The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)

Off-line NFC Tag Authentication

Muhammad Qasim Saeed
Information Security Group (ISG)
Royal Holloway University of London
Egham, UK
muhammad.saeed.2010@live.rhul.ac.uk

Colin D.Walter
Information Security Group (ISG)
Royal Holloway University of London
Egham, UK
Colin.Walter@rhul.ac.uk

***Abstract*—Near Field Communication (NFC), a short range wireless technology, has recently experienced a sharp rise in uptake because of its integration with cell phones. NFC-enabled cell phones interact with NFC tags to retrieve information in a single touch. Such tags can be used in variety of applications like smart posters, product identification, access control etc. The integrity of the data stored on these tags is assured by digital signatures. However, this does not guarantee the legitimacy of tags. They may be replaced with counterfeits. At present the NFC Forum does not provide any mechanism to detect duplicate tags. In an offline environment, when there is no shared secret between the tag and the reader, it is very challenging to differentiate between legitimate and counterfeit tags.**

This paper presents a protocol for the off-line authentication of NFC tags and provides a framework, based on NFC Forum specifications, to support the authentication. The proposal is based on a challenge-response protocol using public key cryptography and a PKI. In order to make the framework compatible with existing NFC Forum devices, a new *Tag Authentication Record*, designed according to the NFC Data Exchange Format (NDEF), is introduced. Our proposed framework successfully differentiates between legitimate and cloned tags which have sufficient resources to perform the required cryptography.

Keywords–Counterfeit Tag; Off-line Authentication; Near Field Communication; RFID

I. Introduction

Near Field Communication (NFC) tags are used to store data in the format specified by the NFC Data Exchange Format (NDEF) specification, published by the NFC Forum [1]. The authenticity of the stored data is guaranteed by a digital signature which follows the Forum's Signature Record Type Definition (Signature RTD) [2]. The signature is computed over the tag's contents and is stored in the signature record on the tag along with the corresponding certificate for verification.

NFC tags are used in a variety of applications like product identification, smart posters, access control etc. There are occasions where copying the contents of an NFC tag to another tag is undesirable. An example of such a scenario is a signed NFC tag attached to a medicine packet storing its chemical composition and expiry date. Any NFC Forum device can read its contents and verify it using the signature. However, a counterfeit medicine and counterfeit tag with the same data will also be authenticated. At present, the NFC Forum does not provide any specification to authenticate the tag. The lack of such a mechanism opens the door to many security threats, and particularly to counterfeit products when NFC technology is used in product identification.

We address this weakness by providing a mechanism based on the NDEF specification to authenticate NFC tags. The main advantage of our proposed specification is its compatibility with existing NFC Forum devices. This contribution to the NFC framework enables the successful authentication of such tags along with their data. It adds another layer of defence to the NFC security framework, making it more secure for future applications. For a read-only tag, the tag authentication scheme can simultaneously provide data authentication at no extra cost whereas the converse is not always true. Therefore we emphasize that tag authentication is an important security measure as it provides both tag and data authentication for read-only tags.

The first part of the paper introduces technical aspects of Near Field Communication (NFC), including the format for NFC messages and the digital signature scheme for data authentication. Next, the types of NFC tags are described, as the countermeasures for counterfeit tags depend upon the computational and storage resources available on the tag. After this, different tag authentication techniques are presented in relation to NFC technology. In the last part, a new NFC *Tag Authentication Record* is proposed that can be used to authenticate at least the tags of NFC Type-4 in an *off-line* environment, as well as other tags with sufficient computational power.

II. Near Field Communication

Near Field Communication (NFC) is a wireless technology operating at less than about 4 cm. The main potential of this technology is its compatibility with contactless smart cards (ISO/IEC 14443) and radio-frequency identification (RFID) [3] operating in the 13.56 MHz frequency band.

An NFC link between a tag and a reader is established by a single touch, making it convenient for users. NFC has three modes of operation resulting in a variety of applications: peer-to-peer mode, read/write mode and emulation mode [4]. The availability of NFC technology in cell phones is currently enhancing the number of its users.

Tags are integrated circuits storing data that can be read by NFC-enabled devices. In order to maintain the interoperability of NFC devices and tags, the NFC Forum has specified four different types of tag [5]:

978-1-908320-08/7/$25.00©2012 IEEE

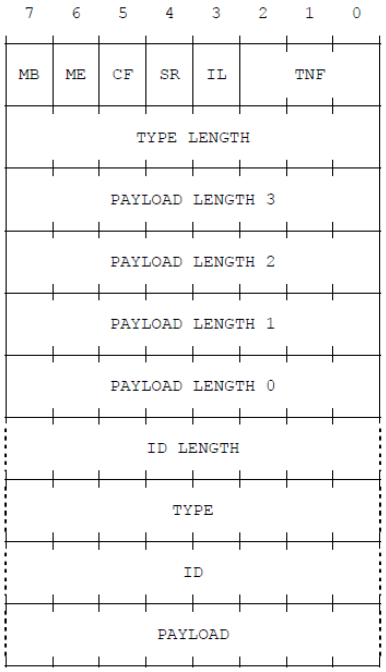

Figure 1. NDEF Record Layout ([1], fig. 3)

- **Types 1 & 2:** These tags are read and re-write capable. Users can configure the tag to become read-only. Memory availability is 48 or 96 bytes, expandable to 2 KB.
- **Type 3:** These tags are based on the Japanese Industrial Standard (JIS) X 6319-4 known as FeliCa. They are pre-configured at manufacture to be either read and rewritable, or read-only. Their memory has a theoretical limit of 1 MB per service.
- **Type 4:** These tags are pre-configured at manufacture to be either read and re-writable, or read-only. There is up to 32 KBytes of memory available per service. The Application Protocol Data Unit (APDU) based on ISO/IEC 7816-4 is used for communication between tag and reader.

III. NFC Data Exchange Format

The NFC Forum was established in 2004 to standardize applications which use NFC [6]. Its Data Exchange Format (NDEF) specification [1] defines a common format and rules to exchange information in the NFC environment. An NDEF message contains one or more NDEF records with the structure shown in Fig. 1. The payload of an NDEF record is described by its *type*, *length*, and an optional *identifier*. The 3-bit TNF *(Type Name Format)* field classifies the content of the *Type* field. Its meaning is shown in Table I.

In this paper we require to extend the NFC Forum well-known type records, for which *TNF*=1, as our proposed *Tag Authentication Record* in §VII-B falls into this category. Each of the well-known types is identified by its name, identifier and a character code as allocated by the NFC Forum. The current list of well-known types is given in Table II.

TABLE I
Type Name Format *(TNF)* Description (*cf* [7], table 1)

TNF	Meaning
0	An empty record with no payload.
1	An NFC Forum well-known type.
2	A MIME media type identifier (RFC 2406).
3	An absolute URI (RFC 3986).
4	An NFC Forum external type.
5	Used when the type of the payload is unknown.
6	Indicates a chunk record.
7	Reserved for future use.

TABLE II
NFC Forum Well-Known Types (*i.e. TNF*=1) [8]

Type Name	Type ID	Hexadecimal Encoding
Generic Control	Gc	0x4763
Text	T	0x54
URI	U	0x55
Smart Poster	Sp	0x5370
Signature	Sig	0x536967

IV. Tag Authentication Scenarios

Since NFC tags can be used in a variety of applications, the techniques for tag authentication also vary a lot. Tag authentication can be categorized as follows into two main categories depending upon the tag's environment [9].

A. Off-line Authentication

There are occasions when there is no shared secret between the tag and the reader. Any reader can access the tag and read its contents. The process of authenticating the tag or the reader or both in such scenarios is called *Off-line* authentication. Normally, it is just the tag that needs to be authenticated. An NFC smart poster or an NFC tag for product identification falls into such a category as its contents are accessible to any reader without the need for a shared secret. Off-line authentication becomes challenging in an RFID environment owing to the low computational power of RFID tags. The typical low cost tag is currently unable to perform any useful public key cryptography.

B. On-line Authentication

In the *On-line* category, there is secret information shared between a tag and the reader as a result of the reader having access to a server containing a database of secrets. This scenario is normally applicable in a closed environment like product identification in supply chain management or access control. The reader accesses the database to obtain the tag's secret and then ascertains whether the tag knows that secret or not. Since the secret is not accessible to an attacker, a duplicate tag lacks it and can be detected.

A review of existing tag authentication techniques is available in [9]. In general, these techniques use on-line servers and execute a challenge-response protocol to authenticate the tag. They cannot in general be adapted successfully to the off-line environment.

V. Tag Authentication

Tag authentication requires a framework that distinguishes a legitimate tag from a counterfeit tag. The counterfeit may or may not store the same data as the original. A duplicate with some alteration in the stored data is obviously a potential threat to the system. However, there are occasions where a duplicate with the same data is not desirable either. We describe such a tag as a *cloned* tag. Examples of such scenarios are ePassports [10], product identification, access control etc.

Conversely, there are cases where a cloned tag may be considered desirable: for example, an NFC tag used as a smart poster where the integrity of the tag contents is protected by a Signature record. The more the smart poster is cloned, the more its contents are advertised.

As observed in Section IV-A, NFC tags may be used for product identification in an *off-line* environment. The information stored in the NFC tag is product specific and aimed to assist an off-line user to know about the specification and legitimacy of the attached product. The data on the tag is protected by the signature record and a valid signature is an indication of a genuine product. Unfortunately, the same data can be stored on a duplicate NFC tag affixed to an inferior product. The signature remains valid as it is the same data as in the original tag. Since the signature is valid, the user is led to believe that the product is genuine, whereas it is not. This happens because the signature specification authenticates only the stored data on NFC tag. An easy way to avoid such attacks is to include the tag's ID in the signature in order to detect a cloned tag with a different tag ID. But an attacker can affix to the counterfeit product a programmable tag which returns the same ID as the original. In this case, the counterfeit is authenticated as a genuine product with very little investment by the attacker.

This attack works because the tag is not authenticated along with its data and a static identifier is used to authenticate the tag. Lack of any tag authenticating mechanism opens doors to counterfeit products being accepted as genuine products. At present, the NFC Forum has not specified any mechanism to authenticate the tag. In the absence of such a mechanism, NFC tags based on the NFC Forum specification cannot be used for secure product identification.

A. Our Contribution

We propose a solution to detect cloned NFC tags used in an *off-line* environment. Our solution is formulated within the NDEF specification and introduces a new *Tag Authentication Record* containing parts of a digital certificate. The main advantage of introducing such a new record is its compatibility with existing NFC Forum devices. The authentication is then performed using a challenge-response protocol employing public key cryptography and a PKI.

VI. Existing Protocols

As observed in Section IV-B, a survey of existing protocols reveals plenty of techniques for RFID tag authentication in the *on-line* environment [9]. Since this paper focuses on *off-line* tag authentication, we now turn to research related to this domain. Pim Tuyls and Lejla Batina claim the first tag authentication model in an *off-line* environment [11]. They used a Physical Unclonable Function (PUF) integrated with the RFID chip (an Integrated PUF or *IPUF*). In their model, several fingerprints are derived from the PUF by sending it multiple challenges and recording the responses. The challenges and corresponding fingerprints are digitally signed and printed on the product (if used in the case of supply chain management). The verifier reads a challenge/response pair from the data printed on the product or packaging and sends the challenge to the tag to compute the response. On receipt, the verifier compares the response with the expected fingerprint. A successful match authenticates the tag.

The main drawback with this scheme is the limited number of challenges and corresponding fingerprints available in the tag's memory or printed on the product. An attacker can record all the challenge/response pairs and program another tag with the same pairs resulting in a successfully cloned tag.

Another anti-cloning approach in the RFID framework, known as *Active Authentication (AA)*, is used in ePassports where an RFID tag is used to add more security to an ordinary passport [12]. This approach uses public key cryptography where the tag digitally signs the challenge received from the reader.

Alex Arbit *et al.* presented a public-key based anti-counterfeiting system for the Electronic Product Code (EPC) standard [13]. They implemented a variant of the well-known Rabin encryption scheme with a 1024-bit key [14].

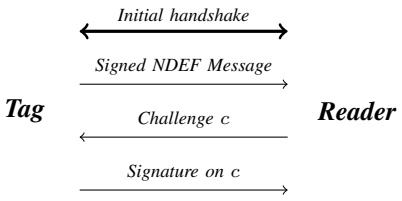

Figure 2. Proposed Tag Authentication Protocol

VII. Proposed Tag Authentication Scheme

As noted in Section IV, NFC tags can be used in both *on-line* and *off-line* environments. Our scheme for authenticating a tag in an *off-line* environment is based on the *Active Authentication* scheme of the ePassport [10] but modified to fit the NFC architecture. The scheme is applicable to at least NFC Type-4 tags as these tags are computationally powerful enough. Such tags satisfy ISO 7816-4 and therefore contain a cryptographic processor. They can compute asymmetric or symmetric key encryption [15]. The scheme may be applied to other tags in future as their computational power increases over time. Moreover, light-weight versions of public key encryption schemes may also appear and allow wider applicability. In the scheme, the tag signs a challenge and the reader verifies the signed response as shown in Fig. 2.

The following assumptions are required for the scheme to work:

- Both the reader and the tag can perform public key encryption/decryption.
- The memory location where the secret key is stored inside the tag is not accessible to any reader.
- The reader knows the public verification key for a certificate held by the tag.

Our scheme differs from the standard methods of authentication used in smart cards/SIM cards because the latter requires an on-line environment. A SIM card stores a secret key K_i at a secure location in the card. The same key is also stored with the mobile network operator. During authentication, the network executes a challenge-response protocol to verify knowledge of K_i by the SIM. A cloned SIM should lack the key and so would be detected. A similar approach is used in smart cards issued by banks for monetary transactions. However, in our context there is no opportunity to share a secret.

A. The Tag Authentication Digital Certificate

Before describing the protocol, it is useful to define the public key certificate which it uses and the structure of the proposed new *Tag Authentication record* which stores part of its contents. The certificate requires at least the following six fields:

1) *Protocol Version*
2) *Challenge Signature Scheme*
3) *Challenge Public Key*
4) *Supplementary Text*
5) *Certificate Signature Algorithm*
6) *Certificate Signature*

The *Protocol Version* field determines which version of the *Tag Authentication* specification is being used. This allows for future expansion and developments. The *Challenge Signature Scheme* field specifies which digital signature algorithm, along with the relevant parameters, is used by the tag to sign the challenge, and the *Challenge Public Key* field stores the public key information associated with verifying this signature. The *Certificate Signature* field is the signature on the records containing the first four fields, computed using the algorithm defined by the *Certificate Signature Algorithm* field. It follows the NFC Forum signature specification scheme [2]. The *Supplementary Text* field has various uses which are described below.

The certificate might follow the X.509 specification [16], or a simplification with fewer critical fields. Clearly, it may be necessary to add further fields in future, such as an expiry date to deter the illegal re-use of tags. In the case of X.509, the *Extensions* field enables the inclusion of the *Supplementary Text*. That field also allows the certificate to be restricted to this NFC application, which is useful because less computationally extensive cryptography is expected than is normally acceptable in other situations. We will not consider the encoding of the certificate any further beyond observing that space is at a premium on a typical tag. Therefore one would want to reduce, for example, the twenty or so bytes used for identification of the signature algorithm in an X.509 certificate to just one byte.

The stored data and data transmitted between tag and reader is in the format of NDEF records. In order to store the public key information, we propose a new *Tag Authentication record*. The first three certificate fields are to be stored in the *payload* field of this record, the *Supplementary Text* is stored in normal NFC Forum text records on the tag, and the last two fields are placed in an NFC signature record.

B. The Tag Authentication Record

The *Tag Authentication Record* serves two purposes: it stores the public key information necessary to verify the signature on a challenge, and its presence is a claim that the tag is equipped with anti-cloning features. Indeed, such records should not be allowed in tags without the ability to enact the authentication protocol. The proposed record follows the NDEF structure given in Fig. 1 with a *TNF* value of 1. Its *Type* should therefore be added to the set of NFC Forum well-known types, and the type name of 'Ta' (for 'Tag Authentication'), with hexadecimal encoding 0x5461, added to the list in Table II. Given the general nature of the construction, the record may have much wider uses in future, authenticating other entities than tags. It may therefore make more sense to call it a *Certificate Record* with a different type identifier.

C. The Supplementary Text Field

As space is limited on tags, it will often be useful to have a single signature covering some or all of the message content in the tag, rather than having separate signatures on the certificate and the message for users. The *Supplementary Text* field enables this to be done by using it for message content. The signature then ties this content to the particular tag. For convenience, it is assumed in the implementation details below that one signature is indeed used to cover both the text message and the *Ta* record fields.

In future, the *Supplementary Text* may have to be structured into subfields if it is used for several purposes.

D. Protocol Execution Sequence

The scheme is executed in two phases:

1) **Initialization Phase.** After selecting the version number and signature scheme, a key pair (K_P, K_S) is generated in a secure way by a trusted party and the secret key K_S is stored inside the tag at a secure location only accessible to the tag processor for prescribed operations. The public key K_P is stored in the *Challenge Public Key* field of the payload of the authentication record. This *Ta* record, along with the other records stored on the tag, is then digitally signed by the same trusted party and the signature is stored in the *signature record* on the tag according to the NFC Forum Signature Specification. This turns the *Tag Authentication record* into a signed digital certificate applicable to NFC tags.

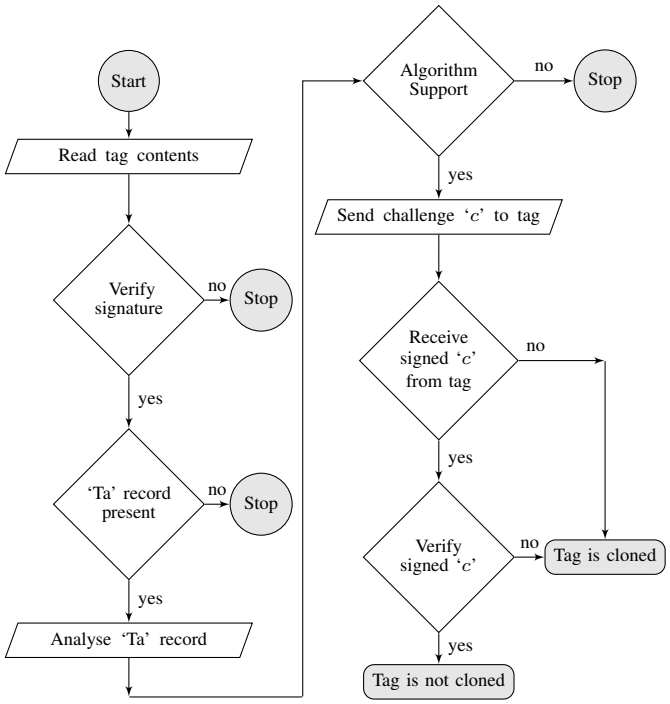

Figure 3. Verification Process

2) **Verification Phase.** The verification phase is executed as follows (see Fig. 3):
   - The reader requests and obtains all the data from the tag. This data is in the form of NDEF records.
   - The reader verifies the integrity of the tag's contents by verifying the signature. A valid signature indicates that the tag contents are authentic.
   - Next, the reader looks for a *Tag Authentication record* by searching for record type 'Ta'. Its absence indicates that the tag is not protected by the anti-cloning feature and the Tag Authentication protocol terminates unsuccessfully.
   - Otherwise, the *payload* of the *Tag Authentication record* is extracted and, assuming the reader can support the required signature scheme, an appropriate challenge c is generated and sent to the tag.
   - The tag now uses its secret key K_S to compute the digital signature of c with the specified padding, and sends the result back to the reader.
   - The reader verifies the signature on c using the public key K_P from the certificate. Successful verification indicates knowledge of the secret key and hence the legitimacy of the tag, whereas failure indicates a cloned or damaged tag.

VIII. Analysis

This scheme successfully detects a cloned tag from an original tag because a cloned tag lacks the secret key K_S corresponding to the public key K_P available in the *Tag Authentication record*. However, there are several issues that need to be discussed in detail.

A. Backward Compatibility

The backward compatibility of the tag authenticating protocol can be assessed by following two scenarios. We use "plain" to describe a reader without authenticating ability, and a tag without authentication response ability.

- **An Authenticating reader and a plain tag.** In this case, the reader starts the verification process as shown in Fig. 3. The plain tag lacks this feature so there should be no *Ta* record in its contents. In this case the verification process stops with the conclusion that the tag cannot be authenticated. However, if there is a *Ta* record, then the plain tag is unable to respond to the challenge. Again the process terminates with the conclusion that the tag cannot be authenticated. Since a plain tag should not contain a *Ta* record, the reader can reasonably conclude that the tag is cloned. Notice that this requires that plain tags are not loaded with a *Ta* record. As we noted earlier, existence of the *Ta* record should be viewed as a claim that the tag *does* support the authentication protocol.
- **A Plain reader and an authenticatable tag.** In this case, the *Ta* record is present in the tag but the reader does not support the tag authentication protocol. Although the reader recognises the *TNF* field value 1, the record type 'Ta' is unknown to it. According to the NFC Forum specification [1] §3.2.10, an NDEF parser receiving an NDEF record with a supported *TNF* value but an unrecognised *Type* field must interpret that record as being of *Unknown* type, i.e. *TNF*=5. So the *Ta* record is ignored. Thus the system remains backward compatible in this scenario as well.

B. Tag Message as a Digital Certificate

It was noted above that the *Ta* record and the rest of the tag message can be signed separately, giving two signature records, or can be signed as one, yielding a single signature record. The former provides a clean separation between the tag authentication processes and the message authentication processes at all levels from signing to verification. However, the latter binds the message to the specific tag: the message cannot be ported to another tag because that tag does not know K_S, and will be detected as noted above even on a tag which does not have authentication capability. This solution also seems preferable because of restricted space. Respectively, these two alternatives have interpretations of the *Ta* record with its corresponding signature record as a digital certificate and the whole message as a digital certificate.

C. Strengths and Weaknesses

The strength of our proposed scheme relies on the strength of the signature scheme, secure location of the secret key K_S inside the tag's memory and the integrity of the public certificate verification key K_{cert}, say, in the reader. The first is a well matured area of information security, and the

emergence of elliptic curve cryptography means that at least the certificate fields on the tag can be signed securely to yield a fairly short signature. However, the cryptography used by the tag to sign the challenge will often be fairly weak because of the low electrical or cryptographic power available to the tag. One needs to recognise that an attacker can send numerous challenges to the tag and record the replies and may therefore be able to break a weak system. The second issue, the maintained secrecy of K_S, depends very much on what the customer is prepared to pay for the tag, and accessibility of the tag during its life. Unless the attacker can recover K_S, he is unable to use the tag's digital certificate on a clone. It is indeed easy for an attacker to extract the key from a cheap tag if it can be taken to a laboratory for further study. Thirdly, if the integrity of the key K_{cert} can be compromised, the attacker can make a successful clone of a tag even when it is protected by a *Ta* record. The attacker stores his own secret key K'_S in the cloned tag and the corresponding public key K'_P is stored in its *Ta* record, which the attacker signs. The public verification key K'_{cert} corresponding to this signature is then used to replace the correct key in the reader. Consequently, the reader believes it has an authentic tag when it verifies the clone. This results in a successful attack.

In our proposed scheme, the integrity of the *Ta* record is assured by digitally signing this record, and perhaps others, according to the signature specification provided by the NFC Forum [2]. Recent attacks on signed NDEF records [7] put a question mark on the integrity of the tag's contents even if they are signed. The *Ta* record can be made inactive in a cloned tag by changing its *TNF* value to 5 with some compensating alteration in the length fields, as mentioned in [7], to preserve the validity of the signature. Since the *TNF* and length fields are not included in the signature, these alterations will not invalidate the signature. Now the verifier will not execute the tag authentication protocol since it does not recognise the *Ta* record as such. Nevertheless, if the reader is expecting an authenticatable tag, it should flag this to the operator. (This referenced vulnerability of the signature specification can be addressed by adding more fields to the signature as discussed in [7].)

IX. Conclusion

Application of NFC technology to monetary and similar transactions requires strict adherence to appropriately sound measures to ensure the necessary high level of security in the NFC framework. The recently published NFC Forum Signature Specification provides assurance of data integrity in NFC tags through the digital signing of NDEF messages. However, no mechanism is provided by the NFC Forum for detecting a counterfeit or cloned tag. This results in various possibilities for malicious activities where a legitimate tag is replaced by a counterfeit tag and the NFC tag reader is unable to detect the counterfeit. We proposed a framework to counter such attacks by providing a tag authenticating mechanism. It introduces a new *Tag Authentication Record* that provides relevant information to authenticate a tag in an *off-line* environment. It employs public key cryptography with digital certificates and so can be used on NFC tags that have sufficient computational power and resources to perform such operations. The *Tag Authentication Record* is based on the NFC Data Exchange Format and is thus compatible with all NFC Forum devices. The NFC tag simply signs a challenge c and returns the signature to the NFC reader. The NFC reader verifies the signature according to the information available in the previously communicated *Tag Authentication* record. A successful verification confirms that the tag is not cloned.

References

[1] *NFC Data Exchange Format (NDEF): Technical Specification*, NFC Forum Std. NDEF 1.0, July 2006. [Online]. Available: http://www.nfc-forum.org/specs/spec_list/

[2] *Signature Record Type Definition: Technical Specification*, NFC Forum Std. SIGNATURE 1.0, November 2010. [Online]. Available: http://www.nfc-forum.org/specs/spec_list/#rtds

[3] C. Mulliner, "Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones," in *The Fourth International Conference on Availability, Reliability and Security, ARES*. Fukuoka, Japan: IEEE, March 2009, pp. 695–700.

[4] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC Devices: Security and Privacy," in *The Third International Conference on Availability, Reliability and Security, ARES*. Technical University of Catalonia, Barcelona: IEEE, March 2008, pp. 642–647.

[5] NFC Forum, "NFC Forum Tag Type Technical Specifications," 2010. [Online]. Available: http://www.nfc-forum.org/specs/spec_list/#tagtypes

[6] ——, "The NFC Forum," 2004. [Online]. Available: http://www.nfc-forum.org/home/

[7] M. Q. Saeed and C. D. Walter, "An Attack on Signed NFC Records and Some Necessary Revisions of NFC Specifications," in *International Journal for Information Security Research (IJISR)*, March 2012, pp. 326–334.

[8] *Record Type Definition Technical Specifications*, NFC Forum Std. [Online]. Available: http://www.nfc-forum.org/specs/spec_list/#rtds

[9] M. Lehtonen, T. Staake, and F. Michahelles, "From Identification to Authentication – A Review of RFID Product Authentication Techniques," in *Networked RFID Systems and Lightweight Cryptography*. Springer Berlin Heidelberg, 2008, pp. 169–187.

[10] *Machine Readable Travel Document*, International Civil Aviation Organization (ICAO) Std. 9303, 2008. [Online]. Available: http://hasbrouck.org/documents/ICAO9303-pt3.pdf

[11] P. Tuyls and L. Batina, "RFID-Tags for Anti-counterfeiting," in *The Cryptographers' Track, RSA Conference, San Jose, CA, USA*, ser. Lecture Notes in Computer Science, vol. 3860. Springer, February 2006, pp. 115–131.

[12] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports," in *The First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. IEEE, September 2005, pp. 74–88.

[13] A. Arbit, Y. Oren, and A. Wool, "Toward Practical Public Key Anti-Counterfeiting for Low-Cost EPC Tags," in *International IEEE Conference on RFID*. Orlando, USA: IEEE, 2011, pp. 184–191.

[14] Y. Oren and M. Feldhofer, "A Low-Resource Public-key Identification Scheme for RFID Tags and Sensor Nodes," in *Proceedings of the Second ACM Conference on Wireless Network Security, WISEC*. Zurich, Switzerland: ACM, March 2009, pp. 59–68.

[15] *Identification Cards – Integrated Circuit Cards*, International Standard Organization / International Electrotechnical Commission Std. ISO/IEC 7816-4, 2005.

[16] *(X.509:) Information technology – Open Systems Interconnection – The Directory: Public key and attribute certificate frameworks*, International Standard Organization / International Electrotechnical Commission Std. ISO/IEC 9594-8, 2008.