

Securing RFID-supported Supply Chains

Florian KERSCHBAUM^a and Manfred AIGNER^b

^a *SAP Research, Karlsruhe, Germany*

^b *IAIK, Graz University of Technology, Austria*

Abstract. Modern RFID-supported supply chains envision a seamless sharing of item-level data across multiple supply chain participants in the “Internet of Things”. However, many companies are reluctant to propagate large amounts of their track and trace information to others, as they fear the uncontrolled disclosure of vital business intelligence. Without built-in safeguards, such systems thus run the risk of hindering the adoption of efficient supply chain management infrastructures.

In this paper we will define the cornerstones of a cryptographically sound security architecture for RFID-supported supply chains that will enable efficient logistical management with minimal data disclosure. We propose to replace the common centralized track and trace approach with an architecture that makes use of strong cryptographic primitives and secure storage on the tag and builds on top of those enhanced authentication and key-agreement protocols. The architecture will thus span the entire technology range from the RFID tag and its network infrastructure to the back-end system that is storing the supply chain information.

Keywords. RFID, Cryptography, Supply Chain Management, Track and Trace

1. Introduction

RFID is becoming a prevalent technology in supply chains. In order to gain the full benefit of this technology companies must share item-level reading data, so called events. A set of standards is emerging for gathering and sharing events across the Internet: the EPCglobal network. This future standard will allow the discovery of events without any security constraints, such that it is possible through repetitive querying to obtain the basic information of organization, time and identifier of any event. Additional event data is supposed to be protected by (role-based) access control, but traditional access control faces several problems related to item-level event data. First, the principals of access control are not always known to the protecting parties, e.g. if they are separated by two stages in the supply chain, and second, each item needs an individual access control policy even in the case of role-based access control, such that the sheer number of policies becomes unmanageable. These unresolved security and privacy issues lead to a reluctance of companies to share data [12,14]. According to a recent study by the University of Freiburg, 29% out of 102 RFID industry users consider unresolved security issues to be a problem (“high” and “relatively high” importance). A further 32% of the companies state that they face serious privacy concerns among customers. Both findings are particularly relevant since 41 out of 106 identified in-house RFID applications are also potentially suitable for cross-company use (such as Material Flow Control, Kanban, Anti-theft Protection, Maintenance etc.) [15].

In this paper we attempt defining an architecture that integrates the real world of the “Internet of Things” in a supply chain with the security objectives of the players. In particular we address the most pressing security concerns of

- *confidentiality*: as already mentioned companies want to reveal data only selectively, remain in control of the access decision and base the decision on sound identification of actors. This concerns are generally address by the security technologies of access control model (what to disclose), access control mechanism (how to enforce) and authentication. In this paper we outline a general model of access control in supply chains, a novel authentication mechanism and rely on distributed database with locally enforced access control.
- *integrity*: decision will increasingly based on supply chain data. Imagine verifying the authenticity of a prescription drug by retrieving the pedigree information in the supply chain of that particular item. If the supply chain data can be tampered with, a competitor may be able to prevent sales of a specific drug. This problem is particularly challenging, since the information is distributed across a number of parties. In this paper we propose a mechanism that ensures the integrity and authenticity of supply chain event data based on the use of enhanced RFID tags. This information can then later also be used to ensure confidentiality.

The remainder of the paper is structured as follows. In Section 2 we outline the envisioned architecture with its structural components and considered applications. Section 3 lists the properties we intend to ensure and achieve by this architecture. In Section 4 we describe the principles and mechanism that can be used to implement the architecture and sketch some initial protocols. Our conclusions from the work so far and a number of possible avenues for future work are listed in Section 5.

2. Architecture

The basic architecture is depicted in Figure 1. Goods equipped with RFID tags pass from the supplier to the buyer. Each company reads the RFID tags and stores related information, an event, in its local database. Later the companies exchange that information in order to run advanced applications. Some applications include:

- *Estimated Time of Arrival*: Based on the events of suppliers the buyer estimates the time of arrival and eventually triggers correction actions.
- *Product Recalls*: Stored events can help with targeted recalls limited to the minimal set of products that needs to be recalled.
- *Benchmarking*: Item-level events allow for the first time precise, supply-chain wide, inter-organizational benchmarks [6] to be computed that could not be computed before, e.g. percentage of returned items per supplier [3].
- *Anti Counterfeiting*: Supply-chain wide tracing allows the identification of counterfeit products and their identification at the point of sale.

Our future security architecture will consist of three interrelated pieces. Our centre-piece is a cryptographically verifiable event stored in a distributed database. If the information collected in an event and obtained from the tag, the company and the environment is authenticated and verifiable by a third party, it can then be used to secure the data exchange, e.g. as basis for a key exchange.

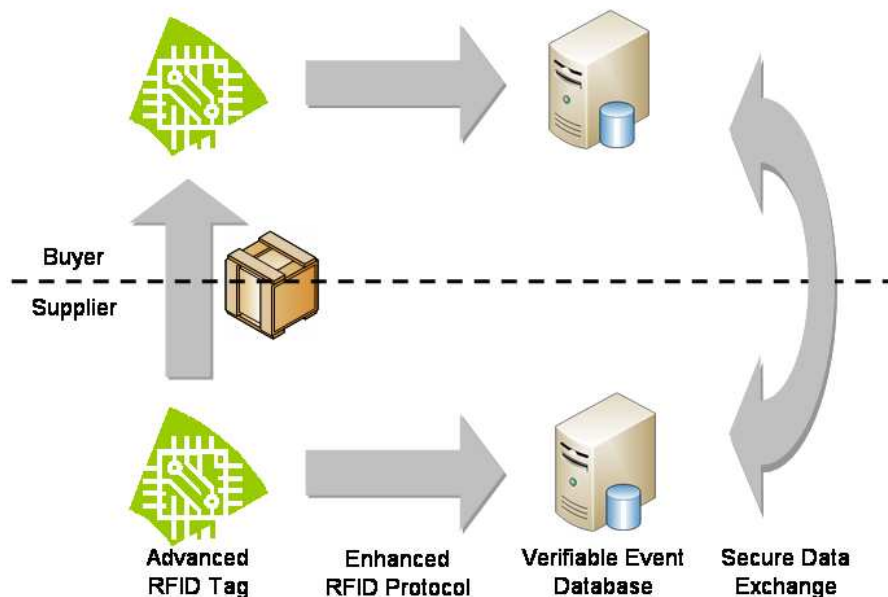


Figure 1. Basic Architecture of Track and Trace

Advanced RFID Tags: In order to guarantee end-to-end security we will need to integrate novel computational capabilities into RFID tags. These include implementations of the cryptographic functionality and new architectures of tag controllers that enable secure integration of additional modules and sensors. Those future tags will implement advanced security services to be used in applications that require signatures by objects, or integrity of sensor data. The security services will also be used to perform secure handover of tags without completely deactivating the tag by the kill command.

Enhanced RFID Protocols: Future RFID communication protocols need to secure communication between passive tags. This will include authenticating the information from the tag and making it usable in subsequent protocols, such as key-agreement protocols or cryptographically enforced access control.

Secure Data Exchange: The information systems at the back-end that collect RFID data need to be interconnected and offer the necessary services for performing the intended applications. We need to solve a novel authentication problem in supply chain back-ends. One has to prove the identity of the company in conjunction with the identity of the item. A recent development is RFID-based authentication and key agreement [11] in which information is passed along the supply chain and then later used by the companies to establish secure session keys for exchanging tracking data.

3. Challenges

The following properties should guide the design of the architecture:

- *Secure*: A formal assessment of the architecture and its components with stated trust assumptions is necessary. It should clearly derive the provided security guarantees proven security.
- *End-to-End*: The architecture spans multiple layers and multiple applications and technologies at each layer, but it should ensure the security and privacy of the data from the gathering at the device to the use within the application. It is therefore necessary that the components are compositional and integrated as well.
- *Flexible*: The architecture needs to be able to cater for different trust levels and apply different security mechanism depending on the business needs.
- *Decentralized*: The architecture should minimize the use of centralized systems, such as trusted third parties. Instead each party should remain independent and in control of its data.

4. A Simple Approach to Cryptographically Verifiable Events

4.1. Enhancing Tag Capabilities with Public-Key Crypto

Due to steady advances of silicon technology, the computational capabilities of tags are steadily rising. The minimal die area of tag chips is limited due to the fact that smaller chips produce higher costs during handling, packaging, and cutting. With current technology the basic functionality of Gen2-tags can be implemented on an area that is close to this limit. Migration to newer technology still makes sense, since the power consumption of the tags (and therefore their reading distance) can be improved by smaller silicon structures. This means, that future tags will provide additional area to implement more functionality without adding additional costs. This area can be used for implementation of cryptographic functionality. The feasibility of symmetric cryptographic operation with state-of-the-art security level is demonstrated in [4]. Newer publications show that it is even possible to implement public-key algorithms under the given requirements for power consumption, area consumption, and throughput [7] [2].

Future RFID tags will differ from contact-less smart cards by their reading distance and the set of cryptographic features they provide. While smart-cards typically provide a rather powerful selection of different cryptographic features, the capabilities of RFID tags will be very restricted to a small set of cryptographic functions. This restriction is necessary due to the available power budget, but also due to the rather high controlling effort that comes with combination of different cryptographic algorithms. Execution of different cryptographic procedures using their associated credentials in a way that security holes are avoided, requires rather complex controlling that will not be achievable on RFID tags in next future.

The execution of a cryptographic algorithm alone does not yet make up a security token that can be used in the proposed system. A private key needs to be stored in a secure way so that is available for the cryptographic operation, but not for an attacker. This memory-area requires secure access control for storage of key-material to avoid illicit access during personalization or key-exchange.

Side-channel analysis (SCA) poses a serious threat which requires additional protection [13]. In the suggested application scenario, the number of executions of the cryptographic operations with one specific key can be limited to a reasonable value, therefore the countermeasures against SCA can be scaled in an effective manner. Additionally to the private key, the tags need to store their public key in form of a certificate that ensures the binding between cryptographic key and the tag's public ID. This certificate needs to be transmitted to a reader before an authentication procedure can take place.

To execute the cryptographic operations additional commands need to be integrated into the tag to reader protocol. Currently, security standardization for RFID protocols is ongoing within ISO. They follow a service-oriented approach which allows a tag to offer available security services to a reader. The reader can decide to use the tag with its capabilities in a secure application or not. Uncritical operations are still possible, even if a tag (or a reader) does not offer advanced services. We expect that successful security standardization, together with foreseeable development of chip technology, paves the way for adoption of public-key crypto tags in commercial wide-scale applications.

4.2. Context-Based RFID Authentication

Existing RFID authentication protocol can be used to securely and privately identify RFID tags. They are secure, because they ensure that only a tag that possesses a secret identifier can successfully authenticate. They are private, because they do not reveal that identifier to rogue readers who are not already in possession of that identifier.

When using RFID in supply chains, neither property is overly important. RFID tags per se provide little resistance to physical cloning and therefore are infrequently used for product authentication. Other mechanisms that can rely on cheaper tags using the collected trace data can be used. Goods in supply chains are not tied to personal data, such that privacy is of little relevance. This changes once the good has been delivered to the customer, but different mechanisms exist for dealing with this problem including the unpopular *kill* function.

The prevalent approach for handling RFID data in supply chains are so-called events. At its very basic an event is a triple $\langle object, time, location \rangle$ stored each time an RFID tag is read.

The *object* identifier is stored on the RFID tag and the secret information used in existing RFID authentication protocols. We can therefore use existing RFID authentication protocols to effectively ensure the confidentiality and integrity of this information. The question is how do we ensure the confidentiality and integrity of the entire event?

Given RFID tags with public-key cryptographic capabilities there is a very simple secure (non-private) RFID authentication protocol. The reader simply sends a challenge r to the tag which responds with its signature. Assuming a public-key infrastructure for the RFID tags, one can verify the identity of the tag. Obviously this simple signature verification protocol must be extended for practical use, but we will use its principle throughout this section.

The *location* identifier can have different degrees of granularity. At a very coarse-granular level it can be just the identifier of the company handling the item. At a very fine-granular level it can be the identifier of the reader. An RFID authentication protocol that also supports reader authentication could be suitable for ensuring integrity of the pair of event data.

Unfortunately this brings along with it a major access control management and key management problem. The tag needs to decide to have a notion of which reader is allowed to read it and this notion must change as it proceeds through the supply chain. Furthermore there are certain limitations to the security any context-based RFID authentication protocol can provide without the use of physical security. As in many uses of trusted hardware, the beneficiaries of the use are not the actual users, such that its acceptance may be low.

Instead we propose to use the company identity as location in our events. Each company – similar to each RFID tag – has its own public-, private-key pair. A challenge is issued to the company which can then prove its identity by signing the challenge.

Given secure (tamper-proof) hardware one can try to generate reliable locations even at finer granularity. Secure hardware equipped with localization technology, such as GPS, can be used to verify its location if it is mobile. In other cases, the hardware can be installed permanently provide other means of authentication. The secure hardware could even be an RFID tag itself and use the same type of authentication as above. Of course, one then needs to ensure that the tag is not removable in addition to being tamperproof. Yoking proofs [8] can provide the assurance that both tags have been read together.

The third piece of information in event is the *time*. This is a global time and we assume synchronized clocks in order to rely on this time information. A trusted source of time might be a time server that issues signed timestamps. This timestamp can then be used in the stored event.

Our enhanced, context-based RFID protocols need to integrate confidentiality and integrity of all three pieces of information in an RFID event.

4.2.1. *Tying The Pieces Together*

So far we have been able to attest the integrity of each individual piece of information in an RFID read event, but our goal must be to ensure the integrity of the event triple. We will outline a simple technique here, that can be used to tie pieces.

Recall, each party – RFID tag, reader (company) and time server – receive a challenge and return it signed. The basic idea is to have each party issue and sign the challenge for the next party.

We start an RFID read event by contacting the time server T . It will issue a signature $S_T(\text{time}, r_T)$ where r_T is a fresh challenge issued by the time server.

Once the company is in possession of the item and the RFID tag, it can then issue this challenge r_T to the RFID tag R .

The RFID tag will respond with a signature $S_R(r_T, r_R)$ where again r_R is a fresh challenge, but this time issued by the RFID tag.

This challenge r_R is finally signed by the company C . One obvious attack remains, since the company can request the timestamp from the time server early and then delay processing. But we can use the same technique in order to have the time server sign a challenge by the company. The company produces $S_C(r_R, r_C)$ and sends r_C to the time server. The time server responds with $S_T(\text{time}', r_C)$. The time the RFID tag has been read is now bound between *time* and *time'*.

4.2.2. *Limitations*

Our protocols follow the security model of distributed systems, i.e. there are n distinct parties. Collusion is an attack no protocol, even given physical security, can prevent from.

Assume an attacker controls parties A and B . He can always create an RFID read event for locations in A while the item is physically in a location of B . Imagine a device that simply relays signals from the reader over the network to a remote RFID tag. This device could trick even a trusted reader into creating a read event for a remote item. More simply the attacker could ship the item for A to B , but also no protocol can prevent relaying messages between A and B , such that an attacker can simply perform the attack on the RFID authentication protocol. This implies that the location of an event can only be as precise as the sphere of control which is our reason for choosing the company identity as granularity for the location. We assume that companies are less inclined to collude.

4.3. Authentication Using Verifiable Events

Each party stores its RFID events in a database. In order to perform the applications mentioned above the parties need to exchange the event data. This process generates “supply chain visibility”. Nevertheless, the gathered data reveals sensitive information about a company’s operation. Companies are therefore reluctant to share this data. Fine-granular access control may help to mitigate the problem.

The access control matrix for event data consists of events associated with an item times the supply chain partners. This access control matrix can become huge, since the number of items is continuously growing. Manageability is therefore key to the database owners.

Access control is usually performed on identity or via indirection on roles. Given that a party has access to all events or type of events, e.g. for a specific product, based on its identity there are many possible inferences. In particular a company can spy on its competition sourcing from or delivering to the same partner. Therefore a company should set its access control specific only to the items shared with a partner.

In order to authenticate for access to data based on shared items one needs to prove possession of an item. The advantage of our context-based RFID authentication protocol is that it produces a verifiable event. The integrity of such an event is ensured, such that other parties can verify and trust its correctness. Then the event can be used in order to authenticate. To request access to event data for item h , a party A simply presents a verifiable event $\langle h, time, A \rangle$ and proves its identity. The queried party can then grant access to data for item h only.

5. Conclusions and Future Work

Our proposed architecture fulfils its set goals of confidentiality and integrity at the very least to the minimal extent necessary. We provide a stronger access control using verifiable events which is enforced locally for each part of the distributed database. The integrity of each event is ensured using cryptographic mechanisms.

Our architecture is therefore *secure*. It involves all components from the tag to the item to the server hosting the database and is therefore *end-to-end* within the supply chain. Each party hosts its own data and entire system is *distributed*.

Although the access control policies may enable a large degree of flexibility, they are limited by the basic principle of access control of the decision to disclose or not to disclose and their enforcement mechanism. In order to increase the flexibility of the

architecture and cater for a wider range of use cases we propose a number of avenues for future research.

5.1. Releasing Aggregate Information

The design of supply chain information with events as building blocks does not consider the information protection needs and desires of the supply chain decision makers. It is entirely unclear the information contained within an event or set of events, e.g. by inference even with previous knowledge [18]. So how is a company supposed to make a decision whether to reveal that information or not? In many cases, it is nevertheless possible to decide on releasing aggregate information; in particular if that information, is necessary or derivable from an application. Imagine only releasing the bit whether a product has been recalled or not. If a company implements recalls – and it might be obliged to by law –, this information is entailed within the application. A decision maker can then easily compare the risks of disclosure with the expected business benefit.

The technical challenge is in implementing applications that are capable of enforcing this type of access control on aggregate (or computed) information. Given a central database this could be enforced by an application tier between user and database (similar to current enterprise systems), but in the supply chain scenario the data is distributed. Now a number of parties each unwilling to disclose its information first has to collaborate in this application.

Secure Multi-Party Computation (SMC) [1,5,17] offers a solution from cryptography. In SMC a number of parties compute a function on joint input, such that no party learns anything about the input of the other parties, but each party learns the output. Completeness theorems prove that this can be done for any function. Nevertheless these general constructions are prohibitively slow, such that researchers are developing special solutions since almost two decades. Selected applications in RFID-supported supply chains, such as batch recalls [16] and computation of key performance indicators [10], have already been proposed, but future research for more general concepts is necessary.

When using SMC new security challenges arise: nobody can verify the correctness of input data of other parties, since it remains confidential. In this way confidentiality and integrity become opposing objectives. An interesting new feature would be to integrate our proposed verifiable events into SMC, such that other parties could verify the authenticity of events without disclosing them. This could be implemented as a SMC itself or as a Zero-Knowledge-Proof. Also anonymous credentials may offer many mechanisms that can help.

5.2. Remote Enforcement of Access Control

Our proposed architecture is centered around the principle of distributed databases. In many systems RFID events are processed as streams, e.g. in publish-subscribe networks. In a publish-subscribe network data sources send events – as soon as they occur – to data sinks. In these cases one cannot rely on local enforcement of access control any more, but the data is disseminated within the network once it has been released by the source and may sooner or later reach any participant. One approach to handle this situation is to encrypt the data and only selectively release the key. This is called cryptographically enforced access control.

Attribute-based encryption [9] offers a mechanism to handle the keys, but it relies on a central key distribution center. Instead it would be necessary to distribute the keys between the supply chain partners (and the items), such that each party can only reveal data for its RFID tags.

This leads to yet another interesting concept. Assume a central storage of information, e.g. with product information and history, and a physical object equipped with an RFID tag, i.e. the item in the supply chain. Can we control access to the central repository using the RFID tag, such that it is ensured that only physical possession of the RFID tag grants access? In this case the RFID tag could be used a physical token that is passed around for controlling access. Our enhanced RFID tags using public-key cryptography can help again, since they can respond to a challenge by signing it. The central repository can verify the signature and the freshness of the challenge and then grant access. This could also be a novel way for remote customer service where the customer even remains anonymous.

References

- [1] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proceedings of the 20th annual ACM symposium on Theory of computing*, 1988.
- [2] H. Bock, M. Braun, M. Dichtl, E. Hess, J. Heyszl, W. Kargl, H. Koroschetz, B. Meyer, and H. Seuschek. A Milestone Towards RFID Products Offering Asymmetric Authentication Based on Elliptic Curve Cryptography. Invited talk at RFIDsec 2008, July 2008.
- [3] S. Chopra, and M. Sodhi. Looking for the Bang from the RFID Buck. *Supply Chain Management Review*. Available at <http://www.scmr.com/article/CA6444375.html>, 2007.
- [4] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. AES Implementation on a Grain of Sand. *IEEE Proceedings on Information Security*, 152(1):13–20, October 2005.
- [5] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. *Proceedings of the 19th ACM Symposium on Theory of Computing*, 1987.
- [6] W. Hedgpepeth. RFID Metrics. *CRC Press*, 2007.
- [7] D. Hein, J. Wolkerstorfer, and N. Felber. ECC is Ready for RFID – A Proof in Silicon. In *Workshop on RFID Security 2008 (RFIDsec08)*, July 2008.
- [8] A. Juels. “Yoking-Proofs” for RFID Tags. *Proceedings of the 1st International Workshop on Pervasive Computing and Communication Security*, 2004.
- [9] A. Juels, and M. Szydlo. Attribute-Based Encryption: Using Identity-Based Encryption for Access Control. Manuscript, 2004.
- [10] F. Kerschbaum, N. Oertel, and L. Weiss Ferreira Chaves. Privacy-Preserving Computation of Benchmarks on Item-Level Data Using RFID. *Proceedings of the 3rd ACM Conference on Wireless Network Security*, 2010.
- [11] F. Kerschbaum, and A. Sorniotti. RFID-Based Supply Chain Partner Authentication and Key Agreement. *Proceedings of the 2nd ACM Conference on Wireless Network Security*, 2009.
- [12] C. Kuerschner, F. Thiesse, and E. Fleisch. An analysis of data-on-tag concepts in manufacturing. *Proceedings of the 3rd Konferenz Ubiquitäre und Mobile Informationssysteme*, 2008.
- [13] T. Plos. Susceptibility of UHF RFID Tags to Electromagnetic Analysis. In T. Malkin, editor, *Topics in Cryptology - CT-RSA 2008, The Cryptographers’ Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008, Proceedings*, volume 4964 of *Lecture Notes in Computer Science*, pages 288–300. Springer, April 2008.
- [14] B. Santos, and L. Smith. RFID in the Supply Chain: Panacea or Pandora’s Box? *Communications of the ACM* 51(10), 2008.
- [15] J. Strüker, D. Gille, and Titus Faupel. RFID-Report 2008 – Optimizing Business Processes in Germany. *IIG-Telematik, Albert-Ludwigs-University Freiburg, VDI Nachrichten*, 2008.
- [16] L. Weiss Ferreira Chaves, and F. Kerschbaum. Industrial Privacy in RFID-based Batch Recalls. *Proceedings of the IEEE International Workshop on Security and Privacy in Enterprise Computing*, 2008.

- [17] A. Yao. Protocols for Secure Computations. *Proceedings of the IEEE Symposium on Foundations of Computer Science*, 1982.
- [18] D. Zanetti, and S. Capkun. Protecting Sensitive Business Information While Sharing Serial-Level Data. *Proceedings of the IEEE International Workshop on Security and Privacy in Enterprise Computing*, 2008.