ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
University of St.Gallen

AUTO–ID LABS

From Identification to Authentication

A Review of RFID Product Authentication Techniques

Mikko Lehtonen, Thorsten Staake,
Florian Michahelles, Elgar Fleisch

Auto-ID Labs White Paper WP-BIZAPP-029

Mikko Lehtonen
Senior Researcher
ETH Zurich

Thorsten Staake
Senior Researcher
University of St.Gallen

Florian Michahelles
Associate Director
Auto-ID Labs ETH Zurich

Elgar Fleisch
Research Director
Co-Chair of Auto-ID Labs
University of St.Gallen and ETH Zurich

Contact:

Auto-ID Labs ETH Zurich/St.Gallen
Swiss Federal Institute of Technology (ETH) Zurich
Department of Management, Technology and Economics
Kreuzplatz 5
8032 Zurich
Switzerland

Phone: +41 44 632 86 24
Fax: +41 44 632 10 45

E-Mail: mlehtonen@ethz.ch
Internet: www.autoidlabs.org

Business Processes & Applications

Abstract

Authentication has an important role in many RFID applications for providing security and privacy. In this paper we focus on investigating how RFID can be used in product authentication in supply chain applications and a review of existing approaches is provided. The different categories of RFID product authentication approaches are analyzed within the context of anti-counterfeiting and fields where future research is needed are identified.

1. Introduction

Since the identification, friend or foe (IFF) systems used in the Second World War, radio frequency devices have been applied to identify physical objects [1-3]. Nowadays radio frequency identification (RFID) enables automated data gathering in various applications like pallet identification [4], cattle tracing [5] and access control [6]. However, identification itself does not guarantee that the acquired identity corresponds to the genuine identity and thus also verification or validation of the claimed identity – authentication – is needed.

Product authentication in supply chain provides great opportunities to fight illicit trade by detecting counterfeit products. Counterfeiting is a rapidly growing world wide problem that affects a great number of industries and harms societies in many ways [7]. Counterfeit players work to get a return on investment for their illegal actions. The overriding requirement of any anti-counterfeiting system is to change the risk-return profile for the counterfeiters – raising the risk and thereby minimizing the return [8]. Product authentication techniques form an important tool in turning the expected return less favourable for the illicit actors thus supporting the legal trade.

In this paper we concentrate on the use of RFID technology in product authentication. Our contribution is to present the requirements of product authentication in supply chain applications and to show how RFID can be used as an enabling technology for product authentication. Our focus is on security and therefore the attack scenarios of counterfeit players and their implications to RFID are presented. Then, categorization and review of existing RFID product authentication approaches are provided. In discussion the presented approaches are analyzed. We finish by identifying fields where future research is needed.

2. Product Authentication in Supply Chain Applications

The role of product authentication is to answer whether a given product is genuine or counterfeit (e.g. product that infringes a trademark). An explicit way to authenticate products is needed in supply chain applications because counterfeits can be very similar or even identical to authentic products. The starting point of automated non-destructive product authentication is to insert a special label or security feature into products, like a hologram or a water mark, and to authenticate this label.

Product authentication can take place in single item level or in aggregated levels. Generally, multiple similar units are authenticated simultaneously, for example when a shipment arrives to a retail store. The desired level of security, which can be defined as the effort an illicit actor has to undertake to break or bypass the security mechanism, has a major impact on the cost of a product authentication system. While minimizing the cost, the level of security should be high enough to protect the item over its entire life-span. Because different products have very varying security requirements, different levels of security and thus different solutions are needed.

The level of security of product authentication system is defined by the level of security of a single security feature and by the granularity of the security features. By granularity we mean here how many products use an identical security feature; for example, applying weak but unique security features to all products can be more secure than using strong but identical feature on the same products. One conceptual problem of automated product authentication is that it is only the security feature that is authenticated and not the product itself – therefore difference between label and product authentication should be made. The general requirements of product authentication system in supply chain application are listed below:

- The system needs to be used by multiple parties from multiple locations
- Authentication of products that are unknown to the system should be supported
- The cost and effort to perform a check need to be low
- The optimal solution should allow also the customers to authenticate products
- The product authentication system needs to have an appropriate level of security

Among the requirements listed above, the level of security demands most attention in the system design. The level of security can be considered as the resistance against attacks that are conducted against the authentication system. In supply chain applications, product authentication is typically performed under the supervision of authorized personnel. This restricts the possible attacks of counterfeit players. The general attack scenarios of illicit actors against product authentication system can be divided into following four categories:

Omission of security features which are applied on the genuine objects refers to the counterfeiters not taking any explicit actions to fool the authentication. These products form a considerable part of the counterfeit trade for example due to consumer demand of counterfeits.

The use of misleading security features means that the fake products are equipped with security features whose role is to make the products avoid closer inspection. Interviews with brand owners and customs reveal that this scenario together with the aforementioned one is dominant especially for all goods which are mass produced or where the consumers do not regularly check for the object's authenticity.

The removal and reapplying of authentic security features remains a threat in all automated product authentication systems if not explicitly addressed by binding the product and the label. However, because acquiring and reapplying authentic labels is costly, this attack does not threaten authentication systems in large scales.

The cloning and imitation of security features is the most obvious attack that a product authentication system has to resist. As the underlying problem of counterfeits is that the products themselves can be cloned, the first line of defence is to integrate such security features into products that are hard to be replicated.

3. RFID Product Authentication Techniques

RFID has considerable potential in product authentication. The benefits of RFID compared to old authentication technologies include non line-of-sight reading, item-level identification, non-static nature of security features, and cryptographic resistance against cloning. RFID systems in general comprise transponders, readers or interrogators, and online database, sometimes referred to as the back-end server. The potential of RFID in anti-counterfeiting is discussed further in [9] and [10].

There are many applications where RFID transponders are already used for authentication, for example access control. While RFID product authentication is very close to RFID access control what comes to the used authentication protocols, product authentication needs specific solutions because of the specific application requirements discussed in the previous section. RFID product authentication can be based on transponder authentication or identification and additional reasoning using online product data. Furthermore, RFID supports for secure ways to bind the label and the product.

To resist cloning and forgery are the most important security properties of authentication tags. The simplest cloning attack against an RFID tag only requires reading the tag serial number and programming the same number into an empty tag. There are two essential obstacles against this kind of replication. First, even the low-cost transponders (e.g. EPC Class-1 Generation-2 [11]) have a unique factory programmed chip serial number (or

transponder ID, TID) that is similar to the unique MAC address of PC network cards. To clone a transponder's TID would therefore also require access to hardware manufacturing.

Second obstacle against cloning is to use read-protected secrets residing on tags and to check if the tag knows these secrets, for example by cryptographic challenge-response protocols. Even though this can provide significant improvements to tag's cloning resistance, there remain many ways to conduct a cloning attack against a single tag. These attacks include side channel attack [12], reverse-engineering and cryptanalysis [13], brute-force attack [14], physical attacks [15] and different active attacks against the tag [16]. In addition, shared secrets based product authentication approaches are always vulnerable to data theft, where the secret PIN codes or encryption schemes of valid products are stolen or sold out by insiders, which would enable criminals to create phoney tags. This scenario is especially interesting for adversaries because it would allow them to clone a large number of tags.

Other RFID security issues that have to be considered in product authentication comprise resistance against denial of service (DoS) attack. In general, DoS causes loss of service to users. Even though it cannot be used to fool the product authentication, it can pose a threat for the overall process. In RFID DoS attack can be conducted, for example, by jamming the readers with hidden blocker tags [17] or by de-synchronizing tag and a database entry [18].

We assume that product authentication is normally performed under the surveillance of authorized personnel or by the customer, which narrows down the possible attack scenarios. Therefore active attacks, where the adversary would need to participate in the authentication session and use special devices in the proximity of the reader (e.g. replay, relay and man-in-the-middle attack), are not considered as realistic threats against RFID product authentication.

4. Review of RFID Product Authentication Approaches

In this section we provide a review of existing and proposed RFID product authentication approaches. The approaches are categorized into four categories depending on what the authentication is based on. The approaches presented in subsections 4.1 and 4.2 authenticate the products without tag authentication, while in approaches presented in subsections 4.3 and 4.4 the tag or the data the tag stores is authenticated.

4.1. Unique Serial Numbering

By definition, one of the fundamental assumptions in identification, and thus also in authentication, is that identified entities possess an identity. In supply chain applications, issuing unique identities can be efficiently accomplished with RFID. We recognize unique

serial numbering and confirmation of validity of identities as the simplest RFID product authentication technique. The potential of unique numbering of objects without tag authentication is discussed by Juels in [19]. There the author provides an example from the art world, where a Victorian painter Alma-Tadema evaded the problem of counterfeiting by writing unique serial numbers on his paintings and cataloguing the numbers. Product authentication without tag authentication has been proposed also by **Takaragi et al.** [20].

Koh et al. [21] proposed ways of RFID product authentication in the pharmaceutical supply chain. One of the proposals was to keep a list of valid product ID numbers in a secure online server so that the absence of a product's ID from that list would serve as an indication of counterfeit. The security of this approach relies on keeping the list secret for counterfeiters while providing needed access for it to licit parties.

Counterfeiters can always try to guess the valid serial numbers, especially when the numbers are issued in a systematic way. Therefore unique serial numbering can be made more secure by assigning the serial numbers in a random way from a large name space. This is possible with RFID, due to the supported long identifiers. The clear unaddressed weakness of unique serial numbering approaches is tag cloning. However, duplicated tags can be detected and are an important indicator of counterfeit. Furthermore, these approaches can be implemented in RFID enabled supply chain systems with little additional cost, as RFID tags are already being used for pallet and case level identification in large scales [4].

4.2. Track and Trace based Plausibility Check

Track and trace [10, 21, 22] refers to generating and storing inherently dynamic profiles of individual goods as products move through the supply chain. The product specific records allow for heuristic plausibility checks, for example a product with a serial number registered for sale in Switzerland is suspicious if offered in an American store at the same time. The plausibility check is suited for being performed by customers who can reason themselves whether the product is original or not, though it can also be automated by suitable artificial intelligence.

Track and trace is a natural expansion of unique serial numbering approaches. Furthermore, track and trace will be used in supply chains also for other purposes, such as for deriving a product's history and for organizing product recalls. In addition, some industries like pharmaceutical industry have legislation that demands companies to document product pedigrees [23]. Therefore track and trace based product authentication can be cost-efficient for companies, as also other applications justify the expenses. However, generating and gathering track and trace profiles of products in multi-party supply chains can be hard and requires cooperation between the partners.

4.3. Secure Object Authentication

Secure object authentication techniques make use of cryptography to allow for reliable authentication while keeping the critical information secret in order to increase resistance against cloning. Because authentication is needed in many RFID applications, the reviewed protocols come from different fields of RFID security and privacy.

One of the first cryptographic privacy enhancing technologies for RFID is the hash-lock of **Weis et al.** [24]. The design principles behind the proposed scheme include the assumption that tags cannot be trusted to store long-term secrets when left in isolation. The authors proposed a way to lock the tag without storing the access key, but only a hash of the key on the tag. The key is stored in a back-end server and can be found using the tag's meta-ID. This approach can be applied in authentication, namely unlocking a tag would correspond authentication. However, the cloning resistance of the scheme is based only on the locked state of the tags and so it is more suitable for protecting privacy. **Henrici et al.** [25] have later extended the randomized version of the original hash-lock scheme [24] for increased privacy and scalability.

Avoine et al. [26] proposed another hash-based RFID protocol that provides modified identifiers for improved privacy and that can be applied for authentication. In the proposed protocol the authors solve scalability issues of the privacy-enhancing scheme from [27] by introducing a specific time-memory trade-off. In addition, hash-based RFID protocols for mutual authentication have been proposed in [28-30]. All these protocols rely on synchronized secrets residing on the tag and back-end server and they require a one-way hash function from the tag. These approaches show how guaranteeing the un-traceability by updating tag identifier increases the workload of back-end servers.

Texas Instruments has developed RFID based authentication techniques for pharmaceutical industry. The model presented in [22] bases on authenticating the products through digital signatures that are written on tags. By using TID and a public key, the transponder can be linked to the signer of the data in a provable way. To improve the traceability of products, tag memory is also used to store chain-of-custody events.

Juels et al. [31] presented an approach to increase tracing and forgery resistance of RFID-enabled banknotes by using digital signatures for RFID authentication. The approach uses re-encryption to avoid static identifiers and optical data on the banknote to bind the RFID tag and the paper. Authentication is performed by verifying that the data on the tag is signed using a valid public key. In order to increase cloning resistance, the authors suggest including some distinctive characteristics of the physical media into the signature (i.e. physical fingerprint of the banknote) and verifying the validity of these characteristics as a part of the authentication process. **Zhang et al.** [32] have later enhanced the protocol by addressing some integrity issues.

Tsudik [33] proposed an authentication protocol called YA-TRAP which provides tracking-resistant tag authentication through monotonically increasing timestamps on the tag. YA-

TRAP requires a pseudo-random number generator (PRNG) from the tag and its basic version is vulnerable to DoS attack through timestamp de-synchronization between the tag and the server. The approach does not require on demand computation for the back-end as a result of a pre-computed hash-table for later tag verification, which means less load for the server than for example in [34]. **Chatmon et al.** [35] proposed anonymous RFID authentication protocols based on YA-TRAP that provide anonymity for authenticated transponders and address some vulnerabilities of the original design, while increasing the server workload.

Juels [36] discussed minimalist cryptography based authentication and proposed a tracking-resistant pseudonym-throttling scheme. This mutual authentication protocol bases on a list of pseudonyms and keys residing on tag and on back-end server. The protocol needs additional memory on tag and uses a way to update the tag's pseudonym list using one-time pads to resist cloning and eavesdropping. However, the communication cost is relatively high because of the tag data updates.

Juels proposed another low-cost authentication in [37], where the read-protected 32-bit kill passwords of EPC Class-1 Generation-2 tags are used to implement ad-hoc tag authentication protocol. The protocol bases on the fact that even though the EPC of a transponder can be skimmed, the kill-password remains secret. Cloned tags can be found by testing, without killing the tag, if the kill password matches the original one stored in a database. Furthermore, the protocol supports for mutual authentication.

Vajda et al. [38] discussed lightweight authentication protocols for low-cost tags. The proposed set of challenge-response protocols includes simply XOR encryption with secret keys (although also complex encryption like RSA was proposed, it's not considered here because it's infeasible in low-cost tags [39]). The cryptographic problem with keys being static in XOR encryption is addressed by re-keying schemes that make use of keys from multiple previous protocol runs.

Juels et al. [39] introduced an approach for low-cost authentication based on the work of Hopper and Blum (HB) [40]. The proposed HB+ protocol makes use of the hardness assumption of statistical "Learning Parity with Noise" (LPN) problem and can be implemented on low-cost tags, as it only requires bitwise AND and XOR operations and one random "noise bit". The security of HB+ against active adversaries has gained publicity in the scientific community and is discussed in details in [41]. The first version of the original protocol [39] was found to be vulnerable against a realistic active attack [16]. Proposals to address the security issues have emerged, including the modified HB++ by **Piramuthu** [42].

Dimitriou [43] proposed a protocol that addresses privacy issues and aims at efficient identification of multiple tags. The enhanced version of the protocol is considered here, since the basic one does not protect the tags against cloning. In this approach the tags need a PRNG and a pseudo random function (PRF) for symmetric-key encryption. The proposed protocol is efficient in terms of tag-to-reader transaction and protects the privacy by avoiding transmission of static IDs. However, since the tags share secret keys, compromise of one tag may reveal information about others. In another work [44] the author proposed a lightweight RFID protocol against traceability and cloning attacks. This approach bases on a refreshing a shared secret between tag and back-end database and requires hash calculations and PRNG from the tag.

Duc [45] proposed communication protocol for RFID devises that supports for tag-to-reader authentication based on synchronization between tag and back-end server. The proposed scheme is tailored for EPC Class-1 Generation-2 tags so that it requires only a PRNG on the tag and pre-shared keys. The approach also takes advantage of the CRC function that is supported by Generation-2 tags. The underlying idea is to use the same PRNG with the same seed on both RFID tag and on back-end side and to use it for efficient key sharing. The encryption and decryption can then be done by XORring the messages.

Ranasinghe et al. [46] presented ways to implement challenge-response authentication protocol on RFID tags without using costly cryptographic primitives. These proposals are based on a Physical Unclonable Function (PUF) residing on the tag, which allows for calculation of unique responses using only some hundreds of logical gates. A possible candidate for the PUF can be found from [47], where the manufacturing variations of each integrated circuit are used to implement a secret key on a tag. The back-end server needs to store a list of challenge-response pairs for each PUF (i.e. for each tag) because, without encryption, a PUF challenge-response pair that is once used, can not be used again since it may have been observed by an adversary. The PUF based security is still an area of active research. Also **Tuyls et al.** [48] proposed the use of PUFs to increase RFID transponders resistance against both physical and communication based cloning attacks and defined an offline authentication protocol. The authors estimated that their anti-clone tag can be built with on the order of 5,000 gates.

Engberg et al. [49] proposed so called zero-knowledge device authentication as an answer to consumer privacy issues. In their proposal the tag must authenticate the reader before it returns any traceable identifier. The scheme is based on shared secrets and requires hash function from the tag. **Also Rhee et al.** [50] proposed a challenge-response protocol for user's privacy. The proposed protocol doesn't update the tag ID and therefore can be applied in an environment with distributed databases. The protocol relies on hash calculations by the back-end database, so that the tag ID is the only necessary shared secret between the devices taking part in the authentication.

Molnar et al. [51] proposed private authentication protocols for library RFID, where the tag and the reader can do mutual authentication without revealing their identities to adversaries. The protocols made use of PRNG residing on the tag**. Molnar et al.** presented in [34] another privacy enhancing scheme where an RFID pseudonym protocol takes care of emitting always a different pseudonym using PRF. In order to relate pseudonyms and real tag IDs, the authors presented an entity called Trusted Centre (TC) that is able to decode the tag responses and obtain the tag's identity. In the same work the authors introduced term ownership transfer that refers to TC giving permissions to only readers of a certain entity to read an RFID tag.

Gao et al. [52] proposed protocols for improved security and privacy of supply chain RFID. In their proposals the tags store a list of licit readers to protect the tags against skimming and therefore need rewritable memory. Other tag requirements include PRNG and hash function. Though the protocol burdens the back-end server with some computational load, the approach is designed to be suitable for a large number of tags. **Yang et al.** [53] proposed a mutual authentication protocol that provides protection against replay attack and MITM attack even when the reader is not trusted and the communication channel is insecure. This mutual

authentication protocol provides privacy protection and cloning resistance with the expense of tag's hash calculations and storing two secrets in the tag and in the back-end server.

Dominikus et al. [54] discussed symmetric RFID authentication protocols in practice and presented five standard challenge-response protocols for reader, tag and mutual authentication. The design focuses on strong authentication for advanced, about 50 ¢ tags with available silicon area of 10,000 gates. The presented protocols use AES encryption (and decryption) on tags in such a way that energy constraints of Class-2 RFID systems are met.

Feldhofer [55] presented an implementation of standard symmetric two-way challenge-response protocol as an extinction to the standard ISO/IEC 18000 RFID protocol. The use of standard authentication protocols with standard communication protocols is important for ensuring the security and interoperability of an approach. Hardware implementation of the same protocol can be found from [56], where **Feldhofer et al.** presented a novel minimalist approach of a 128-bit Advanced Encryption Standard (AES) implementation. The approach provides a promising choice for strong authentication in RFID systems and the proposed low-cost AES hardware implementation is used in various other proposals as an enabler of cost-efficient RFID cryptography.

Also **Bailey et al.** [57] concentrate on integrating common cryptographic standards into RFID by proposing techniques to create RFID tags that are compliant with the EPC Class-1 Generation-2 tags, but offer cryptographic functionality of standards like ISO 7816-4. The proposed challenge-response protocols make use of AES on the tag and can be used for mutual authentication. In particular, the authors define a 32 or 64 bit "one-time password" that could be included in transmitted EPC data fields.

4.4. Product Specific Features

To explicitly address transponder removing and reapplying (and also cloning) attack with low-cost tags, **Nochta et al.** [58] proposed a cryptographic way to bind the RFID transponder and the product that it authenticates. Because of the uniqueness of the approach, we consider it as a separate category of RFID product authentication. In this approach the authentication is based on writing on the tag memory a digital signature that combines the TID number and product specific features of the item that is to be authenticated. These features can be physical or chemical properties that identify the product and that can be verified, such as very precise weight. The chosen feature is measured as a part of the authentication and if the feature used in the tag's signature does not match the measured feature, the transponder-product pair is not original.

The proposed authentication needs a public key stored on an online database. Also an offline authentication is proposed by storing the public key on the tag, though this decreases the level of security. The disadvantage of this approach is that each unit has to be physically verified as a part of authentication.

4.5. Tag Requirements for Authentication

In order to evaluate RFID product authentication in practice, the cost of authentication needs to be considered. One of the most important cost drivers of RFID product authentication is transponder cost that is, for its part, mostly defined by the complexity of the chip (or integrated circuit, IC). The complexity of the chip can be described by several informal metrics [59] like the number of transistors or the gate equivalent (GE), or gate count, that is about a fourth of the number of transistors. The gate count of current low-cost transponders is 5,000 – 10,000 [53] [60], limiting their computational power to only a fraction of that of computers. In addition, the number of gates available for security features is even smaller and estimated to be below 2,000 [61] or below 5,000 [53]. The rule of thumb of gate cost says that every extra 1,000 gates increase the chip price by 1 ¢ [61].

In order to be able to evaluate the transponder cost more precisely, we quantify the transponder's technical requirements. The requirements we consider include first of all additional non-volatile memory (NVM) which is typically EEPROM. Different types of NVM exist: factory-programmable memory (or read only), field programmable memory (or write-once-read-many, WORM) and read-write (RW) memory. Other requirements relate to the transponder's ability to perform logical operations. Logical functionalities can be implemented on chips basically by increasing the gate count and they include first of all the ability to perform primitive bitwise operations (e.g. AND, XOR) that can be implemented with a small number of gates. Other requirements include hash function that is a common cryptographic primitive but so far out of the scope for low-cost RFID transponders – standard cryptographic hash functions like SHA-1 need roughly 20,000 gates [61]. Weis discusses non-linear feedback shift registers as one possible low-cost hash function [61] as it has no complex hardware requirements (besides the register). Interestingly, Yüksel [62] presented implementations of low-cost hash functions, taking only 1,700 gates for block size of 64 bits.

Another tag requirement is pseudo-random number generator (PRNG) that can be implemented for example by keying a hash function. However, it is still unclear how and when adequate PRNG can be deployed on inexpensive RFID tags [24, 63]. Last considered tag requirement is symmetric key encryption, or in general pseudo random function (PRF). Public key encryption is not considered because it is too expensive for RFID transponders [54]. A common example of symmetric key encryption is the Advanced Encryption Standard (AES) block-cipher which can be used to encrypt data using a secret key. Hardware implementations of AES take on the order of 20,000 – 30,000 gates [61], which seemed to constrain it out of the scope of low cost transponders still a few years ago. However, Feldhofer et al. [56] presented an implementation of 128 bit AES encryption which requires only 3,600 gates (and 256 bits RAM) which is considerably fewer than the smallest AES circuit published so far, bringing cost-efficient strong authentication closer to reality for RFID tags.

To illustrate available tag resources for product authentication, the properties of three example tags are summarized in Table 1. The simplest example tag, denoted label tag, provides only a factory programmed label, like the EPC Class-0 [64]. This tag can be used in approaches where only tag identification is required (subsections 4.1 and 4.2). The more advanced smart label presents an EPC Class-0 Generation-2 tag [11] with RW memory

(even though Class-1 tags were originally designed for WORM memory [65], also tags with RF memory are available, e.g. [66]). The cheapest EPC Class-1 tags cost on the order of 15 ¢ in high volumes [67]. The crypto tag presents an advanced (e.g. Class-2) transponder. Such tags cost about 50 ¢ and have silicon area of about 10,000 gates [54].

Table 1. Summary of example transponders' resources

	NVM	RW	Bitwise Operations	PRNG	Hash function	Symmetric key encryption
Label Tag	64 bits					
Smart Label	96 bits	Yes	Yes	16 bit		
Crypto Tag	256 bits	Yes	Yes	64 bit		Yes

5. Discussion

In this paper, we have provided a review of existing RFID product authentication techniques. Four categories of approaches are distinguished based on what is the reasoning behind the check. In general, either the transponder is authenticated or the reasoning is based on identification and additional information in online databases.

The focus of the review is on cryptographic secure object authentication approaches which are by far the most discussed category of RFID authentication techniques within the scientific community. This is partly explained by the fact that the considered secure protocols origin from the field of RFID security and privacy in general and thus they can be applied in transponder and product authentication also. The main motivation to use cryptographic tags for product authentication and anti-counterfeiting is the increased cloning resistance. Even though secure object authentication approaches remain vulnerable to many attacks that can enable tag cloning, they can provide a significantly improved level of security for original products.

However, also other, potentially more cost-efficient solutions exist – for example, also a reliable way to find the duplicated tags could be used to make cloning non-profitable for counterfeiters. The presented categories of low-cost product authentication approaches are unique serial numbering and track and trace based plausibility check. Even though these approaches do not prevent tag cloning, also they can be used to significantly increase the barrier of counterfeit players to distribute fake products. The better cost-efficiency of these approaches compared to cryptographic techniques is supported by two facts. First, they need only low-cost tags and they support for relatively simple authenticity checks. Second, unique serial numbering and track and trace are used also in other supply chain applications and so authentication is not only application responsible for the hardware costs, whilst the increased transponder costs of secure object authentication approaches must be justified entirely by the increased cloning resistance.

All the approaches presented in the review provide a careful trade-off between complexity and security. In order to evaluate the optimal product authentication system for anti-

counterfeiting, the costs and benefits of different techniques have to be evaluated. As stated in introduction, the overriding requirement of any anti-counterfeiting system is to change the risk-return profile for the counterfeiters. The counterfeiter will carry out some form of direct or indirect cost-benefit analysis before embarking on criminal enterprises [8]. Product authentication increases the illicit players' risk of getting caught and decreases the number of counterfeit products in the market. The affected companies will benefit from this for example through additional sales. Though the precise mechanism how companies benefit from product authentication is very hard to be quantified, security of authentication plays an important role as an enabler of those benefits. Therefore the appropriate way to compare different product authentication approaches for anti-counterfeiting is to consider their security and cost.

Security of RFID product authentication can be evaluated by considering cloning resistance, ability to detect cloned tags and resistance against tag removal and reapplying. Active attacks against readers are not considered as realistic threats against product authentication system. Cost of an approach can be evaluated by considering the general complexity of check and cost of transponder. Table 2 summarizes these abovementioned properties of the four general product authentication categories. For more detailed comparison, a comprehensive summary of technical requirements of the presented approaches is presented in Table A-1 (Appendix A).

Table 2. Comparison of different product authentication categories

Approach	Complexity of check	Cost of tag	Cloning resistance	Clone detection	Tag reapplying resistance
Serial Numbering	Low	Low	No	No	No
Track and Trace	Medium	Low	No	Yes	Yes
Secure Authentication	Medium-High	Low-High	Yes	No	No
Product Specific Features	High	Low	Yes	No	Yes

Based on the discussion so far, unique serial numbering and track and trace based approaches are most probable to provide convenient authentication techniques for consumer goods and other low-cost items; secure object authentication techniques can be applied for more expensive products when tag cloning needs to be addressed. However, there are also promising low-cost methods to increase the cloning resistance of all RFID tags, such as the use of unique transponder ID number, which could make cryptographic tags unnecessary for most product categories.

The cost of cryptographic product authentication transponders (e.g. the crypto tag, Table 1) will be determined by the development of minimalist hardware implementations of two most important cryptographic primitives, hash functions and pseudo random functions. The importance of these functions as enablers of secure object authentication approaches can be clearly seen in Table A-1. However, the development of secure protocols that can be implemented using only simple bitwise operations on tags can create a family of truly low-cost tags (e.g. the smart label, Table 1) for secure authentication.

Finally, the review reveals that offline authentication remains unsolved as practically all existing techniques need online servers. Current development of RFID protocols is driven mostly by privacy concerns and the goal is often an efficient use of back-end server to protect customers against tracing. Attempts to be independent from network are rare and they might need further development from the field of physical unclonable functions. Also many network issues remain unsolved. The open questions include key distribution, scalability, generation of track and trace profile in multi-partner environment, ownership transfer and the need for trusted third parties. Furthermore, as in all RFID applications, the role of standards is of primary importance in product authentication and should be taken into account in solution design.

6. Conclusions

This work shows that there is no silver-bullet approach for moving from radio-frequency identification to authentication and therefore accurate and well justified ways to compare the different techniques are needed. The focus of recent development in RFID authentication has been on consumer privacy, but product authentication needs also specific solutions to address the application requirements. Further research is still needed in the field of offline authentication and many network issues, before RFID product authentication will meet all its promises in practice. Furthermore, possible scalability issues of different approaches need to be discovered for example in terms of number of organizations who can read and authenticate the products.

References

[1] Lampe, M. and Strassner, M. (2003). The Potential of RFID for Moveable Asset Management. In Workshop on Ubiquitous Commerce at Ubicomp 2003.

[2] NJE Consulting (2006). RFID in Waste Management. Available at http://www.nje.ca/Index_RFIDWasteManagement.htm (22.6.2006).

[3] RFID in Japan (2005). Shoe RFID expands. News Article, July 10, 2005 (via Nikkei Ryutsu Shimbun MJ, July 6, 2005). Available at http://ubiks.net/local/blog/jmt/archives3/004067.html (22.5.2006).

[4] RFID Journal (2003). Wal-Mart Draws Line in the Sand. News Article, June 11, 2003. Available at http://www.rfidjournal.com/article/articleview/462/1/1/ (11.5.2006).

[5] RFID Journal (2003). Can RFID Save the Cattle Industry? Vertical Focus, December 23, 2003. Available at http://www.rfidjournal.com/article/articleview/1032 (22.5.2006).

[6] RFID Journal (2003). Long-Range RFID for Access Control. News Article, July 8, 2003. Available at http://www.rfidjournal.com/article/articleview/493/1/1/ (22.6.2006).

[7] International Chamber of Commerce (2005). IP Roadmap 2005: Current and emerging intellectual property issues for business. ICC, Paris, 2005, 52 pp. Available at http://www.iccwbo.org/iproadmap/ (19.5.2006).

[8] Organization for Economic Co-operation and Development (OECD) (1998). The Economic Impact of Counterfeiting. Available at http://www.oecd.org/dataoecd/11/11/2090589.pdf (3.5.2006).

[9] U.S. Food and Drug Administration (2004). Combating Counterfeit Drugs - A Report of the Food and Drug Administration. February 2004. Available at http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html (2.5.2006).

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

[11] EPCglobal (2005). Class-1 Generation-2 UHF RFID Conformance Requirements Specification v. 1.0.2. EPCglobal public document, February 2005.

[12] RFID Journal (2006). EPC Tags Subject to Phone Attacks. News Article, February 24, 2006. Available at http://www.rfidjournal.com/article/articleview/2167/1/1/ (4.5.2006).

[13] Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A., and Szydlo, M. (2005). Security analysis of a cryptographically enabled RFID device. Pre-print. Available at www.rfidanalysis.org (4.5.2006).

[14] RFID Journal (2003). RFID, Privacy and Corporate Data. Feature Article, June 2, 2003. Available at http://www.rfidjournal.com on subscription basis.

[15] Weingart, S. (2000). Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defense. In Cetin Kaya Koc and Christof Paar, editors, Proceedings of CHES'00, volume 1965 of Lecture Notes in Computer Science, pages 302--317. Springer-Verlag, 2000.

[16] Gilbert, H., Robshaw, M., and Sibert, H. (2005). An active attack against HB+ – a provably secure lightweight authentication protocol. Manuscript, July 2005.

[17] Juels, A. and Brainard, J. (2004). Soft blocking: Flexible blocker tags on the cheap. In Sabrina De Capitani di Vimercati and Paul Syverson, editors, Workshop on Privacy in the Electronic Society – WPES, pages 1–7, Washington, DC, USA, October 2004. ACM, ACM Press.

[18] [18] Kang, J. and Nyang, D. (2005). RFID authentication protocol with strong resistance against traceability and denial of service attacks. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05, volume 3813 of Lecture Notes in Computer Science, pages 164–175, Visegrad, Hungary, July 2005. Springer-Verlag.

[19] [Juels, A. (2005). RFID Security and Privacy: A research Survey. Condensed version to appear in 2006 in the IEEE Journal on Selected Areas in Communication.

[20] Takaragi, K., Usami, M., Imura, R., Itsuki, R., and Satoh, T. (2001). An Ultra Small Individual Recognition Security Chip. IEEE Micro, November-December, 2001.

[21] Koh, R., Schuster, E., Chackrabarti, I., and Bellman, A. (2003). Securing the Pharmaceutical Supply Chain. White Paper, Auto-ID Labs, Massachusetts Institute of Technology, 2003.

[22] Pearson, J. (2005). Securing the Pharmaceutical Supply Chain with RFID and Public-key Infrastructure (PKI) Technologies. Texas Instruments White Paper, June 2005. Available from http://www.ti.com/rfid/docs/docntr.shtml (28.4.2006).

[23] [RFID Journal (2006). Congress Weighs Drug Anticounterfeiting Bill. News Article, March 2. Available at http://www.rfidjournal.com/article/articleview/2180/1/1/ (19.5.2006).

[24] Weis, S., Sarma, S., Rivest, R., and Engels, D. (2003). Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems. In D. Hutter, G. Müller, W. Stephan, and M. Ullmann, editors, International Conference on Security in Pervasive Computing - SPC 2003, volyme 2802 of Lecture Notes in Computer Science, pages 454-469, Springer-Verlag, 2003.

[25] Henrici, D. and Müller, P. (2004). Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In Ravi Sandhu and Roshan Thomas, editors, International Workshop on Pervasive Computing and Communication Security – Per-Sec 2004, pages 149–153, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society.

[26] Avoine, G. and Oechslin, P. (2005). A scalable and provably secure hash based RFID protocol. In International Workshop on Pervasive Computing and

Communication Security – PerSec 2005, pages 110–114, Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society Press.

[27] Ohkubo, M., Suzuki, K., and Kinoshita, S. (2004). Cryptographic approach to “privacy-friendly” tags. In RFID Privacy Workshop, MIT, MA, USA, November 2003.

[28] Lee, S.M., Hwang, Y.J., Lee, D.H., and Lim, J.I. (2005). Efficient authentication for low-cost RFID systems. In Osvaldo Gervasi, Marina Gavrilova, Vipin Kumar, Antonio Lagana`a, Heow Pueh Lee, Youngsong Mun, David Taniar, and Chih Jeng Kenneth Tan, editors, International Conference on Computational Science and its Applications - ICCSA 2005, Proceedings, Part I, volume 3480 of Lecture Notes in Computer Science, pages 619-627, Singapore, May 2005. Springer-Verlag.

[29] Choi, E.Y., Lee, S.M., and Lee, D.H. (2005). Efficient RFID authentication protocol for ubiquitous computing environment. In International Workshop on Security in Ubiquitous Computing Systems – secubiq 2005, Lecture Notes in Computer Science, Nagasaki, Japan, December 2005. Springer-Verlag.

[30] Lee, S., Asano, T., and Kim, K. (2006). RFID Mutual Authentication Scheme based on Synchronized Secret Information. In Symposium on Cryptography and Information Security, Hiroshima, Japan, January 2006.

[31] Juels, A. and Pappu., R. (2003). Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In Rebecca N. Wright, editor, Financial Cryptography -- FC'03, volume 2742 of LNCS, pages 103--121, Le Gosier, Guadeloupe, French West Indies, January 2003. IFCA, Springer-Verlag.

[32] Zhang, X. and King, B. (2005). Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeiting. In Jianying Zhou, Javier Lopez, Robert Deng, and Feng Bao, editors, Information Security Conference – ISC 2005, volume 3650 of Lecture Notes in Computer Science, pages 74–481, Singapore, September 2005. Springer-Verlag.

[33] Tsudik, G. (2006). YA-TRAP: Yet another trivial RFID authentication protocol. In Inter-national Conference on Pervasive Computing and Communications – PerCom 2006, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.

[34] Molnar, D., Soppera, A., and Wagner, D. (2005). A scalable, delegatable, pseudonym protocol enabling ownership transfer of RFID tags. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[35] Chatmon, C., Le, T.v., and Burmester, M. (2006). Secure anonymous RFID authentication protocols. Technical Report TR-060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA, 2006.

[36] Juels, A. (2004). Minimalist cryptography for low-cost RFID tag. In Conference on Security in Communication Networks -- SCN'04, LNCS, Amalfi, Italia, September 2004. Springer-Verlag.

[37] Juels, A. (2005). Strengthening EPC Tags Against Cloning. In M. Jakobsson and R. Poovendran, eds., ACM Workshop on Wireless Security (WiSe), pp.67-76. 2005.

[38] Vajda, I. and Buttyán, L. (2003). Lightweight authentication protocols for low-cost RFID tags. Workshop on Security in Ubiquitous Computing, October 2003.

[39] Juels, A. and Weis, S. (2005). Authenticating pervasive devices with human protocols. In Victor Shoup, editor, Advances in Cryptology – CRYPTO'05, volume 3126 of Lecture Notes in Computer Science, pages 293–308, Santa Barbara, California, USA, August 2005. IACR, Springer-Verlag.

[40] Hopper, N. and Blum, M. (2000). A Secure Human-Computer Authentication Scheme. Tech. Rep. CMU-CS-00-139, Carnegie Mellon University, 2000.

[41] Katz, J. and Shin, J.S. (2006). Parallel and concurrent security of the HB and HB+ protocols. In Serge Vaudenay, editor, Advances in Cryptology – EUROCRYPT'06, Lecture Notes in Computer Science, Saint Petersburg, Russia, May-June 2006. IACR, Springer-Verlag.

[42] Piramuthu, S. (2006). HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In Collaborative Electronic Commerce Technology and Research – CollECTeR 2006, Basel, Switzerland, June 2006.

[43] Dimitriou, T. (2006). A Secure and Efficient RFID Protocol that could make Big Brother (partially) Obsolete. In International Conference on Pervasive Computing and Communications – PerCom 2006, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.

[44] Dimitriou, T. (2005). A Lightweight RFID Protocol to protect against Traceability and Cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm (to appear), Athens, Greece, September 2005. IEEE.

[45] Duc, D.N., Park, J., Lee, H., and Kim, K. (2006). Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning.

[46] Ranasinghe, D., Engels, D., and Cole, P. (2004). Security and privacy: Modest proposals for low-cost RFID systems. In Auto-ID Labs Research Workshop, Zurich, Switzerland, September 2004.

[47] Lee, J., Lim, D., Gassend, B., Suh, G.E., Dijk, M., and Devadas, S. (2004). A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. Symposium on VLSI circuits, 2004, pp 176-179.

[48] Tuyls, P. and Batina, L. (2006). RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, In Topics in Cryptology - CT-RSA - The Cryptographers' Track at the RSA Conference, number 115-131 in lecture Notes in Computer Science, page 3860, San Jose, USA, February 13-17 2006. Springer Verlag.

[49] Engberg, S., Harning, M., and Damsgaard-Jensen, C. (2004). Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience. In Conference on Privacy, Security and Trust – PST, New Brunswick, Canada, October 2004.

[50] Rhee, K., Kwak, J., Kim, S., and Won, D. (2005). Challenge-response based RFID authentication protocol for distributed database environment. In Dieter Hutter and Markus Ullmann, editors, International Conference on Security in Pervasive Computing – SPC 2005, volume 3450 of Lecture Notes in Computer Science, pages 70–84, Boppard, Germany, April 2005. Springer-Verlag.

[51] Molnar, D. and Wagner, D. (2004). Privacy and Security in Library RFID: Issues, Practices, and Architectures. In Birgit Pfitzmann and Peng Liu, editors, Conference on Computer and Communications Security – ACM CCS, pages 210–219, Washington, DC, USA, October 2004. ACM, ACM Press.

[52] Gao, X., Xiang, Z., Wang, H., Shen, J., Huang, J., and Song, S. (2004). An approach to security and privacy of RFID system for supply chain. IEEE International Conference on E-Commerce Technology for Dynamic E-Business, 2004. Page(s):164 - 168

[53] Yang, J., Park, J., Lee, H., Ren, K., and Kim, K. (2005). Mutual authentication protocol for low-cost RFID. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[54] Dominikus, S., Oswald, E., and Feldhofer, M. (2005). Symmetric authentication for RFID systems in practice. ECRYPT Workshop on RFID and Lightweight Crypto, Graz, Austria, July 14-15, 2005.

[55] Feldhofer, M. (2003). A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags. Stiftung Secure Information and Communication Technologies SIC, 2003.

[56] Feldhofer, M., Dominikus, S., and Wolkerstorfer, J. (2004). Strong authentication for RFID systems using the AES algorithm. Workshop on Cryptographic Hardware and Embedded Systems - CHES 2004, LNCS 3156, pp. 357-370, Springer, 2004.

[57] Bailey, D. and Juels, A. (2006). Shoehorning security into the EPC standard. Manuscript in submission, January 2006.

[58] Nochta, Z., Staake, T., and Fleisch, E. (2006). Product Specific Security Features Based on RFID Technology. Saint-w, pp. 72-75, International Symposium on Applications and the Internet Workshops (SAINTW'06), 2006.

[59] Sarma, S. (2001). Towards the 5¢ Tag. White Paper, Auto-ID Center, MIT, 2001. Avail-able at http://www.autoidlabs.org/whitepapers/mit-autoid-wh-006.pdf (5.5.2006).

[60] Sarma, S., Weis, S., and Engels, D. (2003). Radio-Frequency Identification: Security Risks and Challenges. In RSA Laboratories Cryptobytes, Vol. 6, No. 1, 2003.

[61] Weis, S. (2003). Security and Privacy in Radio-Frequency Identification Devices. Master's Thesis, MIT, May 2003.

[62] Yüksel, K. (2004). Universal Hashing for Ultra-Low-Power Cryptographic Hardware Applications. Master's Thesis, Dept. of Electronical Engineering, WPI, 2004.

[63] Juels, A., Syverson, P., and Bailey, D. (2005). High-Power Proxies for Enhancing RFID Privacy and Utility. In Workshop on Privacy Enhancing Technologies (PET 2005).

[64] EPCglobal (2003). 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification. EPCglobal public document, February 2003.

[65] EPCglobal (2005). Class-1 Generation-2 UHF air interface protocol standard version 1.0.9. EPCglobal public document, January 2005. Available at http://www.epcglobalinc.org/standards_technology/EPCglobal2UHFRFIDProtocolV109122005.pdf (8.5.2006).

[66] Alien Technology (2005). EPC Class 1 RFID Tags Datasheet. Available at http://www.alientechnology.com/products/documents/alien_915mhz_128_bit.pdf (19.5.2006).

[67] Supply Chain Digest (2005). RFID News: Tag Prices Drop, but is it Real? Wal-Mart, Target Push for Sunsetting Class 0 and 1 Tags. News and Views, October 13, 2005. Available at http://www.scdigest.com/assets/newsviews/05-10-13-2.cfm (19.5.2006).

A Summary of Technical Requirements of Different Approaches

This appendix presents a table of technical requirements of different approaches. Descriptions of approaches can be found from section 4. We assume that tags always carry an ID number, such as EPC. Considered tag memory requirements include additional non-volatile memory (NVM) and read-write (RW) capability. Functional requirements include tag's ability to perform basic bit-wise operations, pseudo-random number generator (PRNG), hash function, and sym-metric key encryption. For the sake of simplicity we assume that all approaches that require any of the last three functionalities implicitly require also bitwise operations.

The network requirements include the needed level of secrecy for the online data. This data can be public (e.g. a public key), secret (e.g. a secret key), or semi-public when it is not or it cannot be kept completely secret due to its nature, such as tag serial number. The level of secrecy of back-end data affects how easily an approach can be implemented – if the authentication cannot be performed without access to secret data, for example, mode complex system is required than when only public data is used. Last considered network requirement is the need to update data or to perform computations on the server relating the authentication process. This requirement is referred to as complex database. Reader requirements include complex reader which refers to need to perform computations (e.g. encryption) on the reader side. Physical verification stands for the need to verify a physical property of the product as a part of the authentication.

Table A-1. Comparison of technical requirements of different product authentication approaches (dashed lines separate categories, subsections 4.1 – 4.4)

Approach	*Tag Memory Requirements*		*Tag Functional Requirements*				*Network Requirements*				*Reader Requirements*	
	NVM	RW	Bitwise operations	PRNG	Hash function	Symmetric key encryption	Public	Semi public	Secret	Complex database	Complex reader	Physical verification
Unique Serial Numbering [20, 21]								X				
Track and Trace [10, 21, 22]								X		X		
Juels [37]									X			
Ranasinghe [46][1] (3.A)									X			
Pearson [22]	X	X					X				X	
Juels et al. [31]	X	X					X				X	(X)[2]
Zhang et al. [32]	X	X					X				X	
Juels [36]	X	X	X						X	X		
Vajda et al. [38] (4.1-4.3)	X	X	X						X		X	
Tuyls et al. [48] [1]	X		X								X	
Juels et al. [39]	X		X	(X)[3]					X		X	
Piramuthu [42]	X		X	(X)[3]					X		X	
Tsudik [33]	X	X	X	X					X	X		
Chatmon et al.[35]	X	X	X	X					X	X		
Duc [45]	X	X	X	X					X	X		
Molnar et al. [51]	X		X	X					X		X	
Engberg et al. [49] (III. A)	X		X		X				X		X	
Avoine et al. [26]	X	X	X		X				X	X		
Gao et al. [52]	X	X	X	X	X				X	X	X	
Rhee et al. [50]			X	X	X				X	X		
Dimitriou [44]	X	X	X		X				X	X		
Yang et al. [53]	X	X	X		X				X	X	X	
Weis et al. [24] (5.1.)	X		X		X				X			
Henrici et al. [25]	X	X	X		X				X	X		
Lee et al. [30]	X	X	X	X	X				X	X		
Choi et al. [29]	X	X	X		X				X	X		
Lee et al. [28]		X	X		X				X	X		
Molnar et al. [34]	X	X	X	X		X			X	X		
Dimitriou [43]	X		X	X		X			X	X		
Feldhofer [55], [56]	X		X			X			X		X	
Bailey et al. [57]	X		X	X		X			X		X	
Dominikus et al. [54]	X		X	(X)[4]		X			X		X	
Nochta et al. [58]	X						(X)[4]				X	X

[1]the transponder needs a physical unclonable function (PUF); [2]optional; [3]only one random bit is required, [4]not necessary for all proposed approaches