6-2011

A Solution with Security Concern for RFID-Based Track and Trace Services in EPCglobal-Enabled Supply Chains

Wei HE
Singapore Institute of Manufacturing Technology

Yingjiu LI
Singapore Management University, yjli@smu.edu.sg

Kevin CHIEW
Singapore Management University

Tieyan LI
Institute for InfoComm Research

Eng Wah LEE
Singapore Institute of Manufacturing Technology

DOI: https://doi.org/10.5772/16624

Published in Designing and Deploying RFID Applications, 2011, pp. 95-108
http://doi.org/10.5772/16624

7

A Solution with Security Concern for RFID-Based Track & Trace Services in EPCglobal-Enabled Supply Chains

Wei He[1], Yingjiu Li[2], Kevin Chiew[2], Tieyan Li[3] and EngWah Lee[1]
[1]*Singapore Institute of Manufacturing Technology*
[2]*School of Information Systems, Singapore Management University*
[3]*Institute for Infocomm Research*
Singapore

1. Introduction

1.1 Overview

A supply chain represents the flow of materials, information, and finance as they move through supply chain partners such as manufacturers, suppliers, distributors, retailers, and consumers. The track & trace services in supply chains can help improve supply chain visibility and efficiency, and prevent counterfeiting and stealing of products thus enhance security. Track & trace services in supply chains require identification of items, capture of events as items move through supply chains, and query of events of items. RFID (radio frequency identification) is a technology that allows to identify objects simultaneously in a fully automated manner via radio waves. This advantage has enabled RFID technology to be used in many applications, including supply chain management (Angeles, 2005) and industrial production (Mintchell, 2002). RFID-based product track & trace in supply chains has attracted growing interests from both academic research and industrial practices.

1.2 RFID

The basic premise behind RFID systems is that each item in a supply chain is attached with an RFID tag. Such tag contains a transponder that emits radio waves of messages readable by specific RFID readers. Most RFID tags store identification codes such as customer number or product SKU (stock-keeping unit) code. The EPC (electronic product code) standard is a promising standard used for RFID identification codes. RFID tags may contain writable memories, which can be used to store extra information for sharing by various RFID readers in different locations. This information can be used to track the move of tagged items, and can be made available to each reader (RFID Journal, 1983). RFID tags can be classified in two general categories, namely active and passive, depending on their source of electrical power. Active RFID tags contain their own power sources, usually on-board batteries. Passive tags obtain power from the radio wave signals of external readers. RFID readers also come in active and passive varieties, depending on the types of tags they read.

1.3 EPCGlobal

Facilitating the use of RFID technology in global supply chains with low cost RFID tags and readers, the EPCglobal network is a platform to pass EPC numbers and leverage on the Internet to access large amount of associated information that can be shared among authorized users. Judging by interest in the global marketplace, EPCglobal is considered to be the next generation of automatic product identification system to facilitate object track & trace in real time throughout a supply chain (Tan, 2005). Its objective is to create a universal and open standard for identifying individual objects and sharing information as these objects traverse a supply chain. Besides a string of digits to identify manufacturer and product, EPCglobal adds another set of digits—serial number—which is unique to each object to identify and track a specific object as it moves through a supply chain. The EPCglobal number is stored on the microchip embedded in an RFID tag. An RFID tag reader sends out electromagnetic waves that can power up an RFID tag, enabling it to transmit back the information stored on its microchip. The reader receives the EPCglobal number, queries ONS (object naming service) about where to find the information about the tagged product, and retrieves the PML (physical markup language) data about the product from specific EPCIS (EPC information services) in the network as defined by ONS. Access to an EPCIS server is subject to authorization and authentication based on specific business agreements and contexts.

1.4 Security

Security has become a major concern while product and information move through a supply chain. An example is the product diversion such as smuggling, counterfeiting and terrorism. Questions of concerns include whether a received item is valid, whether an RFID reader is authorized to read its information, and how to keep the information secure among partners in the EPCglobal network. To address these challenges, hundreds of papers have been published in research literature on solving various security or privacy issues (Avoine, n.d.). Many international organizations such as Customs Trade Partnership against Terrorism (C-TPAT), Container Security Initiative, and Auto-ID Center are formed to address security issues in various industries (Auto-ID Centre at St. Gallen, 2006). However, the research for protecting RFID information in global supply chains is still in its infancy stage, and there are many issues to resolve before we can achieve a fully collaborative system (Sheu et al., 2006). In particular, there is a lack of unified RFID track & trace scheme to provide authenticity, integrity, privacy and accuracy for syndicated applications in EPCglobal-enabled supply chains.

1.5 Contribution and organization

The major contributions of this paper are as follows: (1) We propose a solution for RFID based track & trace services in EPCglobal-enabled supply chain with authentication process. (2) We implement a prototype for our solution. (3) We highlight the functionality of EPCIS in our system. (4) We design the models for track & trace services. (5) We summarize the industry interests in our system prototype.

The remaining sections are organized as follows. The related work on this topic is surveyed in Section 2, followed by our RFID-based track & trace solution with security concern in Section 3. The prototype design and implementation in an OM (order management) scenario are discussed in Section 4. Finally, the conclusion is given in Section 5.

2. Related work on RFID applications in EPCglobal-enabled supply chains

EPCglobal is an R&D effort of several reputable universities and institutes led by MIT Auto-ID lab. It has been the standard for the global supply chain track & trace. Based on EPCglobal,

some other R&D efforts have been undertaken for the development of RFID middleware platforms to facilitate RFID application development. For instance, the Accada software package is an open source EPCIS repository and EPC middleware developed by MIT Auto-ID lab and Institute for Pervasive Computing, Zurich (Floerkemeier, Lampe & Roduner, 2007; Floerkemeier, Roduner & Lampe, 2007). Some researchers have also investigated methods of storage and management of RFID data (Derakhshan et al., 2007). RFID data can be stored in the EPCglobal network, RFID tags, or both. For example, Diekmann *et al.* (Diekmann et al., 2007) focused on the study of managing data in a complex RFID environment to deal with frequent data acquisition processes and increased data granularity. They explored the strategy of data management in EPCglobal network vs. RFID tags (i.e., data-on-network vs. data-on-tag) to facilitate the process management and the track & trace services. Other researchers put their efforts on improving the performance in data query response time and data reusability in EPCglobal network. For example, Song *et al.* (Song et al., 2006) proposed a proxy-based EPC track & trace service architecture with a proxy layer inside the EPCIS.

For RFID applications in supply chains, Straube *et al.* (Straube et al., 2007) investigated how to enhance supply chain visibility, efficiency, and performance from various perspectives. The key challenges include the identification and track & trace of items in supply chains, and information management and sharing, as well as security. As an advanced automatic identification technology, RFID allows supply chain partners to have real time information of supplies and demands and to avoid bullwhip effect (Huo & Jiang, 2007). Based on the analysis of SCM (supply chain management) visibility requirements and general RFID visibility potentials, Melski *et al.* (Melski et al., 2008) proposed a four-step approach to show how visibility in supply chains can be improved with RFID-generated data. RFID-enabled SCM is expected to establish item-level tracking, introducing another level of efficiency never seen before (Michael & McCathie, 2000). Previous study shows that RFID can also be used for reducing retailer product shrinkage with greater supply chain visibility (Huber & Michael, 2007). RFID applications have enabled inter-company integration in supply chains; however, it also triggers a high degree of implementation risk (Chuang & Shaw, 2007). This is because it demands for robust IT infrastructure, high investment, accurate and efficient data management (Imburgia, 2006).

In industry, many cases on RFID applications in supply chains have been reported. WalMart is one of the pioneers incorporating RFID in its retailing and supply chain system, and Gillette is one of the first eight companies to participate in the initial RFID pilot with WalMart. They used RFID technology to track their inventories as items move through a supply chain, from a manufacturer to a distribution center, next to a retailer stock room, and then to a shelf on the sales floor. DOD of US is also an early adopter of passive RFID to solve US military's huge logistics challenge (Thornton, 2006). Tibco, IBM and VeriSign jointly developed demo systems to promote the use of EPCglobal standards. All these applications have been developed to enhance product authentication (supplier: Gillette; retailer: WalMart) and new product visibility (manufacturer: Procter & Gamble; retailer: WalMart) (EPCglobal network, n.d.).

Intel introduced the connected digital supply chain in 2005, in which RFID in EPCglobal is the evolutionary enabler for optimizing supply chains and facilitating the acquisition, filtering, aggregation, and distribution of supply chain data for goods movement visibility (Intel, 2005). Partnering with Intel, OAT also developed a supply chain solution. The solution targets on a high-resolution view of product movement across extended supply chains based on OAT EPCIS edge servers and Intel processors. On the other hand, Sun developed an architecture as part of the Sun EPC initiative to integrate real-time data flow from existing business processes and back-end enterprise systems. Oracle developed the Oracle sensor data

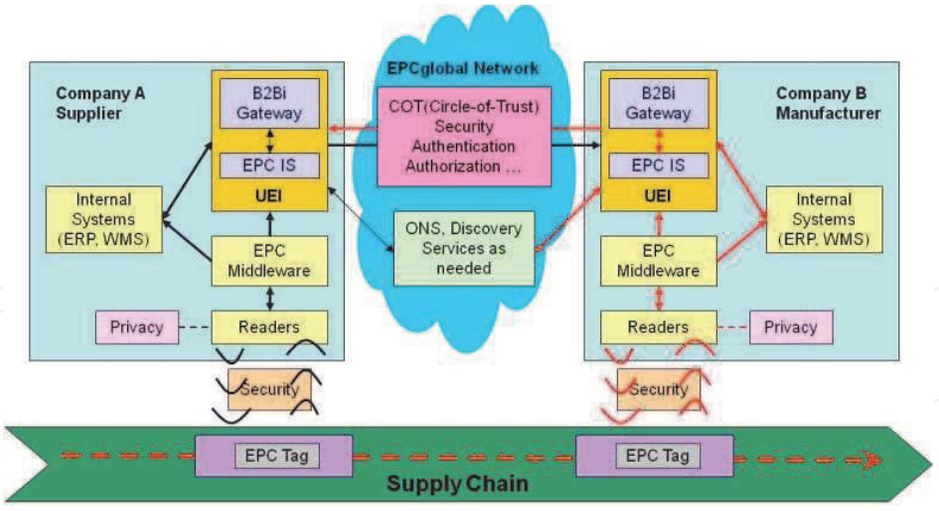


Fig. 1. The solution architecture

manager, in which EPCIS-compliant information service database and discovery services are used for searching for data in EPCglobal network. EPCglobal standards have also been used in developing Electronic Pedigree (E-Pedigree) in pharmaceutical industry against counterfeit drugs (E-Pedigree, n.d.).

3. Our RFID-based track & trace solution with security concern

3.1 The proposed solution

In general, the R&D efforts and solutions of RFID in the EPCglobal network reviewed in the previous section have their particular features and advantages in respective applications. However, there are some common limitations for these solutions, i.e., there are not specific security mechanisms applied to RFID tag authentication and data protection, neither proper security mechanisms at higher level for business information sharing and flow control. As discussed previously, secure and real-time track & trace, flexible business process, information flow control, and their synchronization are becoming increasingly important in supply chains. In view of the gap identified, we propose a solution with security concern for RFID-based real-time track & trace in EPCglobal-enabled supply chains. Figure 1 illustrates the architecture diagram of our solution.

In our proposed solution, track & trace is leveraging on the EPCglobal network. When a product bearing an RFID tag goes through its supply chain, an RFID reader reads the tag data at a reading point of a business step. The RFID data is then passed to EPC middleware for filtering and processing so as to create the EPC events which contain the information of what (the tag data is), when (it is captured), and where (it is captured). A UEI (unified EPCIS interface) designed in the solution captures EPC events and converts them to EPCIS events by adding why (it happened) information which is about the business context. Through the UEI, the B2Bi gateway system will query and retrieve the EPCIS events for business process control. The EPCIS RFID events stored on the EPCIS servers can be shared by other participants in the supply chain through EPCglobal network upon permission of access control.

The B2Bi gateway system (Tan et al., 2006) is a platform developed by SIMTech (Singapore Institute of Manufacturing Technology). It allows companies to participate in B2Bi collaborations to facilitate company collaboration in supply chains. This platform also provides configurable business templates with which users can customize the steps on each business transaction process to allow flexible process configuration. The B2Bi gateway system

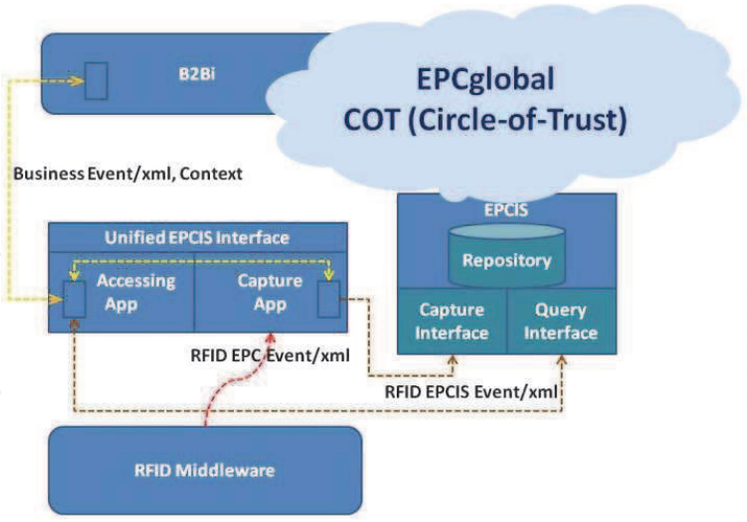


Fig. 2. UEI (Unified EPCIS Interface) architecture

currently only manages business information flow in business processes without involving the track & trace services for the physical items.

As aforementioned, security is important in RFID applications. There are two levels of security that are studied and designed in this solution. One is at lower level, i.e., data security between reader and tag. The other one is at higher level to control information sharing among participants through a COT (Circle-Of-Trust) model proposed for supply chains.

Our solution allows flexible business process configuration, secure information flow control and physical item track & trace in supply chains; and more importantly, it allows the synchronization of all of them. It enables the system and business processes to be fully automated and thus to improve collaboration efficiency. Some technologies developed in the proposed solution are elaborated in the following subsections.

3.2 UEI (Unified EPCIS interface)

As discussed earlier, the track & trace service in supply chains is based on RFID events capturing and querying through EPCIS (EPCIS, 2007), and sharing among participants in the EPCglobal network. In this solution, it is important to address how RFID events are captured into EPCIS and retrieved and used by B2Bi systems. The UEI is designed for this purpose as illustrated in Figure 2. It is one of the main components in the solution which facilitates the connection among EPC middleware, EPCIS, and the B2Bi gateway system.

The UEI consists of a CA (capture application) and an AA (accessing application). The CA serves capturing EPC events from RFID middleware and storing them to EPCIS as EPCIS events. The AA allows enterprise systems to query and retrieve EPCIS events by two ways, namely direct query and subscription. Web-services technologies are used in the UEI to enable loose-coupling among components and to make the design generic.

3.3 COT (Circle Of trust)

In a dynamic supply chain environment with track & trace services, multiple parties need to establish trust between each other to facilitate the secure exchange of sensitive information. In addition, a company may be participating in several supply chains at the same time as a partner collaborating with various companies. There are a lot of information/data sharing and exchange among them. It is critical to establish a trust relationship among partners for protecting business information/data flows in real-time in a dynamic environment. Currently,

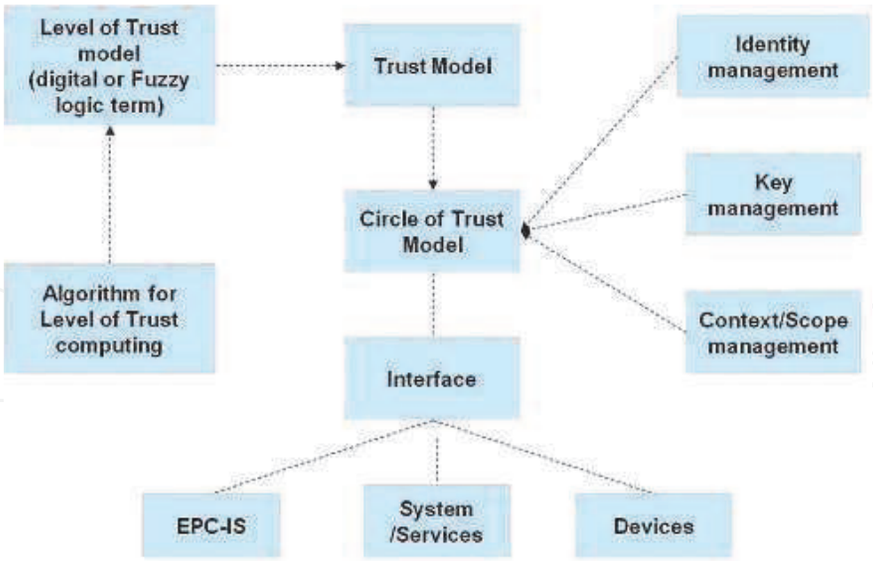


Fig. 3. COT (Circle Of Trust) model

there are mainly four kinds of existing models for trust establishment, namely centralized model, subordinate hierarchy, 2-party trust negotiation, and distributed trust evaluation (Maurer, 1996; Neuman & Ts'o, 1994; Xiong & Liu, 2004; Yu et al., 2000). However, they are not flexible enough to handle multiple parties in a dynamic supply chain environment yet lacking of security.

In our proposed solution, a COT (circle of trust) model is designed for the required purpose. The major components of the COT model consist of a trust algorithm, a trust model for two participants, a trust model of graph-based circle for multiple participants, and their control logic. Figure 3 illustrates the details of the COT model.

In short, the COT model can enable high level business information and low level RFID data to be shared and exchanged securely with different trust levels as specified among participants in a dynamically formed community in supply chains. Different trust levels will determine different levels of information access/exchange. Technical details of the COT design are not convenient to release here because it is under invention filing process.

3.4 Tag-reader security schemes

We design security schemes for protecting a tag at an end system level while it traverses a supply chain. In our schemes, a tag is marked initially at its manufacturer's site, whereas the mark is verified by the downstream partners of the supply chain. The mark is not a fixed one, but subject to changes (re-marked, and then re-verified) made by authorized partners. We adopt the standard security primitives (at the reader side) and tags that conform to specifications for EPC class 1 generation 2 RFID tags. At current stage, we developed three different protection schemes for protecting a tag, namely, a basic scheme, a batch scheme, and an undetachable scheme. The proposed schemes are secure, scalable, efficient, and easy to deploy. On one hand, it can resist un-authorized vendors from producing authentic tags quickly and massively thus raising the bar of difficulty for illegal behaviors. On the other hand, it stimulates the distributors or retailers of a supply chain on validating the goods/tags. This maintains the integrity of the tagged product in a supply chain within a complete EPCglobal network.

Our basic scheme is illustrated in Figure 4. When a tag is initialized at some partners in a supply chain, a security mark is generated and written into its user memory by a reader.

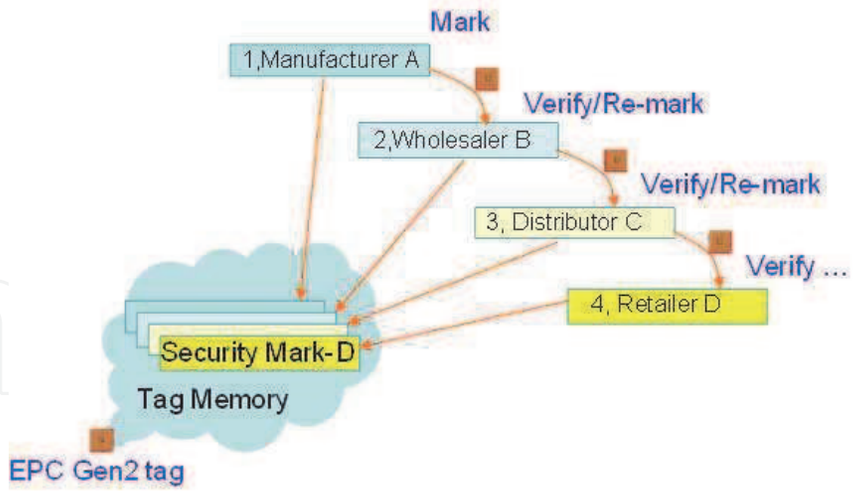


Fig. 4. Basic tag-reader security scheme (a tag is marked, verified, and re-marked when traversing different partners in a supply chain.)

The security mark is calculated based on the information such as tag identifier, reading point and time, and a secret key, all of which make it impossible to reversely disclose the relevant information from the mark. When the tag moves down to the next partner in the supply chain, an authorized reader can verify the mark and also leave its own mark. This process continues until it arrives in the destination of the supply chain. The tag-reader security scheme provides a secure, efficient and flexible verification in the track & trace process of a supply chain, as against risks such as counterfeiting.

Our batch scheme assumes a batch of tags attached to goods (e.g., packaged in a case), Instead of marking all the tags in a batch, the proposed method employs only a batch tag each time and marks it with our secure marking scheme. Moreover, besides the batch tag, an additional (randomly selected) tag, namely a pair-wise tag with the batch tag, is also securely marked. By pair-wising an additional tag at each step, we achieve efficient and secure tracing overall the supply chain.

Our undetachable scheme is suitable for the cases that require the presence of all tags for a complete verification. Our method makes these tags linked with each other so that any missing tag may cause a failed verification. To be efficient, we choose one tag in the set to be marked at each stage. Only by presenting all marks in the whole set can provide a complete verification.

In summary, all of the above methods make use of standard security primitives and conform to EPC class 1 generation 2 RFID tag specification. The proposed system is secure, scalable, efficient and easy to deploy. On the one hand, it can resist counterfeiting vendors from producing authentic tags quickly and massively. In other words, it raises the bar of hardness for the counterfeiting behaviors. On the other hand, it stimulates the distributors or retailers of a supply chain on validating the goods/tags.

3.5 Privacy-enhanced security scheme

In above schemes (subsection 3.4), when a participant of a supply chain leaves its mark on the tag, it also discloses its identity, which is not a good *privacy* property for this participant that may want to preserve its identity. We further devise a privacy enhanced tag protection scheme for marking tags and preserving the privacy of all participants in a secure RFID-based supply chain. This protection scheme provides participants with three privacy options, namely *public*, *limited*, and *private*. For the public option, the identity of a participant can be verified publicly

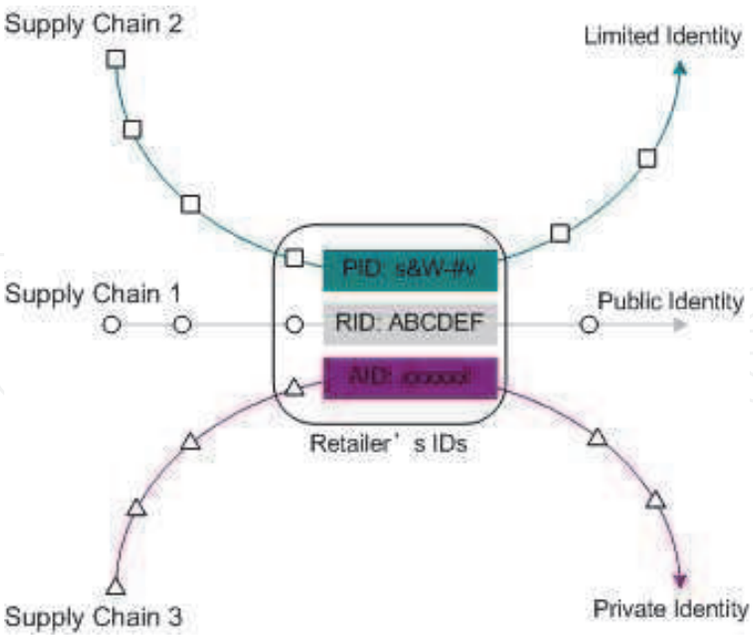


Fig. 5. Privacy-enhanced security scheme: a retailer assigns optional privacy (public, limited, or private) IDs for different supply chains

by any other participants in the supply chain; for the limited option, the verification can only be conducted by a small set of authorized participants; while for the private option, the identity of a participant cannot be disclosed unless being recovered by a legal authority in case of a dispute. Thus, a participant can freely choose a privacy option at any time for any goods in any supply chain. This makes the proposed scheme more secure, efficient and flexible.

For instance, as illustrated in Figure 5, we consider a participant (a retailer) traversing a number of supply chains with different privacy requirements. Firstly, upon receiving an item (with a tag attached) from Supply Chain 1, the retailer may consider it as a "non-privacy" case and continue using its original ID in the transaction documents as well as in our verification scheme. It chooses to put RID (e.g., $RID = ABCDEF$) into the tag in our tag marking equations. When the mark is recovered later on, this original ID will be posed to the verifier. Secondly, suppose that the item is received from Supply Chain 2 where the retailer's ID can be protected limitedly. The retailer uses a pseudo-ID (e.g., $PID = s\&W\text{-}\#v$) by employing the limited protection scheme. Thus, only authorized readers (in Supply Chain 2) can recover the original ID. Lastly, for Supply Chain 3 in which the retailer wants to hide itself against anyone but the trust authority, it can assign the AID (e.g., $AID = xxxxxx$) randomly to the tag protection scheme so that no one except the trust authority can recover its real identity.

4. Prototype implementation

A prototype is implemented for the above proposed solution. A sample application scenario of the prototype for OM (order management) business process is shown in Figure 6.

An OM business process involves two parties i.e., a manufacturer and a supplier. The higher lever business process between these two parties is managed by the B2Bi gateway system and includes the following steps:

- A manufacturer creates a PO (product order) and sends the PO to a supplier;
- The supplier acknowledges and confirms the PO from the manufacturer;

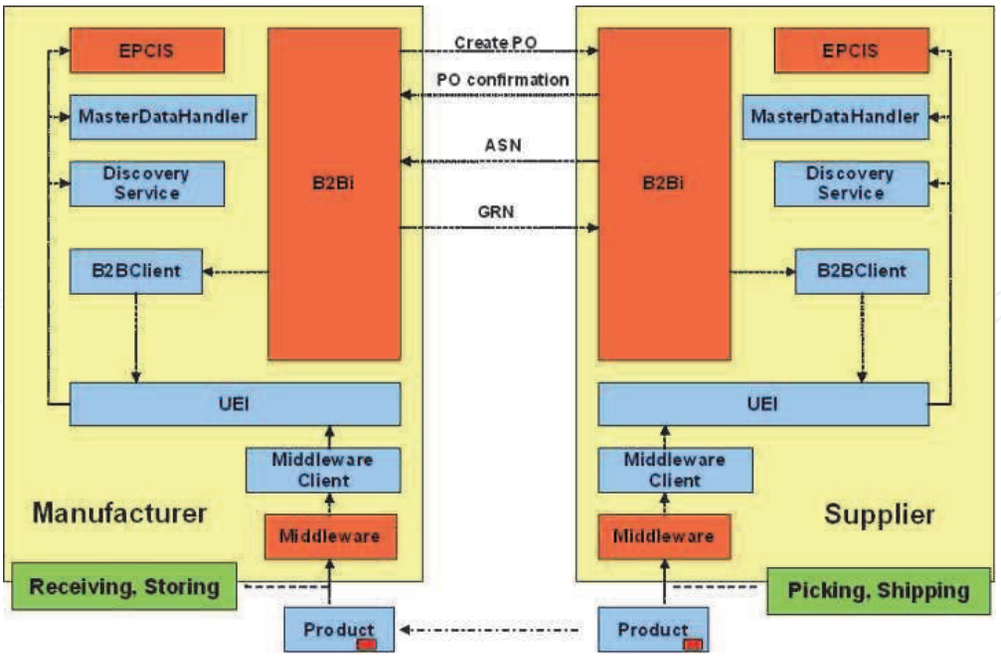


Fig. 6. An application scenario for OM processes

- The supplier sends an ASN (advance shipment notice) to the manufacturer;
- The manufacturer sends a GRN (goods receiving notice) the supplier upon receiving the products.

The physical product flow at the lower level is tracked and traced by RFID. The product states in the process are captured by a supplier when this product is picked up from a warehouse or shipped out, and by a manufacturer when it is received and stored into a warehouse.
In the solution prototype, the information flow and physical product flow are synchronized. The B2Bi process initiates the physical product flow which triggers and automates the business process. For example, when a PO is confirmed, the picking of products from a warehouse to fulfil the order is initiated at the supplier side; whereas at the manufacturer side, the reception and accept of products automatically trigger the GRN sending to the supplier.
In the prototype development and implementation, Accada EPCIS (Accada EPCIS, n.d.) is adopted as the EPCIS server. The EPCIS repository is deployed in MySQL database, while its capture and query interface services are deployed in Tomcat. The capture operation to Accada EPCIS repository is an HTTP-POST action where the data is in XML format (Accada EPCIS User Guide, n.d.). Because Accada's EPCIS repository implements the SOAP/HTTP binding for the query interface, it needs to construct a query for wrapping it into a SOAP request and sending it to the repository.
The data capture and configuration for EPCIS events in the OM process are such defined as shown in Figure 7. In real applications, GLN (global location number) can be used to identify RFID reading points. GRAI (global returnable asset identifier) and SSCC (serial shipping container code) are used for carton boxes and container tagging. The prototype is equipped with four logical readers, i.e., two readers named *s_picking* and *s_shipping* are used to simulate the picking and shipping out RFID gantries of suppliers, indicating business steps of "picking" and "shipping"; while the other two logic readers named *m_receiving* and *m_storing* are used to simulate the receiving and storing RFID gantries of manufacturers, representing business step of "receiving" and "storing". Figure 7 shows some other details, in which the

	Supplier		Manufacturer	
LogicReader	s_picking	s_shipping	m_receiving	m_storing
eventType	ObjectEvent	ObjectEvent	ObjectEvent	ObjectEvent
actionType	OBSERVE	OBSERVE	OBSERVE	OBSERVE
bizStep	urn:sg:pp:bizStep:picking	urn:sg:pp:bizStep:shipping	urn:sg:pp:bizStep:receiving	urn:sg:pp:bizStep:storing
readPoint	urn:sg:pp:rdPoint:001	urn:sg:pp:rdPoint:002	urn:sg:pp:rdPoint:101	urn:sg:pp:rdPoint:102
bizLocation	urn:sg:pp:bizLocation:SupplierWarehouse	urn:sg:pp:bizLocation:SupplierWarehouse	urn:sg:pp:bizLocation:ManufacturerWarehouse	urn:sg:pp:bizLocation:ManufacturerWarehouse
disposition	urn:sg:pp:disp:InProgress	urn:sg:pp:disp:InTransit	urn:sg:pp:disp:InProgress	urn:sg:pp:disp:InProgress

Fig. 7. Data capture in OM process.

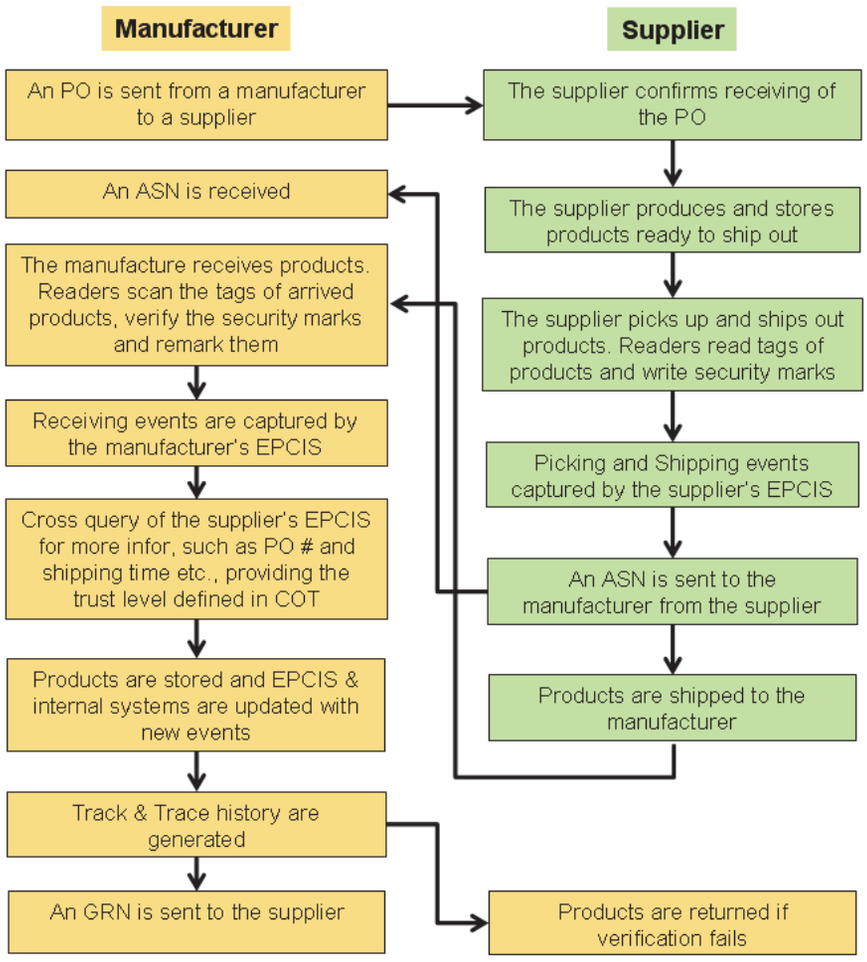


Fig. 8. Logic flow of the OM process enabled by the secure RFID-based track & trace solution

RFID tags used in the prototype are EPC class 1 generation 2 passive tags, and the readers and antennae are from Intermac and Symbol.
Figure 8 shows the logic flow of business information and physical products enabled by the secure RFID-based track & trace solution in the OM process of the prototype. The process

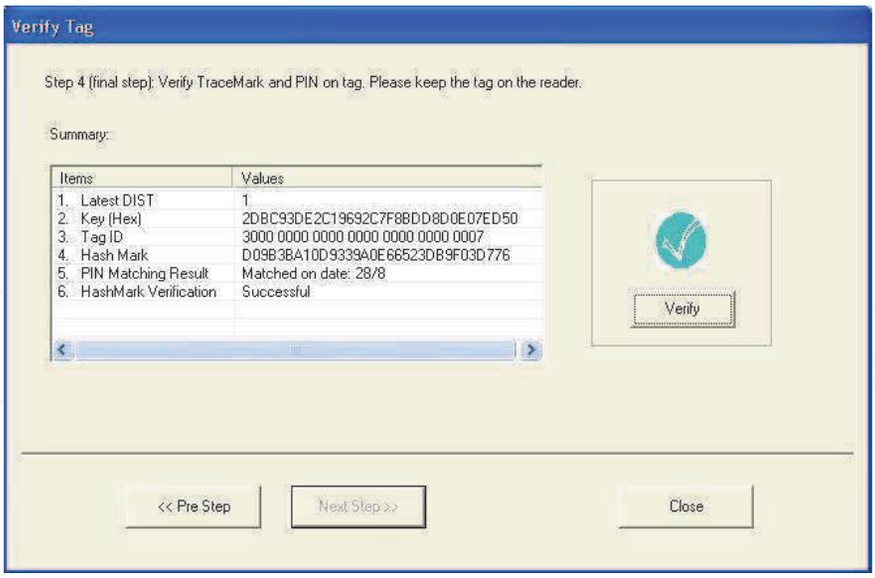


Fig. 9. Tag verification result

begins with a PO initiated and sent from a manufacturer to a supplier. After the supplier confirms the order, the products can be picked up from a warehouse to fulfill the order. After the products are shipped out, an ASN will be sent to the manufacture. During the processes off picking up and shipping out, each RFID tag attached on a product is read by a reader, at the same time a security mark is generated and written into the tag.

When the manufacturer receives the products, an RFID reader reads the tags on the products and checks the authentication of the products by verifying the security marks written in these tags by the supplier. Note that there are a number of ways to mark a tag and verify it later on. Without losing of generality, we hereby briefly introduce a basic scheme to illustrate the marking and verifying processes.

We assume a collision-free hash function $H(\cdot)$ that outputs an m-bit string on an ℓ-bit input message M, i.e., $H(M) : \{0,1\}^{\ell} \rightarrow \{0,1\}^{m}$. This hash function is to be implemented at the reader side. A mark is generated based on the identification information of the reader and the tag (RID and EPC, respectively), and the former mark. Thus, we can calculate the new mark as: $Mark_{new} = H(Mark_{old}||H(RID||EPC))$. In our prototype, we use SHA-1 as the secure hash function which generates a 160-bit hash value. However, we only keep the least significant 32 bits of the hash value as the mark to be stored in the user memory of the tag. We then generate the new PIN code for the tag to protect the memory[1] as: $PIN_{new} = H_k(Mark_{new})$, where k is a secret key only known to an authorized party and $H_k(\cdot)$ is a secure keyed hash function. To make the paper compact, we omit the details on key management, flexible marking processes and online/offline verification mechanisms. Thus far, the tag is assigned with a new PIN and a new mark before being shipped out.

At the receiving side, the verification is actually a reverse process of the generation process. The latest mark is read and checked against the PIN. If they are equal, the product is then accepted as successful verification and stored into the warehouse for storage; otherwise, the verification fails and the product is rejected. Figure 9 shows a case of successful verification result.

[1] Given a valid 32 bits access PIN, the tag is transitioned into what is called a "secured" state. Only at a "secured" state, the tag can be accessed for some restricted functions like read from the reserved memory bank and write to the user memory bank.

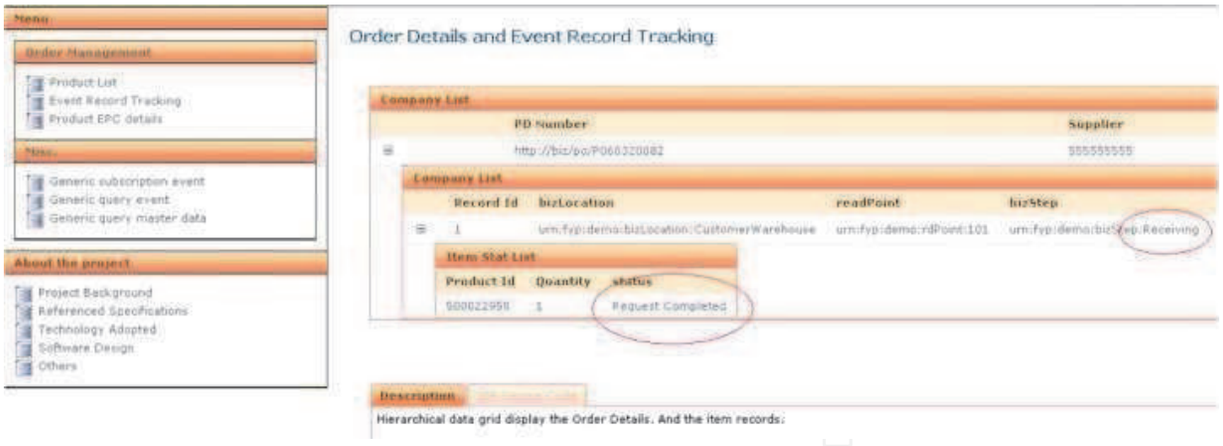


Fig. 10. Web GUI showing order details and RFID event tracking

The track & trace history can be generated through the query of EPCIS servers of both the manufacturer and supplier for further verification. The security ensures that the product manufacturer is from the right source. Additionally, to protect the privacy of the participants (e.g., manufacturers or suppliers) of a supply chain, we build an added optional privacy for those participants to choose. As discussed in subsection 3.5, a current participant can choose to use its real ID (RID) in the marking process, or to use a pseudo-ID (PID) or anonymous ID (AID) to hide its real identity. Thus, only authorized participants can recover the real identifier of a former participant.

Track & trace information and RFID events captured in EPCIS can also be used by an internal enterprise system of a company for decision making and business process control. For example, when the prototype is integrated with the inventory management system at the manufacturer side, the inventory level of the products can be automatically updated. Not only manufacturers but also suppliers can have in-time information of the inventory level of particular product, so that PO can be automatically generated at the manufacturer side or shipment can be automatically triggered at the supplier side when the inventory is below a certain critical preset level. Figure 10 shows a sample of Web GUI displaying the information details and RFID events tracking for an PO.

The system has undergone rigorous tests with some testing cases. The testing results show that products can be properly tracked and traced in an OM process. The security applied can eliminate the chances of counterfeiting products. The solution has significantly improved operation efficiency through the automated processes. Some companies have shown strong interests in our solution.

5. Conclusion

Given the current industrial demand for efficient and secure supply chain management, we have analyzed the issues on how to enable track & trace services (e.g., item identification, event capture and management, information storage, and information sharing among authorized parties) for RFID applications in an efficient and secure manner. We propose an RFID-based track & trace solution with security concern in supply chains based on EPCglobal standards. In this solution, a B2Bi gateway system is designed to manage high-level business information flows and processes, and EPCglobal network is leveraged on to manage the physical product flows. To address the security concern, we have proposed two levels of protection in our solution, namely (1) the COT for high-level business information sharing, and (2) the security schemes at reader-tag level for preserving participants' privacy. We have

shown that our solution can achieve secure information flow control for product track & trace services. We have also implemented a prototype of our solution for OM processes.
The working prototype of our solution has demonstrated high feasibility and efficiency in industrial scenarios under rigorous testing. It has attracted significant interests from industrial participants. While we are patenting the solution at this stage, we plan to commercialize the solution and make it a product of application package in the future.

6. Acknowledgment

This work is partly supported by A*Star SERC Grant No. 082 101 0022 in Singapore.

7. References

Accada EPCIS (n.d.).
URL: *http://www.accada.org/epcis/*

Accada EPCIS User Guide (n.d.).
URL: *http://www.accada.org/epcis/docs/userguide.html*

Angeles, R. (2005). RFID technologies: supply-chain applications and implementation issues, *Information Systems Management* 22(1): 51–65.

Auto-ID Centre at St. Gallen (2006). *Anti-counterfeiting and secure supply chain*.

Avoine, G. (n.d.). *Security and Privacy in RFID Systems*.
URL: *http://lasecwww.epfl.ch/~gavoine/rfid*

Chuang, M.-L. & Shaw, W.-H. (2007). RFID: integration stages in supply chain management, *IEEE Engineering Management Review* 35(2): 80–87.

Derakhshan, R., Orlowska, M. E. & Li, X. (2007). RFID data management: challenges and opportunities, *Proceedings of the 2007 IEEE International Conference on RFID*, Gravevine, TX, USA, pp. 175–182.

Diekmann, T., Melski, A. & Schumann, M. (2007). Data-on-network vs. data-on-tag: managing data in complex RFID environments, *Proceedings of the 40th Hawaii International Conference on System Sciences 2007*, Hawaii, USA.

E-Pedigree (n.d.).
URL: *http://www.axway.com/solutions/healthcare/epedigree.php*

EPCglobal network (n.d.).
URL: *http://www.epcglobalinc.org/about/media_centre/EPCglobal_Network_Demo.pdf*

EPCIS (2007). *EPCglobal EPC Information Services (EPCIS) Version 1.0 Specification*.
URL: *http://www.epcglobalinc.org/standards/epcis/epcis_1_0-standard-20070412.pdf*

Floerkemeier, C., Lampe, M. & Roduner, C. (2007). Facilitating RFID development with the accada prototyping platform, *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops(PerComW'07)*, While Plains, NY, USA, pp. 495–500.

Floerkemeier, C., Roduner, C. & Lampe, M. (2007). RFID application development with the accada middleware platform, *IEEE Systems Journal* 1(2): 82–94.

Huber, N. & Michael, K. (2007). Minimizing product shrinkage across the supply chain using radio frequency identification: a case study on a major australian retailer management, *Proceedings of the International Conference on Mobile Business 2007 (ICMB'07)*, Toronto, Canada, pp. 41–45.

Huo, Y. & Jiang, X. (2007). Research on CPFR and warehousing management: A method to enhance supply chain visibility, *Proceedings of the 2007 International Conference on*

Wireless Communications, Networking and Mobile Computing (WiCom 2007), Shanghai, China, pp. 4645–4648.

Imburgia, M. J. (2006). The role of RFID within EDI: building a competitive advantage in the supply chain, *Proceedings of the 2006 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI'06)*, Shanghai, China, pp. 1047–1052.

Intel (2005). Building the digital supply chain: an intel perspective, *Intel Solutions White Paper: Supply Chain Technology* .

Maurer, U. (1996). Modelling a public-key infrastructure, *Proceedings of 1996 European Symposium on Research in Computer Security (ESORICS '96)*, Rome, Italy, pp. 325–350.

Melski, A., Muller, J., Zeier, A. & Schumann, M. (2008). Improving supply chain visibility through RFID data, *Proceedings of the IEEE 24th International Conference on Data Engineering Workshop (ICDEW'08)*, Cancun, Mexico, pp. 102–103.

Michael, K. & McCathie, L. (2000). The pros and cons of RFID in supply chain management, *Proceedings of the 4th International Conference on Mobile Business (ICMB'05)*, Sydney, Australia, pp. 623–629.

Mintchell, G. (2002). It's automatic: automation shifts transmission assembly into high gear, *Control Engineering* 49(6): 12.

Neuman, B. C. & Ts'o, T. (1994). Kerberos: an authentication service for computer networks, *IEEE Communications Magazine* 32(9): 33–38.

RFID Journal (1983). *A Guide to Understanding RFID*.
URL: *http://www.rfidjournal.com/article/gettingstarted/*

Sheu, C., Lee, L. & Niehoff, B. (2006). A voluntary logistics security program and international supply chain partnership, *Supply Chain Management: An International Journal* 11(4): 363–374.

Song, S., Shim, T.-K. & Park, J.-H. (2006). Proxy based EPC track & trace service, *Proceedings of the 2006 IEEE International Conference on e-Business Engineering (ICEBE'06)*, Shanghai, China, pp. 528–531.

Straube, F., Vogeler, S. & Bensel, P. (2007). RFID-based supply chain event management, *Proceedings of the 1st Annual RFID Eurasia 2007*, Istanbul, Turkey, pp. 1–55.

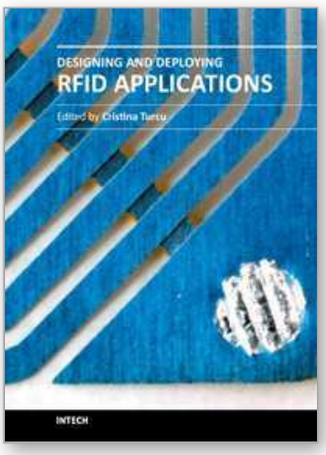
Tan, J. S. (2005). ISO focus, *The Magazine of the International Organization for Standardization* 2(2): 19–25.

Tan, P. S., Goh, A. E. S., Lee, S. S. G. & Lee, E. W. (2006). Issues and approaches to dynamic, service-oriented multi-enterprise collaboration, *Proceedings of 2006 IEEE International Conference on Industrial Informatics (INDIN '06)*, Singapore, pp. 399–404.

Thornton, F. (2006). RFID security, *Syngress* pp. 46–48.

Xiong, L. & Liu, L. (2004). PeerTrust: supporting reputation-based trust in peer-to-peer communities, *IEEE Transactions on Knowledge and Data Engineering (TKDE), Special Issue on Peer-to-Peer Based Data Management* 16(7): 843–857.

Yu, T., Ma, X. S. & Winslett, M. (2000). PRUNES: an efficient and complete strategy for automated trust negotiation over the internet, *Proceedings of the 7th ACM Conference on Computer and Communications Security (CCS 2000)*, Athens, Greece, pp. 210–219.



Designing and Deploying RFID Applications

Edited by Dr. Cristina Turcu

ISBN 978-953-307-265-4
Hard cover, 384 pages
Publisher InTech
Published online 15, June, 2011
Published in print edition June, 2011

Radio Frequency Identification (RFID), a method of remotely storing and receiving data using devices called RFID tags, brings many real business benefits to today world's organizations. Over the years, RFID research has resulted in many concrete achievements and also contributed to the creation of communities that bring scientists and engineers together with users. This book includes valuable research studies of the experienced scientists in the field of RFID, including most recent developments. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices, but also for engineers, researchers, industry personnel, and all possible candidates to produce new and valuable results in RFID domain.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Wei He, Yingjiu Li, Kevin Chiew, Tieyan Li and Eng Wah Lee (2011). A Solution with Security Concern for RFID-Based Track & Trace Services in EPCglobal-Enabled Supply, Designing and Deploying RFID Applications, Dr. Cristina Turcu (Ed.), ISBN: 978-953-307-265-4, InTech, Available from: http://www.intechopen.com/books/designing-and-deploying-rfid-applications/a-solution-with-security-concern-for-rfid-based-track-trace-services-in-epcglobal-enabled-supply

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821