentiality
D4.6.1 Supply Chain Integrity

D4.1.3 - The Economic Relevance of Secure RFID Solutions – a Qualitative Perspective

RFID is a disruptive technology that has a huge potential to change management activities, due to its ability to automate processes and provide accurate, trusted data. Its unique features include the ability to give each physical object a globally unique digital identity which can be read from a distance without requiring line-of-sight and in case of passive RFID, to operate even without a battery. These features provide new ways of measuring and integrating the real world into information systems and because of this, RFID has great potential to change the way we do business. From a security perspective, there are three considerations.

First, when RFID is implemented to improve an existing business process, RFID can enable the automation of activities and thereby reduce the potential business and security risks caused due to human error. Second, RFID itself induces new risks to a process. Security is therefore needed to keep automated aspects and invisible properties under control; otherwise the process could be susceptible to mass abuse. Third, RFID itself can enable completely new business applications due to its properties as a data gathering and process measurement technology. Activities and actions that could not accurately be measured before can now be measured. Again, security plays a major role here, as it provides the accountability needed to enable trust in the data and activities provided by these applications.

The objective is to provide security technology that supports the potential of RFID in mitigating existing business and security risks in processes while at the same time enabling the inherent security problems of the RFID technology to be managed. In addition, we believe that security is not only a must for business cases where RFID improves an existing barcode scenario, but also a completely new opportunity. Applications that are not possible to deploy today as their critical points depend mainly on security, will benefit from the technology developed in WP4. Secure RFID solutions are not just a must, but also an enabler of powerful applications that can increase the competitiveness of organizations tremendously.

The goal of this Deliverable is to highlight the economic relevance of secure RFID solutions. Particularly we want to show that there is more to security than just fulfilling a ‘must’. As the high level goal is to leverage the benefits of RFID, we will not just focus on the improvement of existing business cases but also show that secure RFID solutions can enable completely new and innovative applications. These applications require that supply chain partners are willing to participate and share information that was previously considered proprietary. Therefore, we believe that without complete and secure RFID solutions, the full potential of RFID can never be unlocked. To support our hypotheses, we will employ exemplary case studies that support our line of argument.

D4.2.1 - Tag Security

This Deliverable is dedicated to the development of secure RFID tags. These developments include protection measures on the tag itself, but also of the wireless communication link between the tag and the reader. The protection of the wireless link requires the development of technical protection measures on both tags and readers. Depending on the final application, the developed measures can be used to build anti-tracing and anti-tracking mechanisms for RFID technology or to provide secure authentication of the tags. The goal of the task is to provide suggestions and proof of concept for successful implementation of cryptographic protection that can be applied in open loop RFID systems and that comply with the restricted computing resources of low-cost RFID tags.

The suggested security measures are based on symmetric cryptographic primitives, which can be implemented in a way so that the reading distance of low-cost tags is not reduced. The additional cost due to marginally increased chip area of the tag chips is justified by the additional value such protection functionality can provide. Cryptographic functionality together with proper management of secret keys can be used as “PET” (Privacy Enhancing Technology) and is suggested as such by the Article 29 data protection working party as a measure to protect “personal data” stored on the tag. Additionally such functionality can be used to provide tag and reader authentication with the capability in principle to provide a proof-of-origin of tags and readers. Tags which can provide such authentication facilitate anti-cloning applications, while reader authentication provides the possibility to allow specific access to the tags’ content only for authorized readers (and in turn to prevent that illicit readers read tags or get access to specific data stored on a tag). The suggested solution will therefore provide technical measures for RFID tags to allow complying with data security regulations and principles and to prevent eavesdropping and cloning or the illicit modification of the tag’s memory.

Several subtasks tackle the problem from different perspectives:

- Development of prototyping platforms: We develop three semi-passive tag prototypes that can be easily extended with additional functionality. These semi-passive tag prototypes are fully compatible with the EPC Generation 2 Class 1 protocol.
- RFID pseudonym scheme: Using a semi passive-prototype we demonstrate how the basic security functionality can be used to develop a pseudonym scheme that provides protection of the tag identifier and prevents tracing of the tag history.
- Comparison of crypto primitives: Hash, encryption and stream cipher primitives are compared for incorporation into future secure tags.
- Implementation attacks: Investigation of the threat of “Side-Channel Attacks” to find out whether RFID technology is susceptible to those attacks and to what level of security the tags need to be protected.
- Key management: Investigation into the problems of storing secret keys on tags.

D4.3.1 - Anti-Cloning Tag

The overall aim of Task 4.3 is to combine the developed base technologies of other tasks in WP4 towards a demonstrator system. The demonstrator will perform tag authentication for an anti-cloning prototype system.

We plan to use the prototypes developed in T4.2 and implement a secure authentication scheme that can be embedded into EPC Gen2 communication. The authentication layer will be integrated as a security layer that is built upon unprotected communication.

The authentication layer needs to be defined upon EPC Gen2 to allow compatibility with existing infrastructure. To enable proper specification that allows secure implementation at considerable costs, the development of a cycle accurate Gen2 protocol emulator is planned so that different approaches can be compared on the basis of accurate emulation. A prototype will use as proof of concept of the authentication scheme. A UHF reader firmware will be extended so that it can communicate with the tag prototypes that provide security functionality. Additionally, we plan to investigate alternative approaches for key management that can be applied to applications in the supply chain.

During the first period of BRIDGE, we completed the development of a software emulator for the communication between tags and reader. The firmware of the reader prototype reader was extended in a way so that GEN2 custom commands are supported during the tag-reader communication. Adaptation to the security layer is therefore possible without additional effort. We present initial suggestions for a security layer, which are currently under investigation.

We also present plans for the next period of research. We plan to agree on a security layer and to implement it first in the emulator for further assessment. If the suggestion passes the evaluation without showing any obvious weakness, we will implement the scheme as a demonstrator system. The investigation of additional key management is accompanying the ongoing developments.

D4.4.1 - Trusted Networks: Design of an RFID Trusted Reader

Task 4.4 – RFID Trusted Networks aims to overcome the current barriers to the deployment of secure RFID applications. Security services are fundamental to the success of new RFID applications and in particular to the sharing of supply chain information among different parties in the supply chain.

Within this task the objective is to design and develop a secure RFID reader that provides trusted operation and that is compatible with the EPC Gen 2 standard. The reader is the first device connected to an organization's internal network and forms a key security barrier. The reader is essential to the operation of tag security schemes such as the one developed in task 4.2 and 4.3. It provides a mechanism to avoid recourse to a centralized key server for every tag read. It also provides a control for the information that is injected into RFID applications (e.g. supply chain).

The questions that Task 4.4 is trying to answer is 'how can we allow trusted RFID applications to be installed in the reader?'. And 'how can we validate these applications through an automatic auditing process?'. We attempt to provide a workable practical solution through the use of trusted computing. In particular, we look at the problem where the RFID operator is not the owner of RFID applications or the data owner. In this case we look for solutions that enable the operator to determine access control policies for the service but leave the user in control of which component to install and use.

Our design splits the management of the RFID reader architecture into three roles: manufacturer, operator and users. The manufacturer is the vendor of the base Trusted RFID Reader. The manufacturer provides a module with the basic operation of the reader, allowing the installation of functions by the reader operator, and service instantiation by the reader users. The reader operator is typically the owner of the RFID reader. In our design the reader operator is solely responsible for the installation of new functions onto the reader. Users of the Trusted RFID Reader are granted permissions to use these functions by the reader operator. These permissions allow the user to select functional components to compose into individual, instantiated services.

In Part I of this report we discuss the motivation and concrete requirements for a Trusted RFID Reader. Part II then focuses on the detailed design of the RFID Trusted Reader (and, in associated Appendices, evaluations of the original form of a Trusted RFID Reader, and the different technologies that we hoped to exploit in building an improved form of Trusted Reader). Part III of this report then focuses on the implementation of this design into a real RFID Reader. CAEN has developed a specific hardware board to support the security requirements required by the different software modules. The BT team, together with other T4.4 partners, has focused its effort on the architecture design and the software modules.

D4.5.1 - RFID Network Confidentiality

Task 4.5 – RFID Network Confidentiality aims to overcome the current barriers to the sharing of supply chain information between different parties in the supply chain. This sharing can increase the value of the collected RFID information immensely and enable new supply chain applications and optimisations. This will not happen unless each party can control the release of sensitive business data, or perform operations based upon data from other participants. It is easy to imagine a scenario where no sharing takes place since the risk of attacks on operations outweighs the benefits of end-to-end supply chain visibility.

RFID applications such as the EPCIS, and EPC Discovery Services being developed by WP2, will not exist in isolation. Therefore Task 4.5 seeks to develop a security technology framework suitable for RFID architecture components, but based upon existing security technologies, notably for Web Services.

The question that Task 4.5 is trying to solve is how far we can go with such existing and proposed security technology? We attempt to provide a workable solution to fine-grained access control. Instead of traditional division of information by coarse views, we suggest that the ability to control information based upon fine-grained characteristics such as the EPC, date, or bizStep may be advantageous.

We also look at the unusual problem of Discovery Services where the information owners are not the operator of the service. In this case we look for solutions that enable access control policies to be written by the publishers of information to the Discovery Service as part of a policy set for their organisation. In addition we look at how supply chain communities can be set up, and how emergency policies may be implemented to reduce the management overhead.

Having explored how far we can go given the latest security technology developments in Part II, we consider the real-world demands of supply chains. Part III of this report focuses on how an organisation can assess what is critical information in terms of confidentiality. Such questions are critical before we can assess how such information is shared, and what attacks are possible on our organisation across a range of different information sources.

Finally, this report considers the problem of access control in a real industry scenario, looking at RTI assets within a retail industry. We use this study to elicit some early thoughts on what policies may exist and how they are managed. This early work will then form a basis for more detailed discussions with industry partners to develop a clear vision for access control.

This report represents the work within the first 18 months of T4.5. In the second stage of the project the technical work will shift from the lower enabling layers of technology for access control, to elements around the management of distributed policies. The business focussed work will continue to develop the thinking around what information should be protected, and how different industries will use access control technology in a manner that makes sense for their critical information and supply chain processes.

D4.6.1 - Supply Chain Integrity

Tracking of individual products throughout the company and the entire supply chain enables many new, and allows to optimize existing business processes. The emerging EPC-network standard provides (a blueprint of) an IT infrastructure to automatically capture traces (i.e., observations) of individual products, to store them locally, and to share them with other supply chain participants. If critical business decisions are based on those observations (both from company-internal as well as from external sources) the integrity of the data is of utmost importance. Incorrect, omitted, and inconsistent observations can disturb future supply-chain execution and control processes, for example, by hampering their correct interpretation for anti-counterfeiting, recall, and other purposes.

To ensure the quality and integrity of product-traceability data within the own company and throughout the supply chain, methods are needed to prevent the injection of erroneous data and the manipulation of existing data. Since this is not always possible, tools are needed to detect that there are errors and inconsistencies in the data before it is used for critical business decisions. Identifying specific observations as erroneous (and possibly correcting them) in a set of observations for a particular product in a particular supply chain is also desirable but may not always be necessary.

This report aims at providing an overview of the topic of item-level observation-data integrity, at discussing tools for the detection and mechanisms for preventing violations of this integrity. This report will also discuss fundamental limitations of the discussed approaches and present initial prototype software.

This Deliverable has two main goals. Firstly, to provide a simple, very broad-ranging model in which all the issues relating to supply-chain integrity can be more clearly understood. We will reflect on the meaning of integrity and categorize integrity conditions (or rather integrity violations) in four intuitive categories.

The second goal of this report is to discuss the idea of using the EPC network as a tool for detecting violations to supply-chain integrity. Automated detection of integrity violations can trigger recovery mechanisms, thus helping to maintain the integrity of the supply chain. Along these lines we will present initial conceptual work, including a prototypical implementation of such a tool. We explore our approach of finding evidence of integrity violations through rules, and substantiate the concept by providing several concrete examples. We also present our initial conception of a software implementation of such an integrity checking tool and present an initial prototype in which we have put the general idea to a first test.

During the second part of Task 4.6, we intend to refine those ideas and we will extend the prototype into a configurable software tool, able to detect a wide range of supply-chain integrity violations.