# Trust and Security in RFID-Based Product Authentication Systems

Mikko O. Lehtonen, *Member, IEEE*, Florian Michahelles, and Elgar Fleisch

***Abstract*—Product authentication is needed to detect counterfeit products and to prevent them from entering the distribution channels of genuine products. Security is a critical property of product authentication systems. In this paper, we study trust and security in RFID-based product authentication systems. We first present a formal definition for product authentication process and then derive the general chain of trust as well as functional and nonfunctional security requirements for product authentication. Most of the scientific literature that covers the topic focuses on cryptographic tag authentication only. This paper, however, provides a broader view including also other known approaches, most notably location-based authentication. To derive the functional security requirements, we employ the concept of misuse cases that extends the use case paradigm well known in the field of requirements engineering. We argue that the level of security of any RFID-based product authentication application is determined by how it fulfills the derived set of functional and nonfunctional requirements. The security of different RFID-based product authentication approaches is analyzed. To study how RFID supports secure product authentication in practice, we investigate how the current EPC standards conform to the functional security requirements of product authentication and show how the unaddressed requirements could be fulfilled. The benefits of implementing a service that detects the cloned tags in the level of the network's core services are identified.**

***Index Terms*—Product authentication, product codes, radio frequency identification (RFID), security, system analysis and design.**

## I. Introduction

THERE is an ever growing risk that physical products are not what they claim they are. Along with legally run businesses, there is a full-size underground industry that produces and distributes illegal copies of virtually all kinds of products [17]. As an illustration of the extent of the problem, the German customs secured 117 containers of counterfeit and pirate products in the Hamburg port between August and November 2006, constituting probably the world's largest counterfeit seizure. The infringing goods included, for example, more than one million pairs of counterfeit Nike, Adidas, and Puma sports shoes, counterfeit toys, and over 100 000 counterfeit textiles, with a corresponding overall original retail value of over 383 million euros [24]. In total, the European customs seize up to a hundred million counterfeit and pirated goods every year [49].

Companies can launch countermeasures against counterfeiting at different fronts. These comprise legal actions, consumer education, private investigations, and technological countermeasures. The first three of these are rather inefficient. They are expensive and slow and can only address a part of the problem. In addition, counterfeiters are adaptive and can continue or restart their businesses after these measures. The technological countermeasures, however, have the potential to destroy the counterfeiters' business model: Today mass products flow anonymously and counterfeiters can "free-ride" the supply chain of genuine products. If this licit supply chain would be secured by giving each item an identity and by implementing reliable ways to prove these identities, distributing counterfeit products through this channel would become substantially harder—and economically unattractive.

With the development of mass serialization and Automatic Identification (Auto-ID) technologies, in particular radio-frequency identification (RFID), the technical countermeasures have enjoyed an increasing importance. There are three major motivations for using RFID in product authentication. First, RFID has recognized potential in anti-counterfeiting [18] because it allows for many ways to securely authenticate products [10]. Different RFID-based product authentication approaches are presented in detail in Section II. Second, RFID will be adopted anyway in many applications due to its benefits in retail industry and logistics, so also the potential for secure product authentication will be given. A market study of GS1 and LogicaCMG [19] illustrates the expected adoption rate of RFID in Europe. The study estimates that the number of RFID tags purchased annually in 5, 10, and 15 years in Europe alone is 3 billion, 22 billion, and 86 billion tags, respectively. The same study concludes that the most growth is coming from tagging of (high-value) items, instead of pallets or cases, and the adoption is driven by retail and consumer goods industry. One of the objectives of our study is to identify how the technology should be implemented so that all these tagged products could be securely authenticated with relatively small additional investments. The third motivation to use RFID in product authentication is the emergence of near field communication (NFC) technology. NFC denotes a technology that allows for integrating RFID functionality in a mobile phone, making it both a RFID transponder and a reader device [21]. According to predictions of ABI research, in the year 2011 a total of 450

Manuscript received March 31, 2007; revised September 2, 2007. This work was supported in part by two European research projects of the sixth framework program (IST): building radio frequency identification solutions for the global environment (BRIDGE) Project 033546 and stop tampering of products (SToP) Project 034144.

M. O. Lehtonen and F. Michahelles are with the Swiss Federal Institute of Technology, ETH Zurich, Information Management, 8032 Zurich, Switzerland (e-mail: mlehtonen@ethz.ch; mikkol@ethz.ch; fmichahelles@ethz.ch).

E. Fleisch is with the Swiss Federal Institute of Technology, ETH Zurich, Information Management, 8032 Zurich, Switzerland and University of St.Gallen, Institute of Technology Management, 9000 St. Gallen, Switzerland (e-mail: elgar.fleisch@ethz.ch).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSYST.2007.909820

million handsets (30% of all handsets) will be NFC-enabled [20]. Because the NFC handsets might become the world's largest RFID reader infrastructure in the future, solving the interoperability problems between NFC and other RFID standards, EPC in particular,[1] is of great interest for the industry and actively addressed by both practitioners [22] and the scientific community [23]. If these two technologies will converge, also the end-users and consumers could take part in verifying the authenticity of tagged products. In addition, this could help changing the consumers' risk perception towards RFID [42] by showing them what concrete benefits the technology can give them.

In this paper, we study trust and security in authentication of RFID tagged products. Overall, the existing theoretical knowledge of level of security different product authentication approaches provide or different products require within the context of product counterfeiting is sparse. In particular, formal definitions for level of confidence in product authentication or location-based authentication do not exist, though these concepts have high practical importance. Our goal is not to contribute towards improved RFID tag security, but towards secure overall systems to authenticate tagged products. Therefore, an important contribution is to derive the general chain of trust as well as security requirements of RFID-based product authentication. The set of functional and nonfunctional requirements is meant for designers of product authentication systems and it also can be used to benchmark the level of security of existing systems. Most related scientific literature covers cryptographic tag authentication only, but companies who want to authenticate their tagged products have no such bias. Therefore, we present a broader view of how RFID can be used to implement secure product authentication. Understanding the security requirements of different approaches is important because there are many different proposed RFID-based product authentication approaches (e.g., [10]) but so far no methodology to validate and compare the level of security different approaches provide.

This paper is organized as follows. In Section II, we review related scholarly contributions and distinguish three distinct approaches how products can be securely authenticated plus a fourth category of techniques that cannot provide a comparable level of security. In Section III, we present, first, formal definitions for product authentication process and location-based authentication. Section IV presents the nonfunctional security requirements for product authentication. To derive the functional security requirements in Section V, we apply the misuse case methodology proposed by Sindre and Opdahl [2]. In Section VII, we analyze the security of different RFID-based product authentication approaches from the point of view of the counterfeiter by arguing that the level of security depends on how well the derived requirements are met. In Section VIII, we analyze RFID-based product authentication in practice by presenting how the current EPC network [30], which is the most important standard for networked RFID, conforms to the derived set of requirements. We finish with discussion and conclusions.

[1][Online]. Available: http://www.epcglobalinc.org

## II. Related Work

### A. Authentication and Level of Security

Together with integrity, confidentiality, nonrepudiation, and availability, authentication is one of the common security services. Product authentication has not been formally defined in the scientific community, so we review general definitions for authentication. Kurose and Ross [31] define authentication as the process of proving one's identity to someone else. Schneider [29] defines authentication in cryptography such that it should be possible for the receiver of a message to ascertain its origin. Authentication can be based on different factors, namely what the subject has, what the subject is, what the subject knows, or a combination thereof.

Measuring the level of security is challenging. Schneider [52] proposed that the level of security can be quantified by estimating the cost to break (CTB) of a system that is the lowest expected cost for anyone to discover and exploit a vulnerability in that system. CTB allows replication of the cost/benefit analysis of an adversary, for instance, a system that cannot be broken for less than $1000 is strong enough to protect an asset worth of $100 from an adversary seeking financial gain. This method has good potential in evaluating the level of security of product authentication systems since we can assume that adversaries seek financial gain and the value of the loot can be estimated, but so far no tools exist to evaluate CTB of product authentication techniques. Moreover, Schneider [53] argues that the amount of security that is needed to stop a thief depends also on the probability of getting caught. This can be perceived from the fact that burglars are less reluctant to target houses with an alarm system that increase the burglar's risk. This reasoning is employed also to secure supply chains from counterfeit products, for example, by mandating the use of electronic pedigrees for medicines (e.g., [54]) where all transactions are signed; if an illicit actor does not update a pedigree file, the corresponding product is not valid, and if he does update the pedigree, the illicit actions can potentially be later traced.

### B. RFID in Product Authentication

There are different approaches how RFID tagged products can be authenticated. Based on the authentication factors (see Section II-A), we can categorize known and secure RFID-based approaches into product authentication based on what the product is (object-specific features-based authentication), based on what the product has (tag authentication), and based on where the product is (location-based authentication).[2] In addition, there are techniques that can be used to authenticate products in certain cases but that do not provide a comparable level of security than the first three approaches. We refer to these approaches as weak authentication. We present a short review of RFID-based product authentication techniques of these four categories in the following. A more comprehensive review is given by Lehtonen *et al.* [10].

*1) Object-Specific Features-Based Authentication:* The first general approach to authenticate products is to make the

[2]Product authentication based on what the product knows in included in tag authentication.

products themselves hard to clone. Nochta *et al.* proposed a technique to authenticate tagged products based on so called object-specific features [9]. In their approach, information about physical or chemical features that are unique to that particular product (e.g., weight, electric resistance, geometrics, a serial number printed on the product itself or its packaging, unique patterns in surface material, material concentrations, etc.) is stored on the tag. These object-specific features are denoted *unique product identifier*. The RFID tag stores a signature value that is computed from the unique product identifier, unique tag identifier, signature method, and brand owner's validation key. In this way, an entity who knows the public validation key can verify that the couplet *unique tag identifier* + *unique product identifier* is issued by the brand owner. It follows that the identity of a product can be verified by measuring the object-specific features of the product under study and comparing them to the digitally signed unique product identifier data on the tag.

The reasoning behind this approach is that only one product has that particular feature value; if a genuine tag is put to a counterfeit product, the mismatch between the feature value on tag and the product's real feature value is detected. Another benefit of this approach compared to cryptographic tag authentication is that the tag only needs to store data, which keeps the tag price low, but the cost and effort to check one product high.

*2) Tag Authentication:* The second general approach to authenticate products is to use security features that are hard to clone. RFID tags can be protected from cloning in different ways and many tag authentication protocols have been proposed in the literature. The general property of these protocols is that a reader device (or back-end) verifies if a tag knows a certain secret key. The secret key is never transmitted in clear text over the radio-frequency interface which can be eavesdropped. Knowledge of the key is typically verified through a challenge-response protocol.

Since the cost and computing resources of RFID tags are limited, the protocols have to provide a tradeoff between security, cost, and performance. Proposed low-cost tag authentication protocols are based on cryptographic primitives like bitwise operations and pseudo-random numbers (e.g., [32]–[34]) or hash-functions (e.g., [35]–[37]). Also, different symmetric encryption-based tag authentication protocols exist, for example, based on advanced encryption standard (AES) (e.g., [38]–[40]). Conventional symmetric-key authentication protocol between $\mathrm{A}$ and $\mathrm{B}$ can be formalized as follows:

1) $\mathrm{B} \rightarrow \mathrm{A}$: "I am B";
2) $\mathrm{A} \rightarrow \mathrm{B}$: ch;
3) $\mathrm{B} \rightarrow \mathrm{A}$: $\mathrm{E}_{\mathrm{A-B}}(\mathrm{ch})$;
4) A (verification): $\mathrm{D}_{\mathrm{A-B}}(\mathrm{E}_{\mathrm{A-B}}(\mathrm{ch})) = \mathrm{ch}$.

Here, $\mathrm{E}_{\mathrm{A-B}}$ denotes encryption with the symmetric secret key shared by $\mathrm{A}$ and $\mathrm{B}$, and $\mathrm{D}_{\mathrm{A-B}}$ denotes decryption with the same key. Asymmetric-key authentication protocol differs in the way the verifier $\mathrm{A}$ decrypts the response. When $\mathrm{E}^{-\mathrm{A}}$ denotes encrypting with the secret key of $\mathrm{A}$, and $\mathrm{D}^{+\mathrm{A}}$ decryption with the public key of $\mathrm{A}$, the conventional asymmetric-key authentication protocol can be formalized as follows:

1) $\mathrm{B} \rightarrow \mathrm{A}$: "I am B";
2) $\mathrm{A} \rightarrow \mathrm{B}$: ch;
3) $\mathrm{B} \rightarrow \mathrm{A}$: $\mathrm{E}^{-\mathrm{A}}(\mathrm{ch})$;
4) A (verification): $\mathrm{D}^{+\mathrm{A}}(\mathrm{E}^{-\mathrm{A}}(\mathrm{ch})) = \mathrm{ch}$.

Asymmetric encryption is currently very challenging on RFID tags, but due to advances in elliptic curve cryptography (ECC) it is becoming more and more feasible. ECC allows for less computationally intense encryption for resource-limited devices (e.g., [56]). To illustrate the increased computational efficiency, ECC has enabled implementing the world's smallest SSL Web Server in shape and size of a quarter dollar coin [57]. Wolkerstorfer [55] has shown that ECC could be implemented by respecting the strict power and area constraints of RFID tags. Furthermore, Batina *et al.* [58] have demonstrated how authentication protocols based on elliptic curves can be implemented on a constrained device such as an RFID tag requiring between 8500 and 14 000 gates, depending on the implementation characteristics.

Another way to implement a secret key on the RFID tag is to use a physical unclonable function (PUF). The PUF is a one-way function that allows for the calculation of unique responses using only some hundreds of logical gates without any costly cryptographic primitives [41]. In order to make the use of eavesdropped responses infeasible, several challenge-response pairs have to be stored in a database. It has been estimated that about 800 challenge response pairs are sufficient to distinguish $10^9$ chips with the probability of about $1 - 7 \times 10^{12}$ [26]. When $\mathrm{PUF}(\mathrm{ch}_n) = \mathrm{resp}_n$ denotes the unique response calculated by a PUF from a challenge $\mathrm{ch}_n$, a PUF-based tag authentication protocol works as follows:

1) $\mathrm{B} \rightarrow \mathrm{A}$: "I am B";
2) $\mathrm{A} \rightarrow \mathrm{B}$: $\mathrm{ch}_n$;
3) $\mathrm{B} \rightarrow \mathrm{A}$: $\mathrm{resp}_n$;
4) A (verification): $\mathrm{resp}_n = \mathrm{PUF}(\mathrm{ch}_n)$.

One possible candidate for a PUF is proposed by Lee *et al.* [26]. The idea is to exploit the statistical delay variations of wires and transistors across integrated circuits (ICs) to implement unique secret key on each tag. The evaluation indicates that there exists significant delay variation of wires and transistors across ICs implementing this circuit, and that the idea of leveraging this variation to uniquely identify and authenticate an IC seems promising. The probability that the first measured response bits to a given challenge on a chip is different from the measured response for the same challenge on a different chip is estimated to be 23%–40% depending on the PUF circuit architecture [26]. However, the technology is not yet mature enough for practical adoption.

*3) Location-Based Authentication:* The third general approach how products can be authenticated is based on their location. This approach is often referred to as track and trace-based plausibility check, but in this paper we opt for the more general term. The goal in location-based authentication is not to prevent cloning of products but to detect the cloned products in a defined environment such as a supply chain. For example, if the track and trace data tells that the genuine product is in Switzerland, a product that is seen in Japan claiming the same identity is suspicious. Formal definitions of location-based authentication have not yet been proposed in the

scientific literature, but we will derive one in Section III. The benefit of this approach is that the RFID tags only need to carry an identifier, whereas the complexity is in the back-end side.

Staake *et al.* [8] discuss the potential of track and trace-based product authentication approach within the EPC network and bring forth some of its vulnerability. Also Mirowski [59] has developed what essentially is a location-based authentication system for RFID, however, not in a supply chain application but in an access control application. The developed system can detect some of the cloned tags by searching for deviations from expected behavior, but the method is prone to false alarms.

*4) Weak Authentication:* It must be noted that also serial level identification alone without verification of the identities can be a powerful anti-counterfeiting tool. Juels [11] illustrates this with an example from the art world where a Victorian painter issued serial numbers to his paintings and catalogued them. The author argues that (partly) because of this reason, far less spurious paintings of this particular painter turn up on the market than from other painters. In particular, there are many methods that cannot prove with a high level of certainty that a product is original, but that can prove in certain cases that a product is counterfeit. These methods do not implement secure product authentication as it is defined in this paper but they can, as the aforementioned example from the art world illustrates, be powerful anti-counterfeiting tools. We refer to these methods as *weak product authentication* and they comprise verifying if a product has a valid ID number from a *white list* [14] and counting the number of times a check has been performed.

### C. Requirements Analysis

In this paper, we derive the security requirements of RFID-based product authentication systems. Our scope is broader than tag authentication, which is only one approach to authenticate a tagged product. Finding and defining security requirements of a system takes place in the system design phase. Security requirements exist because people and the negative agents that they create (such as computer viruses) pose threats to systems. Security requirements define the *security goals* of the system that answer the question, "What do you expect security to do for you?" [25]. Moreover, security differs from all other specification areas in that someone is deliberately threatening to break the system [1]. Security requirements are particularly important for product authentication that can be considered a security application because its only function is to provide security against certain threats (i.e., copying of products). Correspondingly, in the absence of these threats, secure product authentication would not be needed because identification alone would always reveal the real identity of a product.

Alexander [1] and Sindre and Opdahl [2] have examined the concept of *misuse cases* that can be used to derive the functional security requirements of a system. Use cases [15] have become increasingly common in requirements engineering, but they offer only limited support for electing security requirements because they model the intended use only. Extending the use case paradigm with misuse cases of illicit actors to model and analyze scenarios in systems under design can improve security by helping to mitigate the threats. Sindre and Opdahl [2] propose the following five-step process for eliciting security requirements with misuse cases:

1) identify critical assets in the system;
2) define security goals for each asset;
3) identify threats to each security goal by identifying stakeholders that may intentionally harm the system;
4) identify and analyze risks for the threats using risk analysis;
5) define security requirements for the threats to match risks and protection costs.

We apply this methodology in Section V and the resulting security requirements are presented in a use/misuse case diagram in Section VI.

## III. Defining Authentication

To provide an unambiguous definition for product authentication, one first needs to distinguish between product's identity and identifier. Identity is something unique that all individual products have, even products that are considered to be identical like cans of soft drink, for instance. Product's identity remains the same throughout the product's lifetime and it does not depend on the identifier or the tag of the product. Product's identifier is a name or a reference to the product's identity and it can be either in product class level, such as the global trade item number (GTIN), or in serial level, such as the serialized GTIN (SGTIN). In this paper, we only deal with the case where products have unique, serial level identifiers. The aforementioned definitions are needed to ensure that changing a product's tag does not change its identity. Based on these definitions, we can derive the following, identity-based definition for product authentication:

$$\text{Product authentication} = \text{Identification} + \text{Verification of the claimed identity.}$$

This definition conforms to the general definition of authentication by Kurose and Ross [31]. When a product's unique identity is linked to additional information, product authentication as defined before can answer whether a product is genuine or counterfeit, diverted from authorized distribution channel, expired, recalled, stolen, has warranty, etc. In this way, our definition also conforms to Schneider's definition for message authentication [29], applied to products.

Product authentication has to deal with uncertainty. There are different ways to verify the claimed identity of a product leading to different levels of confidence. In other words, some authentication methods are stronger than others. If a product under study fails an authentication check, it conclusively is not what it claims, but if it passes the check, it still might not be what it claims (i.e., the security feature is compromised). Thus, different verifications lead to different levels of confidence, which can be seen as the probability that a product that passes a check is what it claims. This principle is also employed in practice, for example, by first verifying the overt security features (e.g., a hologram), then the covert features (e.g., invisible ink), and last the forensic features (e.g., microscopic taggants). Because perfect security does not exist, the 100% confidence level cannot be achieved in theory. In practice, however, the 100% confidence

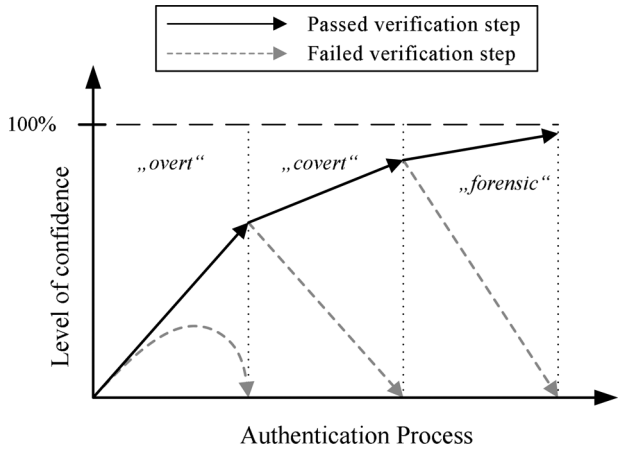


Fig. 1. Level of confidence and verification steps in product authentication process. Zero-level of confidence means that a product is not what it claims.

level can be associated with the most secure techniques. Level of confidence in authentication process is illustrated in Fig. 1. This model can also be used to explain the difference between weak authentication and the three strong authentication approaches (see Section II-B)—the level of confidence of weak authentication approaches can never reach close to 100% since those methods have known and unaddressed vulnerabilities.

### A. Defining Location-Based Authentication

While authentication based on what the subject is and what the subject has are well established, location-based authentication has no formal definition. In this subsection, we present such a definition that explains how products can be authenticated based on where they are. The underlying reasoning behind location-based authentication is that when the location of the subject is known, clones can be found as being in wrong locations. The location can be a geographic location as well as the location or the step in a process, such as *in distribution* or *sold to customer*. If the current location of a product is known without uncertainty, detecting cloned products is straight forward. For example, this is the case when the track and trace data tells that the authentic product is currently in a warehouse while another product with the same claimed identity is observed in customs. However, if the current location of a product is known with uncertainty, the system can only provide a guess whether a product under study is what it claims or not. For example, if the track and trace data tells that the product has been in a given warehouse one week ago but makes no assumptions on its current location, the location-based authentication system must reason whether it is plausible that the authentic product is now in the observed location or not. This leads to a lower level of confidence. The level of security of location-based authentication is further analyzed in Section VII-C.

## IV. Nonfunctional Security Requirements

In this section, we present the nonfunctional security requirements for product authentication systems in general. They arise from the underlying logic of product authentication process and complement the functional security requirements. If left unaddressed, also the nonfunctional security requirements represent vulnerabilities for the authentication process. The first two requirements concern product authentication in general, whereas the third one is specific to location-based authentication.

*1) Complete Coverage of Security Features:* The underlying logic behind any product authentication approach is that if a product cannot prove its identity when it should, it is not genuine (cf. Fig. 1). This implies that it is not enough if only a part of the genuine products have a security feature based on which they can be authenticated. Consider a situation where a pharmaceutical manufacturer wants to improve the security of an expensive drug product and, therefore, it inserts a cryptographic RFID tag on every second product. Though as a result, half of genuine products can prove their identities in a rather secure way, it does not help finding any additional counterfeit products since the lack of the security feature does not explicitly mean that a product is not genuine.

It is worth noticing that this requirement can be overcome when single products have unique identities and the back-end knows which products have which security features. In our previous example, this would mean that every second product should implement a cryptographic tag authentication protocol. In this scenario, it's important that the counterfeiters do not know which products do not have the security features; otherwise, counterfeiters could simply target only the nonprotected products.

*2) Availability:* The fact that products that cannot prove their identity when they should must be considered counterfeits mandates a rigid availability requirement for the product authentication system. Since networked RFID systems are vulnerable to denial-of-service attacks in both network and tag layer, this is particularly worrisome for RFID-based product authentication. RFID tags can be destroyed rather simply for example with handheld devices that send an intensive electro-magnetic pulse [51].

*3) Data Sharing:* Location-based product authentication is possible only if the locations of genuine products can be followed with a high enough degree of spatial and temporal granularity. Today, companies share this kind of information unenthusiastically and rather on a need-to-know basis than on a regular basis. To make sure that a location-based product authentication application has all the information it needs to draw the right conclusions in the presence of adversaries, the custodians of the product need to collaborate and share this data.

## V. Chain of Trust, Threats, and Risks in Product Authentication

Functional requirements state the functionality of a system and they can be modeled with use cases. A use case models a basic functionality of the system and it includes actors who interact with the systems. Use cases are often illustrated in use case diagrams, and all the use case diagrams and their associated details for a specific system form the functional requirements of the system [15]. To derive the functional security requirements for product authentication, we apply the use and misuse case methodology of Sindre and Opdahl [2] presented in Section II. Our use case under study is product authentication by a licit actor (e.g., sales clerk, customs officer, or consumer). The misuse case is an attack where the illicit actor attempts to

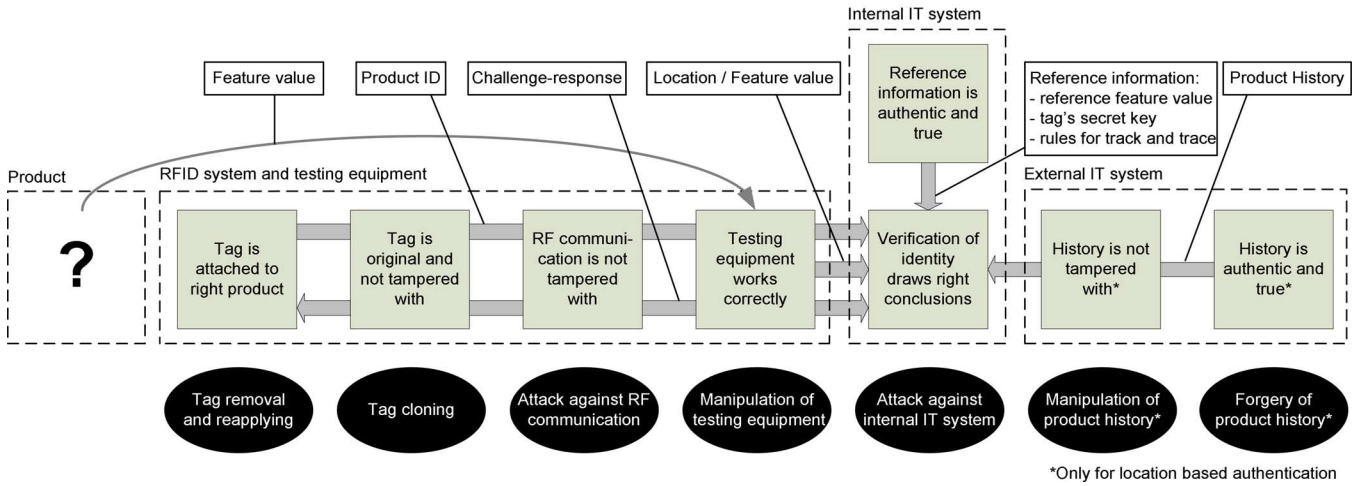


Fig. 2. Chain of trust (rectangles) and threats against (ovals) RFID-based product authentication system. The arrows indicate the different information flows that take place within product authentication process. The product under study is illustrated by a black question mark.

fool the security mechanism to make a counterfeit product pass the check as a genuine one. In this section, we derive the chain of trust of general RFID-based product authentication process to find all critical assets to be secured, and evaluate the threats and risks against the general RFID-based product authentication process. The resulting set of functional security requirements is presented in Section V.

### A. Chain of Trust in RFID-Based Product Authentication

In this subsection, we identify the links in the chain of trust in general RFID-based product authentication process by studying the information flow within the authentication process. The first step in all RFID-based product authentication approaches is identification, where the reader device interrogates the tag attached to the product and the tag answers by transmitting the *serial ID* number. We consider all three approaches how a product can securely prove it has the claimed identity, as presented in Section II.

In product authentication based on object-specific features, the testing equipment measures the product's *feature value* (the product's physical or chemical fingerprint) and transmits this feature value to the product authentication application. We consider the product authentication application a software agent that makes the final decision whether a product is authentic or not and it resides in the internal IT systems of the company that provides the service (e.g., the brand-owner). In order to draw the final decision, the product authentication application compares the measured feature value to *reference information*, the feature value of the genuine product. We call this last process step *verification of identity*. If the two feature values do not match within an interval of tolerance, the product under study is not the genuine one. The verification can be made also in a more general manner where close match between measured and reference feature value result to high level of confidence and vice versa.

In product authentication based on tag authentication, the tag proves its identity by showing that it knows a certain secret key with an authentication protocol. We reviewed general forms of existing protocol in Section II showing that they can be modeled as a challenge-response pair over the radio-frequency interface between the reader and the tag. To know what the correct response for a certain challenge is, the product authentication application needs *reference information* which usually is the tag's secret key (e.g., in [38]). In this approach, the *verification of identity* deduces to comparing binary keys and thus the result is also in binary form.

In location-based product authentication, the testing equipment sends time and location where the product has been observed to the product authentication application. The observed location of the product under study is compared with the last known location of the genuine product. Because products flow across organizational boundaries of different supply chain partners, we assume that the history is retrieved from an external IT system like the EPC network [30]. To authenticate the product, *verification of identity* needs to know the set of rules and constraints that the observation locations must comply to. These rules serve as *reference information* and they can define, for example, the allowed order and time frames of location observations. If the observed location is plausible, the product under study is what it claims. The result can be in binary format, but also a probability (e.g., level of confidence) if the reasoning is done on statistical basis.

In order to guarantee the integrity of the previously mentioned information flows, one has to be able to trust that the tag is attached to the right product, that the tag is original and not tampered with, that the radio-frequency communication is not tampered with, that the testing equipment works correctly, that the reference information is authentic and true, that the product history is authentic and true, and that the product history is authentic and not tampered with. Finally, the verification of identity needs to draw the right conclusions based on the evidences. This chain of trust is illustrated in Fig. 2. The arrows in the illustration indicate different information flows.

### B. Threats in RFID-Based Product Authentication

Each step in the chain of trust is a possible point of attack against the product authentication system. In this subsection, we identify and evaluate a comprehensive set of threats against the product authentication process. These threats are illustrated as black ovals in Fig. 2.

*1) Tag Removal and Reapplying:* Removing and reapplying a tag from a genuine product to a counterfeit one can fool the product authentication application. Without special techniques that bind the tag and the product either logically or physically, only the tag will be authenticated but not the product. Many RFID tags that are used in product serialization are adhesive labels. If not specifically addressed, removing and reapplying them to counterfeit products poses no significant barriers for skilled counterfeiters. This is similar to removal and reapplying of price tags of consumer goods which is an existing threat in the retail industry.

When an RFID tag authenticates high-value items such as airplane spare parts or rare drug products, even the removal and reapplying of a small number of tags can be financially interesting for the counterfeit players. The lack of binding between the tag and the product is especially problematic in the pharmaceutical industry where the RFID tag is never attached to the drug product itself (tablet, ampoule, vial, etc.) but on the secondary or tertiary packaging (blister package, carton package, etc.). Not only is it easy to disassociate the tag from the drug product it authenticates by changing the contents of the package, but it also is a common practice in the industry when the products are repackaged. Drug products are repackaged for example in order to change the language of the package and instructions as the products move to another country. Repackaging of drug products is legal in Europe and in the U.S. but illicit actors can use it to inject counterfeit products to the market by including fakes among the unpackaged genuine products.

*2) Tag Cloning:* Tag cloning refers to cloning a genuine tag and attaching it to a counterfeit product. What is successful tag cloning depends on the functionality of the tag. If the tag only stores static ID numbers, then a successful tag cloning attack only requires reading all data on tag and rewriting it on empty tags. If the tag provides cryptographic authentication protocol, then tag cloning requires copying the secret key of the tag.

If the tag is unprotected, it is easy to clone simply by interrogating it and by writing the acquired ID number on another tag. We refer to this attack as ID number copying. Interrogating tags without permission is referred to as clandestine scanning [11] and most RFID tags are not protected from it. Furthermore, so called rogue scanning using a sensitive reader equipped with a powerful antenna or an antenna array and possibly output power that exceeds the legal limits can exceed the nominal read range. For example, Kfir and Wool [12] suggest that the rogue scanning range for ISO 14443 tags can be five times higher than their nominal reading range.

Once a reader has powered a tag (or initiated communication with an active tag), a second reader can monitor the tag emission by passively eavesdropping the signal and capturing the product ID number for cloning. The maximum distance where a tag can be eavesdropped may be even larger than the rogue scanning range [11]. Also, the reader-to-tag communication can be eavesdropped, though this channel is less frequently used to transfer tag-specific information. Because the reader transmits at much higher power than the tags, however, eavesdropping range for the reader-to-tag channel is much greater than for the tag-to-reader channel [13].

Numerous techniques have been developed to protect tags from cloning. The principal techniques are reader authentication where the tag makes sure it communicates with an authorized reader prior to enclosing any sensitive information (preventive countermeasures), tag authentication where the reader makes sure the tag is genuine (reactive countermeasure), and mutual authentication that incorporates both these approaches. Since reader authentication is only a partially preventive countermeasure, it cannot be considered a complete solution against tag cloning. Even though tag authentication protocols can provide significant improvements to a tag's cloning resistance, there are many ways to conduct a cloning attack even against a protected tag. These attacks include side channel attack that is based on information gained from the physical implementation of a cryptosystem (e.g., [3]), reverse-engineering and cryptanalysis that includes brute force attack but also much more sophisticated techniques (e.g., [4], [6]), and physical attacks where the goal is to read the secret key directly from tag's memory (e.g., [5]). In addition, tag authentication approach is always vulnerable to data theft where the secret encryption schemes of genuine tags are obtained from insiders through means of manipulation and fraud (*social engineering*) or even through threatening and blackmailing (*rubber-hose cryptanalysis*).

*3) Attack Against RF Communication:* Also, an attack against the radio-frequency (RF) communication can fool the product authentication system. In this case, the product does not have a copied tag that would pass the check. An adversary could conduct a replay attack by hiding a replay device close to the reader device (or even together with a product) to replicate genuine tags. A replay device is basically an RF tape recorder that can scan and then replicate tags, and building such a device requires only little money or expertise [16]. Even complex tag authentication protocols can be vulnerable to relay attack where the adversary who resides between a genuine tag and a reader captures and retransmits the challenge from the reader to the genuine tag, and again retransmits the correct response to the reader device.

*4) Manipulation of Testing Equipment:* The testing equipment includes the RFID reader and, for object-specific features approach, a device that can measure the features of the product under study. If the testing equipment is compromised, it can no longer be trusted to give right answers. In the simplest case, the testing equipment can be hard coded to let all products pass the check. In a more complicated attack, it could try to claim a wrong location to the product authentication application, for example, the known location of the genuine product so as to fool the location-based plausibility check.

*5) Attack Against Internal IT System:* The most important functionalities and data of a product authentication system reside in the internal IT system of the company that provides the authentication service. These comprise the reference information of genuine products and the part of the system that draws the final conclusion about the authenticity of a product. Specific attacks comprise data theft to steal the secret keys and encryption schemes, or manipulation of the product verification agent. Therefore, also the internal IT system is a possible point of attack for adversaries.

*6) Manipulation of Product History:* The history of a product can either move together with the product as a pedigree (e.g., [27]), reside in distributed database of all the custodians of the product (e.g., [8]), or reside in one central database. Depending on the actual implementation, the history of a genuine product is vulnerable to different ways of manipulation. We consider the following three cases of manipulation: addition of bogus events to "relocate" the product, removal of existing events for example to hide the fact that the product is already sold, and modification of attributes (time and location) of existing events. All cases of manipulation of history can be used to fool the location-based plausibility check.

*7) Forgery of Product History:* In addition to manipulation of an existing product's history, also the creation of a falsified history from scratch can threaten location-based product authentication. We refer to this threat as forgery of product history and it includes creation of a completely new identity that it given to the counterfeit product and injection of the forged history to the external IT system.

### C. Risks in RFID-Based Product Authentication

In this subsection, we assess the risks in RFID-based product authentication. Risk assessment is needed to know which of the identified threats are the most serious and, therefore, require most attention. The organizational context of this risk analysis is a company that is affected by product counterfeiting and that employs product authentication within the licit supply chain.

Risks can be assessed by evaluating exposure (or consequence) and uncertainty (or likelihood) of known threats [28]. For us, consequence means the number of products that are compromised (how many counterfeit products can fool authentication after a successful attack). Likelihood of a threat is commonly measured by the frequency of incidents, but since RFID-based product authentication is still very immature, the threats have not yet realized in such scales that counting them would provide any statistically significant estimates. Therefore, we evaluate the likelihoods of threats in terms of how easily the corresponding attach could be conducted, in scale low-medium-high. When affected companies get data from real incidents, this risk assessment should be redefined accordingly.

Manipulation of product history would require an attack against a database or a communication channel. Single events in the history are not likely to be signed, except for e-pedigree [27], so manipulation could be potentially done without leaving any signs. However, we consider existing network and database security mechanisms good enough so that when they are properly employed, this threat is not particularly likely. A successful attack could compromise one or multiple products, depending on the target, but since the manipulation needs to be carefully chosen, replicating this attack is not without additional effort.

Forgery of a complete product history requires successful impersonation of the brand owner. This could be achieved by breaking the brand owner's signing key or through man-in-the-middle-attack in the network. One successful attack can compromise multiple, even unlimited number of products, for example by creating a phony product history repository. However, as shown previously, we consider network authentication mechanisms good enough so that when they are properly employed, this threat is not particularly likely.

Attacking the RF communication is complex and requires hiding special equipment in the proximity of the authenticating reader device. Doing this is hard in practice since the authentication takes place in a controlled environment under the supervision of authorized personnel such as in customs or in an authorized retailer. Therefore, the likelihood of such an attack is low. Similarly, since the testing equipment is handled by authorized personnel only, we conclude that manipulation of testing equipment is also not likely to happen. When succeeded, however, both these attacks would compromise all products that pass through the compromised check point.

Attacks against the internal IT systems have the potential to compromise unlimited number of products, making it especially interesting point of attack. It is likely that the internal IT system where product authentication service is run needs to be online to provide an interface for remote parties to authenticate products. The other less likely option is to have so called offline authentication where all needed information is stored on tag and on reader, which is technically harder. This threat is not specific to RFID systems and can be addressed by standard techniques of network security and security engineering [29], but as for other online system, the risk cannot be completely mitigated.

Last two threats are cloning as well as removal and reapplying of genuine tags. Unprotected tags do not provide protection against cloning. The use of protected tags increases the counterfeiter's barrier to clone the tags, but does not completely mitigate the threat of tag cloning. To clone a large amount of tags in one attack, illicit actors could target consignments or employ social engineering inside the supply chain, keeping the cost of this attack lower. Overall, we evaluate the likelihood of tag cloning high. Furthermore, if the product authentication system is not able to detect cloned tags for example by location-based authentication, cloning one genuine tag compromises unlimited number of products because a counterfeiter can copy the same genuine tag on multiple fake products without an increased risk of getting caught.

Removal and reapplying of genuine tags is perhaps harder to be completely prevented than tag cloning, but it is much more costly for the counterfeit player in larger scales and thus less likely. If a counterfeiter cannot get genuine tags from inexpensive sources such as diverted genuine packages from scratch or repackaging, he would have to buy genuine products to get the genuine tags. This would add the price of one genuine product to the cost of one counterfeit product and ruin the counterfeiter's business case. Therefore, tag removal and reapplying is not likely to happen in large scale but only to the extent of how much genuine tags counterfeiters can easily get. A summary of the risk assessment is found from Table I.

## VI. Functional Security Requirements

The functional security requirements of RFID-based product authentication system are the security goals that are needed to mitigate all applicable threats. If a threat is not mitigated, the system has a vulnerability that counterfeiters can exploit and

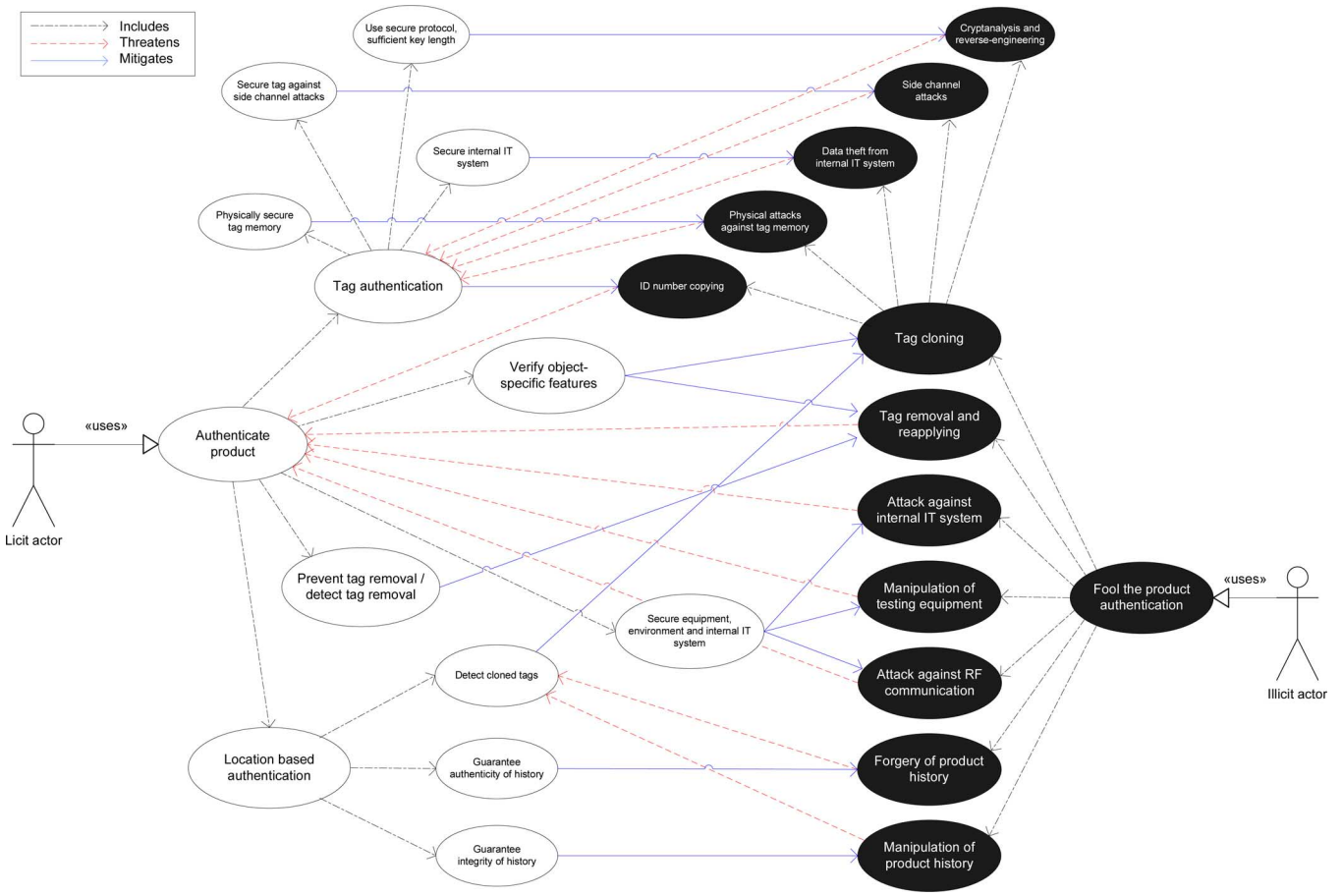


Fig. 3. Use/misuse-case diagram of functional security requirements of RFID-based product authentication. The white ovals are the security goals of the system and the black ovals present the threats. The overall requirement is to mitigate all applicable threats with security goals. In particular, the diagram shows that security officers of product authentication systems have much more than the tag cloning attack to worry about.

TABLE I
RISK ASSESSMENT

| Threat | Consequence | Likelihood |
|---|---|---|
| Tag cloning | $\infty$ | High |
| Tag removal and reapplying | 1 | Medium |
| Attack against internal IT system | $\infty$ | Medium |
| Manipulation of testing equipment | N | Low |
| Attack against RF communication | N | Low |
| Forgery of product history | $\infty$ | Medium |
| Manipulation of product history | N | Medium |

Consequence denotes how many counterfeit products can fool authentication after a successful attack: $1 =$ one; $N =$ multiple, but limited number; $\infty =$ unlimited number.

the cost to break the system is low. Therefore, the level of security of a product authentication system depends on how well the functional requirements are met. Like Schneider [52], we assume that counterfeiters will break through where the barrier is the lowest, so the level of security of a product authentication system equals the level of protection of the least satisfied functional security requirement. The security goals and threats against RFID product authentication are illustrated in a use/misuse-case diagram (see Fig. 3). The diagram illustrates that different approaches have different threats and that there are multiple combinations of security goals that mitigate all the threats, corresponding the different product authentication approaches we identified in Section II. Most importantly, there are three different strategies on how to deal with the tag cloning attack.

A simple ID number copying attack is sufficient against unprotected tags. If this attack is mitigated by a tag authentication protocol, the illicit actor still has physical attacks against tag memory, data theft from internal IT system, side channel attacks, and cryptanalysis and reverse engineering in his disposal. The licit actor must respond by physically securing the tag memory, by securing the internal IT system against key theft, by securing the tag against side channel attacks, and by using secure protocols and long-enough keys. This is how Fig. 3 illustrates the war of escalation between the licit and illicit actors.

The threat of tag removal and reapplying attack must be mitigated either by preventing the tag removal, detecting the tag removal (e.g., with a seal), or by verifying the object-specific features to detect if the tag is attached to the right product (see Section II-B1). One way to prevent the removal of RFID tags in practice is to integrate the tag in such a way that the chip will detach from the antenna if the tag is removed. This method is applied, for example, in some sprayer perfume bottles where the tag resides between the bottle top and the glass bottle—and if the bottle top is removed, the antenna will stay attached to the glass bottle while the chip comes off with the bottle top.

TABLE II
SECURITY IN DIFFERENT PRODUCT AUTHENTICATION APPROACHES

| Approach | Cost to copy $N$ products | Probability to detect a copied product |
|---|---|---|
| *Object-specific features* | $N$·(*cost to replicate product*) + $N$·(*cost of tag*) | 0 |
| *Tag authentication* | *cost to break a crypto tag*+ $N$·(*cost of crypto tag*) | 0 |
| *Location based authentication*[1] | $N$·(*cost of ID number*) + $N$·(*cost of tag*) | $(1\text{-}Pr(detect\ clone))^n$ |
| *Hybrid*[2] | $N/2$·(*cost to break a crypto tag*) + $N$·(*cost of crypto tag*) | $0^2$ |

[1]NB: This approach is completely secure if $Pr(detect\ clone) = 1$
[2]Assuming tag authentication together with weak location-based authentication, which means here that a maximum of two copies of a product can be injected into a secured channel without the risk of clone detection

Attack against internal IT system, manipulation of testing equipment, and attack against RF communication needs to be mitigated by securing the internal IT systems from outsider and insider attacks, by guaranteeing the integrity of the testing equipment and by securing the verification environment, respectively. Since these countermeasures are not specific to RFID, this paper will not go deeper on how these security goals can be achieved. Fig. 3 reveals that these three security goals are the only ones that cannot be replaced by any other and thus they apply for all RFID-based product authentication systems. For the sake of clarity of illustration, we have bundled them into one oval in Fig. 3.

Last, the threat of manipulation of product history must be mitigated by guaranteeing the integrity of the history, and the threat of forgery of product history must be mitigated by guaranteeing authenticity of the history. We present in Section VIII how this can be achieved in the EPC network.

## VII. LEVEL OF SECURITY OF RFID-BASED PRODUCT AUTHENTICATION APPROACHES

In this section, we analyze the level of security of different RFID-based product authentication approaches. According to Schneider, cost to break [52] and risk of getting caught [53] define the level of protection against adversaries seeking for financial gain. We assume that the adversaries are counterfeiters who are motivated by money and seek to compromise the system for a large number of products. Therefore, we define the level of security of a product authentication system in terms of cost to copy $N$ products and the probability that a copied product is detected. $N$ should be chosen as the number of counterfeit products that are in one consignment that is inspected, for example by customs, and thus the detection of even one copied product leads to the loss of all $N$ products as the whole lot is likely to be confiscated. The results are summarized in Table II.

### A. Object-Specific Features-Based Authentication

Security of this approach is based on utilizing random variances of manufacturing processes that are hard or even possible to be replicated. The use of forensic security features like microscopic or magnetic taggants can be an artificial way to implement these features. Since a successful object-specific features-based check mitigates both tag cloning and tag removal and reapplying attack, in principle, this approach is the most secure way to authenticate products. The cost to copy multiple products is dominated by the cost to replicate a genuine product including the unique feature. We assume that the signature method used to authenticate the feature value is secure. If a counterfeiter succeeds in replication of the feature, however, this approach provides no support to detect the copied products.

All products have object-specific features if the measuring equipment allows for high enough resolution, but the difficulty is to find such features that are robust to changes and can be easily measured [9]. An interesting example candidate for such feature for paper and cardboard is a unique pattern of how the surface material reflects laser light that is swept over a chosen path [43]. Since the object-specific features need to be measured as a part of the check, the check needs to be done in part manually. The function of the RFID tag is to provide a large enough digital memory to store the digital signatures and other data.

### B. Tag Authentication

Assuming secure RF interface, testing equipment, and internal IT systems, security of tag authentication approach is based on cloning resistance of the RFID tags and on tag-product integrity to prevent reuse of genuine tags in counterfeit products. Even though having a cloning resistant tag can have a major effect on the tag price [38], there are also many low-cost approaches to increase the barrier to clone RFID tags. In addition to low-cost cryptography (e.g., [7], [32]–[34]), also the unique factory programmed read-only transponder ID (TID) number that is similar to the unique MAC address of PC network cards can increase the cloning resistance of low-cost (ca. 0.10–0.20 Euro) tags such as EPC Class-1 Gen-2 [44]. TID is not cryptographically secure but it represents a practical barrier, requiring a chip manufacturer to knowingly write copied TID numbers on their products or the use of nonstandard tags. It is not yet known, however, how big a barrier the cloning of TID number will be in practice. Furthermore, not all off the shelf Gen-2 chips implement the unique TID number, but the feature might be offered in special anti-counterfeiting tags only (e.g., Monza/ID chip [60]).

Cost to copy multiple products in this approach is dominated by the cost to break one crypto tag. Once a secret key and encryption scheme are known, reproducing multiple copies of the tag is possible. As an illustration of the cost to break one crypto tag, researchers at Johns Hopkins University and RSA Laboratories [4] have broken the 40-bit proprietary encryption of a commercial RFID transponder with a PC and a few hundred dollars worth of commodity equipment. The authors further estimated that the cost to construct a device to skim a genuine tag, crack the key, and simulate the genuine tag would be several hundred dollars. Product counterfeiters, however, cannot use such simulator devices but they also need to reproduce the tag itself, which represents another practical challenge especially when nonstandard hardware and software are used.

### C. Location-Based Authentication

Security of location-based product authentication is based on a high probability to detect the cloned products. Assuming that the location-based product authentication system can always detect if there are multiple copies of one ID number among the $N$ samples, the counterfeiter needs to insert tags with different genuine ID numbers on all $N$ counterfeit products to fool the system. As defined in Section III, when the location of the subject is known, clones can be found as being in the wrong locations. To show what factors influence the probability to detect a cloned tag, we identify three problem scenarios where location-based authentication fails.

*1) Identical Location Problem:* When the genuine product and a copied one are in identical location, location-based authentication cannot make difference between these products. What is identical location depends on the granularity of the location data.

*2) Identity Swap Problem:* Location-based authentication might detect the presence of cloned products without being sure which product is the genuine one. This might lead to false acceptance of the copied product and false rejection of the genuine one. We denote this problem identify swap and it can happen always when the exact location of the genuine product is not known.

*3) Missing or Incomplete Trace Problem:* After a consumer product reaches the end-user, it is likely that its trace is not updated anymore. When the system looses the visibility of a product, it can no longer securely authenticate the products in this stage of the product's life cycle. For example, when a product is returned to the after sales service and its history says it is bought two years ago from a destined location, the system cannot reason based on the location information whether the product under study really is the claimed one or not. The problem with incomplete trace in location-based product authentication has been brought forth also by Staake *et al.* [8].

As a result, it can be seen that in all cases the probability to detect cloned products and thus the level of security depends on how well the location of the genuine product is known. As the uncertainty in location information decreases, the probability to detect cloned products increases. Most importantly, when the location of the genuine product is known without uncertainty, all cloned products can be detected. This is an important result since it suggests that location-based authentication really can implement strong authentication.

Also low probability to detect clones can significantly increase the level of security of a product authentication system when combined with tag authentication. Assume that a counterfeiter knows he can securely inject only two products with the same ID number into a secured channel. Hence, instead of copying the same cracked tag to all $N$ products, he needs to crack $N/2$ different tags. The cost to copy the products is increased accordingly, as illustrated by the Hybrid approach in Table II. This means that even modest tag cloning resistance can have a major impact on counterfeiter's business case if clones can be detected with some probability.

## VIII. Product Authentication in the EPC Network

In this section, we investigate how RFID implements product authentication in practice. To do this reality check, we study how the EPC standards conform to the functional security requirements of product authentication (see Section VI). Electronic product code (EPC) is an industry driven RFID standard of EPCglobal Inc.[1] EPC standards are supported by major industrial players especially from the retail industry—among the top 30 Fortune 500 companies there are 13 EPCglobal members,[1] [61]—and thus EPC is the most deployed standard for networked RFID. EPC systems are built for increased supply-chain efficiency and we identify how they can be used in product authentication and what is needed for full support of all functional security requirements. Because the challenges that the nonfunctional security requirements (see Section IV) represent are mostly organizational and not technical, nonfunctional security requirements are omitted from this analysis.

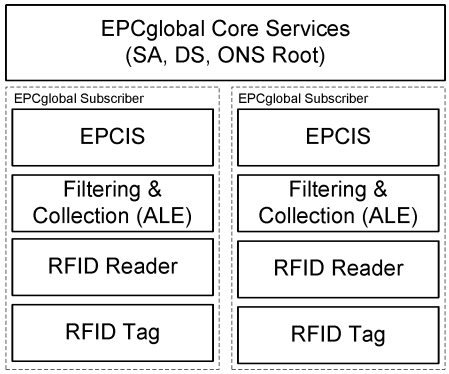


Fig. 4. Illustration of the hardware and software roles of the EPCglobal architecture framework [30]. EPCglobal standards define the interfaces between the roles.

The hardware and software roles defined by EPCglobal are illustrated in Fig. 4. These comprise EPCglobal core services that are common for the whole RFID network, as well as roles that are specific to each EPCglobal subscriber, i.e. a company. The security functions of the EPCglobal architecture are distributed among different roles and interfaces [30]. Most EPC tags are inexpensive (below 0.20 Euro) passive tags (EPC Classes 0/1/2) for item-level tagging with optional user memories. In addition to tags, readers, and filtering and collection layer that erects application layer events (ALE), EPCglobal also develops standards for sharing the item-level data to enable a complete RFID network. The main network components are EPC Information Services (EPC-IS), Object Naming Service (ONS), and Discovery Services (DS) [30].

The EPC-IS defines standard interface for capturing and querying EPC-related data and the related security mechanisms, authentication and authorization [45]. The EPC-related data, events about single or aggregated items, is stored in EPC-IS repository.

The ONS uses the Internet's existing domain name system (DNS) for looking up (resolving) information about a certain product from the manufacturer's database [46]. EPCglobal provides the root ONS as a part of the core network services and it is up to each subscriber to run the local ONS that replies to the lookup requests.

The DS locates all EPC-IS services that may have information about a specific EPC and, additionally, also provides a cache for some EPC-IS data [30]. The DS is not yet a defined part of the

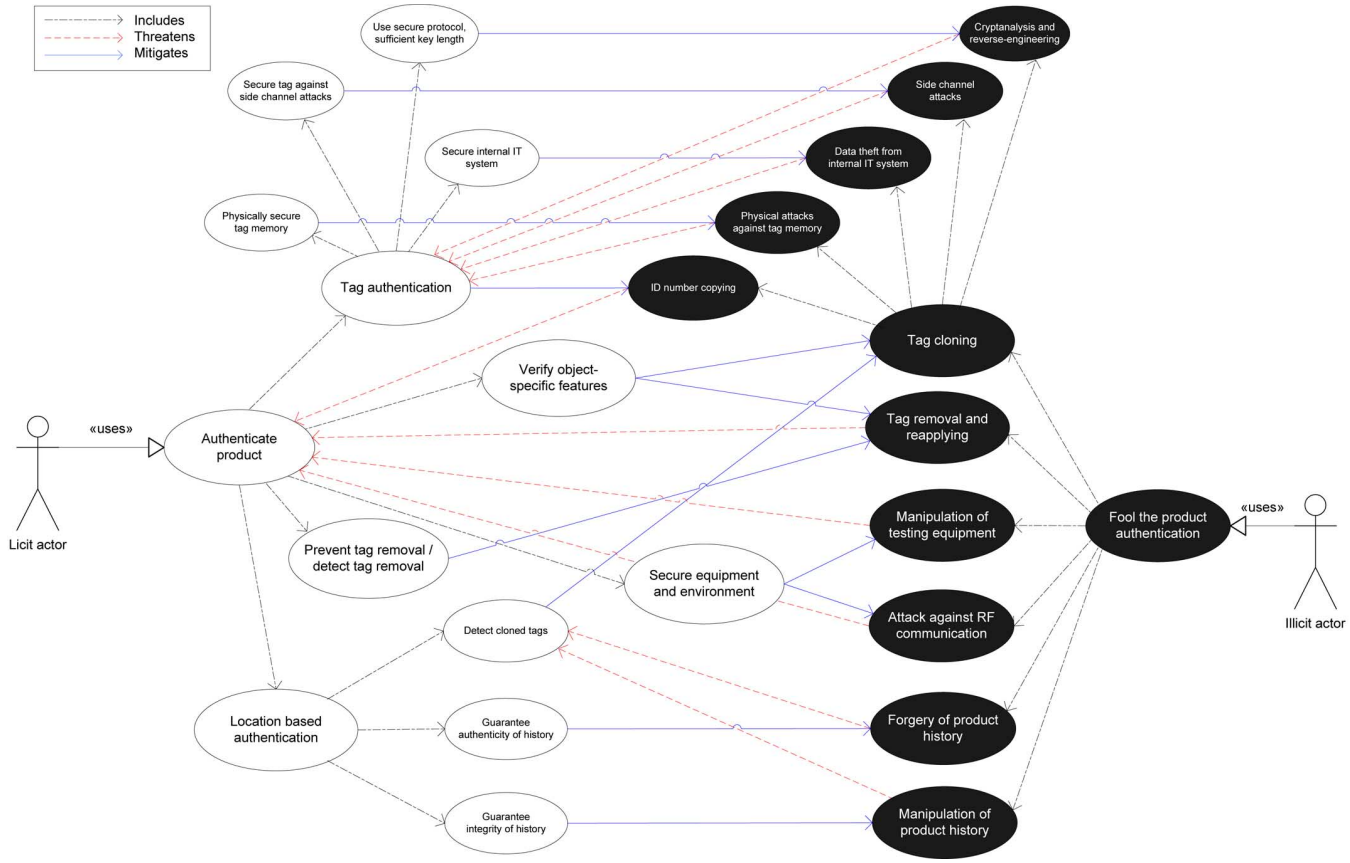


Fig. 5. Illustration of product authentication in the EPC network. (*Planned but not yet defined service; **Proposed new service)

EPCglobal architecture framework, but its general functionality is known. In addition, the core services of the EPCglobal architecture include subscriber authentication (SA) service.

### A. *Conformance to the Functional Security Requirements*

In this subsection, we go through the functional requirements of product authentication and analyze how the existing EPC standards conform to them. The conformance of some of the functional requirements is mostly defined not by the standard itself but by how it is implemented. Therefore, we omit the following requirements from this analysis: prevent and detect tag removal, secure equipment, secure environment, and secure internal IT system.

*1) Tag Authentication:* The current EPC network does not directly support tag authentication. Furthermore, to our knowledge there are currently no cryptographic RFID tags commercially available that operate in the UHF band that is likely to dominate in supply chain applications, as most existing cryptographic RFID tags operate in the HF band and normally conform to ISO 14443 (proximity card) or to ISO 15693 (vicinity card) standards. There are, however, first implementations of a tag crypto module for advanced encryption standard (AES) [50] that fulfill the requirements of both HF and UHF tags in terms of chip size and power consumption. Though tag authentication in the EPC network is not yet reality, the concept of tag authentication in the EPC network has been addressed in the literature. The EPC Class-1 Gen-2 (UHF) tag standard [44] includes factory programmed transponder ID number (TID) that can be used to increase the tag's cloning resistance as presented in Section VI. In addition, Juels [7] has shown how to leverage the PIN-based access control and privacy enhancement mechanisms (KILL command) of EPC Class-1 Gen-2 tags to achieve a crude challenge-response authentication. The EPC Class-1 Gen-2 standard also exploits the difference between reader-to-tag and tag-to-reader eavesdropping ranges that, as presented in Section II, can vary a lot. When transmitting a PIN to a tag, the tag first transmits a random secret to the reader that encrypts the PIN code using XOR. This protects the reader-to-tag transmission from eavesdroppers who cannot listen to the weaker tag transmissions [13], making cloning harder for eavesdroppers.

In order to bring advanced cryptography to the EPC network, Staake *et al.* [8] proposed to extend it with a so-called EPC Product Authentication Service (EPC-PAS) that would store the secret keys and calculate challenges for authentication protocols. This is illustrated by the mechanism number 1 in Fig. 5 where different product authentication mechanisms in the EPC network are illustrated. The EPC-PAS would complement the EPC-IS by separating the cryptographic service from the data repository and it could reply to accessing applications whether a tag is authentic or not. This review shows that the concept of tag authentication in EPC network is well addressed but the remaining research challenge is how to bring tag authentication into reality in a scalable and cost-effective way that can guarantee the needed level of availability.

*2) Object-Specific Features-Based Authentication:* The object-specific features-based approach, as defined by Nochta *et*

*al.* [9], requires that the network provides a secure way to distribute the public key of the brand-owner for verification of the signature that is written on the tag. Both EPC-IS and EPC-PAS could be used to store this public key, given that authentication and integrity can be guaranteed. Additionally, this approach could be implemented by storing the complete feature value (unique product identifier) on the back-end instead of the tag. All this is feasible within the EPC network architecture.

*3) Guarantee Integrity of History:* The location-based product authentication system has to have correct and complete history of the product under study for the highest level of security. In order to conform to this requirement, the network has to guarantee two things: that the events are not tampered with and that all the events for which the accessing application is authorized are returned when requested. The former can be achieved in the EPC network by securing the communication and protecting the data in EPC-IS repositories. The EPC network's conformance to the latter depends on the discovery services module (DS) that is not defined yet.

If the DS cannot guarantee that it locates all the services in the ECP network that publish events about a product, then the product authentication application is not sure to have the complete visibility for the detection of cloned tags, potentially leading to false positives and false negatives. For example, consider a case where products are imported for sales to another country and the receiving company scans the products and publishes the reception event in its EPC-IS. If the products are later authenticated at the sales point based on their location but the DS does not locate the events that are published in the receiving company's EPC-IS, the product authentication application does not know that the products are imported to that country (Missing or incomplete trace problem, Section VII) and might consider them counterfeits.

Because of the illustrated reason, the DS needs to guarantee that the complete product history is located from the EPC network. This needs to be taken into account in the design of the future DS functionality of the EPC network.

*4) Guarantee Authenticity of History:* Authenticity of history in the EPC network is guaranteed by authentication of different entities using public-key infrastructure which is defined by EPCglobal certificate profile [47]. These entities are users inside the EPC network (people), services/servers (EPCIS, ONS, etc.), and readers and other devices. Even though this mechanism does not allow authentication of the history itself but only authentication of the entities that provide it, the provided security mechanism is sufficient because the entities that provide the history have to be trusted parties. Even when a company signs the events, there is no undisputable proof that the product really was in the claimed location. Therefore, it is possible to inject false information to the EPC network, which is currently not addressed.

*5) Detect Cloned Tags:* The current EPC network does not provide direct support for detection of cloned tags but it does provide means for subscribers to do this by themselves. A subscriber can query the EPC-IS repositories for events about a product and reason himself whether the product under study is genuine or a cloned one. This is illustrated by mechanism number 2 in Fig. 5. This mechanism has two shortcomings. First, the EPC-IS servers answer to queries according to the authorization of the accessing application and can disclose any amount of information they want which can be less than requested. Therefore, only those subscribers who are authorized to access the product's history in all the product's custodians' EPC-IS repositories have the full visibility for detecting the cloned tags. This also means that only subscribers of the EPC network who are authorized to follow the movements of the product can authenticate the product at all. That restriction is likely to make this authentication mechanism out of the reach of, for example, consumers. Second, a party interpreting the track and trace data might not have all the needed knowledge about the restrictions concerning the movement of the genuine products to draw the right conclusion whether a product under study is genuine or a cloned one. For example, it is important to know if the genuine products are distributed only through a small number of authorized dealers and how the traces of genuine products normally look like in order to detect suspicious events in traces. Also, knowledge of the exceptional movement of the genuine products, for example, when products move upstream in the supply chain due to mistakes in shipments, can be useful to avoid false alarms.

As a result, EPC network's support for detection of cloned tags is far from optimal. This is also the biggest lack of conformance to the functional requirements and we propose in Section VIII-B how the problem could be overcome.

### *B. Improved Support for Detection of Cloned Tags*

To overcome the structural shortcomings in the EPC network's support for detection of cloned tags, we propose promoting this functionality to the level of the core services of the EPC network. We call this new service the EPC trace analysis service (EPC-TAS) and it requires that all parties who handle the products agree to share certain events like reception and shipping notifications. In this way, the EPC-TAS would obtain a comprehensive visibility about the movement of the products and thus it could in real time analyze the complete traces of products to detect the cloned tags. The EPC-TAS would probably need to be a trusted third party in practice. The primary functionality of this service would be to receive queries of triplets {*EPC, Location, Time*} and to answer whether the product under study is genuine or a cloned one. This is presented by the mechanism number 3 in Fig. 5.

The envisioned service would have the best possible visibility to detect cloned tags. In addition, the EPC-TAS would disclose only a minimal amount of information about the product under study when answering to queries (e.g., is authentic/is not authentic). Therefore, this product authentication mechanism could be made accessible to many users, for example to consumers, without the fear of disclosing sensible information like past locations of the product. This service would have to be run under the authority of the brand-owner to give necessary credibility, or even legal status, to the answers. Therefore, the service could utilize the brand-owner's knowledge about the restrictions and irregularities in the distribution channel of the genuine products in order to configure the system with best possible *a priori* knowledge to enable the most sensible interpretations of the track and trace data.

One major difference between EPC-TAS and other product authentication mechanisms is that EPC-TAS could detect the counterfeit products without specific authenticity checks initiated by the custodians of the products. This means that the system could provide product authentication capability as a background, monitoring service. Furthermore, the EPC-TAS could aggregate the results into business intelligence, for example, by identifying the most likely entry points of counterfeit products in the distribution channel. The precise functionality of the proposed service, especially concerning the automated decision making process, and integration of this service to the existing EPC network, remain open research questions.

## IX. Discussion

For a company affected by product counterfeiting, RFID tag authentication represents only one possible technique to authenticate products, and RFID only one candidate technology for the solution. Therefore, we believe that the broader view to authentication of RFID-tagged products that this paper promotes is relevant to the practitioners. In addition, since the existing theoretical knowledge of level of security different product authentication approaches provide or different products require is sparse, our formal investigation also provides a theoretical contribution.

This paper addresses security in terms of how well the functional and nonfunctional security requirements are satisfied, but it is important to note that the level of security of a running product authentication system is, ultimately, defined by its *security policy* and *security mechanisms*. Security policy is a specific statement of what is and is not allowed and security mechanisms enforce the policies [25]. In practice this means, for example, that it is not enough to have a secure tag authentication protocol if the people using the system do not verify the tag-product integrity. Moreover, technology alone is not enough to secure a product authentication system; for example, injection of false information remains an unaddressed threat in the EPC network because there is no undisputable proof that a custodian really has the product. In addition, the brand owners need to trust that entities who use the product authentication system want to use it to detect fake products and know how to do it. Also, secure and scalable key distribution is not yet solved for RFID. Solving these problems represents major organizational challenges for affected companies.

Our results can also be generalized beyond RFID. Although we derived the security requirements for RFID-tagged products, they can be extended to product authentication in general by considering tags as any kind of identifier or security feature that is used to identify and authenticate a product, such as barcode label or invisible ink. For example, the RFID tags could be replaced by 2-D barcodes without any implications to the level of security of location-based authentication, given that the back-end infrastructure remains unchanged.

Alexander [1] states that neutralizing all possible threats by misuse case analysis would be wishful thinking and cannot be stated as a requirement, but recognizes that also partial mitigations are useful as long as they afford a realistic increase in protection at a reasonable cost. This supports our claim that the derived set of functional security requirements can be used to benchmark the level of security of any RFID-based product authentication system. Understanding the level of protection different product authentication approaches provide is very important in order to provide the amount of protection a product needs depending on its sales price, distribution channel, life-cycle, and liability. Sandhu [48] argues that the level of security of a system should always be *good enough* but not more because too high levels of security lead to unnecessary costs, decreased flexibility, and reduced usability. The remaining research challenge is to find out, which approaches presented in this article provide this good enough security for which products. In particular, it is not yet known what the minimum level of visibility is that is needed to secure a distribution channel with the location-based authentication approach.

## X. Conclusion

Even though the vast majority of related literature only focuses on cryptographic RFID tag authentication, the ultimate goal behind these scholarly contributions is secure authentication of RFID-tagged products. Therefore, we have approached the problem from a broader perspective that is more similar to that of the affected companies who in the end will be the actual users of RFID technology. We have presented tag authentication, verification of object specific features, and location-based authentication as comparable options for authentication of tagged products. We have formulated a formal definition for product authentication process and derived the functional and nonfunctional security requirements for product authentication based on the underlying chain of trust. We have taken steps towards quantifying the different threats against the authentication process by assessing the involved risks in terms of consequences and likelihood. This risk assessment can be further revised by affected companies with product specific data when it will be available. We have estimated the level of security of different approaches in terms of cost to copy multiple products and probability of detecting copied products, which we argue are the elements that define the level of protection against adversaries seeking for financial gain. In particular, we argue that even modest tag cloning resistance can have a major impact on a counterfeiter's business case if clones can be detected with some probability, since then the counterfeiter needs to crack not one, but multiple tags. Our analysis of the EPC network shows that tag authentication is supported conceptually but not yet in practice, and that the forthcoming EPC discovery services will play an important role in guaranteeing the completeness of the history for location-based product authentication. Last, we uncovered structural shortcomings in the EPC network's support for location-based product authentication and presented how the shortcomings could be overcome by an EPC trace analysis service residing in the network's core service level.

## Acknowledgment

The authors would like to thank M. Aigner and A. Ilic for their support, and the anonymous reviewers whose comments helped to improve this paper.

## REFERENCES


[1] I. Alexander, "Misuse cases: Use cases with hostile intent," *IEEE Softw.*, vol. 20, no. 1, pp. 58–66, Jan./Feb. 2003.

[2] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," in *Requirements Engineering*. New York: Springer-Verlag, 2005, vol. 10, pp. 34–44.

[3] M. C. O'Conner, "EPC tags subject to phone attacks," *RFID J.* Feb. 2006 [Online]. Available: http://www.rfidjournal.com

[4] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically enabled RFID device," in *Proc. 14th USENIX Security Symp.*, 2005, pp. 1–16.

[5] S. Weingart, "Physical security devices for computer subsystems: A survey of attacks and defenses," in *Proc. Workshop Cryptographic Hardw. Embedded Syst.*, 2000, pp. 302–317.

[6] H. Gilbert, M. Robshaw, and H. Sibert, "An active attack against HB+—A provably secure lightweight authentication protocol," *Electron. Lett.*, vol. 41, no. 21, pp. 1169–1170, Jul. 2005.

[7] A. Juels, "Strengthening EPC tags against cloning," in *Proc. ACM Workshop Wireless Security*, 2005, pp. 67–76.

[8] T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC network—The potential of RFID in anti-counterfeiting," in *Proc. Symp. Appl. Comput.*, 2005, pp. 1607–1612.

[9] Z. Nochta, T. Staake, and E. Fleisch, "Product specific security features based on RFID technology," in *Proc. Int. Symp. Appl. Internet Workshops (SAINTW)*, 2006, pp. 72–75.

[10] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch, "From identification to authentication—A review of RFID product authentication techniques," presented at the Workshop on RFID Security, Graz, Austria, 2006.

[11] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[12] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard systems," in *Proc. 1st Int. Conf. Security Privacy Emerging Areas Commun. Netw. (SECURECOMM)*, 2005, pp. 47–58.

[13] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Proc. Int. Conf. Security Pervasive Comput. (SPC)*, 2003, pp. 454–469.

[14] R. Koh, E. Schuster, I. Chackrabarti, and A. Bellman, "Securing the pharmaceutical supply chain," Auto-ID Labs White Paper, Boston, MA, 2003. [Online]. Available: http://www.autoidlabs.org

[15] S. S. Alhir, *Learning UML*. Sebastopol, CA: O'Reilly Online Books, 2003.

[16] J. Westhues, "Hacking the prox card," in *RFID: Applications, Security, and Privacy*. Reading, MA: Addison-Wesley, 2005, pp. 291–300.

[17] Organization for Economic Co-operation and Development, Paris, France, "The economic impact of counterfeiting," 1998.

[18] U.S. Food and Drug Administration, Rockville, MD, "Combating counterfeit drugs—A report of the food and drug administration," 2004.

[19] GS1, Brussels, Belgium, "European passive RFID market sizing 2007–2022," 2007 [Online]. Available: http://www.bridge-project.eu/data/File/European%20Passive%20RFID%20Market%20Sizing%202007-2022-v1.pdf

[20] K. Norton, "Contactless payment comes to cell phones," *Business Week*, Nov. 21, 2006 [Online]. Available: http://www.nfc-forum.org

[21] NFC, "NFC Forum," 2007 [Online]. Available: http://www.nfc-forum.org/aboutus/

[22] C. Swedberg, "TwinLinx proposes to marry NFC and EPC," *RFID J.* (2006, Dec.) [Online]. Available: http://www.rfidjournal.com

[23] T. Wiechert, F. Thiesse, F. Michahelles, P. Schmitt, and E. Fleisch, "Connecting mobile phones to the Internet of things: A discussion of compatibility issues between EPC and NFC," presented at the Americas Conf. Inf. Syst. (AMCIS) Keystone, CO, 2006.

[24] German Customs Administration, "Dem Zoll in Hamburg gelingt vermutlich weltweit größter Plagiataufgriff—117 Container mit gefälschter Ware sichergestellt," Berlin, Germany, (2006, Nov.) [Online]. Available: http://www.zoll.de

[25] M. Bishop, "What is computer security?," *IEEE Security Privacy Mag.*, vol. 1, no. 1, pp. 67–69, Jan./Feb. 2003.

[26] J. Lee, D. Lim, B. Gassend, G. E. Suh, M. Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Proc. Symp. VLSI Circuits*, 2004, pp. 176–179.

[27] J. Pearson, "Securing the pharmaceutical supply chain with RFID and public-key infrastructure (PKI) technologies," Texas Instruments, Dallas, TX, White Paper, Jun. 2005. [Online]. Available: http://www.ti.com/rfid/docs/docntr.shtml

[28] G. A. Holton, "Defining risk," *Financial Analysts J.*, vol. 60, pp. 19–25, 2004.

[29] B. Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code in C*. New York: Wiley, 1996, ch. 1.

[30] EPCglobal, Boston, MA, "EPCglobal architecture framework version 1.0," Jul. 2005. [Online]. Available: http://www.epcglobalinc.org/standards/

[31] F. Kurose and K. Ross, *Computer Networking*. Amsterdam, The Netherlands: Addison-Wesley, 2003, ch. 8.

[32] A. Juels, "Minimalist cryptography for low-cost RFID tag," in *Prod. 4th Conf. Security Commun. Netw.*, 2004, pp. 149–164.

[33] I. Vajda and L. Buttyán, "Lightweight authentication protocols for low-cost RFID tags," presented at the Workshop Security Ubiquitous Comput., Seattle, WA, 2003.

[34] G. Tsudik, "YA-TRAP: Yet another trivial RFID authentication protocol," in *Proc. Int. Conf. Pervasive Comput. Commun. (PerCom)*, 2006, pp. 640–643.

[35] G. Avoine and P. Oechslin, "A scalable and provably secure hash based RFID protocol," in *Proc. IEEE Int. Workshop Pervasive Comput. Commun. Security (PerSec)*, 2005, pp. 110–114.

[36] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *Proc. IEEE Conf. Security Privacy Emerging Areas Commun. Netw. (SecureComm)*, 2005, pp. 59–66.

[37] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID," in *Proc. ECRYPT Workshop RFID Lightweight Crypto*, 2005, pp. 17–24.

[38] S. Dominikus, E. Oswald, and M. Feldhofer, "Symmetric authentication for RFID systems in practice," in *Proc. ECRYPT Workshop RFID Lightweight Crypto*, 2005, pp. 25–31.

[39] M. Feldhofer, M. Aigner, and S. Dominikus, "An application of RFID tags using secure symmetric authentication," in *Proc. 1st Int. Workshop Privacy Trust Pervasive Ubiquitous Comput. (SecPerU)*, 2005, pp. 43–49.

[40] D. Bailey and A. Juels, "Shoehorning security into the EPC standard," in *Proc. Int. Conf. Security Commun. Netw.*, 2006, pp. 303–320.

[41] D. Ranasinghe, D. Engels, and P. Cole, "Security and privacy: Modest proposals for low-cost RFID systems," presented at the Auto-ID Labs Research Workshop, Zurich, Switzerland, Sep. 2004.

[42] F. Thiesse, "RFID, privacy, and the perception of risk: A strategic framework," *J. Strategic Inf. Syst.*, vol. 16, no. 2, pp. 214–232, 2006.

[43] Bayer Technology Solutions, Leverkusen, Germany, "Protexxion product brochure," Oct. 2006. [Online]. Available: http://www.bayertechnology.com/eng/press/79_6540.php

[44] EPCglobal, Boston, MA, "Class-1 generation-2 UHF RFID conformance requirements specification v. 1.0.2," (2005, Jan.) [Online]. Available: http://www.epcglobalinc.org/standards/

[45] EPCglobal, Boston, MA, "EPC information services (EPCIS) version 1.0 specification," 2006.

[46] EPCglobal, Boston, MA, "Object naming service (ONS) specification version 1.0," (2005, Oct.) [Online]. Available: http://www.epcglobalinc.org/standards/

[47] EPCglobal, Boston, MA, "EPCglobal certificate profile ratified specification 1.0," (2006, Mar.) [Online]. Available: http://www.epcglobalinc.org/standards/

[48] R. Sandhu, "Good-enough security," *IEEE Internet Comput.*, vol. 7, no. 1, pp. 66–68, Jan./Feb. 2003.

[49] Taxation and Customs Union, Brussels, Belgium, "Community-wide statistics for 1999–2005," 2006. [Online]. Available: http://www.ec.europa.eu/taxation_customs/customs/customs_controls/counterfeit_piracy/statistics/index_en.htm

[50] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *Proc. Workshop Cryptographic Hardw. Embedded Syst. (CHES)*, 2004, pp. 357–370.

[51] Chaos Communication Congress, Hamburg, Germany, "RFID-Zapper," 2006. [Online]. Available: http://www.events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)

[52] S. E. Schechter, "Quantitatively differentiating system security," presented at the 1st Workshop Economics Inf. Security, Berkeley, CA, May 2002.

[53] S. E. Schechter, "Toward econometric models of the security risk from remote attacks," *IEEE Security Privacy Mag.*, vol. 3, no. 1, pp. 40–44, Jan./Feb. 2005.

[54] SupplyScape, Woburn, MA, "PS-ePedigree: How it works," 2007 [Online]. Available: http://www.supplyscape.com/products/security/pedigree/
[55] J. Wolkerstorfer, "Is elliptic-curve cryptography suitable to secure RFID tags," in *Proc. ECRYPT Workshop RFID Lightweight Crypto*, 2005, pp. 79–91.
[56] Sun Microsystems, Santa Clara, CA, "Elliptic curve cryptography: The next generation of internet security," 2002. [Online]. Available: http://www.research.sun.com/projects/crypto/ECC-Whitepaper.pdf
[57] T. P. Morgan, "Sun creates world's smallest SSL Web server," *Computerwire*, Jan. 2005. [Online]. Available: http://www.computerwire.com/industries/research/?pid=C55355B9-B6CD-42EC-80BC-ACFDA6F2CDD3
[58] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "An elliptic curve processor suitable for RFID-tags," Cryptology ePrint Archive, Graz, Austria, Report 2006/227, 2006. [Online]. Available: http://www.eprint.iacr.org/
[59] L. T. Mirowski, "Detecting clone radio frequency identification tags," B.S. thesis, School Comput., Univ. Tasmania, Tas, Australia, Nov. 2006.
[60] Impinj, Seattle, WA, "Impinj RFID product overview, Monza/ID," 2007. [Online]. Available: http://www.impinj.com/rfid/
[61] CNN Money, Atlanta, GA, "Fortune 500—Annual ranking of america's largest corporations," 2007. [Online]. Available: https://www.money.cnn.com/magazines/fortune/fortune500/2007

**Mikko O. Lehtonen** (M'07) was born in Helsinki, Finland, in 1981. He received the B.S. and the M.S. degrees (in communications engineering and telecommunications management) from Helsinki University of Technology, Helsinki, Finland, in 2006, and the diploma in multimedia communications from the Eurecom Institute, Sophia-Antipolis, France. He is currently pursuing the Ph.D. degree from the Swiss Federal Institute of Technology, ETH Zürich, Zürich, Switzerland.

He has worked as a Research Assistant with the Signal Processing Laboratory, Helsinki University of Technology, and with the IDIAP Research Institute, Martigny, Switzerland. He has previously worked on signal processing and speech recognition. His current research interests include technical and business aspects of RFID in product authentication and product-centric information management.

Mr. Lehtonen is a member of the Finnish Association of Graduate Engineers, TEK.

**Florian Michahelles** received the M.Sc. degree (Diplom-Informatiker Univ.) in computer science and psychology from the Ludwig-Maximilians-University of Munich, Munich, Germany, in 2001, and the Ph.D. degree from ETH Zürich, Zürich, Switzerland, for his research in participative design of wearable computing applications and the development of innovative business cases for ubiquitous computing, in 2004.

He is currently the Associate Director of the Auto-ID Laboratory, Zürich/St. Gallen, Switzerland, and the Manager of the Laboratories of Prof. Fleisch with the Department of Management, Technology, and Economics, ETH Zürich. In Spring 2000, he was a Sloan Visiting Fellow with MIT Sloan School of Management, Boston, MA, where he focused his studies on entrepreneurship and management of innovation. He was a Researcher in the former group of Prof. Bernt Schiele with ETH Zürich, where he worked for the EU-funded Smart-Its project lead by Prof. Hans-Werner Gellersen and the ETH-funded Wearable Computing Poly Project lead by Prof. Gerhard Tröster. His research interests include the following topics centered among the internet of things: RFID applications, extending the EPC network for sensing capabilities, technical approaches against anti-counterfeiting, and RFID applications for the end-consumer.

**Elgar Fleisch** was born in Bregenz, Austria. After graduating from the School of Engineering in Bregenz, he studied business administration and computer science at the University of Vienna, Vienna, Germany, and wrote his Ph.D. thesis at the Vienna University of Economics and Business Administration and the Institute for Advanced Studies in the area of artificial intelligence in production scheduling.

Since October 2004, he has been the Professor of information management with the Department of Management, Technology, and Economics, ETH Zürich, Zürich, Switzerland. He is also the Professor of technology management and the Director of the Institute of Technology Management, the University of St. Gallen. Currently, he conducts research on information management issues in the ubiquitously networked world, including the dynamics of information systems in conjunction with business processes and real world problems. Together with Prof. Friedemann Mattern of the Institute of Pervasive Computing, ETH Zürich, he leads the M-Laboratory and cochairs the Auto-ID laboratories, which specify the infrastructure for the "Internet of Things." He is a cofounder of Intellion AG. In 1994, he was with the University of St. Gallen, where he focused on "Business Networking." In 1996–1997, he founded and served IMG Americas Inc., Philadelphia, PA, as its CEO. In 2000, he was an Assistant Professor with the University of St. Gallen, St. Gallen, Switzerland.

Prof. Fleisch is a member of curators of SAP Research, advisory board of Executive School for Management, Technology, and Law (HSG), registered association of business-school professors, the Swiss computer scientist association, and a member of several steering committees in research, education, and industry.