RFID Product Authentication in EPCglobal Network

Tieyan Li[1] and Wei He[2]
[1]*Institute for Infocomm Research*
[2]*Singapore Institute of Manufacturing Technology*
Singapore

1. Introduction

Estimated by the International Chamber of Commerce (ICC) in 2006, nearly 5-7% of the global world trade is in counterfeit goods, with the counterfeit market being worth approximately US$600 billion annually. Existing technical countermeasures, such as holograms, smart cards, biometric markers and inks, represent a flexible portfolio of solutions against some counterfeiting behaviors. Recently, RFID was reportedly used in product authentication solutions to achieve a higher degree of automation when checking the authenticity of a product. For example, Euro banknotes are attached with RFID chips to com- bat counterfeiting by European Central Bank. The United States Food and Drug Administration (US FDA) has issued a report that endorses RFID as a tool to combat counterfeiting of pharmaceuticals. So far, these RFID-based solutions seem pretty promising [28]. With wide adoption of RFID technology witnessed in various industries, the future of RFID for product authentication purpose looks optimistic.

The main objective of a product authentication solution is to distinguish a genuine product from a fake one. The basic concept of applying RFID to product authentication lies in its original function of *identification*. Imagine a scenario in the future, in which every object will be attached with an RFID tag that contains a unique number belonging to the object. Once the tag is interrogated, the unique object number is emitted and interpreted by the back-end system to identify the object. If, for instance, all the unique object numbers are stored in a database, we can then check the database to verify the identity of an object. Unfortunately, identification alone is insufficient for solving the anti-counterfeiting problem. Problems exist in such a straightforward solution. For example, the unique object number can be eavesdropped and copied onto blank tags to produce clones, and the database would not be able to distinguish a legitimate tag from a cloned tag containing the same object number. There are many other ways to attack such a simplified identification system. For example, in a “tag removal and reapply” attack, counterfeiter can remove a tag from an authentic product, perform reverse engineering on the tag to extract out key attributes, and replicate these attributes onto blank tags.

In fact, product authentication has stronger requirements on security and needs a more complex system to implement. RFID-based product authentication solutions leverage on the benefits provided by the RFID tags and the back-end information system within the RFID-

Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria

enabled production and distribution flow. RFID tags can have certain security functions implemented in them, which raises the barrier for counterfeiting them. Furthermore, a counterfeiter would now need to counterfeit both the product and the tag, which raises his costs for counterfeiting. The back-end information system assists in drawing and maintaining real-time profile over the movements and activities of goods, thereby facilitating fast tracking of the goods. Essentially, a simplified product authentication system could consist of the following components - the object that is to be protected, the RFID tag that is attached onto the object, the RFID reader and the back-end system. Fig. 1 depicts the components in a generic RFID-enabled product authentication system.

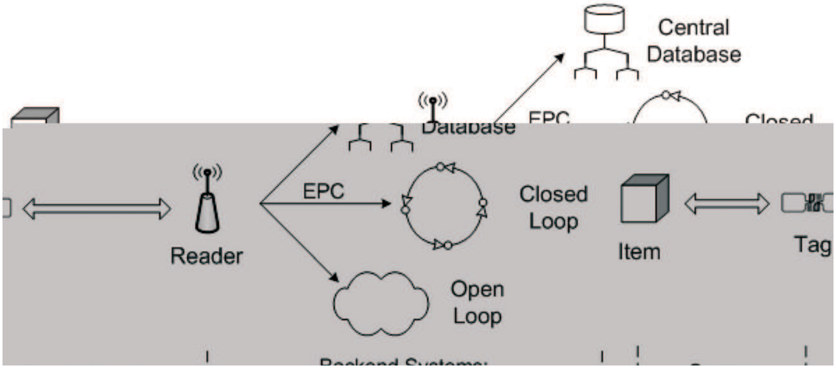


Fig. 1. RFID Product Authentication System.

Traditional product authentication methods rely on optical technologies such as watermarks, holograms and micro-printing to authenticate and verify goods. Other more advanced methods include the use of biological, chemical, or even nano-technologies (*e.g.*, using DNA markers, nano-level material characteristics, *etc.*). RFID technology, with the use of RFID tags that are attached to goods, opens up a new way to authenticate products. Like optical solutions, RFID technology authenticates the information stored on an external object (the RFID tag) rather than the product itself. If the RFID tag is authenticated, we claim that the product is authenticated too. To ensure the effectiveness of such a solution, the RFID tag needs to be securely bound to the product. Some secure binding mechanisms that are used in RFID systems will be discussed in greater detail in Section 5.

The authentication of an RFID tag is carried out through interactions with an RFID reader. RFID tag-to-reader authentication protocols resemble much of the existing two party authentication protocols based on challenge-response. In fact, a large number of research works conform to this principle and rest on symmetric or public key cryptographic primitives. We summarize these solutions in section 6. Unfortunately, these solutions do not provide a practical solution in realistic product authentication scenarios. This is because most RFID tags (for example, those being used on fast moving consumer goods) are too cheap to incorporate even lightweight cryptographic primitives. Currently, there exists a gap between what needs to be implemented for a substantial level of security on the tag and what could be realistically supported on the tag. Achieving proper authentication with low-cost RFID tags is still very challenging.

Besides the secure binding of an RFID tag to an object and the authentication between an RFID tag and a reader in the end system, another area that needs to be considered for a more complete product authentication solution is that of the back-end system. In a supply chain, as the goods are moved from one part of the world to another, many different activities can be taking place at each intermediate point. In fact, each intermediate point could potentially represent a point of vulnerability, where counterfeiting behavior might exist. Hence, in addition to checking at the end points, checks may need to be conducted at each intermediate point as well. This requires a systematic back-end support that connects itself to all the intermediate points. The simplest back-end system is a single standalone database that records up-to-date information on the goods by collecting data at each intermediate point. A verifier can then check the database for the details and/or status (*e.g.,* ID, some stored secret, current location, history, *etc.*) of a particular product, and based on this knowledge, determine the authenticity of the product. With a powerful database, there is a high chance that even a perfectly cloned tag can be detected. However, collecting and collating all relevant information into one single database is rather ambitious and unlikely to be scalable. How to disseminate these information into decentralized locations is very much desirable in both closed loop solutions and open loop solutions.

Product authentication solutions may be customized for different product distribution scenarios by considering hybrids involving the closed loop and open loop solutions. For example, an e-pedigree solution for combating counterfeit drugs is promoted and piloted as a major anti-counterfeiting effort of the US FDA. The potential high risk of drug misuse and increasing market of counterfeit drugs are the main drivers of this countermeasure. In general, for a product authentication solution to be feasible, the cost of implementing the solution must be lower than the losses suffered due to counterfeiting activities. Moreover, the cost of breaking the system should be high in order to provide a substantial barrier against counterfeiting behavior. Hence, when customizing a product authentication solution, we need to consider the cost-effectiveness of the customizations. Challenges arise when we face dynamic and complex application environments, such that each of them requires a different security level. In such cases, it would be difficult to design an optimal solution that fits all the requirements.

The rest of this chapter is organized as two parts: Part 1 introduces the security issues and countermeasures with RFID systems, which includes Section 2-the common threats that are faced by RFID systems; Section 3-the security and privacy issues with RFID systems; and Section 4-the countermeasures. Part 2 presents various RFID product authentication solutions including the secure binding of an RFID tag to the target object in Section 5; RFID authentication protocols in Section 6; and some network level solutions in Section 7 and 8. Finally, we conclude the chapter with some remarks.

PART 1: RFID SECURITY ISSUES AND COUNTERMEASURES

2. Common threats against RFID systems

The proliferation of RFID tags implies that RFID enabled systems might suffer from unintended risks. For example, unauthorized data collection, where attackers gather illicit information by either actively issuing queries to tags or passively eavesdropping on existing tag-reader communications. RFID threats refer to malicious user abuse in RFID context and are categorized as *Gather*, *Mimic*, and *Denial of Service (DoS)* [2]. *Gather* threats include *Skimming*, *Eavesdropping* and *Data tampering*; *Mimic* threats include *Spoofing*, *Cloning* and

Malicious code; *Denial of Service* threats include *Killing*, *Jamming* and *Shielding*. The details of these threats are explained as follows:

- *Skimming* data is the unauthorized access of reading of tag data. Data is read directly from the tag without the knowledge or acknowledgement of the tag holder.
- *Eavesdropping* is unauthorized listening/intercepting, through the use of radio receiving equipment, of an authorized transmission to monitor or record data between the tag and reader for the purpose(s) of: collecting raw transmissions to determine communications protocols and/or encryption; collecting the tag's data, or determining traffic patterns.
- *Data tampering* is unauthorized erasing of data to render the tag useless or changing of the data.
- *Spoofing* is defined as duplicating tag data and transmitting it to a reader. Data acquired from a tag is transmitted to a reader to mimic a legitimate source.
- *Cloning* is defined as duplicating data of one tag to another tag. Data acquired from a tag is written to an equivalent tag. A cloned tag is indistinguishable from its original tag.
- *Malicious code* insertion of a executable code/virus to corrupt the enterprise systems is hypothetically possible given a tag with sufficient memory and range.
- *Denial of Service* occurs when multiple tags or specially-designed tags are used to overwhelm a reader's capacity to differentiate tags, rendering the system inoperative. E.g., A blocker tag [19] is a kind of denial of service that confuses the interrogators so that they are unable to identify the individual tags.
- *Killing* of a tag (electronic or mechanical) is an operational threat in that the physical or electronic destruction of the tag deprives downstream users of the tag data.
- *Jamming* is the use of an electronic device to disrupt the reader's function.
- *Shielding* is the use of mechanical means to prevent reading of a tag.

Utilizing a combination of above threats, more serious attacks can be launched on RFID systems including unwanted location tracking of people and objects (by correlating RFID tag sightings from different RFID readers). Beyond these threats, RFID tags suffer from a variety of subtle attacks such as physical invasive attack, where an adversary physically compromises the inlay of an RFID tag and reads the memory for any information; and side channel attack, where an adversary uses timing analysis, power analysis or electro-magnetic analysis (e.g., [24]) to extract tag information. The design of RFID product authentication solutions shall consider appropriate countermeasures to defend against all possible threats.

3. RFID security and privacy issues

3.1 RFID security issues

In traditional IT systems, security means to prevent unauthorized reading and changing of data in the systems. RFID security means protecting the data on the tag, the data transmitted between the tag and reader, and even the data on the reader, to ensure it is accurate and safe from unauthorized access. RFID systems must employ mechanisms to achieve one or more of the security objectives such as confidentiality, integrity, availability, authentication and access control, to alleviate various security concerns. In the following, we describe the security objectives in details and show that meeting these security objectives eliminates the security threats posed by inherent weaknesses in low cost RFID systems.

Confidentiality involves a mechanism to keep information from all but those that are authorized to see it. In an RFID system, sensitive data such as a secret key needs to be kept confidential either when it is stored on tag or reader, or transferred between a reader and a tag.

Integrity ensures that information has not been altered by unauthorized or unknown means. Alteration in an RFID context may involve the capture, substitution, or deletion or insertion of information and the retransmission of that altered information to a reader or a tag.

Availability in RFID systems is important since readers need to be ready to detect tags that may enter their reading range at certain intervals of time. RFID systems meeting the availability criteria will ensure that there are services in place to thwart a DoS attack.

Authentication The objective of authentication in RFID context can be expressed as authenticating the devices involved (the tags and the reader) or in a supply chain application where the tags are used to label products, as product authentication. The objectives of tag and reader authentication and product authentication are discussed below.

- Tag/Reader Authentication: In RFID context, authentication simplifies to the proofs of the claimed identity of a tag or a reader. Authentication is an important RFID security measure for preventing counterfeiting behaviors. In some applications where perhaps the tag is an integral part of the tagged object, authentication of the tag may be adequate to guarantee the authenticity of the object to which it is associated.
- Product Authentication: In certain use cases where tags are placed as an external label to a high value item, authentication of the tag is not sufficient to guarantee the authenticity of the product to which the tag is attached. Since these tagged goods are subject to some specific attacks such as the "remove and reapply" attack. Hence, product authentication refers to the establishment of the authenticity of a product by the secure binding of the identity of a tag and the legitimacy of the product with an irrefutable link between the product and the tag that can be verified by a third party.

Access Control implies a mechanism by which a tag or a reader grants access or revokes the right to access some data or perform some operation in the interaction between RFID readers and tags. Generally tags will require access control mechanisms to prevent unauthorized access to tag contents.

To achieve these security objectives, RFID systems require solid implementations of appropriate security mechanisms. While security cannot be solely accomplished by these mechanisms, we stress that proper legislation, procedural techniques and enforcement of laws are also required.

3.2 RFID privacy issues

Compared with security properties, privacy is not easily defined, as many different interpretations can be found under a variety of real situations. It is not possible to enumerate every scenario in which RFID technology may potentially compromise personal privacy, because those scenarios depend on the application of RFID technology and on the personal information involved. However, most such scenarios have a common root cause stemming from the potential to automatically associate human identification information with object identification information. The objectives of a privacy preserving RFID system include anonymity and untraceability as explained below.

Anonymity is probably the concealment of the identity of a particular person involved in some processes, such as the purchasing of an item, visiting to a doctor or a cash transaction.

In RFID context, mitigating the problem of anonymity will involve the prevention of associating an EPC of an item with a particular individual. As the EPC can be used to obtain information regarding a particular process and that information may be associated with a particular person.

Untraceability is defined as a means by which the ability of other parties to learn or track the location of people, based on information obtained from RFID tags in possession of that person, is prevented. Hence, providing untraceability would need to involve the prevention of other parties from obtaining RFID tag data without the tag owners' consent; and/or the prevention of associating an EPC of an item with a particular individual; and/or preventing tags from emitting any kind of a unique identification information; etc.

Note that existing barcode system may have many of the same privacy risks, as the barcode can be read and cloned easily. However, RFID deployments present more potential vulnerabilities for those operations to be performed over the air and apparently obtrusive on an immense scale. It is good to know that privacy is a multi-dimensional issue involving many aspects. The successful implementation of privacy objectives above will not only require security mechanisms but will also require the formulation of public policies, legislation and the enforcement of the law by the relevant law enforcement agencies. Public policy is a vital aspect because the security mechanisms used to ensure privacy are most effective when implemented in conjunction with a well-defined policy. In fact, there are existing privacy polices that can be applied directly in RFID systems. They may however need to be clarified, refined or amended to cover aspects specific to RFID Systems.

4. Countermeasures

Toward these RFID security and privacy issues, many countermeasures have been proposed. To our knowledge, a couple of hundreds of research articles addressing RFID security and privacy problems have been published (refer to [17] for a literature survey). Countermeasures can be categorized from basic to sophisticated. In general, the more sophisticated the countermeasures, the more expensive the tag. Furthermore, not all countermeasures are applicable to all threats. No single countermeasure is 100% effective in all situations. Combinations of countermeasures can be used to improve RFID security. The countermeasures are categorized into 4 classes as follows.

4.1 Physical protections

RFID deployments have some practical limitations, which can be considered as effective protection mechanisms. Firstly, the tag-to-reader channel is assumed to be private, since the backscatter channel from the tag to the reader has a relatively shorter range (*e.g.,* several centimeters) than that of the forward channel. The low power of the backscatter channel relates to the fact that while the reader-to-tag communication can be eavesdropped from a long way away, it is only possible to eavesdrop on the tag-to-reader channel if the person is close to a legitimate reader. Thus, an attacker, not within the range, cannot get reply from the tag. In the case of the "clipped tag", the range can be further reduced by tearing off part of the tag's antenna. Alternatively, one can use Faraday cages or other shielding mechanisms to protect a tag within certain (safe operation) range.

Secondly, one can permanently deactivate a tag with physical tag removal or destruction. For example, one can use a momentary switch, electrical, or physical add-on to alter the readability of a tag. Thirdly, a level of security is provided by wafer programming, in which the True Write-Once-Read-Many (WORM) tags are programmed at the fabrication facility with a unique code that cannot be changed. For instance, wafer programming of a WORM device at the IC foundry prevents data from being inadvertently or clandestinely altered later in the supply chain. ISO/IEC 15963 [1] defines a unique tag identification (Tag ID) encoded by the I.C. manufacturer. A Tag ID shall be serialized in accordance with the standard to uniquely identify the chip and then locked by the I.C. manufacturer. The Tag ID can be used to authenticate that the chip is the original and not a copy, but only if one assumes that an attacker cannot obtain a tag in the unlocked state and program his own unique ID. In other words, all chip manufacturers have to agree to lock such memory at manufacture time - if any one chip manufacturer sells a tag in which this memory is unlocked, this countermeasure will not be effective.

Last but not least, the likely detection of physical presence of an attacker, who tries to hide between a legitimate reader and a tag in an active session, can defend some obvious man-in-the-middle attack. And technically, it is not easy to intercept a message and modify the message over the air in real-time without being detected, because of shared bearing medium plus the error detection codes that the protocols employ. This could make the possibility of launching active man-in-the-middle attacks low.

4.2 Access controls

Proper access control mechanisms can prevent the tags from certain unauthorized accesses. As one example, memory lock is typically used to disable the write/rewrite function on the tag or a given block of memory, and prevent unauthorized users from deleting or changing data or inserting unexpected data. In another example, the EPC UHF Gen2 specification defines a *Kill* command, which will totally disable a tag once issued. Another command, *Access*, is also defined to allow for either read or write operations to tag mem- ory after presenting a correct “Access Password”.

To provide privacy protection on tags' identifiers, a cloaking mechanism can be used to alter the transmitted EPC code to a different encoded code, thereby obfuscating the identity of the item to which the tag is attached. In the research field, one widely adopted assumption is that tags can support a one-way hash function, which incurs a family of researches on hash based ID variation protocols. For example, the very first one is the hash-lock scheme [29], which is improved with a randomized hash-lock scheme [33]. These are extended to a class of hash chain model [25] by embedding some hash functions in a tag. By changing the IDs or pseudonyms of a tag each time being queried, the *untraceability* property of the tag is protected.

4.3 Cryptographic countermeasures

Above we assume that the RFID tags can support some cryptographic primitives such as hash function. Traditional security systems rely on cryptographic solutions to achieve the security properties like confidentiality (by using encryption) or integrity (using authentication code). If an RFID tag can support cryptographic primitives like traditional security devices, we can just apply existing security solutions to solve the security problems with RFID tags. However, to implement symmetric ciphers, or even asymmetric ciphers on a low-cost RFID tag is still too heavy, because of the extreme resource constrains on those tags. A fair comparison in terms of power consumption, chip area, and clock cycles on the implementations of some standardized cryptographic algorithms (*e.g.,* SHA-256, SHA-1, MD5, AES-128, and ECC-192) on passive RFID tags is presented in [14].

The primary goal of implementing a cryptographic primitive in an RFID tag is to achieve (mutual) authentication of the tag and reader, as in contrary to the common sense (of applying encryption first). The objective of the authentication protocol is for the RFID reader to verify whether a tag knows a secret key. The reader first sends a challenge to the tag. The tag uses the challenge and its secret key as the inputs to some cryptographic function and computes a result. The response will then be checked by the reader, since the reader shares the same secret with the tag. More details of privacy preserving authentication protocols proposed so far are given in Section 6.

4.4 Active devices

To protect the wireless channels between the tag and the reader, we can alternatively choose some active countermeasures by using active tags or proxy devices. For instance, a `blocker' tag is proposed in [19] as a device that simulates RFID tags during tree-walking singulation. The blocker tag works by responding to singulation queries of a reader such that the reader is led to traverse the entire tree or a sub-tree. This way, the presence of actual tags that are to be protected is hidden from unauthorized readers.

In [26], a "selective RFID jamming" mechanism is proposed, in which a battery-powered mobile device is used to selectively transmit jamming signals to block responses from tags. The mobile device holds an access control list (ACL), which specifies the queries that may be allowed from readers. Based on the ACL, the device checks whether a query sent from a reader should be allowed. When a disallowed query is encountered, the device blocks off the tag response to the query by transmitting a jamming signal. Hence, unauthorized reading of a tag can be prevented.

Similarly, an "RFID Enhancer Proxy" (REP) is proposed in [27], which is a high power proxy device that can acquire the identity of RFID tags. Tags that have their identities acquired by the REP will remain in dormant mode until their identities are released back to them. The REP will then take part in the singulation process on their behalf. For security, the REP is equipped with the capability to authenticate readers to ensure that private information is only communicated to authorized readers.

With active countermeasures, we can alleviate some of the security and privacy problems encountered in RFID systems. However, non-trivial cost will be put on building such devices with comprehensive security functionalities.

PART 2: RFID PRODUCT AUTHENTICATION SOLUTIONS

5. Secure binding between tag and object

An RFID-enabled product authentication system typically authenticates the RFID tag attached to the product, instead of the product itself. Hence, the authenticity of the product can only be ensured if the RFID tag is securely bound to the product and is not tampered with. There are generally two categories of secure binding - physical binding and electronic binding.

Physical binding refers to the use of physical means (which may involve the use of mechanical or chemical mechanisms) to pack the RFID tag with the product tightly so that the binding is either impossible to be tampered with (tamper-resistant) or leaves clear evidence when the it has been tampered with (tamper-evident). An example of such binding is the electronic seal used to guarantee the integrity of containers [21]. Secure physical binding is used to defend against attacks based on removal and re-attachment of RFID tags.

Electronic binding refers to methods in which the unique fingerprint of a product is stored on the RFID tag. During authentication, an authentication device would be used to re-generate the fingerprint and compare it with the value stored on the RFID tag. The fingerprint is typically signed by the manufacturer of the product and can be verified by the authentication device. The digital signature guarantees the authenticity of the product, but not the authenticity of the tag, since the fingerprint, together with its signature, can be skimmed and copied onto other tags. It is possible that the cloned tag not only contains a part of authentic information, but also some other misleading information about this product. Thus, it is natural to bind the RFID tag with the product using methods proposed in [22] (the secure binding of object unique feature on tags) and [23] (the integration of tags on machine readable documents).

In [22], the authors proposed a method of secure binding that is achieved by signing on the unique features of the product, as well as that of the attached tag. For the tag, the Tag (or Transponder) IDentification number (TID) was used as the unique feature. The TID is essentially a globally assigned unique number that is programmed onto the tag by the chip manufacturer and set to a "locked" state. One cannot easily "unlock" the state and change the TID, although dedicated attackers might break it with some invasive attacks. The EPC is another globally assigned unique number for a specific product, but it is written by the product manufacturer and can be erased and overwritten with another EPC so that the tag can be re-used. In short, it is easy to clone the EPC, but difficult to clone the TID [4]. Hence, we consider the TID to be a good authenticator of an RFID tag that can be used to tighten the binding proposed in [22].

Here, we stress that there is no "absolute security". All security measures can very likely be broken given the time and resources. Nonetheless, for a product authentication solution to provide "good enough security", it should guarantee cost-effectiveness in preventing and detecting massive counterfeits in a timely manner. For the products that require very high level of security, strict security design techniques should be used and stringent tests and analysis should be carried out on those techniques before they can be put to deployment.

6. Tag-to-reader authentication

The RFID security research community has been paying a lot of attention on RFID authentication. Over several years, a large number of privacy-enhanced authentication protocols have been proposed in the literature. We focus our attention on tags that come with the capability to store some secret values, and we categorize these tags into three different classes based on the resources available on them - namely Crypto-tag, Light-tag and Gen2-tag. Crypto-tags support classic cryptographic primitives and hence, traditional authentication schemes can be applied here. Light-tags can not perform cryptographic functions, but can conduct bitwise operations such as XOR. Gen2-tags conforming to the EPC Class 1 Generation 2 specification [9], which can only perform 16 or 32 bits bitwise operations and are embedded with 16-bit PRNG and CRC functions.

6.1 Authentication with classic cryptographic primitives

The objective of such an authentication protocol is for the RFID reader to verify whether a Crypto-tag knows some secret key that is shared between the reader and the tag. The reader first sends a challenge to the tag. The tag uses the challenge and its secret key as inputs to some cryptographic function and computes a result, which is returned to the reader as a response to the challenge. The response will then be checked by the reader for verification. If the reader needs to authenticate a lot of tags, it has to store the IDs and secrets of all these tags, which is not scalable.

With regards to Crypto-tags, one widely-adopted assumption is that these tags can support a one-way hash function. The very first approach of using hash function was the hash-lock scheme, proposed by Sarma *et al.* [29]. Following that, a lot of RFID authentication protocols based on hash functions have been proposed. Besides these hash-based solutions, there were other solutions that require a Pseudo-Random Function (PRF) on a tag or make use of symmetric ciphers instead of hash functions. Another work [18] even assumed the use of public key cryptographic primitives, in which tags update their IDs with a re-encryption scheme. Although public key cryptography can reduce the key management overload, it is still too heavy to be implemented on medium-cost Crypto-tags.

Promisingly, there are some ongoing research efforts that lead to ultra-lightweight cipher designs. For example, the block cipher PRESENT-80 [6] features a compact implementation of only 1, 570 Gate Equivalents. Comparable lightweight stream ciphers, like Grain, has about 1, 300 Gate Equivalents [16]. More efficient hardware/software stream cipher designs are proposed and evaluated (currently within the ECRYPT project) for minimal footprint hardware implementation even in low-cost RFID tags.

6.2 Authentication with lightweight primitives

Light-tags are restricted to a much lower gate count (less than hundreds of GEs) than Crypto-tags for the implementation of security features. Some authentication schemes that do not rely on assumptions on classic cryptographic primitives have been proposed so that they can be supported on low-cost tags.

HB family of Authentication Protocols. In 2005, Weis *et al.* introduced the Hopper and Blum Protocol (HB) under the RFID setting [32]. The protocol can achieve sound security and can be implemented with extremely less circuits. Subsequently, Juels and Weis proposed a lightweight authentication protocol (HB$^+$) in [20]. The security of both the HB and HB$^+$ protocols are based on the Learning Parity with Noise (LPN) problem, whose hardness over random instances remains as an open question. However, Gilbert *et al.* showed that HB$^+$ is not secure against a simple man-in-the-middle attack [15]. To defend against such active attacks, Bringer *et al.* extended the protocols to HB^{++} protocol [5]. Later on, the HB family of protocols is enriched by several other complementary designs. But the protocols are still not mature enough to be applied in practical due to inherent security and performance pitfalls.

Ultra-Lightweight RFID Authentication Protocols. In 2003, Vajda and Buttyan presented a set of extremely-lightweight challenge-response authentication protocols [31] that are suitable for authenticating tags, but their protocols can be broken by a powerful adversary as was shown in [7]. Besides this, there are a number of approaches employing existing or self-designed mathematical primitives to build ultra-lightweight mutual authentication protocols for low-cost RFID tags. Unfortunately, almost all such light-weight protocols are being attacked in one way or another, and their practical deployment could be at risk unless strict security analysis is conducted beforehand.

6.3 Authentication with Gen2 functions

Some approaches, conforming to EPC Gen2 specifications [9] that rely solely on the specified functions like 16-bit CRC and PRNG, have also been proposed. For instance, in 2006, Duc *et* *al.*'s authentication protocols used 16- bit PRNG, CRC and XOR operations to replace the 128-bit strong cryptographic PRNG and MAC functions [8]. But the tradeoff of the replacement is the reduced (perhaps better than nothing) security. Thus far, all of the authentication protocols based on Gen2 functions are vulnerable even under a weak security model. Obviously, Gen2 tags provide almost no security at this moment, but the security issues are being investigated and improved in the next generation (Gen3) specification. With the fast development of lightweight cryptographic research and semiconductor technologies, we are optimistic on expecting lower-cost and stronger-security RFID tags being massively produced in the near future.

6.4 Further discussion

A secure tag-to-reader authentication scheme might enable a completely of- fline RFID product authentication solution. Suppose an RFID-tagged product is dispatched by the manufacturer, distributed along the supply chain, and finally comes under possession by an end user. The end user would verify the product with a standalone authentication device, which means that the end user can only rely on this device to check the authenticity of the product. In this case, the verifier scans the tag to obtain its ID and takes part in a challenge-response authentication protocol to prove that the tag owns some shared secret. As long as the secret on the tag is not disclosed, the authentic- ity of the tag is guaranteed. This can resist certain copycat attacks where all data except the secret of the tag is cloned on another tag.

In such a solution, the requirements on the authentication device are high. The device integrates a combination of functions including cryptographic algorithms, physical feature extraction functions and huge memory to store the relevant information for all tags. The end system is expensive due to the cost of tag, the binding and the authentication device. However, the system/network overhead is rather low in this ubiquitous setting.

7. Legacy product authentication solution

Above we described an extreme case of authentication involving an authentication device in the end system that can authenticate the tag and product without any online support. Such an ideal solution requires a secure binding between the RFID tag and the product (Section 5) and the tags must be capable of taking part in an authentication protocol (for example, the Crypto-tags in Section 6). The high cost of such an end system limits its application to supporting high-value products only. For ordinary products, a more economical anti-counterfeiting solution would have to be used and the cost-effectiveness of the solution has to be weighed carefully. To support high-volume usage, the item-level tags for ordinary products would have to be extremely low-cost and thus, it is unlikely that there would be sufficient resources to support security features.

Even when Crypto-tags are used, these tags could still be compromised by side channel attacks [24]. Hence, under some circumstances, there might be a need to rely on a back-end system for stronger authentication. This gives rise to the other extreme case, where a central database dominantly grasps all product information. Suppose the centralized database maintains all the product's activities during its life cycle, it can check the history of the product to see whether the information in the online request is logically sound (*e.g.*, a drug that is mandated to be sold only in US should not be available in South Africa). The result of this check is sent back to the verifier. In this case, the cost of the end system is relatively low, while the cost of maintaining the centralized back-end database is extremely high. The collection and analysis of the status information of a tag is not likely to be easy. Moreover, defining the granularity of the information collected is also important. Other challenging issues include the sensitivity and/or privacy of the data that is to be shared and the requirement for protecting against a single point of failure. Hence, this is another impractical solution since it does not scale well and potentially suffer from Distributed Denial of Service (DDoS) attacks and result in a single point of failure. Next, we shall study some distributed product authentication solutions that are practical, economical and reasonably scalable.

One good example of such a distributed solution is the existing **E- pedigree** solution in pharmaceutical supply chain. Initially promoted by the US FDA, the E-pedigree specification was then ratified by EPCglobal in the beginning of year 2007 [12]. The purpose of the new standard is to provide the pharmaceutical supply chain partners with a common format on collecting pedigree information and building their pedigree software platforms. The standard comprises instructions on how supply chain partners can create an E-pedigree, update information on it and digitally sign it. Many companies are accelerating their initiatives towards integrating E-pedigree pilots into existing legacy supply chain systems to enhance product integrity and further protect patient safety.

An E-pedigree system consists of all partners involved in the distribution of a medicine, including its manufacturer, the wholesaler, the retailer, and the pharmacy or any other entities administering or dispensing the medicine. These partners form a limited distributed system and establish some business relationship between each other (Public Key Infrastructure, or PKI, is typically assumed in this scenario for establishing entity trust relationships). As the medicine goes through the distribution path, it forms a growing certified chain of custody while each participant contributes to the E-pedigree. Here, we briefly describe how an E-pedigree system works:

1. 1. A medicine is produced by a manufacturer and attached with a unique RFID tag. The manufacturer starts to build the initial E-pedigree with the medicine's serial number, transaction information and other product- related information. Then, the E-pedigree is digitally signed with the pub- lic key of the manufacturer. The E-pedigree, together with the digital certificate of the manufacturer, is ready to be sent to a downstream partner (typically before the medicine is shipped out).
2. 2. On receiving the E-pedigree, the downstream partner first authenticates the E-pedigree by verifying the digital signature with the public key in the certificate. If the verification is successful, the partner continues to match the information on the E-pedigree with that on the product (assuming the medicine has been shipped in at this moment). A successful match completes the verification procedure. If the medicine is going to be shipped out, the partner needs to update the E-pedigree with its own information and signs on the renewed E-pedigree. Once again, the updated E-pedigree, together with the certificate of the partner, is ready to be transmitted to the next downstream partner in advance.
3. 3. The same procedure is repeated by every participant in the distribution path until the medicine reaches its destination. The procedures described above actually represent a typical (aggregated) document authentication flow. It does not really need to involve an RFID tag, except that a tag's ID is recorded in the E-pedigree for an additional match. In fact, the tag can be made more useful by strengthening its binding with the E-pedigree.

As in Section 4.1, we know that the tag could be a good authenticator due to its fabricated TID. A manufacturer can combine the tag's unique feature with the initial E-pedigree tightly by signing on them together and storing the signature on the tag (take for example TI's electronic marking scheme [30]). Then, the signature can be verified by the forthcoming partners. Under a secure access infrastructure, this piece of additional information can even be encrypted to ensure its confidentiality. The strong binding between the tag and the E-pedigree provides another layer of security.

The E-pedigree solution has been adopted rapidly in pharmaceutical supply chains since it is a natural extension of the legacy IT systems. Many of them already have existing internal, closed-loop RFID systems. Although the solution is promising, its success in real world applications will depend more on the non-technical issues such as privacy protection and legal agreements among multiple partners.

8. Product authentication with EPCglobal network

An E-pedigree solution revolves product authentication around a number of supply chain participants. However, it is more desirable that individual products can be tracked throughout the global supply chain to realize the greatest benefits of RFID technology. This inspires a globally available service - an **EPCglobal network** that offers another huge opportunity to obtain services from an open and standard interface (via Internet). As an essential part of the new supply chain management system, the emerging network enables real-time visibility of all products throughout the supply chain, improves efficiency in inventory control and reduces occurrences of product loss. Thus, EPCglobal network will provide a more open and efficient infrastructure for product authentication solutions.

8.1 EPCglobal network architecture

EPCglobal network resembles the Internet, but constructs an overlay of the Internet architecture. EPCglobal network architecture is shown in Fig. 2.

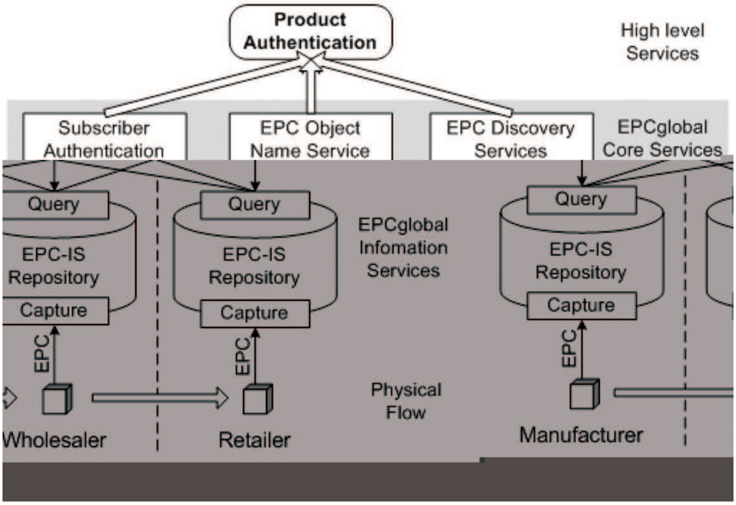


Fig. 2. EPCglobal Network Architecture.

The EPCglobal network [10] employs Electronic Product Code (EPC) to allow companies to track individual product through the global supply chain. The network provides (near) real-time tracking and product life cycle monitoring that make business processes more efficient. To realize these benefits, the EPCglobal committee specifies a standard framework to regulate the tracking, security and collaboration between different supply chain partners. The EPCglobal network manages RFID information through a number of core services: *Object Name Service (ONS)*, *EPC Information Services (EPC-IS)*, and *EPC Discovery Services (EPC-DS)*. Of which, the EPCglobal Architecture Framework identifies three possible ways to locate the informative service according to a specific EPC of an object:

- A party may use the Object Name Service (ONS) to locate the EPC-IS service of the EPCglobal Subscriber who commissioned the EPC of the object.
- A party may know in advance exactly where to find the information by means of being given the network address of the other party's EPC-IS service as part of a business agreement.
- A party may use Discovery Service (EPC-DS) to locate the EPC-IS services of trading partners that have information about the object, including partners other than the one who commissioned the EPC of the object.

Briefly, these core services can be described as below:

ONS: With an EPC that uniquely identifies a single product unit, one can query the ONS to look up the address of the product manufacturer's EPC-IS. Thus, ONS can be thought of as a lookup service that takes an EPC as input, and produces as output the address (in the form of a Uniform Resource Locator, or URL) of an EPC-IS repository designated and implemented by the EPC Manager of the EPC. This is similar to the Domain Name Service (DNS) on Internet, which matches the internet domain names to the IP addresses. From the EPC Manager's EPC-IS repository, one can then obtain detailed product information relating to the EPC.

EPC-IS: EPC-IS regulates the specification for supply chain partners to share EPC-related data. It controls the storage and retrieval of detailed product information on individual product units. It provides a standard data model to enable track and trace, product authentication, diversion detection, and other use cases involving supply chain partners across multiple industries. EPC-IS defines a capture interface and a query interface to obtain and share business event information. In fact, EPC-IS is the foundation for increasing visibility, accuracy, and automation throughout the supply chain.

EPC-DS: The product information might be stored not only at the manufacturer's site, but at different sites along the supply chain (for example the ship-in and ship-out information of a product might be stored at intermediate locations where the product transits). This raises the question of how a trading partner identifies and locates all of the other parties who may have relevant EPC-IS data. The EPC-DS provides the lookup service to all these fragmented sources of information. It serves as a search engine for the EPCglobal Network with restricted access, where subscribers can query it with an EPC to obtain a list of EPC-ISs that they can query directly for more detailed information.

EPC-SAS: Additionally, EPCglobal specifies the Certificate Profile [11] for building Subscriber Authentication Service (EPC-SAS). The authentication of entities (subscribers, services, physical devices) operating within the EPCglobal network serves as the foundation of any security function incorporated into the network. It is expected, however, that the X.509 authentication framework will be widely employed within the EPCglobal network. To ensure broad interoperability and rapid deployment while ensuring secure usage, the specification defines a profile of X.509 certificate issuance and usage by entities in the

EPCglobal network, which are based upon two Internet standards, defined in the IETF's PKIX Working Group, that have been well implemented, deployed and tested in many existing environments.

Integrating these core services, EPCglobal network can provide product life cycle visibility and traceability, which are the foundations of advanced product authentication solutions.

8.2 EPCglobal network threats and mitigations

As being composed by millions of individual RFID systems, the EPCglobal network will be much more complex than any standalone system. It may suffer many new or even more serious security threats coming from internal systems or existing Internet.We identify some of these threats in this section and point out possible mitigations.

ONS Security

ONS is similar to the Domain Name Service (DNS) on Internet, which matches the internet domain names to the IP addresses. An ONS server can be considered as a DNS server (typically, ONS can share the same server with DNS). Therefore, the security threats related to DNS server are also applicable to ONS. Security Threats such as file corruption, unauthorized updates, ONS cache poisoning, IP address spoofing, packet interception, query prediction and all threats from client to server or from server to server, are all to be addressed [13].

We shall take a similar way on protecting ONS as we did on securing DNS (e.g., using DNS Security Extensions-DNSSEC [3]). To protect ONS data, we need to provide security properties like confidentiality, origin authentication and data integrity, by using a brunch of security measures like key exchange protocols, digital signature and mutual authentication schemes. On safeguarding the systems, typically firewalls and intrusion detection systems are to be installed. Also, some good security practices such as secure backing-up of the files, applying proper read and write permissions; defining access control lists, are to be applied. However, if ONS server is to be implemented together with DNS server, privacy issues will arise and have to be investigated.

EPC-IS Security

EPC-IS repository can be considered as both a database server serving internal enterprise applications and a web server serving Internet requests. Thus, it suffers all threats coming from internal or outside. Some of them are traditional database threats like SQL injection, viruses, insider attacks; some are intrusion, worms, DoS attacks from Internet.

To protect the EPC-IS repository, we consider the whole set of system level security measures: authentication, authorization, access control and auditing. We rely on security tools like ant-virus softwares and hardwares, firewalls and intrusion detection systems, and backup mechanisms. The database SQL injection attack can be typically prevented by checking for buffer overflows, validating and sanitizing input data before passing it to SQL Query, disabling web script execution by outside sources, setting up appropriate access rights and enforcing access control policy, etc.

EPC-DS Security

EPC-DS provides visibility in the supply chain for all parties who have a right to know. The discovery of where data resides, the actual exchange of data, and the security policies governing these activities are all related. Of which, authentication and authorization are intimately connected with discovery. For example, merely discovering that one party in a supply chain has information about a particular EPC may or may not be privileged information subject to data authorization policies. Serving as a search engine for the EPCglobal Net- work with restricted access, EPC-DS server suffers both new threats from the subscribers (insider attacks) and common threats from the existing network infrastructure (similar to above threats on ONS and EPC-IS).

On the one hand, the EPC-DS infrastructure must define elegant access control and authentication policies to securely manage the information to be discovered and shared. Note that EPC-DS specification is still an on-going effort. On the other hand, all system level security measures (introduced above) have to be applied to protect EPC-DS servers.

EPC-SAS Security

EPC-SAS can be considered as a Trusted Third Party (TTP) to provide (web-based) information service. It shall have a higher level of security compared with above services. All subscribers' registration information are to be protected well and kept in secure storage. It is essential to authorize and authenticate legitimate subscribers based on their credentials and provide only the appropriate data that is relevant to them. Besides, EPC-SAS servers suffer all above common threats like intrusions, trojans, injections, and is especially sensitive to DoS attacks.

EPC-SAS depends on many traditional public key cryptographic mechanisms to authenticate the identity of an EPCglobal subscriber and issue credential to the subscriber. Then, without other prior arrangement, a subscriber can authenticate itself to any EPCglobal services providers and use those network services. Additionally, all system level security protection mechanisms (as introduced in EPC-IS security) have to be applied here. Specially, a distributed architecture is expected to avoid the central point of failure caused by DoS attacks.

8.3 EPCglobal network product authentication service

The ongoing efforts of the committee also includes the establishment of some specific business cases such as brand protection, product authentication and chain of custody. These use cases could utilize a combination of the core services described above. For example, the *EPC Product Authentication Service* (EPC-PAS), once regulated, might provide an all-in-one interface for the entities within a supply chain to authenticate a product.

While the EPC-PAS solution is very much desirable, it is not easy to regulate and could potentially encounter many obstacles when put under real operations. One of the major challenges in the design is the privacy of partners along the supply chain. There can be issues with regards to how much information a partner would want to keep with itself instead of sharing them with other partners; and how to define the minimal level of authentication-relevant information that should be shared. If there is insufficient information available on product visibility, then one cannot make a good judgement on the authenticity of a product.

In addition, the solution provided by EPC-PAS faces other limitations. Firstly, only authorized personnel can access the service, which is in conflict with our expectation towards a public service where everyone can authenticate a tagged product in hand. Secondly, even if the service is not provided to all, but to a group of subscribers, there could exist several desired service levels for different groups (*e.g.,* for ordinary users or for supply chain partners). Under such circumstances, how to define the privacy levels for different groups in a dynamic deployment setting would be a big issue. Thirdly, we need to think of how to prevent these services from abuse for malicious purposes, such as the tracking of a particular person. In addition, there is also a lack of practical experience on handling such a huge information system. Beyond that, there are also other issues like the likelihood of social acceptance and legislative support.

9. Conclusion

In this chapter, we presented a high level view on RFID-based product authentication solutions. Firstly, we exposed the threats that might be launched on RFID systems. We also investigate the security and privacy issues with the RFID systems and reviewed some countermeasures against the threats. As a promiscuous and ubiquitous technology, RFID presents unique security features and requirements. Assessing RFID's security and privacy risks requires a case-by-case analysis, due to the diversity of possible RFID deployments. The risk evaluation depends on the type of RFID used, the information stored on the chip, and the context in which the implementation is deployed. Accordingly, taking effective and balanced security measures to mitigate the risk is necessary to avoid jeopardizing RFID's usability. We stress that the success of RFID relies on all kinds of factors like professional devotion, social acceptance and legislative support.

Secondly, we pay attention on the security requirements and potential mitigations with EPCglobal network. With EPCglobal network, RFID not only acts as an additional authenticator for authenticating a product, but also provides an easy way to share a product's information throughout the global supply chain. Although the solutions are not perfect at this moment (and is unlikely to be in the near future), they look promising with the potential to act against massive counterfeits. The heartening thing is that the product authentication solutions are being piloted and deployed at many companies. With these precious experiences gained, implementors should be equipped with better knowledge and be in a better position to design optimal security solutions in their fight against counterfeiters.

10. References

[1] Information technology - Radio frequency identification for item management - Unique identification for RF tags. ISO/IEC 15963:2004.

[2] Information technology - Radio frequency identification for item management - Implementation guidelines - Part 4: RFID guideline on tag data security. ISO/IEC PDTR 24729-4:2008.

[3] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, DNS security introduction and requirements, *Request for Comments - RFC 4033*, March 2005.

[4] AIM Global Analysis: Counterfeit Tags, Jun. 2005.

[5] J. Bringer, H. Chabanne, and E. Dottax. *HB*$^{++}$: a Lightweight Authentication Protocol Secure against Some Attacks. In: *Proc. of SecPerU'06*, pp. 28-33. IEEE Computer Society Press, 2006.

[6] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe PRESENT: An Ultra-Lightweight Block Cipher. *Cryptographic Hardware and Embedded Systems - CHES 2007*, Vienna, Austria, Sept. 2007.

[7] B. Defend, K. Fu, and A. Juels. Cryptanalysis of two lightweight RFID authentication schemes. In *Fourth IEEE International Workshop on Pervasive Computing and Communication Security (PerSec) Workshop*, March 2007.

[8] D.N. Duc, J. Park, H. Lee, K. Kim, Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning, In *The 2006 Symposium on Cryptography and Information Security*, 2006.

[9] EPCglobal Inc., EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz Version 1.1.0, EPCglobal Standards, Oct. 2007.

[10] EPCglobal Inc., Architecture Framework Standard v1.0 http: //www.epcglobalinc.org/ standards/architecture/Architecture 1 0-StandardApproved-20050701.pdf

[11] EPCglobal Inc., EPCglobal Certificate Profile v1.0.1 http://www.epcglobalinc.org/ standards/cert/cert 1 0 1-standard-20080514.pdf

[12] EPCglobal Inc., Pedigree Standard v1.0 http://www.epcglobalinc.org/standards/pedigree/Pedigree 1 0-StandardRatified-20070105.pdf

[13] B. Fabian, O. Gunther, and S. Spiekermann. Security Analysis of the Object Name Service for RFID. In: *Proc. of SecPerU'05*, IEEE Computer Society Press, 2005.

[14] M. Feldhofer, J. Wolkerstorfer. Strong Crypto for RFID Tags-a Comparison of Low-Power Hardware Implementations, In: *IEEE International Symposium on Circuits and Systems (ISCAS 2007)*, pp.1839-1842, New Orleans, USA, May 27-30, 2007.

[15] H. Gilbert, M. Bobshaw, H. Silbert, An Active Attack against HB^+-A Probable Secure Lightweight Authentication Protocol, *Cryptology ePrint Archive, Report 2005/237*, 2007.

[16] T. Good, W. Chelton, and M. Benaissa. Hardware Results for Selected Stream Cipher Candidates. In *SASC 2007*, February 2007.

[17] A. Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2): 381-394, Feb. 2006.

[18] A. Juels and R. Pappu. Squealing euros: Privacy protection in RFID-enabled banknotes. In: *Proc. of FC'03*, LNCS 2742, pp. 103-121. Springer-Verlag, 2003.

[19] A. Juels, R. L. Rivest, and M. Szydlo, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, in *Proc. of ACM Conference on Computer and Communications Security (ACM CCS) '03*, pp. 103-111, Oct 2003.

[20] A. Juels and S. Weis. Authenticating pervasive devices with human protocols. In: *Proc. of CRYPTO'05*, LNCS 3126, pp. 293-308. Springer-Verlag, 2005.

[21] R. Johnston, Tamper-Indicating Seals, *American Scientist*, Nov-Dec 2005.

[22] Z. Nochta, T. Staake, E. Fleisch, Product Specific Security Features Based on RFID Technology. In *Proceedings of the International Symposium on Applica- tions and the Internet* Workshops. IEEE Computer Society, 2006.

[23] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch, Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. In *Conference on Ambient Intelligence Developments - AmID,* Sophia-Antipolis, France, September 2006.

[24] Y. Oren and A. Shamir. Remote Password Extraction from RFID Tags. In: *IEEE Transactions on Computers*, 56(9):1292-1296, 2007.

[25] M. Ohkubo, K. Suzuki, and S. Kinoshita. "Cryptographic approach to privacy- friendly tags." In: *Proc. of RFID Privacy Workshop*, 2003.

[26] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags, in *Proc. of the 13th International Workshop on Security Protocols*, Apr 2005.

[27] A. Juels, P. Syverson, and D. Bailey, High-Power Proxies for Enhancing RFID Privacy and Utility, in *Proc. of the 5th Workshop on Privacy Enhancing Technologies (PET '05)*, 2005.

[28] T. Staake, F. Thiesse, E. Fleisch, Extending the EPC Network-The Potential of RFID in Anti-Counterfeiting. In *Proceedings of the 2005 ACM symposium on Applied computing*, pp. 1607-1612. New York (NY): ACM Press.

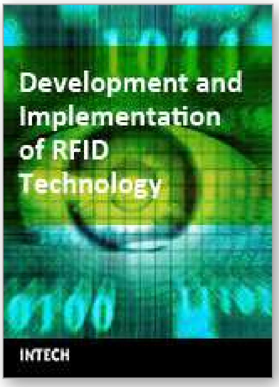
[29] S. Sarma, S. Weis, and D. Engels. RFID systems and security and privacy implications. In: *Proc. of CHES'02*, LNCS 2523, pp. 454-469. Springer-Verlag, 2003.

[30] Texas Instruments and VeriSign Inc.: Securing the pharmaceutical supply chain with RFID and public-key infrastructure technologies. *Whitepaper*, 2005.

[31] I. Vajda and L. Buttyan. Lightweight authentication protocols for low-cost RFID tags. In: *Proc. of UBICOMP'03*, 2003.

[32] S. Weis. Security parallels between people and pervasive devices. In: *Proc. of PERSEC'05*, pp. 105-109. IEEE Computer Society Press, 2005.

[33] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In: *Proc. of 1st Int. Conf. on Security in Pervasive Computing*, LNCS 2802, pp. 201-212. Springer-Verlag, 2003.



Development and Implementation of RFID Technology
Edited by Cristina Turcu

ISBN 978-3-902613-54-7
Hard cover, 450 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. 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 experienced technical professionals and RFID aficionados.

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