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

Security Technology Roadmap

Authors: Manfred Aigner (TU Graz), Trevor Burbridge (BT Research), José Juan Cantero (AT4 wireless), Alexander Ilic (ETH Zurich), Jasser Al-Kassab (SAP Research), Oliver Kasten (SAP Research), Antonio Plaza (AT4 wireless)

June 2009

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 provides a technology roadmap for the results developed by BRIDGE WP4 "Security". These results represent security enhancements to the EPCglobal network architecture and aim to support the adoption of RFID technology.
For each security enhancement, the relevance from a consumer, solution-provider and end-user company point of view is described. Moreover, an assessment of the maturity of each security enhancement is provided. To understand the roadmap towards a wide-scale application in practice, further research and development work is discussed.

Disclaimer:

Authors and Contributors

Work package leader	Andrea Soppera (BT Research)
Task leader	Alexander Ilic (ETH Zurich)
Authors	Manfred Aigner (TU Graz) Trevor Burbridge (BT Research) José Juan Cantero (AT4 wireless) Alexander Ilic (ETH Zurich) Jasser Al-Kassab (SAP Research) Oliver Kasten (SAP Research) Antonio Plaza (AT4 wireless)

Table of Contents

1. Introduction 5
2. Enhancing the Security of EPCglobal Networks 6
   2.1. Results overview 6
   2.2. Categorization 7
   2.3. Visualization of Roadmap 8
3. RFID Tag and Reader 9
   3.1. Prototyping Platform Based on Semi-Passive Tags 9
   3.2. Identity Protection Based on Standards Compliant Pseudonym Scheme 11
   3.3. Symmetric Crypto Algorithms and Side-Channel Attacks 13
   3.4. Anti-Cloning Demonstrator for RFID Tags 14
   3.5. Security layer for RFIDSim and ISO 18000 Enhancement Proposal 15
   3.6. Trusted RFID Reader 16
4. Data Exchange 19
   4.1. Secure Discovery Service 19
   4.2. Access Control Framework for EPCIS Data Exchange Services 22
5. Application Software 25
   5.1. Tool for Rule-Based Analysis and Visualization of EPCIS Events 25
   5.2. RFID Track-and-Trace Based Integrity Checking and Alerting Tool 26
6. Conclusion and Outlook 29

1 Introduction

This document provides a technology roadmap for the results developed by BRIDGE WP4 “Security”. These results represent security enhancements to the EPCglobal network architecture and aim to support the adoption of RFID technology.
For each security enhancement, the relevance from a consumer, solution-provider and end-user company point of view is described. Moreover, an assessment of the maturity of each security enhancement is provided. To understand the roadmap towards a wide-scale application in practice, further research and development work is discussed.
The goal is to disseminate the key results of BRIDGE WP4 to the public, outline further research needs and identify relevant commercialization opportunities necessary to bring the security enhancements of the EPCglobal network to the market.
This document is structured as follows. The next section structures the results and presents a technology roadmap. Afterwards, each of the developed security enhancements in the categories “RFID Tag and Reader”, “Data Exchange”, and “Application Software” is presented. Finally, a conclusion is given to discuss when the developed results are likely to hit the market and enter the RFID mainstream world.

2 Enhancing the Security of EPCglobal Networks

The technology roadmap shows how BRIDGE results can complement the EPCglobal network architecture. The work done in BRIDGE WP4 is focused on adding more security to this architecture. The next sections provide an overview of the results, their roadmap categorization and a visualization of the technology roadmap.

2.1 Results overview

Table 1 shows the ten selected results of BRIDGE WP4 and the main contributors responsible for developing them.

Table 1. Security enhancements developed in BRIDGE and contributors

Result Name	Contributors
Prototyping Platform Based on Semi-Passive Tags	TU Graz, Confidex, CAEN
Identity Protection Based on Standards Compliant Pseudonym Scheme	TU Graz, BT Research
Symmetric Crypto Algorithms and Side-Channel Attacks	TU Graz, Fudan University
Anti-Cloning Demonstrator for RFID Tags	TU Graz, Confidex, CAEN, BT Research
Security layer for RFIDSim and ISO 18000 Enhancement Proposal	TU Graz, ETH Zurich
Trusted RFID Reader	BT Research, CAEN, ETH Zurich
Secure Discovery Service	AT4 wireless, BT Research
Access Control Framework for EPCIS Data Exchange Services	BT Research, AT4 wireless, ETH Zurich, SAP Research
Tool for Rule-Based Analysis and Visualization of EPCIS Events	ETH Zurich, BT Research
RFID Track-and-Trace Based Integrity Checking and Alerting Tool	SAP Research

2.2 Categorization

To show at what architectural layers the BRIDGE results enhance the security of the EPCglobal network architecture, we use the following categorization scheme. Since the EPCglobal specifications range from several hardware to software layers relevant for RFID systems, we use the following simplified grouping:

- **RFID Tag and Reader:** Protocols and hardware components of tags and readers that enable secure communication over the air and ensure the integrity of the components
- **Data Exchange:** Data pre-processing and look-up software that enable secure information sharing along the supply chain in modes of 1:n and n:m
- **Software Application:** Basic to advanced software applications that use the EPCIS access interface and interpret EPCIS event data

The second important categorization for the roadmap is the maturity scale. BRIDGE is a time-limited project based on three years and the BRIDGE results are a collection of completely new ideas and extensions of existing concepts. We have rated the maturity of the BRIDGE results to provide the reader with an idea about the remaining research and development effort needed to bring the results to the mainstream market. We have used the following scale:

- **Idea:** The problem description is complete and requirements are verified with potential future users. Interviews, often in depth, have been conducted with end users.
- **Concept:** A detailed description of a solution concept was developed based on the requirements. Moreover, a reviewed design exists and the feasibility of the solution concept was discussed.
- **Demonstrator:** The key aspect of the solution concept has been implemented in hardware and/or software and can be shown to interested users.
- **Prototype:** A detailed design and reference implementation of the solution concept exists. Further research and development is needed to increase the quality for a market-grade deployment and further optimize performance.
- **Product:** The product exists in a first version of market-grade quality. The product is sold already or is currently undergoing final commercialization steps.

2.3 Visualization of Roadmap

Figure 1 shows each of the BRIDGE WP4 results categorized by maturity stage and architectural layer.

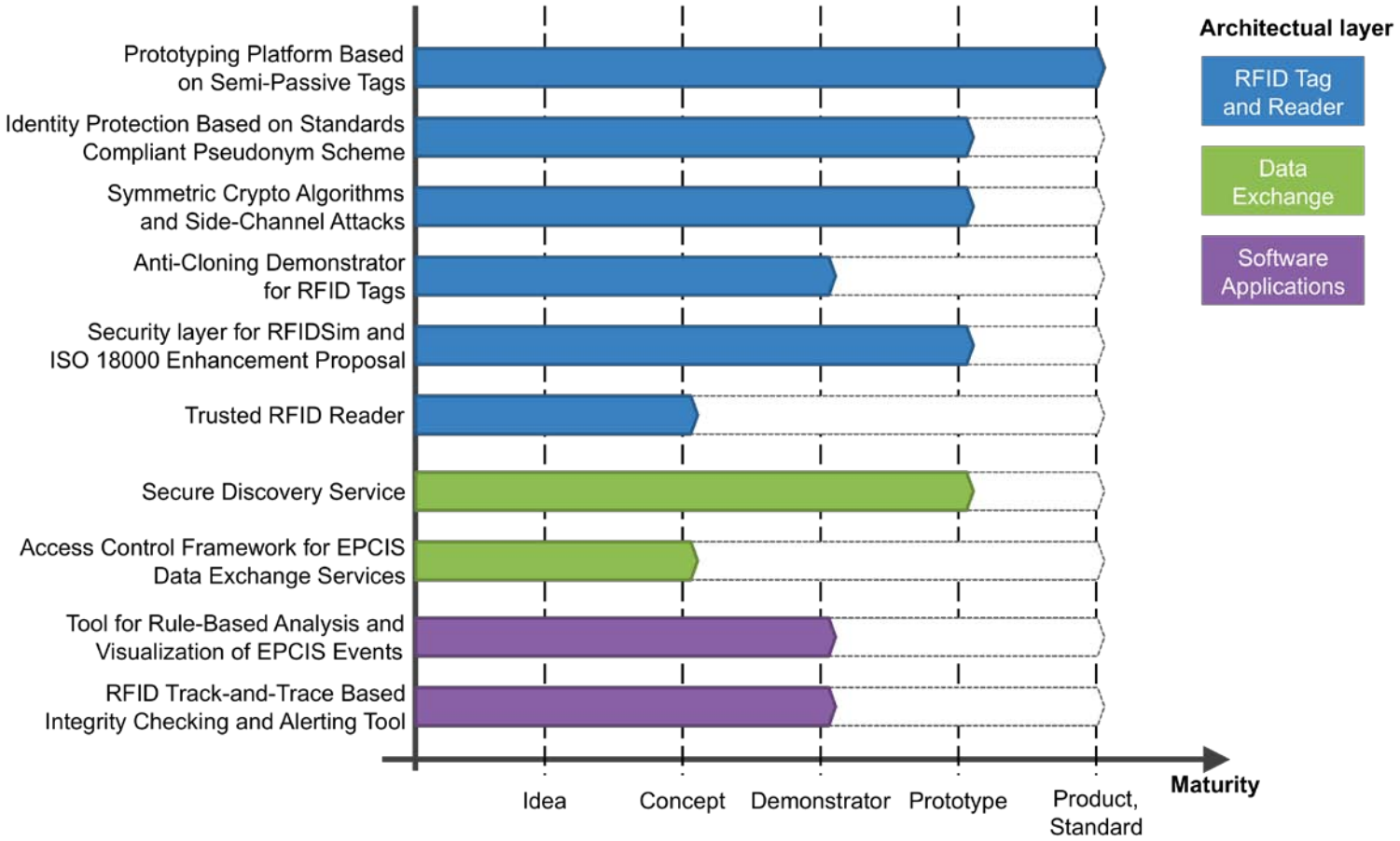

Figure 1. Technology roadmap illustrating the further R&D efforts needed to bring the BRIDGE results to product stage

3 RFID Tag and Reader

This section provides details on the BRIDGE WP4 results in the RFID tag and reader layer. For each result, a description of the achieved results and details on next steps and research opportunities are given.

3.1 Prototyping Platform Based on Semi-Passive Tags

3.1.1 Relevance for Consumers, Solution-Providers and Users

BRIDGE WP4.2 developed a prototyping platform on basis of semi passive tags. The advantage is that new cryptographic protocols can be implemented rapidly and tested with UHF readers. Within BRIDGE we have examined AES, TEA and IDEA lightweight implementations that are attractive in terms of gate count, power and timing, and in future asymmetric schemes may become economical. On top of these basic cryptographic capabilities we can experiment with a wide range of protocols and custom instructions for authentication and to preserve the confidentiality and integrity of the data on the tag.
The prototyping tag is a versatile tool for developing new Class-2 and Class-3 tags and can be used during system development in a stage when final tags are still under production. Demo implementation of systems can be built without the need to implement tags with extended capabilities in hardware, which is a rather cost intensive process.

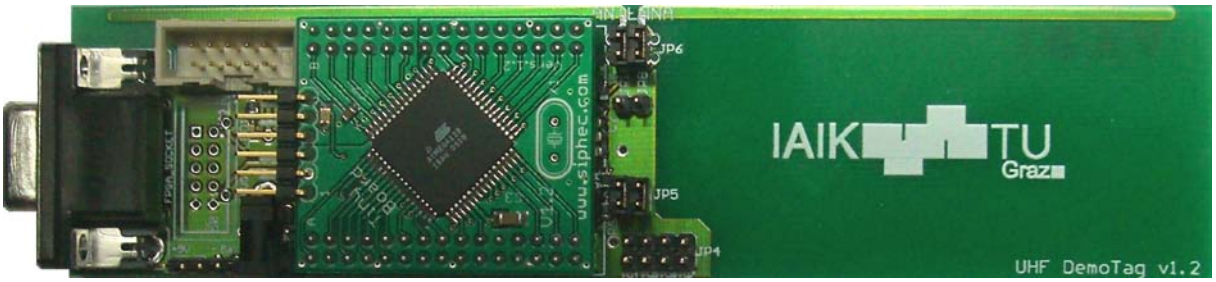

Figure 2. Photo of semi-passive prototyping tag

3.1.2 Result description

The prototyping tags are fully compatible to passive tags, but allow extension of their functionality. WP4.2 developed solutions to protect the communication between tag and reader on basis of cryptographic operation computed on the tag. The underlying assumption is that a tag carries a cryptographic key and computes a cryptographic algorithm to enable security services like authentication or encryption. No budget was available for development of fully passive RFID tags, therefore a semi passive platform was developed to demonstrate the concept. This semi-passive tag is not restricted to security functionality but can also be extended to incorporate other functionality.
The prototyping tag allows researchers, tag manufacturers and protocol designers to experiment with the requirements and capabilities of different encryption and protocol schemes before going to chip manufacture. It also fulfils an important role for researchers and students without the expertise or facilities to manufacture tags.

3.1.3 Roadmap

The semi-passive tags are available from the IAIK webshop[1]. First customers purchased the tags after presentation during RFIDSec 2009. Our customers are mainly academic research groups who try to investigate capabilities of future RFID tags. We will go on to promote the platform on conferences. So far we produce the tags in-house, since the purchased volume is currently quite low. As soon as we get more requests we will outsource the production of

[1] http://jce.iaik.tugraz.at/sic/products/rfid_components/uhf_rfid_demo_tag

tags to a company that provides high volume PCB production and mounting facilities. The semi-passive tags are developed from standard components; therefore no special equipment is needed for production or programming. Newer versions of the tag will allow extension of the platform with FPGAs to allow testing of digital designs for the tag-extensions directly on the board. We have also considered extending the tag by inclusion of a dedicated interface for the attachment of sensors.

3.2 Identity Protection Based on Standards Compliant Pseudonym Scheme

3.2.1 Relevance for Consumers, Solution-Providers and Users

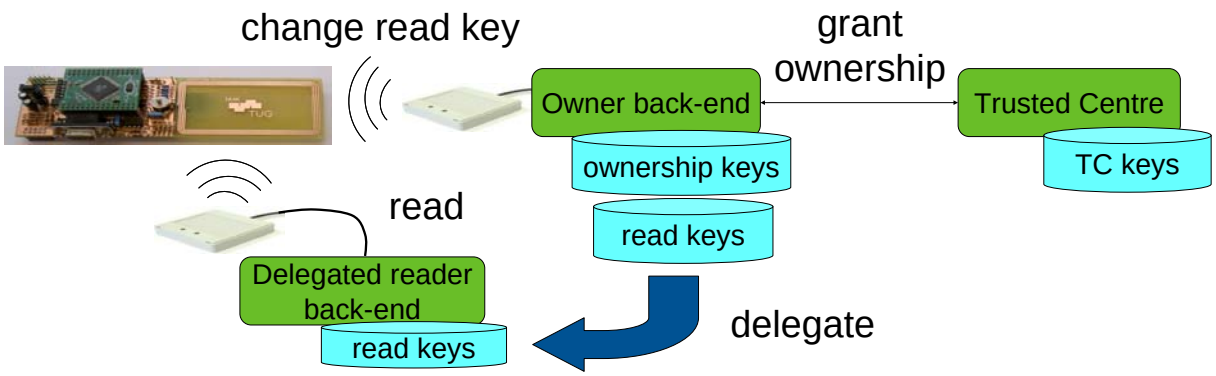

Figure 3. Pseudonym scheme

3.2.2 Result description

Protocols to perform tag authentication or provide memory access control are straightforward using symmetric key cryptography as provided by the secure tags developed within the BRIDGE project. Since the tag does not hide its (claimed) identity, this can be used to identify the correct shared key to use in the standards-compliant custom command to the tag.

The problem is much more complicated if the confidentiality of the tag identity is required. Naïve solutions try every known tag secret until the tag response is decoded. This is clearly not scalable for item level supply chain solutions. Instead, schemes have been developed that structure the tags into a tree to enable scalable tag identification. However the problem with these schemes is the time required to identify the tag.

In BRIDGE we developed a scheme that uses multiple levels of tag access and management rights. The Trusted Centre (for example operated by the tag manufacturer or independent body within a supply chain industry) operates a scalable pseudonym scheme using industry compliant custom commands to the tag. However, individual parties attempting to identify the tag are delegated a single read key. At such local level we trade off between the performance of the back-end reader system and the requirement to be able to perform fast reads of large numbers of tags. Using a single key the encrypted tag identifier can be read using the standard inventory command.

Our scheme also allows the controlled transfer of tagged products or assets between owners, giving the new owner the ability to revoke any previous access rights, along with the ability to delegate (and revoke) reading ability to its own readers and trusted partners.

We have shown that pseudonym schemes that provide scalable tag management along with high speed reading can be implemented using standard tag protocols given symmetric cryptographic capabilities on the tag. Such schemes can be used where privacy is a major concern (such as after point-of-sale) or where highly confidential supply chain as operated (such as for military assets).

3.2.3 Roadmap

Although pseudonym schemes using symmetric cryptography are possible, the problem is much simpler using asymmetric cryptography. Using asymmetric cryptography the identity of the tag can be simply encrypted using the public key of a trusted identification server. We expect that the industry will work towards the deployment of such asymmetric secure tags in

the short term and such capabilities may be available before the need to deploy pseudonym schemes becomes paramount.
Whether symmetric or asymmetric cryptography is used to implement the pseudonym scheme, tag standards should allow the sending of a random number from the reader to the tags during the inventory command. Such facility is currently missing from the standards and consequently our prototype. Without this ability it is possible that an attacker may listen to the responses from tags and pretend that the tag exists elsewhere in the supply chain by replaying these responses. Thus, if authentication is also required an additional authentication operation is necessary preventing high processing rates.
Although the development of security capable tags is unlikely to be driven by identifier confidentiality concerns, the market will be driven by product and asset authentication. Once secure tags are attached to products and assets for authentication it becomes a simple tweak to also implement a pseudonym scheme for confidentiality or privacy purposes.

3.2.4 Related publications

- Academic publications
    - Christian Tutsch, Andrea Soppera, Trevor Burbridge, Manfred Josef Aigner , “RFID Tag Pseudonyms with Efficient Reading and Scalable Management “, Internet of Things (IoT) 2008, Zurich. http://www.iot2008.org/adjunctproceedings.pdf
- BRIDGE deliverables
    - D4.2.1, “Tag Security”, http://www.bridge-project.eu/data/File/BRIDGE_WP04_tag_security.pdf

3.3 Symmetric Crypto Algorithms and Side-Channel Attacks

3.3.1 Relevance for Consumers, Solution-Providers and Users

Our work demonstrates that proper protection of cryptographic hardware is also necessary for RFID technology. Countermeasures against Side-Channel Analysis (SCA) attacks need to be applied as soon as cryptographic functionality is implemented on RFID tags. Due to the scarce power budget available the design of such countermeasures is not straightforward. Solutions from smart card technology cannot be adopted directly. Proposals for implementation of such countermeasures exist already in scientific literature. We highly recommend producers of secure tags to familiarise themselves with the topic of side-channel analysis.

3.3.2 Result description

In recent years a new sort of attack has been published that allows extraction of information about secret keys stored on RFID tags from “side-channel” data, such as the continuous power consumption of a device (power analysis) or it’s EM-emanation (EM analysis). In respect to RFID technology, this sort of attack has been meaningless so far, since no cryptographic keys were stored on the tags. With the application of cryptographic capabilities on RFID tags, these attacks become relevant for RFID, since attackers can easily get tags and operate them within a controlled environment. These so-called implementation attacks often use sophisticated statistical methods of power and EM-traces of multiple (up to millions) of encryptions to find out the secret key. When we started our investigations, it was considered that EM attacks (attackers sample the EM-radiation emitted from devices) were not meaningful, since the surrounding reader field produces too much noise. Power attacks were not considered as dangerous since the tags do not have a dedicated power terminal where attackers might measure power consumption and passive tags derive the power they need from the surrounding field. Our results revealed that these assumptions do not hold in practice. Our experiments revealed that the continuous power consumption of UHF tags can be observed as parasitic backscatter signal. A reception circuit, such as a standard UHF reader, is sufficient to get a data dependent signal that is strong enough to be exploited in side-channel attacks. It is therefore necessary to include countermeasures against these sort of attacks when cryptographic primitives are implemented on RFID tags. Additionally we tried to separate the antenna from the chip of a tag and verified if it is possible to still operate with the tag afterwards. It was easily possible to measure the power consumption of the tag after separating antenna and chip. Basic equipment which is typically available in any student’s lab is sufficient to perform such modifications.

3.3.3 Roadmap

We will expand our research activities to include fault analysis attacks - a new class of implementation attacks. A new class of countermeasures specifically tuned for application on RFID tags needs to be developed. This type of countermeasure takes advantage from RFID specific characteristics, e.g. rather low throughput and possible high latency. When countermeasures against such implementation attacks are considered early in the tag design, during definition of protocols, the implementation can be less expensive in terms of power and area consumption. Future work will be directed towards raising awareness of the existing threats and development of efficient countermeasures. Additionally we will perform further research towards implementation of asymmetric cryptographic primitives on UHF RFID tags. So far it is not yet possible to provide asymmetric cryptographic functionality small enough to be acceptable for low cost tags. Newer process technology will provide more effective area on RFID tag chips, and can therefore open the way for more complex computations.

3.4 Anti-Cloning Demonstrator for RFID Tags

3.4.1 Relevance for Consumers, Solution-Providers and Users

The motivation for the development of the Anti-Cloning demonstrator is to familiarize a non-technical audience with the principle and the advantages of secure tag authentication. The anti-cloning properties of the tag can be incorporated into a tag authentication system as shown in the demonstrator. Such tag authentication can then be used to authenticate goods, preventing counterfeiting and allowing identification of asset ownership.

3.4.2 Result description

The final demonstrator consists of a reader application with an easy-to-handle graphical user interface (GUI), a UHF reader which is able to communicate with secure RFID tags, some semi-passive UHF tags with secure tag-authentication functionality, a web service and key database to provide information about the tags and an optional EPCIS conformant repository to store authentication results for historical analysis.
During the definition of the demonstrator we considered a scenario with RTI (returnable transport items), where the owner of the RTI wants to protect against cloned assets or the acceptance of other parties assets into it's supply and maintenance pools. We consider that RTIs include a tag with secure authentication capability. A cryptographic challenge-response protocol is executed, which is computed using AES symmetric encryption. Since we expect that the owner of the tags and the verifying party are the same organisation (or have high levels of trust) the scenario allows the local production of the tag challenge (improving tag throughput) and the option of storing the authentication secrets locally (improving the resilience and latency of the authentication check). For other scenarios the challenge and key storage may be managed remotely by other parties.
The scenario was chosen for demonstration of the anti-cloning functionality to a non-security audience. The demonstrator is a simple RFID system that consists of a database server, a Reader and semi-passive anti-cloning tags attached to objects acting as the RTI. The demonstrator allows definition of "cloned tags" that use the ID of an original object, but do not have information about the secret key that is stored on legal tags to display how the system reacts on cloning attacks. Conventional systems using standard RFID tags cannot distinguish such clones from original tags.
The demonstrator system has been shown in a dedicated booth during the BRIDGE dissemination day after the RFIDSec 2009 conference. Other events where the demo will be exhibited are currently being discussed.

3.4.3 Roadmap

We plan to exhibit the demonstrator at more conferences and workshops. Currently an interface for an EPCIS repository is implemented, which can provide successful or unsuccessful authentication information to upper layer information services. We currently rely on ad-hoc EPCIS query clients to display this data, although in future this information can be displayed by specialist authentication analysis software.

3.5 Security layer for RFIDSim and ISO 18000 Enhancement Proposal

3.5.1 Relevance for Consumers, Solution-Providers and Users

Secure tags feature additional functionality that can be accessed by the reader. To execute the security relevant operations a protocol extension for the communication between tags and readers needs to be defined. WP4.3 defined such an extension with respect to maximum compatibility to existing and established standards as well as minimal performance overhead in standard situations. Assessment of the protocol when such tags with extended functionality are not yet available is not trivial. On the other hand, it is very expensive to produce tag prototypes that are flexible enough to change the implemented protocol execution for investigation. Protocols for security extensions additionally require security analysis in various situations. Due to the randomized nature of the inventory procedures it is impossible to calculate the exact behaviour in situations where a high number of tags are involved. Additionally, current RFID protocols, like EPC Gen2, offer various different possibilities and strategies to extend the functionality. Straightforward estimation of the resulting performance of a certain implementation in different scenarios with different numbers of tags concurrently in the reader field is not possible.

3.5.2 Result description

To allow an accurate performance and security assessment before implementation of anti-cloning tag prototypes and anti-cloning demonstrator we implemented the security extensions in the simulation platform RFIDSim. Different implementation options were implemented and accurate performance and security assessment was performed on the basis of extensive simulation of different scenarios. Our investigations concentrated on authentication of the tags as a core feature to prevent cloning.
The results of the simulations show that an interleaved protocol that uses separate commands for sending of the challenge and receiving the responses is preferable. Different reader strategies for addressing tags were compared to find optimum parameters. A scientific publication that summarizes the results is currently under review.
The defined and simulated security layer was the starting point for a new work item proposal for future versions of ISO 18000. Meanwhile a working draft for “file management and security services for RFID” is under construction. The security related parts are based on the inputs developed by the BRIDGE WP4 team. The task leader for WP4.3 (TU Graz) supports the editing of the document.

3.5.3 Roadmap

Our suggestions are currently considered in the development of the document ISO/IEC WD 29167 as optional extension of ISO/IEC 18000-6. Bridge WP4 members will follow the specification process and consult with the ISO team providing their expertise. Discussions within the ISO working group can refer to our results of BRIDGE WP4.3 when feasibility or performance of the suggested approach is discussed. The fact that the presented approach is implemented in a simulation platform like RFIDSim and in the BRIDGE Anti-Cloning demonstrator improves the chances for early acceptance as standard extension for ISO/IEC 18000-6.

3.6 Trusted RFID Reader

3.6.1 Relevance for Consumers, Solution-Providers and Users

A wide range of products and asset authentication techniques have been examined within BRIDGE and in the wider industry. Within BRIDGE we have looked at how a Trusted RFID Reader can be used to improve the performance and security of these techniques. The secure identity of the Trusted Reader can be used to ensure that supply chain events are not spoofed from other readers or directly into the network, and also provides the basis for secure communication channels from the reader (to avoid eavesdropping, alteration or injection of data).

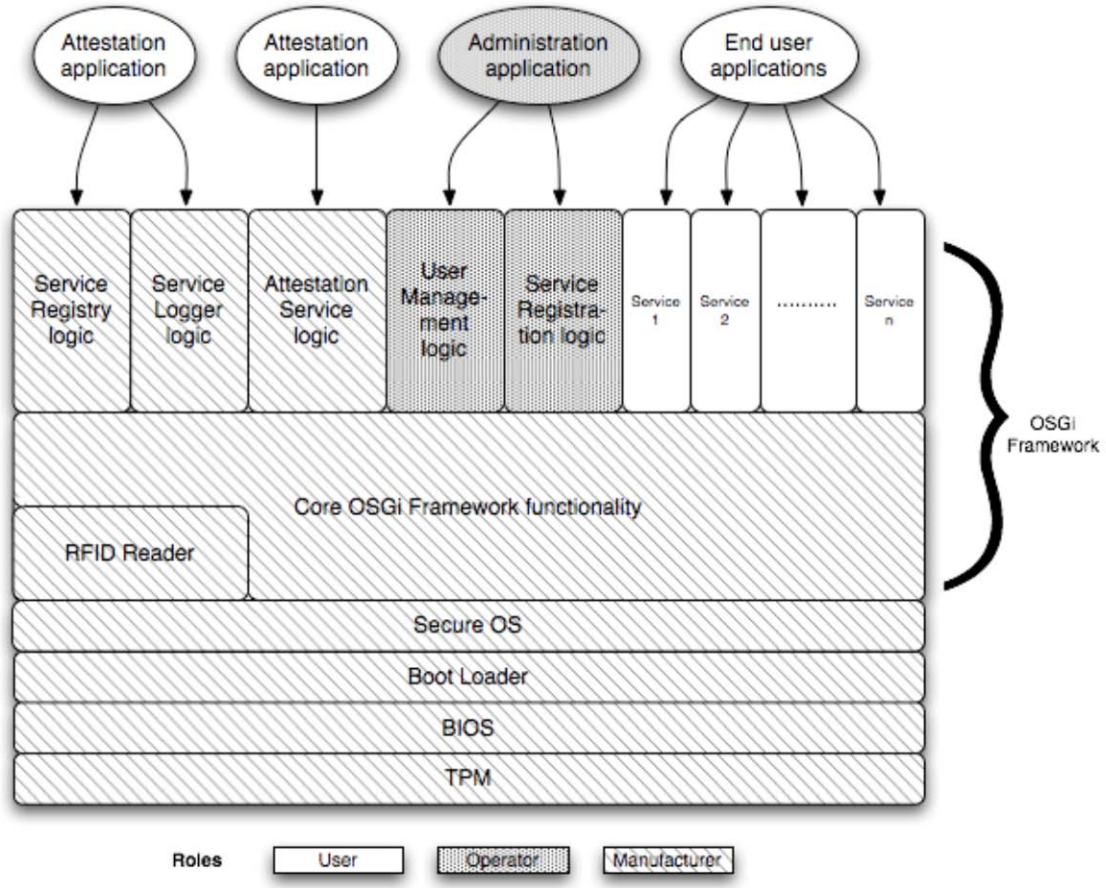

Figure 4. Trusted reader architecture

3.6.2 Result description

The use of a Trusted Platform Module (or TPM) within the reader means that physical or network attacks on reader vulnerabilities will not reveal the secrets that allow events to be spoofed from another point in the network. Furthermore, we can check the integrity of the reader to ensure that no unauthorised or modified code is operating on the platform. This then provides a very secure base for running local authentication processes, and even storing the secrets and keys used in the authentication process. Any secrets can be sealed by the TPM and only available to the correct, and uncorrupted, local authentication application. Since each authentication process can be given a secure area within the Trusted Reader, multiple schemes can be run concurrently for multiple authenticating parties (such as multiple product manufacturers) without compromising their integrity or confidentiality. The use of the Trusted Reader is especially powerful where the reader is deployed at locations by parties within the supply chain who are not fully trusted (either in motivation or

their ability to secure their systems). While the operator of the Trusted Reader may grant permission for authentication processes to be operated on the reader, they do not gain any ability to subvert the process.
We have also developed a supply chain control application for deployment on the Trusted Reader that allows supply chain controllers to specify permissible routes across the supply chain. Any deviances from these routes (including the introduction of counterfeit items) are detected through the use of trace signatures on the RFID tags. These signatures are replaced at each checkpoint by the Trusted Reader, preventing upstream operational information from being leaked along the supply chain.

3.6.3 Roadmap

Within BRIDGE we have proved that the implementation of a Trusted Reader is feasible in both hardware and software. We have developed a Trusted Reader architecture that provides a local multi-service environment that is ideal for operating multiple user services such as authentication. These local processes improve the performance of the processes (especially if the network or back-end systems fail).
The next step in the industry is to take the prototype reader developed within BRIDGE into a fully commercial offering. We have shown that this can be achieved with a limited increase in processing power and memory within the reader, along with integration of an inexpensive TPM unit. Such increases in processing power are expected in future readers in order to incorporate new interfaces such as message buses. These readers could therefore be available to the market as an enhanced version of the current premium range of RFID readers. Once such readers are available, this will stimulate the development of distributed supply chain applications with local processes operating on the reader. We have already seen more restricted development along these lines by an industry vendor who offers service management and message based communications capabilities for OEM use by reader manufacturers.

3.6.4 Related publications

- Academic publications
    - David Molnar, Andrea Soppera, David Wagner, “Privacy For RFID Through Trusted Computing”, Workshop on Privacy in the Electronic Society (WPES) 2005, Alexandria USA, http://www.cs.berkeley.edu/~dmolnar/papers/wpes05-camera.pdf
    - Andrea Soppera, Trevor Burbridge, Valentijn Broekhuizen, “Trusted RFID Readers for Secure Multi-Party Services”, EU RFID Forum 2007, Brussels, http://www.rfidconvocation.eu/Papers%20presented/Technical/Trusted%20RFID%20Readers%20for%20Secure%20Multi-Party%20Services.pdf
- BRIDGE deliverables
    - D4.4.1, “Design of an RFID Trusted Reader”
    - D4.4.2, “Secure RFID Reader”
    - D4.3.1, “Anti-Cloning Tag”

4 Data Exchange

This section provides details of the BRIDGE WP4 results in the data exchange layer. For each result, a description of the achieved results and details on next steps and research opportunities are given.

4.1 Secure Discovery Service

4.1.1 Relevance for Consumers, Solution-Providers and Users

The key driver behind the EPCglobal network is the end-to-end visibility of RFID data and lifecycle information for each and every product inside the supply chain. This data visibility, obtained by means of networked services such as EPCIS (EPC Information Service) or Discovery Services, is the basis of a very relevant potential improvement of existing business processes and uncovers new business opportunities. In this scenario, the ability to control the disclosure of the right information only to authorized partners is one of the fundamental requirements for supply chain managers.
Discovery Services allow supply chain participants to notify other that they hold information about particular items in their information services. However, even the fact they hold information is often commercially sensitive information that must be withheld from competitors and other parties.

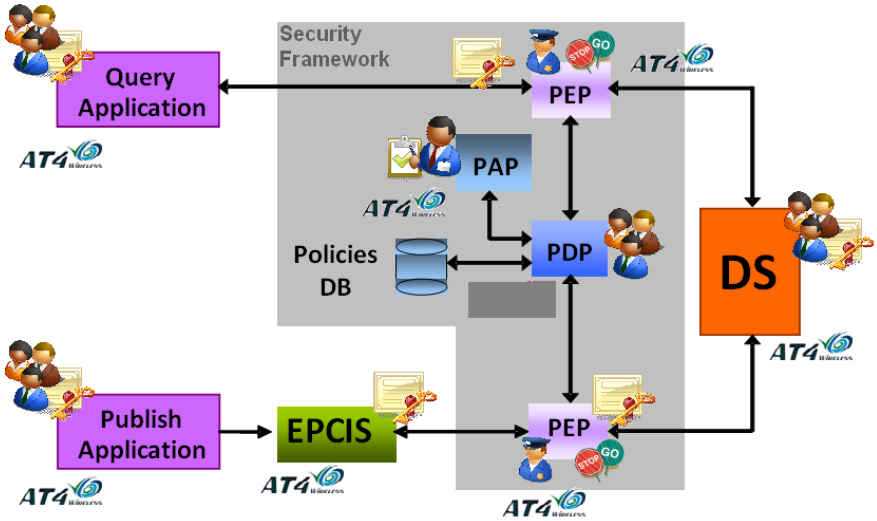

Figure 5. Secure Discovery Service

4.1.2 Result description

Security mechanisms capable of providing vital features, such as authentication, authorization, confidentiality, integrity and non-repudiation, are required in order to deploy secure networked services. All these features are covered in a scalable and efficient way by the security framework designed and implemented within the scope of Task 4.5, based on OASIS (Organization for the Advancement of Structured Information Standards) specifications and widespread security technologies, such as WSS4J (Web Services Security for Java), PKI (Public Key Infrastructure), X.509 certificates and XACML (eXtensible Access Control Markup Language).
Components of the designed security framework have been developed: PDP (Policy Decision Point), PAP (Policy Administration Point) and PEP (Policy Enforcement Point). A demonstration and validation mock-up scenario has been deployed, integrating the security framework components with the Discovery Service prototype developed within the scope of WP2 (see figure above).

For the validation of the mock-up scenario some access control policies have been defined using XACML, demonstrating its flexibility to define fine-grained access control policies in order to fit challenging requirements needed in complex scenarios.
Having obtained the expected results and having demonstrated the feasibility of the proposed solutions in terms of security aspects, the BRIDGE project is actively helping product and service vendors build trust with final users and hence increase the level of adoption of EPCglobal standards in supply chains.
Along with the access control components for the BRIDGE Discovery Service we have also looked wider at the issues of Discovery Service security, for example, analysing the advantages of different Discovery Service communication models, and considering the problems of service ownership and peering. Through this work we have supported the EPCglobal JRG on Data Discovery to develop realistic requirements, including those for security.

4.1.3 Roadmap

Although, for demonstration and validation purposes the security framework has been integrated with the Discovery Service prototype, it is equally suitable to be integrated with the other networked services present in the EPCglobal network, such us EPCIS or ONS.
However, other security considerations are unique to the Discovery Service since data is hosted by a third party and managed remotely. We have shown that XACML is capable of expressing such delegated rights, yet the scalability for fine-grained policies remains questionable. The Discovery Service also has key security considerations coming from the desire to be able to peer trusted Discovery Services together to form a wider network, yet still be able to control the release of business information. This area will form one of the most challenging areas for Discovery Service research in the next few years.
Taking into account the potential complexity of real supply chain scenarios, it could be interesting to research tools to help final users in the definition and management of complex fine-grained policies using XACML. One method would be the tighter integration of the EPCIS and Discovery Services and the automated exporting of both data and policies to the Discovery Service based on business processes.
Security features have focused on external aspects such as communication interfaces and how to authorize the access - this means that internal aspects as how to protect stored information in Discovery Services or EPCIS have not been taken into account, so these are potential future areas to be considered.
From the business point of view, different models to exploit commercially Discovery Services should be defined and analyzed.

4.1.4 Related publications

- Academic publications
    - Trevor Burbridge, Mark Harrison, “Security Considerations in the Design and Peering of RFID Discovery Services”, IEEE RFID 2009, Orlando. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4911171&isnumber=4911159
    - J.J. Cantero, M.A. Guijarro, G. Arrebola, E. Garcia, J. Baños, M. Harrison, T. Kelepouris, “Traceability applications based on discovery services”, Emerging Technologies and Factory Automation (ETFA) 2008. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4638572&isnumber=4638343
- BRIDGE deliverables
    - D4.5.1, “RFID Network Confidentiality”
    - D4.5.2, “Final Report on Network Confidentiality”

  - D2.1, “Serial Level Lookup Requirements”
  - D2.2, “Working Prototype of Serial-Level Lookup Service”
  - D2.4, “High Level Design for Discovery Services”
- Other sources where to find more information
  - EPCglobal JRG on Data Discovery (membership and opt-in required)

4.2 Access Control Framework for EPCIS Data Exchange Services

4.2.1 Relevance for Consumers, Solution-Providers and Users

In RFID supply chains information will be collected by many parties within the supply chain as they observe and handle the tagged products or assets. Some of this information will be used internally within the site or company that made the observation, but the full value of the information can only be realised if it can be shared amongst other partners to improve the end-to-end supply chain. Such full supply chain information is also required to analyse the pedigree of a product (e.g. fresh meat), monitor diversion (e.g. pharmaceuticals) and prevent counterfeit products from being introduced (e.g. branded goods). Unfortunately full supply chain information will only be shared by each partner if they can be assured that their confidential business operations are protected.

4.2.2 Result description

Since different goods will be received from, and shipped to, different partners coarse-grained access control based solely on identity is not sufficient. A customer of one item should not be able to see information about similar items shipped to their competitors.

In BRIDGE we have examined the applicability of fine-grained access control policies, written in industry standard languages such as XACML, to the protection of RFID data. We have shown that a wide range of policies can be supported, including the delegation of access rights to share data with onward parties and emergency policies for events such as product recalls. These policies can protect the information services such as an EPCIS repository, and can also protect shared services such as the Discovery Service or shared supply chain analytic services.

We have also studied how businesses might define confidential information, and how these concepts can be mapped to the dynamic access control of the underlying RFID data.

4.2.3 Roadmap

Although we have shown that fine-grained access control is feasible given today's security technology, the next steps for the industry should be to work in three directions:

- Firstly each industry sharing RFID data needs to consider when it is willing to share their data. This will lead towards a set of common security assertions that all players can then use in their access control policies. Business roles can then be created to issue and federate such assertions. Such assertions will include identity, but are also likely to include other supply chain events such as product recalls, custodianship (or holding) of the product, owner of the product etc.
- Secondly the industry needs to adopt the technology into their products and services and look towards improving performance. This is likely to include restricting the flexibility of the policy language (for example in terms of the attributes that can be used or the flexibility of delegation rules).
- Thirdly the industry needs to take steps to automate or assist the generation and distribution of access control policies. It is not feasible for a supply chain manager to

create policies for every product they handle. Solving this challenge will require intuitive user interfaces and high-level business meaningful languages, but will also require interfacing with existing supply chains systems (such as the receiving and shipping systems).

4.2.4 Related publications

- Academic publications
    - Trevor Burbridge, Mark Harrison, “Security Considerations in the Design and Peering of RFID Discovery Services”, IEEE RFID 2009, Orlando. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4911171&isnumber=4911159
- BRIDGE deliverables
    - D4.5.1, “RFID Network Confidentiality”
    - D4.5.2, “Final Report on Network Confidentiality”
- Other sources where to find more information
    - EPCglobal JRG on Data Discovery (membership and opt-in required)

5 Application Software

This section provides details on the BRIDGE WP4 results in the application software layer. For each result, a description of the achieved results and details on next steps and research opportunities are given.

5.1 Tool for Rule-Based Analysis and Visualization of EPCIS Events

5.1.1 Relevance for Consumers, Solution-Providers and Users

The EPCIS specification allows for sharing item-level event data between business partners in a standardized way. The Supply Chain Visualizer is a tool for detecting inconsistencies, security risks and inefficiencies in EPCIS data. It allows non-technical users to quickly identify problem areas in complex RFID data sets.

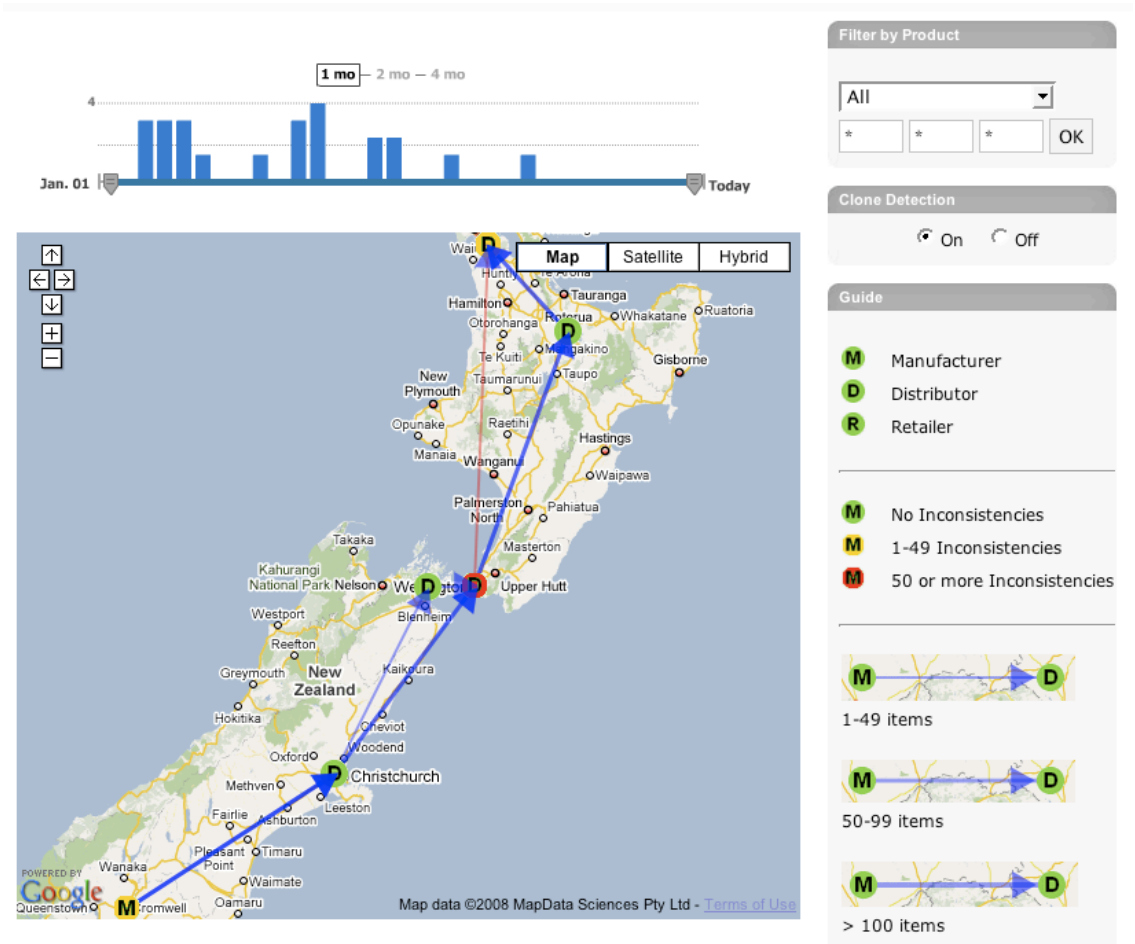

Figure 6. Screenshot of the user interface of the Supply Chain Visualizer

5.1.2 Result description

In order to deal with the overwhelming number of single events that are generated during operations, we propose a mix of automated analysis techniques and human effort. The Supply Chain Visualizer combines the concept of geographical visualizations with rule-based analysis techniques of the specific problem domain of standardized EPCIS data. Our tests with various data sets showed that an analysis based on generic consistency rules can deliver useful insights that would otherwise remain undetected. By utilizing the semantics of EPCIS data and through selective aggregation, problematic areas in a supply chain are visualized as ‘hot spots’ to help users in locating sources of potential problems. We support

the user in exploring the data by offering various time and categorical filtering capabilities combined with useful performance metrics and activity indices.

5.1.3 Roadmap

The Supply Chain Visualizer is currently only implemented as a demonstrator. For a potential use in practice, the application has to be further optimized for speed and integrated with other enterprise systems. There is significant potential for extending the existing business intelligence rules implemented in our demonstrator.
Discussions with several end-user companies showed that there is a need for industry specific rule sets and best practices. In a next step, we want to further explore this area and extend our research data analysis and business intelligence applications based on the EPCIS standard.

5.1.4 Related publications

- Academic publications
    - *Increasing Supply Chain Visibility with Rule-Based RFID Data Analysis*, A. Ilic, T. Andersen, F. Michahelles. *IEEE Internet Computing*, vol. 13, no. 1, pp. 31-38, Jan./Feb. 2009, doi:10.1109/MIC.2009.10
    - *EPCIS-based Supply Chain Visualization Tool*, A. Ilic, T. Andersen, F. Michahelles, Auto-ID Labs White Paper, 2009
    - *Analyzing Product Flows with the Supply Chain Visualizer*, A. Ilic, T. Andersen, F. Michahelles, E. Fleisch, Demo at Internet of Things Conference 2008, Zurich, Switzerland, 2008
- BRIDGE deliverables
    - *Supply Chain Integrity*, J. Farr, M. Harrison, A. Ilic, O. Kasten, A. Soppera, D. Zanetti, BRIDGE Deliverable D-4.6.1, 2007, http://www.bridge-project.eu/data/File/BRIDGE_WP04_Supply_Chain_Integrity.pdf
    - *Supply Chain Integrity Model & Prototype*, M. Harrison, A. Ilic, O. Kasten, A. Soppera, BRIDGE Deliverable D-4.6.2, 2009, forthcoming

5.2 *RFID Track-and-Trace Based Integrity Checking and Alerting Tool*

5.2.1 Relevance for Consumers, Solution-Providers and Users

Counterfeiting and product piracy constitute a serious and ever growing problem against legally run businesses and owners of intellectual property rights. Counterfeiting is not specific to any industry but it affects a large number of sectors such as the music, software, and luxury goods industries, and also pharmaceutical industry, automobile industry, fast moving consumer goods industry, and toys. According to the International Chamber of Commerce, "[c]ounterfeiting and piracy are growing exponentially in terms of volume, sophistication, range of goods, and countries affected - this has significant negative economic and social impact for governments, consumers and businesses [...]."
The potential of RFID and the EPCglobal network in enabling novel anti-counterfeiting and anti-fraud techniques is well recognized. Even though it seems that there will not be one silver bullet solution against illicit trade, industries and academia see mass-serialization among the most promising single countermeasures. There are two major reasons for using EPC network technology in anti-counterfeiting: First, RFID allows for new, automated and secure ways to efficiently authenticate physical items. Second, as many companies invest in networked RFID technology for various supply chain applications, the item-level data will be gathered in any case – so why not using it to detect counterfeit products?

5.2.2 Result description

With the rule-based anti-counterfeiting approach (see Figure 7), companies can specify conditions that indicate evidence of counterfeits in the supply chain. The conditions are specified in the form of business rules over track-and-trace data, which is retrieved through the existing EPC infrastructure.

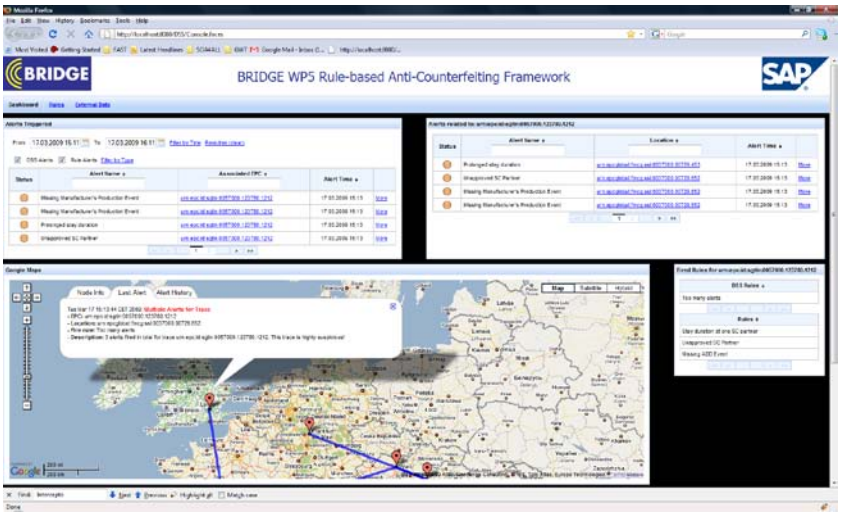

Figure 7. Rule-Based Anti-Counterfeiting Framework

Rules can take industry- as well as company-specific business information into account (e.g., by the means of interfaces to existing ERP systems). They are implemented using a declarative programming style, based on first order logic. Besides industry-independent rules, such as checking whether the genuine right owner issued the production event in its EPCIS system, industry- and company-specific rules can be specified. Companies' anti-counterfeiters are assisted by a decision support system (DSS), because only certain combinations of alerts should trigger anti-counterfeiting measures. Customs authorities, once equipped with RFID/EPC-readers (mobile or fixed) and gaining access to anti-counterfeiting rule-sets – both company-specific and company-independent – can leverage their checking activities while scanning products on item, case- and pallet-level, thus making automated mass checks at borders possible.

5.2.3 Roadmap

The rule-based anti-counterfeiting framework can be used with standard, low-cost UHF-tags. With this approach in place, tagged products can be authenticated throughout the whole supply chain, helping to pinpoint counterfeiter's injection points and thus making it possible to early detect counterfeits in licit supply chains, in order to deter their further propagation. From an evaluation point of view, the rule-based anti-counterfeiting framework proved to be a scalable and fast approach able to support customs organization and affected companies to enable mass authentication and to give counterfeit indications, therefore supporting anti-counterfeiters and especially customs organization to "find the needle in the haystack". However, the approach depends on anti-counterfeiting rules, created and maintained by the company/industry. But according to findings from the industry interviews, this is also where it strengths lies, since the rules can be defined to fit the company's or industry's requirements. Besides the anti-counterfeiting rules, further rules that are build on the integrity checking RFID and track-and-trace infrastructure, such as the support the management of returns (e.g., recalls), or the detection of shrinkage activities, for example, can be easily added in the framework.

5.2.4 Related publications

- Academic publications
    - Al-Kassab, J., Condea, Delchev, I., C., Gaeth, M., Huelss, H., Kasten, O.: *"Runtime-configurable Analysis of Supply-Chain Integrity Based on Product*

Traces", Industry Demonstration at the Internet of Things Conference 2008, 26th-27th of March 2008, Zurich, Switzerland.

- BRIDGE deliverables
    - *Supply Chain Integrity*, J. Farr, M. Harrison, A. Ilic, O. Kasten, A. Soppera, D. Zanetti, BRIDGE Deliverable D-4.6.1, 2007, http://www.bridge-project.eu/data/File/BRIDGE_WP04_Supply_Chain_Integrity.pdf
    - *Supply Chain Integrity Model & Prototype*, M. Harrison, A. Ilic, O. Kasten, A. Soppera, BRIDGE Deliverable D-4.6.2, 2009, forthcoming
    - BRIDGE D5.4 Prototype Report
    - BRIDGE D5.5 Evaluation Report
    - BRIDGE D5.6 Application Guideline and Implementation Roadmap Report

6 Conclusion and Outlook

The area of RFID security is a challenging research topic and a crucial aspect in fostering the adoption of the EPCglobal network. This goal of this document was to make the public aware of the most important results of BRIDGE WP4. We have provided a description how these results can extend the security of the EPCglobal network and in what maturity stage the results are.

Throughout all our work, we have used existing standards and open specifications. We identified several cases, in which existing standards can be extended to make advanced security features a commodity for every user. We are currently actively engaged in several activities where we support standardization initiatives with our inputs and learnings.

A technology roadmap has been proposed to highlight starting points for further advancing the results towards standards or mainstream products. We would like to encourage the RFID community to join us in taking this into the next level. As a starting point, we have made available several references providing detailed descriptions of our work in form of research papers, public deliverables and online demonstration tools.