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

Using the Trusted Reader for product Authentication

Authors: Trevor Burbridge (BT Research), Andrea Soppera (BT Research), Jeff Farr (BT Research), Mikko Lehtonen (ETH Zürich), Alexander Ilic (ETH Zurich)

October 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 report describes how the use our Trusted RFID Reader can enhance the various processes associated with RFID-based Product Authentication. It is a companion to the report D4.2.2A which describes the hardware specification of a near product implementation of the reader, and which forms the second part of the project deliverable itself. 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.

Disclaimer:

Executive Summary

This report describes how the use our Trusted RFID Reader can enhance the various processes associated with RFID-based Product Authentication. It is a companion to the report D4.2.2A which describes the hardware specification of a near product implementation of the reader, and which forms the second part of the project deliverable itself. 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.

Whilst the trusted reader has been designed as a general purpose, secure RFID reading component, this report focuses on how it should be configured in order to enhance the performance, or widen the applicability of the full range of Product Authentication schemes explored in WP's 4 (Security) and 5 (Anti-counterfeiting) within BRIDGE. In some usage contexts, described in the report, the enhancements provided by trusted reading will be so significant as to be the determining factor in whether an authentication scheme will effectively 'work'.

The report begins with a reminder of the problems of counterfeiting and grey-market distribution, and the need for various parties to be able to authenticate that a particular item is indeed genuine (or has followed an authorised distribution route). A second background section then reviews the purpose and general design of the trusted reader itself.

The main part of the report is divided into two sections: the first covering the general advantages to authentication provided by a trusted reader, and the second covering the specific advantages and configurations necessary for each particular authentication scheme. General advantages include the facts that:

- a trusted reader cannot be surreptitiously 'swapped' for another, illegitimate or maliciously-acting, reader
- a trusted reader cannot have its processing surreptitiously modified. Apart from crudely interfering in the physical-level reading process itself (for example blocking or overwhelming the reading process itself) – the integrity of the reading process itself is generally assured.
- a trusted reader can be trusted to hold confidential information (including powerful security keys) that allow local processing of authentication algorithms.
- multiple different parties can simultaneously, but independently use capabilities of the trusted reader to support their own (different) authentication schemes. This flexibility and independence is crucial in enabling a single reader to act effectively on behalf of many (even competing) supply chain routes.
- strong security of the data transmitted to and from the reader itself to the back-end RFID information network is assured, due to the fact that all transmissions can be encrypted in order to preserve data integrity, and prevent eavesdropping.

Aside from the security benefits, other system benefits may accrue from using a trusted reader. In particular, the facilitation of local (trusted) processing on the reader permits alternative authentication protocol exchanges that can create greater scalability and lower network usage.

Specific advantages come from using the trusted reader in a particular authentication scheme (though bear in mind that, as stated, the trusted reader might be used to support several such schemes simultaneously). The schemes investigated include those already promoted within the industry, as well as more innovative solutions developed during the lifetime of BRIDGE, and within the project itself. Depending upon the capabilities of the RFID tag itself, differing authentication schemes are possible: basic tags can be authenticated using user memory allocation and/or standardised TagID or TID numbers; cryptographic tags can be directly, strongly authenticated; and all types of tag can have their distribution route verified by analysing their trace history. The report shows how each of these processes, and their variants, are enhanced through the application of the Trusted Reader.

In summary, trusted computing technology has proven to be both technically and commercially viable to the domain of RFID reading. The advantages of this technology now need to be widely publicised to the RFID community in order to stimulate the actual market for such products, and trusted computing based solutions.

Contents

1 Introduction

In this document we look at how the concept of a Trusted Reader, as outlined in our earlier deliverable D4.4.1 can be used to support and enhance the authentication of products within a supply chain.

The subject of product authentication (without using secure tag support) has been studied within WP5: Product Authentication of the BRIDGE project. Within D5.4 four approaches are outlined using data both on and off the tag to perform authentication of goods. These approaches are:

1. Transponder TID numbers
2. Synchronised Secrets
3. Rules-Based
4. Statistical Analysis

In this document both Rules-based and Statistical Analysis are discussed within a single section on “Track and Trace Data” analysis since both of these schemes gain the same benefits from the use of the Trusted Reader.

In addition to the schemes described by WP5, we also examine product authentication using the secure tag capabilities developed within WP4: Security. We look at two cases, one in which the identifier of the tag is transmitted freely, and another where a pseudonym scheme is used to protect the confidentiality of the tag ID:

5. Symmetric cryptography (with public identifier)
6. Pseudonym schemes

In this document we examine whether the concept of a trusted reader may support the operation of these schemes. Benefits may come from: the increased scalability of the system by reducing load of central components; reduced costs through minimising network traffic; increased security through the participation of the RFID reader.

Furthermore we also present a final additional scheme designed specifically for the Trusted Reader. In this scheme the tags are signed to produce a step-by-step validation of the supply chain path:

7. Signature Re-signing

All of these schemes are presented in greater detail within the following sections of this document.

2 The Problem of Counterfeit Goods

In the modern global marketplace there is an ever increasing threat that physical products are not what they claim they are. Technology, infrastructure, and know-how to manufacture and package even sophisticated products are widespread over the globe. Furthermore, intellectual property (IP) such as brands, trademarks, and patents account for an increasing share of the value of physical products. As a result, product counterfeiting, i.e. illegal copying of products, has become a relatively easy but profitable practice. Against this background, it is not surprising that the world has witnessed a boom in product counterfeiting and piracy during the last twenty years. Moreover, if the economic and social conditions remain favourable for the counterfeiters, it is unlikely that the problem will diminish by itself.

Product counterfeiting is a threat against legally run businesses, governments, and unsuspicious consumers. Since almost twenty years already, counterfeiting is not anymore specific only to luxury goods industry but affects manufacturers of practically all kinds of branded products [Bush et al. 1989]. Counterfeit products substitute genuine products leading to losses of sales for the brand owners [Staake 2007]. Counterfeit luxury goods decrease the associated exclusiveness of the high-end brands. Counterfeit articles which have inferior quality decrease the perceived quality of the genuine products. Furthermore, public incidents about counterfeiting of health, safety, and security related products have the potential to hamper the sales of the affected brands.

Perhaps the most serious cases of product counterfeiting are those where a consumer unknowingly and unwillingly consumes a counterfeit product that exposes him to an unperceived health, safety, or security risk. This can be the case with, for instance, counterfeit medicines and counterfeit car spare parts. Moreover, unknowing consumption of counterfeit products often happens when the counterfeit products are injected into the distribution channel of the genuine products. Even though the vast majority of counterfeit products never enter the distribution channel of the genuine products, those that do can have serious consequences. No statistics are available of the actual number of such cases, but example cases are enough to proof that the problem exists. For example, in a recently published case counterfeit perfume bottles entered into the supply chain of the Swiss retailer Migros, all the way to the sales floor, without being recognized during several months[1].

This deliverable presents how the trusted reader platform can strengthen RFID-based countermeasures that enable product authentication and protect the supply chain networks of the genuine products. Product authentication answers whether a product is genuine or not. These techniques are employed to keep the licit supply chain clean from counterfeits but also to detect counterfeit products outside the supply chain through inspections. For more a detailed problem analysis of product counterfeiting, refer to deliverable D5.1 of the BRIDGE project [Lehtonen et al. 2007].

[1] http://www.migrosmagazin.ch/index.cfm?id=17144

3 The Trusted Reader

The Purpose of the Trusted Reader

The trusted reader itself has been designed to ensure that that reading and reporting of RFID tags is performed in a highly trustworthy manner. For example, a *trusted* reader can be configured to ensure that the reader will only read and report certain, agreed types of tags (for example, those associated with unsold products manufactured by Sony). Or, the trusted reader can be configured to ensure that the tag data actually read is not manipulated in any way before being sent to a data repository[2] (for example, the time stamp of an event cannot be altered in order to make it appear that the item was observed at other times).

In this way, a trusted reader can be seen to greatly enhance the confidentiality (consumer privacy, and commercial confidentiality) and data integrity offered at the key interface between the physical world (as represented by the tags themselves) and the information model (as held within the back-end EPCglobal network).

But our design of a trusted reader goes beyond these basic functions. Ours is designed for a 'open' environment in which many different types of tags, owned and managed by possibly competing parties, use the same reader to independently and securely manage their own needs. In a super-market, for example, a single reader might be used to scan items from a competing set of product suppliers. Each product supplier needs to be confident in the accuracy (integrity) and confidentiality afforded to the data associated with its products. It wishes to be assured that its data is not shared with its competitors, and that the super-market (who actually owns and operates the trusted reader) does not discriminate against them by maliciously, or inadvertently manipulating the read data.

As well as the different product suppliers (who each need to trust the operations of the reader), the super-market itself may wish to apply its own policies to the reader. In order to protect its customers' privacy, for example, it may wish to ensure that the reader is unable to read tags on items already purchased (at that, or possibly other shops) by the customer. Importantly, rather than customers blindly trusting the super-market to apply such a policy, the trusted reader allows such policies to be independently and remotely verified by third parties.

[In our terminology, used later, all the parties who need to independently configured and trust the operation of the reader are called 'Service Users'. The trusted reader provides a shared, common reading 'service' that can be configured and trusted by different users].

As previously stated, the goal of this report is to show how trusted readers can helpfully support a range of different authentication schemes. It is crucial to appreciate the ability of our trusted reader to *simultaneously but independently* support a range of different authentication schemes. In the super-market scenario, for example, an electronics manufacturer might want to use the reader to check the authenticity of their TVs using a secure tag scheme[3]. Simultaneously, a pharmaceutical company might wish to use the reader to authenticate their pharmaceutical products using a combination of TagID[4] and rule-based[5] schemes.

[2] In EPCglobal terms, an EPCIS or EPC Information Service repository

[3] Scheme #5 above, and detailed in Section 8

[4] Scheme #1 above, and detailed in Section 5

[5] Scheme #3 above, and detailed in Section 7

The trusted reader we have designed has the potential to support all such requirements simultaneously, and for such requirements to be dynamically and remotely altered. In this way it provides a highly flexible and secure reading infrastructure.

Trusted Reader Design

The section provides a very brief overview of the design of our trusted reader, and describes in general terms how it needs to be configured[6]. In the design, the two key aspects of the reader, trustworthiness and flexibility, are supported by Trusted Computing and OSGi technologies respectively (Figure 1).

In use, we need to distinguish between two primary types (*roles*) of user. The owner of the trusted reader will usually be its *Operator*, who will act as its administrator in terms of configuring its use by other *Service Users*. In the previous super-market scenario, the super-market operator themselves would play the role of the Operator, and the electronic and pharmaceutical manufacturers along with the super-market themselves would be configured as Service Users.

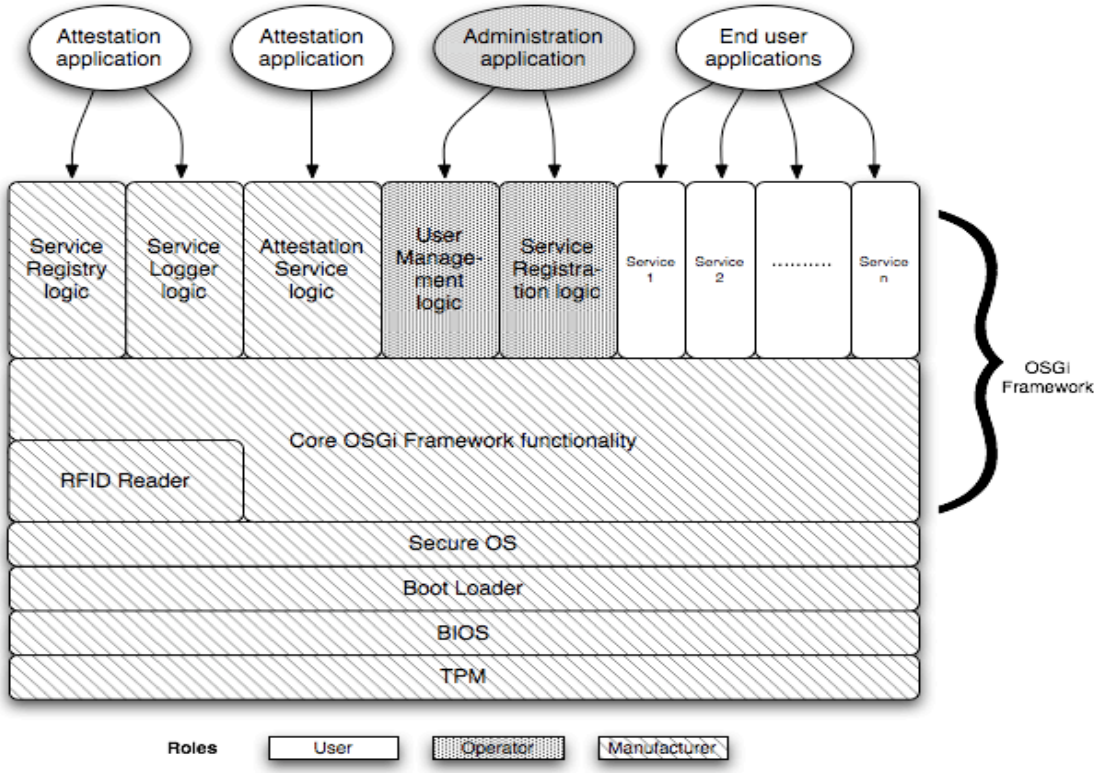

Figure 1. The Architecture of the Trusted Reader

The role of the Operator is principally to manage the access rights to different software bundles and attestation services for each of its Service Users. The Operator may also provide some basic services that they expect, or require, all Service Users to use. In our super-market example, this could be a service module that *filters* all the

RFID tags the reader reads to ensure that all previously-sold items cannot be read by the reader [and hence, in a fundamental way, the Service Users are prevented from writing any code that could circumvent this process and inappropriately snoop on others' tags].

[6] A much more thorough description of the design is given in a previous Deliverable, D4.4.1 'Design of a Trusted Reader', February 2008.

The Operator will thus use a management application, provided by the manufacturer as part of the trusted reader itself, to configure and install service bundles on behalf of all its Service Users, and it is these 'end user applications', labelled 'Service 1', 'Service 2',…'Service n', that will actually contain the Service User -specific processing required – which in the case of this report is primarily the logic to the range of different authentication schemes.

[In fact, the service bundles are sufficiently flexible and re-usable that several different Service Users, who might wish to use the same basic authentication scheme, might be able to use (share) the same authentication scheme code whilst still having separate Service instances to handle the encryption and sending of the data to their remote repositories and using their own authentication secrets or rules].

4 General Authentication Advantages of the Trusted Reader

For any of the approaches detailed below, the use of a Trusted Reader in the authentication process provides a number of general advantages.

Identity – Prevention of Reader Spoofing

Many authentication schemes may be defeated by an attacker pretending to be a legitimate reader. By spoofing a reader an attacker may, for example, inject RFID events into the network to pass supply chain analysis checks (such as checking of a manufacturing record). Alternatively a spoofed reader may participate in an authentication challenge, and thereby subvert the challenge process.

The use of a Trusted Reader prevents the spoofing of a Reader by using the identity provided by the TPM. This utilises a unique key that is stored securely within the TPM and never released. This key is used to sign (within the TPM) authentication exchanges between the reader and other systems. Such systems can use the public key provided by a Trusted Certificate Authority such as the TPM or reader manufacturer to ensure that they are communicating with the correct reader/TPM.

Software attacks on the reader cannot yield the unique key which is held securely within the TPM hardware. Physical attacks would have to go to the extreme lengths of removing and scanning the TPM chip to obtain the key.

An attacker may consider physically stealing the entire TPM reader. However, this will avail the attacker little since the identity of the stolen reader may be simply blacklisted so that no supply chain information is accepted from it.

Secure Communications – Prevention of Eavesdropping and Data Manipulation

The unique TPM key used to authenticate the Trusted Reader can also be used to secure the communication channel (or individual messages) between the reader and the authentication system. This can prevent other parties accessing the communications channel, either for the purposes of eavesdropping, or for the purposes of altering or adding additional data.

The securing of the communications channel prevents an attacker of an authentication system from performing several activities:

- The attacker is prevented from learning supply chain operations (and thus calculating where counterfeit goods may be introduced)
- The attacker is prevented from learning any secrets that are used in the authentication process (and thus being able to pass authentication checks for counterfeit goods)
- The attacker is prevented from adding additional RFID sightings (to subvert a supply chain analysis authentication scheme)
- The attacker is prevented from changing the information in the reader response to any authentication challenge (in order to pass a challenge for a counterfeit good)
- The attacker is prevented from signalling that a tag is authentic when the authentication process has not been fulfilled
- The attacker is preventing from understanding and thus performing targeting interception of any alarms raised by the authentication process (from or to the reader). Such interception may still be possible by analysing the timing and size of the secure communications.

Although similar benefits may be achieved by using public key cryptography with a private key stored in persistent memory on the reader, this key may be vulnerable to attacker since it will not be secured within the TPM hardware. Either physical attacks on the reader to dump the memory contents or unauthorised access to the reader system through the communications network (e.g. through the spread of trojans) may be used to access such secrets.

Integrity Checking – Prevention of Reader Corruption

The use of the TPM provides both detection of reader corruption, and the limitation of the damage that may be caused by such intrusion.

The TPM capabilities of the trusted Reader can be used to check the integrity of each layer of the reader (BIOS, boot-loader, operating system, service layer, application) on booting of the reader. Any alteration to these components may either halt the reader start-up procedure, or log the change that has occurred. A remote operator may also request that an integrity check of the current known state of the Trusted Reader is performed. In this case a fingerprint of each of the trusted reader components is signed using the unique TPM key. These fingerprints may then be compared with the expected versions of these components. The use of the secure operating system ensures that as long as the operating system has not been subverted (tested by checking the fingerprints of the BIOS, boot-loader and operating system kernel), then we can have confidence that no unauthorised applications are executing, and no unauthorised access to the storage has been made. This is the case since the security extensions to the operating system kernel allow us to enforce control of which applications are allowed to run and which can access specific storage areas or files. For our design of the Trusted Reader only the service framework is allowed to execute, and this in turn has security features that control which services are installed and instantiated (executed) within the framework.

These features minimise the routes through which an attacker can attempt to gain entry to the Trusted Reader (since only a very restricted range of trusted components are allowed to execute). Once access is gained by an attacker, any attempt to run alternate versions of software components will be blocked. Similarly any attempt to change configuration files and other data will also be blocked.

Secure Storage – Prevention of Access to Confidential or Secret Information on the Reader

After gaining entry to the reader and attacker may also attempt to gain secrets or confidential information that are stored on, or pass through, the reader. Gaining access to the flows of information through the reader should be prevented by blocking any application capable of doing so from executing. In extreme cases only restricted versions of the operating system shell will be allowed to execute. Files containing secret or confidential information may be secured using the secure storage features of the TPM. This enables individual applications to encrypt their files with keys which are held within the secure hardware registers of the TPM. The application can only gain access to such keys (and hence access to their information) after passing an integrity check. Thus an attacker cannot access such files either by replacing legitimate applications or executing other applications. In either case the application may be blocked from executing, and will fail to gain the secure storage keys from the TPM.

Secure Multi-Party Services – Managing Operator and Service Concerns

Our design of the Trusted Reader provides clear separation of the Reader Operator and multiple Service User roles. This allows the operator to install approved local authentication services on the reader which can be instantiated by permitted users.

The advantage of this is that the Trusted Reader can be used to manage contention between the operator and the authentication service user. For example, a local authentication service may be used to authenticate a set of RFID operations, but only report back to the authentication service user when goods fail the authentication process. In this manner the reader operator may protect the confidentiality of their RFID operations from the authentication service user, while the user may be ensured that the authentication service will operate as expected and report any counterfeit goods that are observed.

5 Authentication Using Transponder ID (TID) numbers

5.1.1 Technical background to TID numbers

ISO/IEC 15963 [ISO 2004] describes the use of an allocation class identifier, and this is used within the EPCglobal Class-1 Gen-2 standards [EPC] to indicate two structures for the Transponder ID (TID) memory bank. In the first option the TID is primarily used as a tag class identifier to indicate class functionality to the reader and the TID number is not serialized (Figure 2). For example the TID may be used to identify a class of tags that has a specific user memory capacity, or that implements a temperature sensor function. This has limited use to protect against product counterfeiting since the attacker has only to obtain a blank tag of the same class and write the Electronic Product Code (EPC) to make it indistinguishable from the original.

TID MEM BANK BIT ADDRESS	BIT ADDRESS (In Hex)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
10_h-$1F_h$	TAG MDID (last 4-bits)				TAG MODEL NUMBER (12-bits)											
00_h-$0F_h$	11100010_2=$E2_h$								TAG MDID (first 8-bits)							

Figure 2: TID memory structure in the current EPC standards [5] (non-serialized TID)

The second TID structure allows the tag fabricator to install a unique serialised identifier. Although each tag is uniquely identified using this variant, it becomes harder for the reader to identify and use tag class capabilities since it must index the unique tag identifier against an external database to obtain the tag class. The forthcoming EPC Tag Data Standard is likely to combine both approaches to provide the ability to store a serialised tag identifier along with direct class information. For more detailed technical background to TID numbers, refer to D5.4 of the BRIDGE project [Al-Kassab et al. 2008].

The assumption used widely by the industry is that by having a unique TID on every tag it becomes harder for an attacker to clone a tag. In order to produce a physical clone of a tag with a unique TID number, an attacker must be capable of instructing the fabrication of new tags with similar tag identifiers to those they are trying to clone, or alternatively (and more usefully) obtain tags that allow the TID to be written after the tag fabrication process. Although we do not know of any tags available today that allow the TID to be written, it should be strongly noted that the standards allow for such tags (for the purposes of recommissioning),and even were the standards to be changed, there is a strong possibility of black-market tags emerging with writable TIDs. Thus, there are no guarantees that any authentication scheme relying on TID will remain secure, even in the very short term [Lehtonen et al. 2009].

Furthermore, cloning a tag is only a matter of building a system that simulates those particular signals produced by the authentic tag. There is no need to know or copy the internal structure of the tag - the only important factor is to be able to replicate the TID. Thus other mobile devices may be programmed to simulate an RFID tag, and present the same TID.

This report simply acknowledges that TIDs are used for current authentication processes and explains how such a process can be enhanced by the Trusted Reader.

Authentication is performed by simply reading both the EPC and the serialised TID from the product tag. The reader passes both identifiers to the back-end system which then checks that the TID corresponds to the EPC. If this check fails then the tag is assumed to be cloned. A detailed analysis of the vulnerabilities and level of security of the TID scheme will be a part of the D5.5[7] of the BRIDGE project.

Using a Trusted Reader for TID-based Authentication

The Trusted Reader can function as a normal reader, performing the tag inventory. Since the Trusted Reader provides an open service platform, any party wishing to operate an authentication service (including the reader operator) may install such an additional service. This local service can be

[7] D5.5 Evaluation Report (M36)

configured to automatically retrieve the TID from any tags within particular identifier ranges (for example all products within a particular product range, or within a particular batch of serial numbers).

The advantage of the Trusted Reader is that this further interrogation of the tags does not have to be performed by an additional back end system, removing any additional network delays or back-end bottlenecks. The local authentication service on the Trusted Reader can then transmit the product identifiers and corresponding TID numbers for authentication checking to a networked authentication service. This transmission can be performed over a secure channel using the secure identification capability of the Trusted Reader, removing the ability for an attacker to inject falsified tag readings with the correct TID directly to the network authentication service.

The network authentication service can also perform integrity checks upon the Trusted Reader to check that falsified product sightings are not being introduced by a compromised reader. Without such protection it is theoretically possible for an attacker to compromise an RFID reader so that any request to read a TID would result in the reader fetching the legitimate TID value in any case where only a class TID was retrieved from the tag.

To reduce the reliance on a network authentication service (and the delay of communicating with such a service) we can also imagine that the Trusted Reader could hold the database of legitimate TID numbers and perform the authentication locally. However in many applications the size of this database may mean that it is better to hold such details in local network storage. The Trusted Reader can still perform the authentication check after retrieving the TID numbers from the local network database. The advantage of performing this authentication check on the Trusted Reader is that a bespoke service can be operated in parallel for different users (such as different manufacturers). Each service can determine its own behaviour in event of counterfeit detection, such as contacting the manufacturer systems or raising a local reader operator alarm (which may be provided by the operator as a reusable service on the Trusted Reader).

Furthermore the reader operator and authentication service user gain some protection from each other by using the trusted capabilities of the reader. For example, the operator can be confident that the service will not transmit routine supply chain information to the product manufacturer unless a counterfeit is detected. The manufacturer can have confidence that their authentication checks are being performed even if they do not entirely trust either the competence or the motivation of the local operator to do so.

High Level Protocol

Reader to Tag Protocol	**Trusted Reader Protocol**	**Network Authentication Controller**
1. Inventory command from the reader 2. Tag transmits 96-bit EPC Identifier 3. TID reading command from the reader 4. Tag transmits the TID	1. Trusted Reader receives database of TID and Identifier number tuples to perform local authentication 2. Trusted reader perform local authentication by comparing the TID 3. In the event of counterfeit product a specific predefined action is taken	1. Check the integrity of the trusted platform through the TPM component. 2. In the event of a compromised the system administrator should be notified.

6 Authentication using Synchronised Secrets

The synchronised secrets [Al-Kassab et al. 2008, Ilic et al. 2008, Lehtonen et al. 2009] approach uses randomised trace codes written into the tag user memory each time the product is read at a participating supply chain node. These random codes are called *synchronized secrets*. When the tag is read at the next point in the supply chain, a network authentication system is used to check that the synchronised secret possessed by the tag is the one written by the upstream supply chain point. Figure 3 illustrates the protocol between the tag and the back-end system.

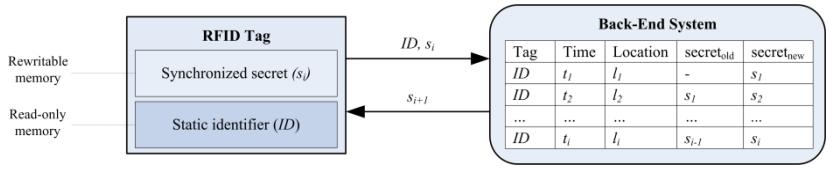

Figure 3: Illustration of the synchronized secrets protocol [Al-Kassab et al. 2008]

The system relies on the fact that an attacker attempting to introduce counterfeit goods will not have knowledge of the synchronised secret. This implies that the supply chain nodes writing and checking the secret are trusted not to introduce counterfeit goods or leak such secrets themselves. If they do so, the counterfeit good with a cloned tag will be detected as the tag is read multiple times with the same secret.

If access to the legitimate goods is available to the attacker then the synchronised secret should be held in access controlled tag memory. Similarly if the attacker can eavesdrop on the secret writing process then a cloned tag can be produced. Any communication to the back-end system should be secured, and if the back end performs the authentication check then the secret does not need to be released to the party performing authentication. The new secret can be generated and communicated between the writer and the back-end through a secure channel.

With the synchronised secrets scheme we must also consider attacks on the integrity of the authentication system. An attacker can attempt to de-synchronise the secrets between the back-end and the tag by disrupting the writing of the synchronised secret to the tag or the back-end system), or simply re-writing the secret once it is in the tag. To mitigate such attacks the tag can use access controlled memory for the storage of the secret, although this then introduces a problem of key management between legitimate supply chain readers wishing to perform authentication.

Authentication is performed by simply reading both the EPC and the synchronized secret from the tag memory. The reader passes both identifiers to the back-end system which then checks that the synchronized secret written on the tag corresponds to the one written on the back-end. If this check fails, an alarm is triggered. In the case that the synchronized secret in the tag is expired – i.e. it has been issued by the back-end before, but it is not the most recent one – then only the cloning attack is revealed, but it is not sure which of the physical products is the genuine one. The final verification can be done by physically inspecting the tagged product. A detailed analysis of the level of security of this scheme will be a part of the D5.5[8] of the BRIDGE project.

Using a Trusted Reader for Synchronised Secret Authentication

The Trusted Reader has an important role in securing the communication between the reader and the back-end system. Since the Trusted Reader identity and integrity can be checked before any secrets are disclosed, there is little opportunity for an attacker to impersonate a reader to obtain the secrets (request secrets for tags that are not actually read). Furthermore, the opportunity for attacks that de-synchronise or corrupt the secrets held in the central database and the tag are reduced. Since the communication channel between the reader and central system, along with the reader itself is protected from intrusion or disruption (except denial-of-service or physical attacks), then any de-synchronising attack must focus on disrupting or impersonating the reader-tag communication.

The trusted reader can help to support the confidentiality in the synchronised secret based authentication. In particular, this is not needed in the TID-based scheme where the security relies on

[8] D5.5 Evaluation Report (M36)

the fact that the TID cannot be programmed by an attacker. If the reading of the synchronised secret is protected (to stop leakage and cloning of the tag/product) or if the writing of the synchronised secret is protected (which is advisable to prevent vandalism of the synchronised secret), then the reader must know the password(s) to read and write the synchronised secret. These passwords may be released from the central system, along with the previous and new versions of the synchronised secret. Such release can be authenticated using the unique certified identity of the trusted reader and encrypted using a secure connection between the central system and the Trusted Reader.

Since the passwords and the synchronised secrets can be given to the authentication service instantiated in the Trusted Reader there is no need to trust the reader operator to use and store such secrets securely. Although the passwords and secrets may be obtained from eavesdropping on the reader-tag communication, such secrets may not be obtained from corrupting the reader operators systems or intercepts within the network.

High Level Protocol

Reader to Tag Protocol	**Trusted Reader Protocol**	**Network Authentication Controller**
1. Inventory command from the reader *2. Tag transmits EPC 96 bit Identifier* *3. 'Read tag memory command' to retrieve the 'Synchronized Secret'* *4. Tag transmits the 'Synchronised Secret'* *5. 'Write tag memory command' to rewrite the 'Synchronized Secret'*	*1. Trusted Reader receives from the controller the following information: EPC, Current Synchronised Secret and Future Synchronised secret* *2. Trusted reader perform local authentication by comparing the Current Synchronised Secret* 3. *If the comparison is 'TRUE' - Trusted reader writes in the tag user memory the Future Synchronised Secret* 4. *Trusted reader sends an acknowledgement of a successful update to the controller*	1. Check the integrity of the trusted platform through the TPM component. 2. In the event of a compromised the system administrator should be notified.

7 Detection of Counterfeit Products from Track and Trace Data

RFID technology enables supply chain visibility where the movement of every single product is tracked along the supply chain. The information about how a single product flows within the supply chain is called a trace record. The trace record provides unique information about the path that the product has followed in the chain.

This unique information could be used to measure supply chain performance such as estimate time of arrival and delivery, level of inventory in specific location. But a unique trace record can also be used to detect potential issues in the supply chain such as products not following appropriate paths a potential sign of grey market practices and duplication of paths a potential sign of a duplicate tag or counterfeited product.

The general approach behind detection of counterfeit products from track and trace data is to analyze supply chain trace records for different counterfeit indications [Al-Kassab et al. 2008]. In an EPC enabled supply chain this trace information would be distributed among the different EPC ISs and discovered by an appropriate discovery service. We can imagine having a shared supply chain authentication service that collects different traces among different EPC ISs and then with specific industry-knowledge is able to infer supply chain issues related to counterfeiting. As a good is received, the supply chain player that handles the receivables can query the authentication service. The authentication service will then confirm if the product has an authentic trace record. Alternatively, the authentication can also work completely automatically as a background process, triggered by new track and trace events, and only inform the stakeholders when an alarm is triggered.

Detection of cloned products from the track and trace data is straightforward if the current locations of the products are precisely known; for instance, if the track and trace data tells that the product is currently in Switzerland at the same time when a product with the same ID is scanned in Japan, the system can conclude that it is probable that the product in Japan has a cloned tag. However, when the track and trace data says that the product was observed in Switzerland one week ago but it does not tell its current location, authentication becomes harder and false alarms become possible. Deliverable D5.4 of WP5 [Al-Kassab et al. 2008] investigates different approaches to detect cloned tags from imperfect RFID traces.

Using the Trusted Reader for track and trace based checks

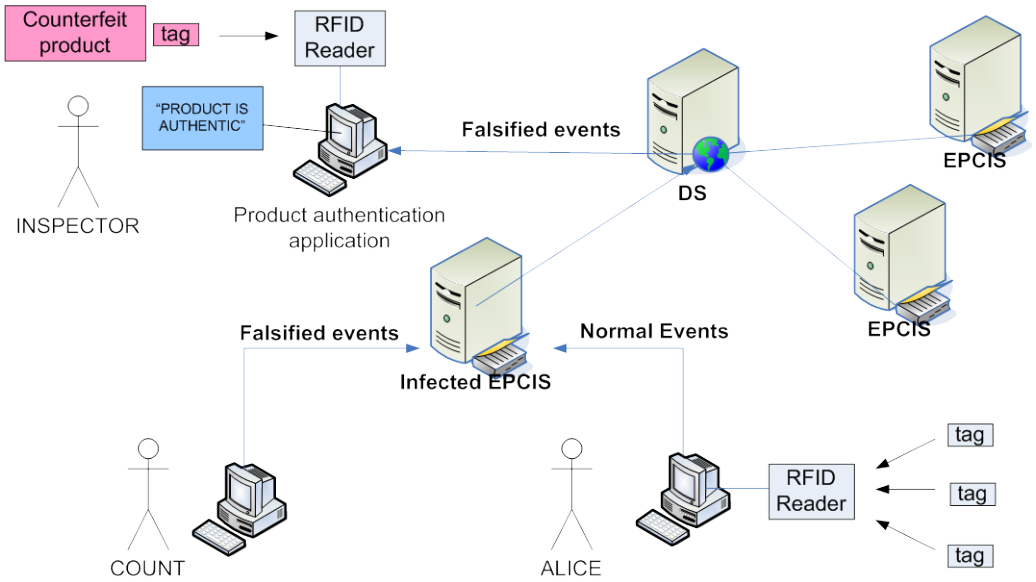

Figure 4. Without trusted reader platform, falsified events can be injected into an infected EPCIS, which can be used to fool the product authentication application

The Trusted Reader platform can secure the presented clone detection scheme by providing authenticity and integrity of the trace events. In theory, an adversary ("COUNT") could produce falsified events that fool the product authentication application and make a counterfeit product pass a check. For example, this could be achieved by forging the complete track and trace record from manufacturing until the point where the counterfeit product will be injected to the licit supply chain (Figure 4).

When Trusted Readers are employed, the event storage system and anti-counterfeiting system can trust that the events sent by the readers have really occurred. It means that the events are *authentic*. An adversary cannot manipulate the Trusted Reader to send tailored events. In addition, the Trusted Reader can guarantee that the *integrity* of events are not manipulated. This means, for example, that the time and location attributes of events are signed by the Trusted Reader. In addition, the readers can be configured so that only the manufacturer (or another restricted player) can write events with *action* = *ADD* (denoting that a genuine product with this ID number exists), or *bizLocation* = RP-MFG#xxx.

Furthermore there a number of advantages that are provided by the operation of *local* track & trace data checks on the Trusted Reader. Instead of operating all data analysis within a central location, checks can be distributed to local read points. Some of these checks may be performed at a single location (for example checking a blacklist). Other checks may need to be distributed to two or more locations with limited communications between the distribution points (for example checking that every product aggregated at one location is dis-aggregated at another). Finally pre-analysis at the Trusted Reader can provide confidentiality for the reader operator while still enabling central checks. As an example, Trusted Readers could provide encoded digests of the tags within aggregation or dis-aggregation events instead of the confidential data itself. This is matched by the protection of which analysis and/or rules checking are being performed from the reader operator. Such checks may be confidential since their leakage can provide material for potential attackers and reveal supply chain concerns

The multi-service platform allows easy configuration and verification of which supply chain events are available to which analysis services operated on the Trusted Reader. Finally the operation of local processes provides increased performance, higher resilience and lower communications costs.

High Level Protocol

Reader to Tag Protocol	Trusted Reader Protocol	Network Authentication Controller
1. *Inventory command from the reader* 2. *Tag transmits EPC 96 bit Identifier*	1. *Trusted Reader can be configured to write events with restricted attribute values (e.g. restricted business location or business step)* 2. *Trusted Reader performs pre-analysis to protect confidentiality and improve performance* 3. *Trusted Reader signs the events so that EPC IS can verify their integrity*	1. *Check the integrity of the trusted platform through the TPM component.* 2. *In the event of a compromised the system administrator should be notified.*

8 Authentication using Symmetric Cryptography

We have discussed the ways in which basic RFID tags can perform product authentication by offering enhance supply chain visibility and by using traces or TID embedded in the memory of the tags. As we have noted however the tag can be easily cloned and this could undermine the performance and the value of previous discussed solutions.

EPC Class 1 Gen 2 tags [EPC] have no explicit counterfeiting protection mechanism - an attacker can simply read the tag, and with a certain level of experience and capabilities, program the tag data into another tag or other wireless device which can simulate a tag. We have discussed mechanisms to protect user access memory with a pin or a password but these mechanisms are weak against potential eavesdropping. Furthermore the password distribution to multiple operators will present a substantial risk that the password will be leaked, which the use of the secure reader can only partially reduce.

In principle, a better mechanism towards eliminating the problem of tag cloning for product authentication can be found using symmetric-key cryptographic algorithms. A simple challenge-response protocol is implemented by sharing a key K between the tag and the authentication service. The tag identifies itself by sending its EPC identifier to the reader. The reader checks if the tag is a secure tag and it identifies which security protocol it supports. This operation can be performed by checking a remote database using the EPC or the TID.

Assuming that the reader has the key K and is trusted to perform the authentication, the reader will generate a random challenge N (nonce) and transmit it to the tag. The tag will compute an authentication message X= AES(K, N) and send it to the reader. The reader verifies that X is equal to AES(K, N). If the reader is not trusted to hold K, then a trusted authentication service may be employed to store K and compute the correct response for comparison by the reader. Furthermore, if the reader is not trusted to participate in the authentication process then the challenge production and response comparison may be performed by the trusted authentication service. The weakness of using a centralised trusted authentication service is that authentication cannot be performed in the service of unavailable sue to network or service failure. Another problem is the delays that are introduced into the authentication process. Although these problems are mitigated by distributing the keys to local operators, there is then a significant risk that such keys will be compromised.

With a symmetric key scheme we must also consider replay attacks. In this case an attacker has had a previous opportunity to observe challenge and response messages. Although the nonce N outlined above stops the replay of tag responses to legitimate challenges, an attacker who is able to control which challenge is produced will be able to produce the correct response. This is easily solved by using a second nonce produced by the tag itself. Encrypting this second nonce in the response ensures that subsequent tag responses will be different even for the same challenge.

We also need to consider man-in-the middle or relay attacks. In this case the attacker has control of an authentic RFID tag in a remote location. The attacker will listen to the challenge and forward the challenge to a remote reader that authenticates the tag following the normal protocol. A simple countermeasure for this kind of attack is a mechanism that controls the time permitted between when the challenge is transmitted by the reader and the answer is received.

Using a Trusted Reader for Symmetric Cryptography Authentication

The Trusted Reader can function as a normal reader and perform the tag inventory command, however, the reader also provides an open service platform to operate a local authentication service. In addition the service separation offered by the Trusted Reader allows multiple authentication services to be executed by different users (e.g. different manufacturers) to authenticate their own goods. The separation of secure services protects the secrets or supply chain operational data known by one authentication service from another.

The use of secure RFID tags without a Trusted Reader presents a problem. Tags that implement authentication require a secret to read the tag. Similarly, tags that implement access control also require such secrets. To prevent the leakage of secrets, the secret storage and authentication function must be performed by a secure back-end service. If the network or authentication system is unavailable then RFID tag will not be authenticated and a decision has to be made on whether to reject the goods. Depending upon the industry sector, either allowing counterfeit goods to enter the

supply chain, or alternatively holding genuine goods will be more costly. Such continuous network lookups are costly in terms of network and server provision. In addition, if the tag is held within the reader field while the authentication system produces a challenge and a response is obtained, then the maximum read rate of tags past the reader will be reduced. If the reader is allowed to produce the challenge then this problem can be partially overcome, however the reader system is them open to attacks that subvert the challenge production or collusion by the reader operator.

One potential solution to this problem is to generate an 'access list' of derived secrets that is unique for each participating reader [Tan et al. 2008]. Each entry in the list is generated for a hash of the reader ID and the tag secret. Thus an attacker that obtains such an access list from a reader will not be able to convince a different reader of the authenticity of a cloned tag. However the risk remains that an attacker can gain enough information from different readers to compromise the supply chain operations.

The Trusted RFID Reader allows the implementation of a local authentication function. A lightweight key server can download secrets to these functions (or a has of such secrets and the reader ID following the scheme of Tan et al.) with assurances that the secrets will be stored securely (should the reader be compromised), and that such secrets will not be leaked to other application services on the reader, or to the reader operator. The secrets may be held in secure storage on the Trusted Reader itself, or more likely on local networked storage in an encrypted form available to multiple local Trusted Readers. The key required to decrypt the individual tag secrets is then stored securely within the Trusted Reader and only available to a particular authentication service. Thus the key store can meet the needs of multiple authentication services (e.g. from multiple manufacturers) with the tag secrets encrypted with different service keys. If an authentication service is corrupted then it will be unable to pass an integrity check and retrieve the tag secret decryption key from the TPM.

Such secrets can be downloaded in advance of the tag arriving at the reader based upon intelligent analysis of the supply chain process. If the decryption function on the reader cannot obtain the correct key locally, then irregular communications with a back-end system can result in the retrieval of the key for that tag, along with a cache of likely keys that may be required in the near future (such as products in the same batch).

High Level Protocol

Reader to Tag Protocol	**Trusted Reader Protocol**	**Network Centralized Authentication Controller**
1. *Inventory command from the reader* 2. *Tag transmits EPC 96 bit Identifier* 3. *Authentication challenge sent with a nonce* 4. *Tag computes authentication message X= AES(K, N)*	1. *Trusted Reader receives from the centralized controller a couple (EPC, K) for each tag* 2. *Trusted reader performs local authentication comparing X with the local secret* 3. *If the comparison is 'TRUE' then the tag is authentic*	1. Check the integrity of the trusted platform through the TPM component. 2. In the event of a compromised reader the system administrator should be notified. 3. If the reader is not compromised the secrets can be downloaded to the reader

9 Authentication using Pseudonym Schemes

Similar to the symmetric cryptography scheme described above, a pseudonym scheme uses a secret shared between the tag and the authorisation service. The difference is that a pseudonym scheme is designed to protect the confidentiality of the product or tag identifier. A pseudonym scheme can also provide tag authentication.

In one such a scheme the tag will receive an authentication challenge (in the same manner as cryptographic authentication tags). The tag will use the random nonce N provided as the challenge, and a second nonce M produced by the tag, to encrypt the response M,X where X= AES(K, N, M, ID) and ID is the product or tag identifier. The use of the second nonce is required to stop the tag being traced by correlating the responses to the same repeated challenge.

The problem with this scheme is that the reader will not know which key K is being used by the tag. This results in the reader attempting to apply all known keys to the response until one is successful in decrypting N,M and revealing an ID that matches the ID stored along with the key. In order to implement such a scheme within current protocol standards there are two options. Either the challenge N must be submitted to the tag before the inventory command, or alternatively the inventory command can be disabled (perhaps producing a simple acknowledgment) and the authentication command implemented as a custom command. The former approach may be preferred since it can allow the tree-walking algorithm for the inventory of large numbers of tags.

An alternative approach is to have the tag produce a sequence of seemingly random outputs without using an explicit challenge. An early scheme presented by [Okubo et al. 2003], used a series of one-way functions from an initial secret seed value to produce a chain of pseudonymous outputs. A reader receiving the pseudonym may attempt to reproduce the pseudonym from all know seed values. The seed value that successfully reproduces the pseudonym is used to indicate the identity of the tag. This scheme also provides a level of authentication since an attacker will not know the seed value, and thus cannot produce a pseudonym that relates to a specific tag.

The scalability of both the pseudonym approaches outlined can be improved through the structuring of the pseudonym response using a set of secrets organised into a tree [Molnar & Wagner 2004]. Each tag is assigned to a leaf on the tree and stores the secrets associated with each node in the path from the root to the leaf. Each secret is the used to produce a part of the pseudonym. By using each part of the pseudonym in turn, the authentication service can test against a limited set of keys (equivalent to the branching factor of the tree) and identify the tag with logarithmic complexity. Only once the authentication service has proved it is able to understand part of the pseudonym is the next part revealed by the tag. The scheme increases the secrets that need to be stored (on the tag and authentication service), increases the number of rounds of communication with the tag and the overall time to identify and authenticate the tag. However, the decrease in the time taken by the authentication service for O(n) to O(log n) is essential for large numbers of tags.

Using a Trusted Reader for Pseudonym-based Authentication

Largely we can consider the authentication of a tag using a pseudonym scheme to be similar to that presented before using a mutual authentication scheme (with the tag identifier sent it the plain). The main difference of a pseudonym scheme is that the tag identifier is also included within the encryption instead of just the authentication response. The benefits concerning local processing and key storage remain the same. However we should consider the two differences between a mutual authentication with the tag or product identifier public and a pseudonym scheme including authentication.

The first obvious difference is that for the pseudonym scheme we do not initially possess the tag identifier to assist with the key singulation. The second difference is that for the pseudonym scheme the key allows both the read access to the identifier as well as the ability to authenticate the tag.

Concerning the initial unavailability of the tag identity, if a hierarchical key scheme is used then a number of rounds of interaction with the tag are required to perform identification and authentication. Due to this, the use of a back-end authentication service may be much more prohibitive than for a single round authentication-only scheme. The tag must be held whilst every round is completed and the load on the authentication server is increased by the number of rounds performed (depth of the tree) and the number of secrets that must be tested at each level (tree branching factor). Thus the ability to be able to securely distribute such secrets to a local secure store under the control of the Trusted Reader may be essential to the practical implementation of such schemes. The secrets can be placed in a local datastore encrypted with a key stored in the TPM of the Trusted Reader. Only the secure service on the reader can obtain this key after passing integrity checks.

Concerning the use of the same secret to protect both read access and authentication, it is not possible to delegate such secrets to a local reader for the purpose of tag authentication, but not for identifying the tag (or vice-versa). Using the Trusted Reader, such secrets can be given to individual services within the Trusted Reader. One secure service will use the secret to perform authentication while another uses the same secret to perform identification. Different users (or onward services) can thus be granted either identification or authentication capabilities without providing them with the common underlying secrets.

High Level Protocol

Reader to Tag Protocol	**Trusted Reader Protocol**	**Network Centralized Authentication Controller**
5. Tags are issued with random nonce *6. Inventory command from the reader* *7. Tag computes authentication message X= AES(K1, N, M, ID)* *8. Tag transmits pseudonym part* *9. Authentication system finds K,ID that matches pseudonym response* *10. Reader authenticates to tag that it is able to decrypt pseudonym* *11. Next part of pseudonym is produced….*	*4. Trusted Reader receives from the centralized controller a tuple (EPC, K1..Kn) for each tag* 5. *Trusted reader perform local authentication comparing X with a loca lsecrets* 6. *If the comparison is 'TRUE' then the tag is authentic and has also been identified*	4. Check the integrity of the trusted platform through the TPM component. 5. In the event of a compromised reader the system administrator should be notified. 6. If the reader is not compromised the secrets can be downloaded to the reader

10Supply Chain Control through Tag Re-Signature

In this section we present a scheme specifically designed for implementation of the Trusted Reader. We also present an alternative approach implemented using a centralised trusted service that can adopt the functionality of the Trusted Reader at the cost of communications, operational dependence and the sacrifice of business confidentiality to the centralised trusted service.

The scheme presented uses signatures within the tag user memory to verify that goods are flowing along authorised paths and to stop the intrusion of other unauthorised goods into those paths. It has been inspired by the implementation of Virtual Private Networks (VPNs) in the world of communications, and hence we coin the phrase “physical VPN” for similar operations within the physical supply chain network.

The Physical VPN – Securing the Supply Chain Path

In the literature today there are largely two approaches to preventing counterfeiting. The first is to attach secure labels to the product that are hard to clone. Techniques such as the holograms have become common and with the use of RFID in product we have seen techniques with secure labels such as the TID (discussed in section 5) deployed as a simple mechanism for product authentication. The downside of label/tag approaches is that the label costs are often increased and many solutions require and always-on connectivity with a back-end authentication system. Furthermore such solutions only seek to determine whether a label, and hence a product is genuine. They do not seek to control the supply path of the goods. Such an approach can prevent the introduction of counterfeit goods but also provide better visibility and control over the distribution path (for example to control grey market activities or prevent damage. For example only parties who have the correct training and equipment may be authorised to participate in the supply chain.

An alternative approach is to build an electronic pedigree (e-pedigree). This involves collecting supply chain information throughout the life of the product. At the point of authentication, such supply chain information is analysed to detect inconsistencies. For example, if a product doesn’t have a plausible manufacturing and shipping record, then there is a high probability that it is a counterfeit good that has been introduced into the supply chain. The major downfall of this approach is that all parties in the supply chain must share information in order to be able to detect anomalies. The manufacturing and shipping information required is considered by many to be sensitive information about their business operations. Proposals along these lines often involve sending the information to the manufacturer, or the use of a Trusted Third Party. Another problem with this approach is that it is hard to set a decision mechanism under which goods are rejected as counterfeit. For example, perfectly legitimate goods might be sold outside the usual distribution routes through outlets that are not equipped, or have no agreement, to send their information to the e-pedigree system.

The *Physical VPN* approach attempts to bypass the problems of the above two approaches. Trace information is written by standard RFID readers onto cheap unsecured supply chain tags. This trace information is used by each party co-operating in the system to verify that the previous holder of the tag is an authorised upstream supply chain partner. Counterfeit goods being injected into the supply chain will lack such upstream credentials and can be detected immediately by the supply chain partner, with much greater potential to take action against the counterfeiters. Since each partner need only check that the goods have arrived from their immediate upstream partners, the solution is very scalable both in terms of trace information on the tag, and the number of secure keys that must be held. In addition each partner does not gain more information about the supply chain operations than they need. For example, a partner can only validate that the goods have been sent from the authorised partner immediately upstream. They do not gain any knowledge of other partners further upstream that have been involved in the supply chain.

Using Signatures to Create a Physical VPN

The objective is to allow one or more parties to define acceptable supply routes between authorised nodes for different products. For example a manufacturer may specify an authorised distribution chain for its goods to flow to the franchised dealers. The use of the same infrastructure to implement a number of authorised supply chain networks for different parties provides the *virtual* private network within the overall supply chain graph.

A downstream node should be able to check that a product has arrived along an authorised upstream path. However, it should not know which parties were involved in the upstream supply chain in order to preserve sensitive business information.

This approach can be used to prevent counterfeit goods entering the supply path, and also to control the supply chain to detect grey market and diverted goods. For example, a counterfeit good will not have travelled a prescribed path from the legitimate manufacturer. A product that is diverted from another market will fail to follow the correct distribution chain. This can be achieved by the upstream node using a cryptographic key to sign shipment of the product. The secret part of the public-private key pair is unique to the upstream partner and the signature is performed on the product identifier (and potentially TID) obtained from the RFID tag. The signature is written into additional memory registers on the identification tag, or may be written onto a separate additional electronic tag.

The downstream partner, in possession of the public part of the key may check that the good has been dispatched from the expected source. This operation is the same as checking that a PGP signed email has arrived from the correct sender.

10.1.1 Potential Issues with a Re-signature Approach:

1. Malicious Player - in a supply chain the simple operation outline above may not be sufficient. A trusted upstream partner in the supply chain may introduce counterfeit or redirected goods back into the authenticated supply chain.
2. Policy Requirements - the downstream partner needs to maintain policies on whom it will accept certain goods from. It is clearly inadequate where third parties other than the shipper and receiver want to specify a legitimate supply path and may not have complete trust in every supply chain partner.
3. Supply Chain Confidentiality - the last upstream node participating in the authenticated supply chain may not be the upstream partner with whom we have a business relationship. For example, a manufacturer may wish to ensure that goods flow through a selected number of exporters, but does not wish to constrain the import supply path to the retailer. In this example, the retailer needs to know that the goods have arrived from a legitimate exporter for them, but should not be able to determine which exporter was used as they have no business relationship with them and this may be sensitive business information.

10.1.2 Using a Third Trusted Party

Using a third party service provider to perform the re-signing operations can solve these problems. When the goods arrive, the supply chain participant sends the product identifier and upstream product signature to the service provider, along with its own identification credentials.

The service provider checks permitted upstream routes through which that product may arrive at the current holder of the goods. If one of these routes matches then the route is verified by checking the upstream signature. In this case the service provider then generates a new signature using a key that is unique to the new holder of the product. The signature is returned to the holder of the goods whereupon it is written onto the product tag. The holder is now free to ship the goods onward to further authorised destinations.

This solution overcomes the problems of authorised supply chain parties being able to introduce counterfeit or diverted goods. It also solves the problem of upstream operation confidentiality. However, this solution requires continual on-line access to the service provider similar to the e-pedigree and some secure label solutions. If the network or service provider is unavailable, then the goods cannot be resigned. Onward shipping will result in later parties being informed that the product has not passed through a required part of the supply chain, and product diversion or counterfeiting may be suspected. The on-line operation also requires the product to remain in the field of the RFID reader between the read and write operations to the electronic tag(s). This restricts the placement of such readers and where the re-signing operation for the goods can take place.

Another problem is that the service provider performing the re-signing operation becomes aware of the transit of every good in the supply chain. Ideally we want the service provider to be able to specify allowed paths for products, without gaining knowledge of the flow of individual goods.

10.1.3 Using a Trusted Reader

We propose that these problems are overcome through the use of a Trusted Reader. This allows the service provider to run the checking and re-signing operation in a secure environment where the reader operator, or anyone else, cannot tamper with it. The Trusted Reader can similarly protect the private keys used in the signing operation, such that they cannot be leaked to the reader operator or any other party. Since the operations are performed locally on the Trusted Reader the service provider does not gain any knowledge of legitimate supply chain operations (or indeed any operation if the alerts are sent directly to other parties such as manufacturers).

It should be noted that multiple service providers (or other parties) can use the trusted re-signing platform to perform their own supply chain validation checks. Thus a supply chain participant dealing with several pharmaceutical manufacturers may allow each to install their own keys and permitted policies onto the re-signing platform. Each can use the Trusted Reader feature of remote attestation. Remote attestation allows each participant to ensure that the software running on the re-signing platform has the expected digital fingerprints and has thus not been tampered with or corrupted. Thus they can expect that supply chain policies they load onto the re-signing platform are being enforced, and that their secrets are not being released to other parties.

The Trusted Reader for the Physical VPN scheme may be implemented as a trusted computing system to which is attached any ordinary reader capable of reading and writing the memory of the electronic tag. This reader may be used for simultaneous routine supply chain applications, along with the supply chain validation and re-signing operations. We may also expect to see integrated Trusted Readers with onboard TPM hardware that incorporate the validation and re-signing functions into the same housing. This may provide an easy integrated solution for some supply chain participants. The provider of the re-signing platform

or integrated readers may also maintain and operate the platform on behalf of the supply chain participant. This model may be particularly attractive for integrated readers sold to smaller participants on a rental model, or those with less Information Technology skills.

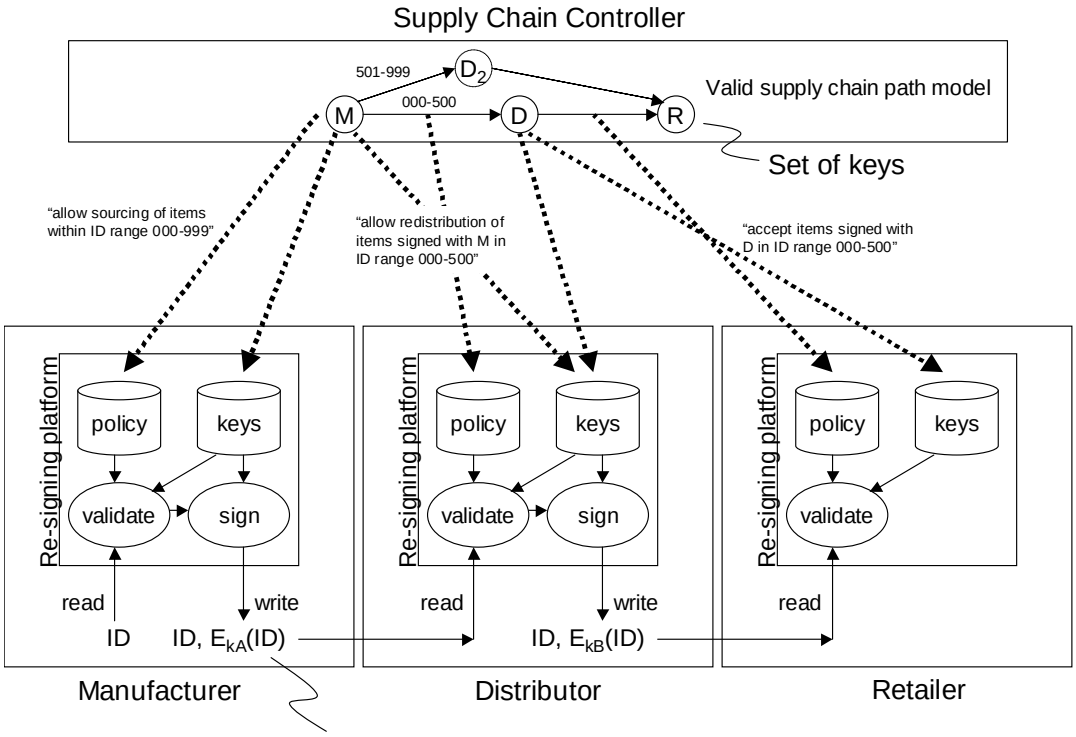

Figure 5: Physical VPN implemented on Trusted Reader

The supply chain controller (shown in Figure 5) defines an authorised path across the supply chain. The controller generates, coordinates and distributes the various validation and translation keys among the different trusted reader platforms, along with the local authorised path policies.

The controller will receive the information on how products should flow in the chain from the end-user of the authentication and control service (e.g. the manufacturer). The model will define the acceptable parties in the supply chain along with valid routes for certain products. The controller will then create and distribute the correct keys to the various Trusted Reader services.

The first step in the supply chain process is for the manufacturer or other initiating party to produce the initial signature for the tag. This is performed using a private key for the initiator provided from the supply chain controller. This initial signature may be produced by a trusted Reader, but the initiator may also be trusted to hold and perform this operation (since they are likely to be the party specifying the authorised paths to the supply chain controller. The advantage in using a Trusted Reader at this stage is that such private keys can be held securely within the secure storage of the Trusted Reader.

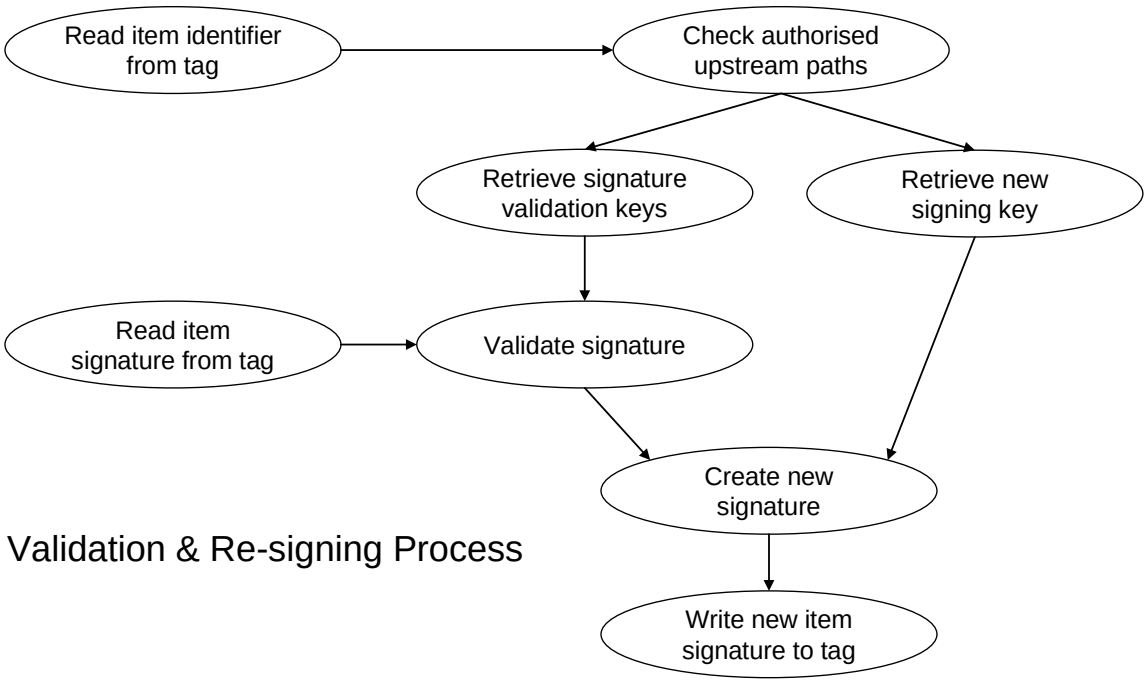

Figure 6: Trusted Reader Re-signing Process

Figure 6 outlines the various steps performed by a downstream supply chain participant operating on the re-signing platform:

1. **Read item signature and identifier from the tag.** The RFID reader passes the tag information to the trusted platform. The information contains an ID (e.g. EPC 96 bit and optionally TID) and the signature.

2. **Retrieve Validation Key.** The platform checks if there is a policy associated with that specific tag identifier. If the specific policy is present then the policy manager gets the public validation key associated with the identifier.

3. **Validate Signature and uniqueness test.** The platform decrypts the signature using the validation key and checks the results against the identifier of the tag. If the values match then the tag has followed a legitimate path in the supply chain. The platform also performs a uniqueness test. It checks that the tag is unique and that no tag with a similar ID has been previously validated by the platform. This check can be performed by storing the previous identifiers in a database, or by including previous identifiers in a bloom filter to reduce storage overheads.

4. **Retrieve Signature Key.** If the product is authentic then the policy manager instructs the trusted platform to sign the tag with the private key associated with the forward path in the supply chain. Notice that the signature key is associated to a specific path and a specific set of identifiers. In this manner the controller can select exactly which products flow along paths where a supply chain path splits into multiple downstream paths.

5. **Create New Signature.** The trusted platform generates a new signature using the retrieved signature key. Following this action the platform communicates to the reader to write the new signature on the tag.

Alternative Business Models

There are two approaches to the use of this invention for constructing secure physical supply chain paths.

- **Central Service Provider** - The keys can be generated and distributed from a central trusted service provider. In effect, this provider controls the permitted routes in the supply chain. Parties wishing to take part in the authenticated supply chain must apply to the service provider. This allows one or more parties (such as the manufacturer) to have visibility and control of the supply chain through the service provider. A slightly different model is to use multiple service controllers which have permission to configure the same re-signing service on the Trusted Readers.

- **Peer-to-Peer** - Although the equipment and IT solution may be supplied from a single vendor, the establishment of trust takes place between consecutive partners in the supply chain. An exchange of key information takes place to allow the downstream partner to check that the product has arrived from an expected upstream partner. In this case we assume that there is no need for a centralised authority. We can see that each downstream party performs the role of the supply chain controller in order to control the goods it receives from its upstream partners.

Since both models can be viewed as a number of supply chain controllers configuring the re-signing service on the Trusted Reader (or even running multiple re-signing services), the two approaches can be operated in parallel. Dominant supply chain partners such as the manufacturer may establish some overall supply chain controls. Individual parties within the supply chain may then add additional constraints for checking their own receiving operations, or adding further controls via a trusted controller service to further downstream partners.

11Conclusions

Through the analysis of some known authentication techniques we have demonstrated that the use of the Trusted Reader can provide tangible benefits, both in terms of security, resilience and operational costs to many RFID authentication technologies. We have also presented a new authentication and supply chain control scheme designed specifically for the Trusted Reader. Without the Trusted Reader such signatures could not be securely replaced, resulting in a scheme where upstream operations would be visible to all downstream parties.

It is also important to note that in addition to the enhancement of each authentication technology, the use of the Trusted Reader provides a secure multi-service platform where local authentication components can be operated by multiple parties using different technical approaches. Without the Trusted Reader this would result in costly systems integration by each reader operator involved in the schemes for each authentication technology and each authentication service (e.g. manufacturer).

12References

[Al-Kassab et al. 2008] J. Al-Kassab, M. Lehtonen and F. Michahelles, “Anti-Counterfeiting Prototypes Report”, Deliverable D5.4 of the BRIDGE project, 2008.

[Bush et al. 1989] R. Bush, P. Bloch and S. Dawson, “Remedies for Product Counterfeiting,” Business Horizons, January-February 1989.

[EPC] EPCglobal Inc.: Class-1 Generation-2 UHF Air Interface Protocol Standard Version 1.09, Available at http://www.epcglobalinc.org/ standards technology/specifications.html.

[Ilic et al. 2008] A. Ilic, M. Lehtonen, F. Michahelles and E. Fleisch, “Synchronized Secrets Approach for RFID-enabled Anti-Counterfeiting”. Demo at Internet of Things Conference 2008, Zurich, Switzerland, 2008

[ISO 2004] Information technology — Radio frequency identification for item management — Unique identification for RF tags - INTERNATIONAL STANDARD ISO/IEC 15963 - First edition 2004-09-01

[Lehtonen et al. 2007] M. Lehtonen J. Al-Kassab, F. von Reischach, O. Kasten and F. Michahelles, “Problem-Analysis Report on Counterfeiting and Illicit Trade”, Deliverable D5.1 of BRIDGE Project, 2007.

[Lehtonen et al. 2009] M. Lehtonen, F. Michahelles and D. Ostojic, “Securing RFID systems by detecting tag cloning”. In the Seventh International Conference on Pervasive Computing, Pervasive'09, Japan, May 2009.

[Lehtonen et al. 2009] M. Lehtonen, A. Ruhanen, F. Michahelles and E. Fleisch, “Serialized TID Numbers – A Headache or a Blessing for RFID Crackers?”, In IEEE RFID 2009 Conference, Orlando, Florida, April 2009

[Molnar & Wagner 2004] D. Molnar and D. Wagner, “Privacy and Security in Library RFID: Issues, Practices, and Architectures", ACM Computer and Communications Security (ACM CCS) 2004.

[Okubo et al. 2003] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A Cryptographic Approach to 'Privacy-Friendly' tag", RFID Privacy Workshop, November 2003.

[Staake 2007] T. Staake, “Counterfeit Trade – Economics and Countermeasures”, Dissertation in the University of St. Gallen, Switzerland, 2007.

[Tan et al. 2008] C. C. Tan, B. Sheng and Q. Li, “Secure and Serverless RFID Authentication and Search Protocols”, IEEE Transactions on Wireless Communication, Vol. 7, No. 4, April 2008.