Security Vulnerabilities of the NDEF Signature Record Type

Michael Roland, Josef Langer
NFC Research Lab Hagenberg
Upper Austria University of Applied Sciences
{michael.roland, josef.langer}@fh-hagenberg.at

Josef Scharinger
Department of Computational Perception
Johannes Kepler University Linz
josef.scharinger@jku.at

***Abstract*—The NFC Forum has released a first candidate for their Signature Record Type Definition. This specification adds digital signatures to the NFC Data Exchange Format (NDEF), which is a standardized format for storing data on NFC (Near Field Communication) tags and for transporting data across peer-to-peer links between NFC devices. With an increasing number of applications of the NFC and NDEF technology, more and more security threats became apparent. The signature record type is supposed to increase security for NDEF applications by providing authenticity and integrity to the NDEF data. This paper takes a close look on the recently published Signature Record Type Definition and discusses its various security aspects. First, we introduce the signature record type and its usage. After that, we analyze the security aspects of the current signature method. Finally, we disclose multiple security vulnerabilities of the current Signature Record Type Definition and propose measures to avoid them.**

I. Introduction

Near Field Communication (NFC) is a contactless communication technology standardized in [1], [2]. It is an advancement of inductively coupled proximity Radio Frequency Identification (RFID) technology. Therefore, NFC supports contactless smartcard systems based on the standards ISO/IEC 14443 and FeliCa. Besides standardization through normative bodies like ISO/IEC and Ecma International, further specification of data formats, protocols and NFC applications is driven by the NFC Forum[1].

A basic principle of the NFC technology is "*it's all in a touch*" [3]. This means that simply touching an object with an NFC device immediately triggers an action. NFC offers so-called tags (based on existing RFID transponders) that can be used to store various data structures. In an NFC ecosystem these tags are used to store content like Internet addresses (URLs), telephone numbers, text messages (SMS) or electronic business cards. The user can access the information on a tag by simply touching it with an NFC device (e.g. a mobile phone). The data on a tag is structured according to the NFC Data Exchange Format (NDEF, [4]). NDEF is a standardized format for storing formatted data on NFC tags and for transporting data across a peer-to-peer link between two NFC devices.

The use cases for NDEF cover smart posters, the exchange of business cards and using NFC as an enabler for other, especially wireless, communication technologies. For instance, a tag may convey an Internet address which provides further information about an advertised service, a telephone number for an advertised hotline or a ready-made SMS message for a ticket ordering service.

With the increasing number of available applications, the threat of abuse and security vulnerabilities increases continuously. An example is the manipulation of NFC tags. An attacker may replace (unprotected) tag content or even replace whole tags with modified tags. By, for instance, manipulating Internet addresses or telephone numbers in smart poster tags it is possible to redirect the user to a forged website for phishing user credentials or to trick the user into sending an SMS message to a costly premium rate service.

The NFC Forum has created the Signature Record Type Definition to escape these problems. The specification adds digital signatures to the NFC Data Exchange Format. Thus, receivers of NDEF messages can establish trust into the received data.

This paper gives a short introduction to the NFC Data Exchange Format. Furthermore, we outline various aspects of digitally signing NDEF records that have been identified in related publications. Finally, we discuss several security vulnerabilities of the current Signature Record Type Definition and propose measures to avoid them.

II. NFC Data Exchange Format

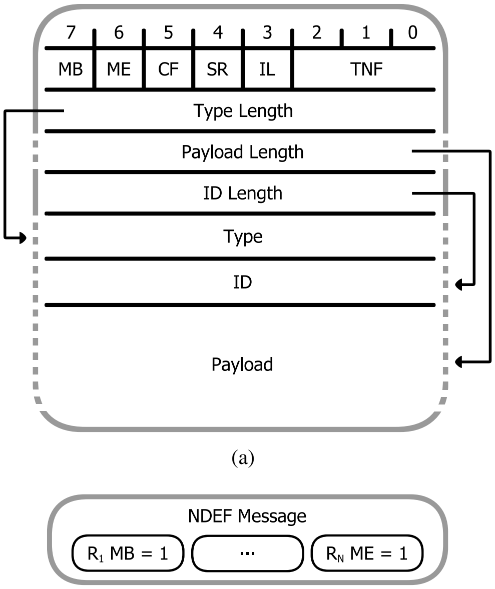
The NFC Data Exchange Format (NDEF, [4]) defines a common format and rules for exchanging data structures through NFC. Application specific data structures along with type information are packed into NDEF records. Multiple records form an NDEF message. Fig. 1 depicts the layout of an NDEF record (a) and that of an NDEF message (b).

An NDEF record consists of multiple header fields and a payload field. The header contains five flags – *Message Begin* (MB), *Message End* (ME), *Chunk Flag* (CF), *Short Record* (SR) and *ID Length Present* (IL) – a type classification (*Type Name Format*, TNF), the length information for fields of variable length, a type identification (Type) and an optional record identifier (ID).

MB and ME mark the first and the last record of an NDEF message respectively. The flag CF specifies that the payload of that record is continued in the next record. SR defines whether

[1] http://www.nfc-forum.org/

DOI 10.1109/NFC.2011.9
© 2011 IEEE



(a)

(b)

Fig. 1. An NDEF record (a) consists of multiple header fields and a payload field. The header contains five flags – *Message Begin* (MB), *Message End* (ME), *Chunk Flag* (CF), *Short Record* (SR) and *ID Length Present* (IL), a type classification (*Type Name Format*, TNF), the length information for fields of variable length, a type identification (Type) and an optional record identifier (ID) [4]. Multiple records form an NDEF message (b). The flags MB and ME are set for the first and the last record respectively.

the size of the Payload Length field is reduced from a 4-byte unsigned integer to a 1-byte unsigned integer. The flag IL determines if the optional ID field and its corresponding length field are present.

The value of the TNF field determines the format of the type information:

0h: The record is empty. The fields Type, ID and Payload are not present and their length fields are set to zero.
1h: Type is the relative URI (Uniform Resource Identifier) of an NFC Forum well-known type according to the NFC Record Type Definition (RTD, [5]).
2h: Type is a MIME media type identifier (RFC 2046).
3h: Type is an absolute URI (RFC 3986).
4h: Type is the relative URI of an NFC Forum external type according to the RTD.
5h: The record contains data in an unknown format. No type information is present and the length of the Type field is zero.
6h: The record continues the payload of the preceding chunked record. No type information is present and the length of the Type field is zero.
7h: Reserved for future use.

The ID field may be used to specify a unique identifier for each record. This identifier can be used to cross reference between records.

The NFC Forum has defined a set of well-known type specifications. They cover basic data types as well as complex data structures for specific use cases. Examples of basic data types are the Text record [6] and the URI record [7]. An example for a complex type is the Smart Poster record [8]. The Smart Poster record extends a URI record with additional information like descriptive titles, an icon, and an action.

TABLE I
RECORD FIELDS WEIGHTED BY THE BENEFITS OF NOT SIGNING A FIELD AND THE DRAWBACKS THROUGH THE POSSIBLE ATTACK SCENARIOS [11].

Field name	**Signature useful**[a]	**Possible on top of JSR 257**[a]
Message Begin (MB)	−−	−−
Message End (ME)	−−	−−
Chunk Flag (CF)	+	−−
Short Record Flag (SR)	+	−−
ID Length Present Flag (IL)	+	−−
Type Name Format (TNF)	+	−−
Type Length	+	++
Payload Length	+	−−
ID Length	+	++
Type	++	++
ID	++	++
Payload	++	++

[a] Possible weights are ++, +, − and −− (with ++ being a definitive *yes* and −− a definitive *no*.)

III. Related Work

Madlmayr et al. [9] indicate that (without proper protection) NDEF-based applications are prone to various attacks. Mulliner [10] further investigates these assumptions and provides several practical attack scenarios against applications that use the NFC Data Exchange Format.

In [11], we evaluate methods to avert the risk of such malicious behavior. The result is that digital signatures provide the necessary properties to prevent many attacks: authentic, unforgeable and non-reusable [12]. However, digital signatures must be used in a proper way to diminish the security deficiencies of the NFC Data Exchange Format. Especially the trustworthiness of certificates and the permissions associated with certain certificates have to be thoroughly planned [13].

In [11], we further investigate the various methods of signing NDEF messages. We explain that signature is only useful for some elements of an NDEF record. It is important to sign some elements, while other elements should never be signed. Table I gives an overview of the usefulness of signing certain fields of an NDEF record. It also lists those fields that can and cannot be reliably retrieved on top of Java's Contactless Communication API (JSR 257). We conclude that "*a minimum of integrity and authenticity is achieved by signing the Type, ID, and Payload fields*" and that the flags "*MB and ME [. . .] should never be signed to allow [for] moving blocks of signed records within an NDEF message*" [11].

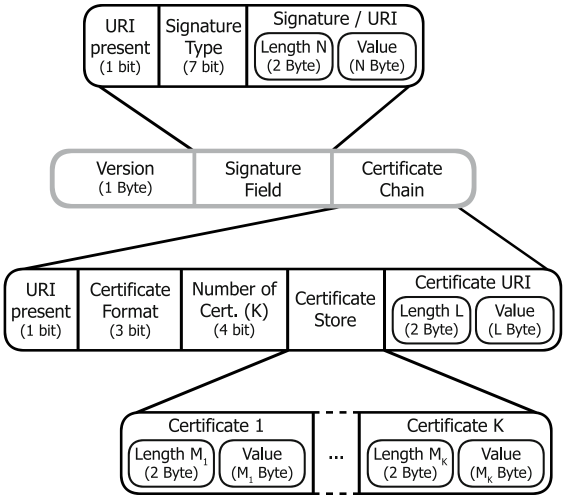


Fig. 2. The payload field of a signature contains the record's version information, a signature part and a certificate chain [13].

IV. Signature Record Type Definition

The Signature Record Type Definition [14] adds digital signatures to NDEF. It offers a trustworthy method for providing information about the origin of NDEF data and provides users with the possibility of verifying the authenticity and integrity of data within an NDEF message [14]. The NFC Forum released their first candidate for the specification in November, 2009[2].

An open-source implementation of an NDEF signature library for Java is already available[3], although, as of today it does not comply to the current version of the Signature RTD.

A. Signature Record

A signature record's payload consists of three parts: a version information, a digital signature, and a certificate chain. The complete layout is outlined in Fig. 2. The signature field contains either a signature or a URI reference to a signature over the signed data. The certificate chain is a list of certificates followed by an optional URI reference that points to a continuation of the list. The list starts with the certificate for the signing key and ends with a certificate that is issued by one of the trusted root certificate authorities. Each certificate in the list certifies the preceding certificate.

B. Signed NDEF Messages

Each signature record signs all preceding NDEF records starting either from the beginning of the NDEF message or from the record that follows the previous signature record (Fig. 3). Only the Type, ID, and Payload fields are considered for the signature. The remaining fields (header byte and length fields) of the records are not covered by the signature.

A special placeholder signature record, without signature and without a certificate chain, can be used to mark the beginning of a signed group of records while the preceding records remain unsigned.

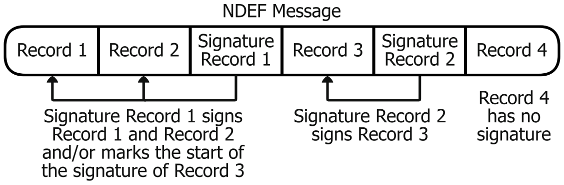

NDEF Message
Record 1
Record 2
Signature Record 1
Record 3
Signature Record 2
Record 4
Signature Record 1 signs Record 1 and Record 2 and/or marks the start of the signature of Record 3
Signature Record 2 signs Record 3
Record 4 has no signature

Fig. 3. Each signature record signs all preceding NDEF records starting either from the beginning of the NDEF message or from the record that follows the previous signature record [13].

V. Weaknesses of the Signature RTD

The signature record signs only the Type, ID, and Payload fields of NDEF records. According to [11], this is the worst case scenario, which only guarantees a minimum of integrity and authenticity of the signed records, but allows for the use of signatures on top of Java's Contactless Communication API. Therefore, we further analyzed the Signature Record Type Definition based on the results of [11]. We discovered several practical attack scenarios which are the result of weaknesses of the NDEF Signature Record Type and of missing instructions on the usage and interpretation of signatures.

A. Establishing Trust

Methods for establishing trust in the legitimacy of signed data are out of the scope of the Signature Record Type Definition. Implementers have to decide on their own how trust is handled and how trust relationships between content, issuers, receiving devices, and users can be established. Signature records only provide integrity and authenticity.

The problem of trust is explained in [15]: "*It is particularly important to distinguish between trust in a signature and trust in the owner of a signature. Under the right conditions digital signatures can provide confidence that a person (or an entity) has signed a data item but still say nothing about the trustworthiness of the person concerned.*"

In other words the receiver of a signed NDEF message can take as a fact that the issuer of the signature was in possession of the secret signing key and that the signed data is unmodified. Yet, a signature allows no assumptions about the trustworthiness of the issuer. This is where certificates come into play. With certificates, an ultimately trusted third party certifies that the issuer of the signature can be trusted in regard to certain actions. For instance, a certificate could associate an issuer with certain URIs and type names, or with the issuer's name.

B. Partial Signatures

Each group of one or more adjacent records can have its individual signature. As a consequence, a single NDEF message can contain multiple individually signed parts. It is even possible to combine signed and unsigned content into one NDEF message. Each signature can be associated with

[2] http://nfc-forum.org/specs/spec_dashboard/, retrieved on Oct. 22th, 2010
[3] http://www.nfcsigning.org/

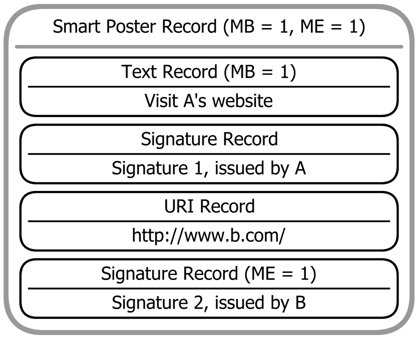


Fig. 4. A smart poster record can contain multiple record groups with different signatures.

a different certificate. Thus, an NDEF message can be an aggregate of multiple records signed by different parties.

As a consequence, an attacker could take records from existing NDEF messages that were legitimately signed by trusted parties and combine them with other records. These other records could either be unsigned or signed by a second party. This is not an issue as long as the individual record groups are independent of each other. In that case, the receiver can treat each record group individually and can base its trust on a single certificate chain. But things are different as soon as there is a relationship between multiple record groups. One context could contain signed and unsigned records or records signed by different parties. Then, the receiver has to decide whether to trust certain parts of that context or the context as a whole.

An example for such a context is the smart poster record. Its payload is an NDEF message that contains one URI record and multiple other records that describe the URI. When the smart poster record is signed as a whole (i.e. the smart poster record itself is signed) then the trust in the smart poster record and all its sub-records can be based on that signature and its certificate. The same applies to the case where all the sub-records of the smart poster are signed by a single party.

But the smart poster's sub-records could also be divided into multiple record groups. An example of such a record is depicted in Fig. 4. It contains a text record and a URI record. While the text record is signed with signature 1 (issued by party A), the URI record is signed with signature 2 (issued by party B). Therefore, the receiver has to evaluate if it trusts A's text and if it trusts B's URI. The result of this evaluation could be that the text ("Visit A's website") is legitimate for A and the URI ("http://www.b.com/") is legitimate for B. Nevertheless, in context of the smart poster record the text is a misleading description for the URI. An attacker could abuse this by replacing the smart poster URI with his own, signed URI. As a consequence, the receiver has to determine if it is safe to associate A's text with B's URI.

According to [16], three types of signing categories exist for static messages:

- comprehensively signed content,
- (partially) unsigned content, and
- signed content groups.

Comprehensively signed content has only one signature for all data and, thus, can be trusted based on this signature. The other two categories add a potential risk to the trust relationship.

With partially unsigned NDEF messages, the receiver can only trust the signed parts of the message, while the unsigned parts have to be regarded as untrusted. With signed content groups, the receiver's actions depend on the relationship between the content groups. On the one hand, as long as the groups are unrelated, each group and its signature can be handled individually. If, on the other hand, multiple content groups share a common context, they must also share a common origin (i.e. the signatures must be issued by the same party.)

As a general rule we propose that each and every record of a common context, like a smart poster, should be signed by the same party in order to be regarded as trustworthy.

C. Record Composition Attack

A complex record type, like the smart poster record, which consists of more than one NDEF record can be assembled from multiple individually signed records. As we showed in the previous section, all records that belong to a certain context should be signed by the same party. Even if this rule is obeyed, there is the possibility for an attack. We introduce a new type of attack against signed NDEF messages which we call the "*Record Composition Attack*". Such an attack is achieved in two steps (see Fig. 5):

1) Choose multiple unrelated NDEF records that were signed by one trusted party.
2) Combine these records into a single context to create a new meaning.

Exemplary use-cases are denial-of-service attacks and fraud. A denial-of-service attack can be achieved by composing a message that triggers misbehavior in the receiving application. The fact that, despite the misbehavior, all records are properly signed, could lead the user into additional confusion. Mulliner [10] explains that "*denial-of-service attacks can be used for destroying the trust relationship between the customer and the service provider.*" As the signature strongly binds the records to a certain issuer, trust in this issuer is severely endangered by such attacks.

Mulliner [10] also gives a scenario for fraud at snack vending machines. The concerning vending machines have an SMS-based payment system. NDEF tags with smart poster records are used to provide the user with a ready-made SMS message. During the proposed attack, the NDEF tag of vending machine 1 is replaced by that of vending machine 2. As a result, whenever a customer tries to pay at machine 1, the payment is triggered at machine 2, where the attacker receives the paid goods.

This attack can be circumvented by a combination of unique textual descriptions in the smart poster record and digital signature. Therefore, the smart poster explicitly describes which vending machine the payment applies to. Yet, based on

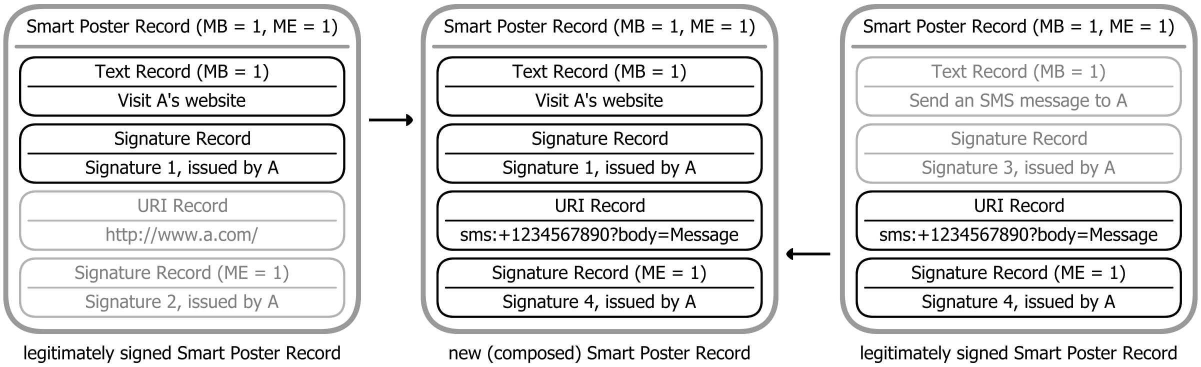


Fig. 5. Record Composition Attack: Parts of two legitimately signed smart poster records can be selectively combined into a new legitimate-looking smart poster record with a different meaning.

the record composition attack, a malicious smart poster record can be created from the text record of vending machine 1 and the URI record of vending machine 2.

At first glance, this attack seems to be possible only if each sub-record has its own separate signature. But on closer examination, records can be selectively hidden from signed NDEF messages. The fact that only the Type, ID, and Payload fields of NDEF records are included in the signature opens up for attacks as described in [11]. A malicious party can, for instance, manipulate a signed NDEF message so that the TNF header field of any unwanted record is set to “unknown”. Consequently, any such record is virtually masked out of the NDEF message. Similarly, by reducing the value of the Payload Length field, parts of the Payload field can be chopped off the end of a record. The trimmed parts can then be hidden in a new “unknown” record.

Fig. 6 shows an example for a record composition attack with selective record hiding: An adversary takes two smart poster records that are legitimately signed by party A. Then, the unwanted parts of each message (i.e. the URI record of the first message and the text record of the second message) are hidden by setting the TNF field to “unknown”. The NDEF messages are then combined into a new smart poster record. While the new record looks as if it was legitimately signed by A, it does not convey A’s intents.

These scenarios demonstrate that even when an NDEF message is signed by only a single party there is not necessarily a trust relationship between the signed records. Only if records are signed by the same signature record and, thus, form a single content group, they can be trusted to belong to each other. We propose the following guidelines to bypass the vulnerabilities caused by the NDEF records’ unsigned header fields:

- The receiver should only trust the relationship of records if they are signed and if they share a common signature record.
- The issuer of records should only sign related records with a common signature. Unrelated records should be signed with separate signatures to circumvent recomposition with receivers that obey the above guideline.

D. *Using Remote Signatures and Certificates*

A further potential weakness of the signature record type is the use of remote signatures and certificates referenced by URIs. This could open up for security vulnerabilities and privacy issues. The main problem is that the data referenced by the URIs has to be retrieved prior to verifying any signature. Therefore, the URIs within a signature record have no integrity and authenticity protection. As a result, an adversary could try to use these URIs to trigger maloperation.

First, the URIs are likely to be retrieved in the context of the user. Several possibilities arise for an attacker:

- It may be possible to use cookies and other identification data during the retrieval of the referenced URIs. An attacker could abuse this to access services that are usually only available to the user. For example, the URI could send a message on an on-line platform like Facebook in the context of the user that received the NDEF message.
- Furthermore, the URI could reference locations or services that are only available in the context of the receiving device. This includes local network resources and services that have IP address based access control and, therefore, can only be used from that device.
- There might even be a possibility to trigger the execution of program code (e.g. through buffer overflows) on the receiving device.

Second, the retrieval of remote URIs causes a privacy problem. When the URI references an Internet location, identification data (like an IP address and cookies) can be collected at a central service (cf. [17]). This could be used to collect usage data on tags even without the need for the user to actually access the services offered by the tag. As the URIs have to be retrieved prior to the verification of the signed NDEF data, the receiver cannot make any trusted assumptions on the offered service at the time the URI resource is accessed.

VI. Conclusion

While the Signature Record Type Definition adds integrity protection and authenticity to the NFC Data Exchange Format, it also opens up for several security vulnerabilities. We explained the problem of establishing trust in signed data

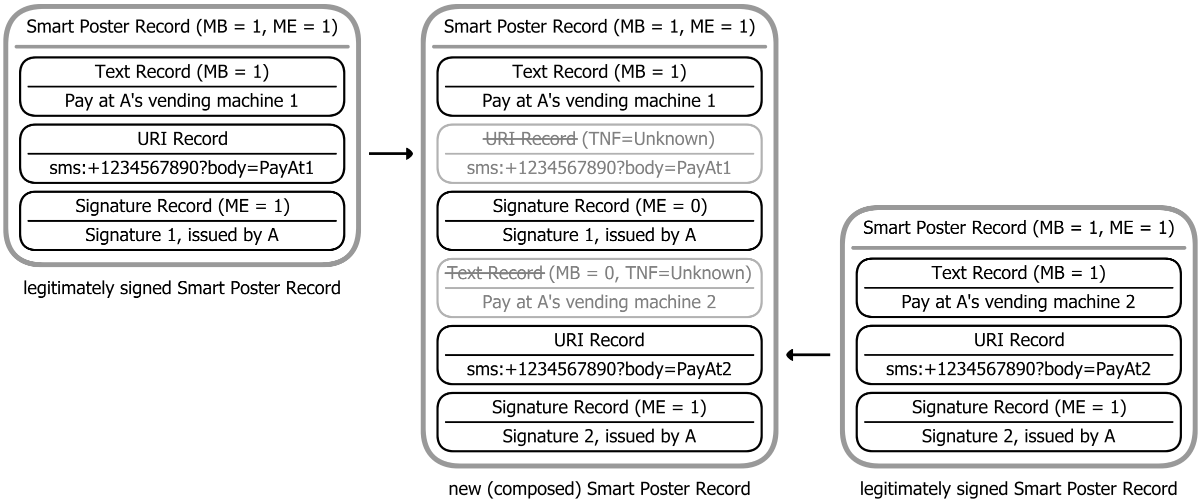

Smart Poster Record (MB = 1, ME = 1)
Text Record (MB = 1)
Pay at A's vending machine 1
URI Record
sms:+1234567890?body=PayAt1
Signature Record (ME = 1)
Signature 1, issued by A
legitimately signed Smart Poster Record
Smart Poster Record (MB = 1, ME = 1)
Text Record (MB = 1)
Pay at A's vending machine 1
~~URI Record~~ (TNF=Unknown)
sms:+1234567890?body=PayAt1
Signature Record (ME = 0)
Signature 1, issued by A
~~Text Record~~ (MB = 0, TNF=Unknown)
Pay at A's vending machine 2
URI Record
sms:+1234567890?body=PayAt2
Signature Record (ME = 1)
Signature 2, issued by A
new (composed) Smart Poster Record
Smart Poster Record (MB = 1, ME = 1)
Text Record (MB = 1)
Pay at A's vending machine 2
URI Record
sms:+1234567890?body=PayAt2
Signature Record (ME = 1)
Signature 2, issued by A
legitimately signed Smart Poster Record

Fig. 6. Record Composition Attack: Parts of two legitimately signed smart poster records are hidden. The NDEF messages are then combined into a new legitimate-looking smart poster record with a different meaning.

and its origin. We showed several practical attack scenarios against signed NDEF messages. Further, we proposed a new class of attacks against signed NDEF records, which we call the "*Record Composition Attack*". In an example, we demonstrated how this could be exploited in an actual NFC application. Nevertheless, we also outlined basic guidelines to avoid the risk of such attacks. Finally, we highlighted an other potential problem of the signature record type that potentially leads to security and privacy leaks.

ACKNOWLEDGMENT

This work is part of the project "4EMOBILITY" within the EU programme "Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)" funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

REFERENCES

[1] *Near Field Communication Interface and Protocol (NFCIP-1)*, Ecma International Std. ECMA-340, Rev. 2, Dec. 2004.

[2] *Near Field Communication Interface and Protocol -2 (NFCIP-2)*, Ecma International Std. ECMA-352, Rev. 1, Dec. 2003.

[3] E. Chen, "NFC: Short range, long potential," News Article, Aug. 2007. [Online]. Available: http://www.assaabloyfuturelab.com/FutureLab/Templates/Page2Cols____1905.aspx

[4] *NFC Data Exchange Format (NDEF)*, NFC Forum Technical Specification, Rev. 1.0, Jul. 2006.

[5] *NFC Record Type Definition (RTD)*, NFC Forum Technical Specification, Rev. 1.0, Jul. 2006.

[6] *Text Record Type Definition*, NFC Forum Technical Specification, Rev. 1.0, Jul. 2006.

[7] *URI Record Type Definition*, NFC Forum Technical Specification, Rev. 1.0, Jul. 2006.

[8] *Smart Poster Record Type Definition*, NFC Forum Technical Specification, Rev. 1.0, Jul. 2006.

[9] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC Devices: Security and Privacy," in *Proceedings of the Third International Conference on Availability, Reliability and Security (ARES '08)*, Barcelona, Spain, Mar. 2008, pp. 642–647.

[10] C. Mulliner, "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones," in *Proceedings of the International Conference on Availability, Reliability and Security (ARES '09)*, Fukuoka, Japan, Mar. 2009, pp. 695–700.

[11] M. Roland and J. Langer, "Digital Signature Records for the NFC Data Exchange Format," in *Proceedings of the Second International Workshop on Near Field Communication (NFC 2010)*, Monaco, Apr. 2010, pp. 71–76.

[12] B. Schneier, *Angewandte Kryptographie*. Addison-Wesley, 1996.

[13] J. Langer and M. Roland, *Anwendungen und Technik von Near Field Communication (NFC)*. Springer Berlin Heidelberg, 2010.

[14] *Signature Record Type Definition*, NFC Forum Candidate Technical Specification, Rev. 1.0 Candidate 1, Oct. 2009.

[15] B. Gladman, C. Ellison, and N. Bohm, "Digital Signatures, Certificates and Electronic Commerce," Jun. 1999. [Online]. Available: http://jya.com/bg/digsig.pdf

[16] J. Davis, "Application Guidelines on Digital Signature Practices for Common Criteria Security," in *MSDN Magazine*, Nov. 2009.

[17] P. Schaar, *Datenschutz im Internet: Die Grundlagen*. Verlag C.H. Beck München, 2002.