Security & Privacy Issues of the Signature RTD

Michael Roland

FH OÖ Forschungs & Entwicklungs GmbH
NFC Research Lab Hagenberg

2012-01-30

Introduction

The purpose of this document is to outline known security vulnerabilities and attack scenarios of the current Signature RTD specification [1].

Vulnerability 1: Partial Signature

The Signature RTD [1] defines that only the Type, ID and Payload fields of NDEF records are signed. The remaining fields (length, header byte) are not covered by the signature (see Fig. 1).

We found that by changing the remaining header fields (especially the Type Name Format/TNF) it is possible to manipulate the semantics of signed records [3], [4], [5]:

- Data can be moved between the three signed fields.
- Records can be hidden from processing.
- Records can be joined into a preceding record's payload.
- Parts of an NDEF record's payload can be extracted into separate records.
- Multiple signed NDEF messages can be combined into a new NDEF message without voiding the signatures.

Moving Data between Type, ID and Payload Fields

By changing the Length fields, it is possible to move bytes between the Type, ID and Payload fields. A record, that has the external type "mroland.at:myapp", an empty ID and the payload "1234567890" could be changed to a record with the external type "mroland.at:my", the ID "app" and the payload "1234567890"

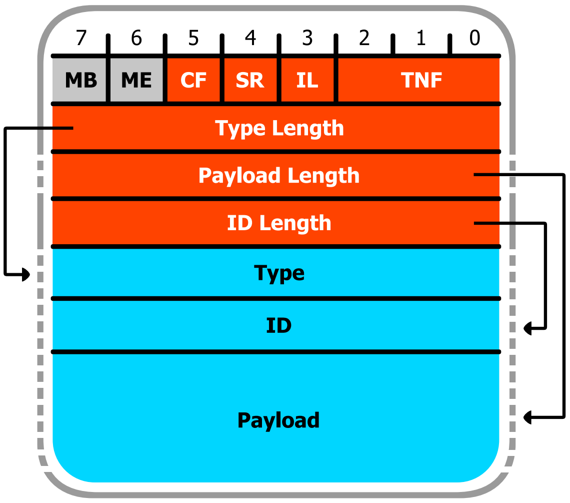

Fig. 1 Signed NDEF Record (**blue**: covered by signature, **red**/**gray**: not covered by signature, **gray**: must not be covered by signature)

Downloaded from
www.mroland.at

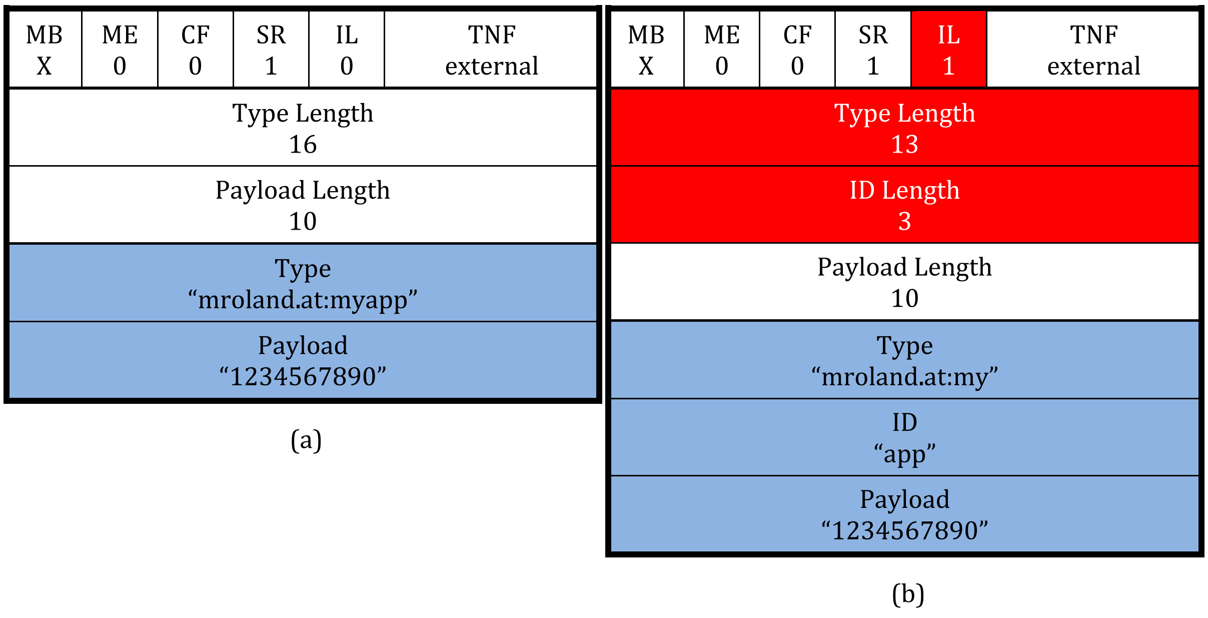

Fig. 2 Moving data between fields within a record: (a) is the original record, (b) is after moving the data

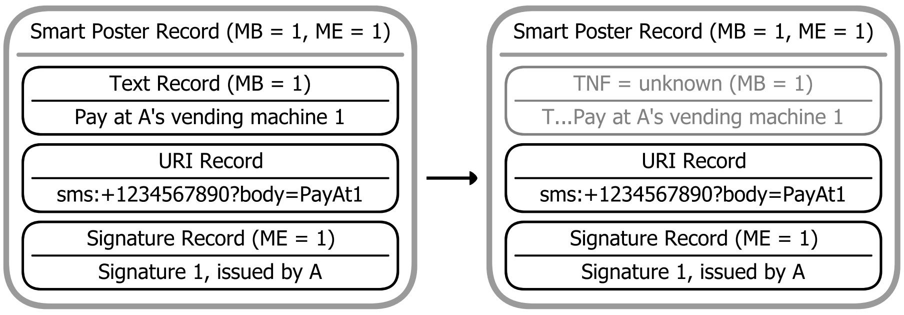
Smart Poster Record (MB = 1, ME = 1)
Text Record (MB = 1)
Pay at A's vending machine 1
URI Record
sms:+1234567890?body=PayAt1
Signature Record (ME = 1)
Signature 1, issued by A
Smart Poster Record (MB = 1, ME = 1)
TNF = unknown (MB = 1)
T...Pay at A's vending machine 1
URI Record
sms:+1234567890?body=PayAt1
Signature Record (ME = 1)
Signature 1, issued by A

Fig. 3 A text record is hidden from a signed NDEF message.
The text record's Type field is merged into its Payload field.

(Fig. 2). In both cases the signed data is "mroland.at:myapp1234567890" (**blue**), only header fields that are not covered by the signature are changed (**red**).

Record Hiding

Record hiding can be achieved by setting a record's TNF field to 0x5 ("unknown"). For unknown TNF, the specification [2] says:

> *"Regarding implementation, it is RECOMMENDED that an NDEF parser receiving an NDEF record of this type, without further context to its use, provides a mechanism for storing but not processing the payload."*

Therefore, a receiver of NDEF records should ignore such records. Consequently, with the current signature specification an attacker has a means of selectively hiding records from signed NDEF messages without voiding the signature (Fig. 3).

Joining Records

By changing the Length fields of the first record and removing the header byte and Length fields of subsequent records, multiple consecutive records can be joined into one record. For example, a record that has the external type "mroland.at:number", an empty ID and the payload "1234567890" and a record that has the external type "mroland.at:text", an empty ID and the payload "ABCDEFG" could be joined into one

Downloaded from
www.mroland.at

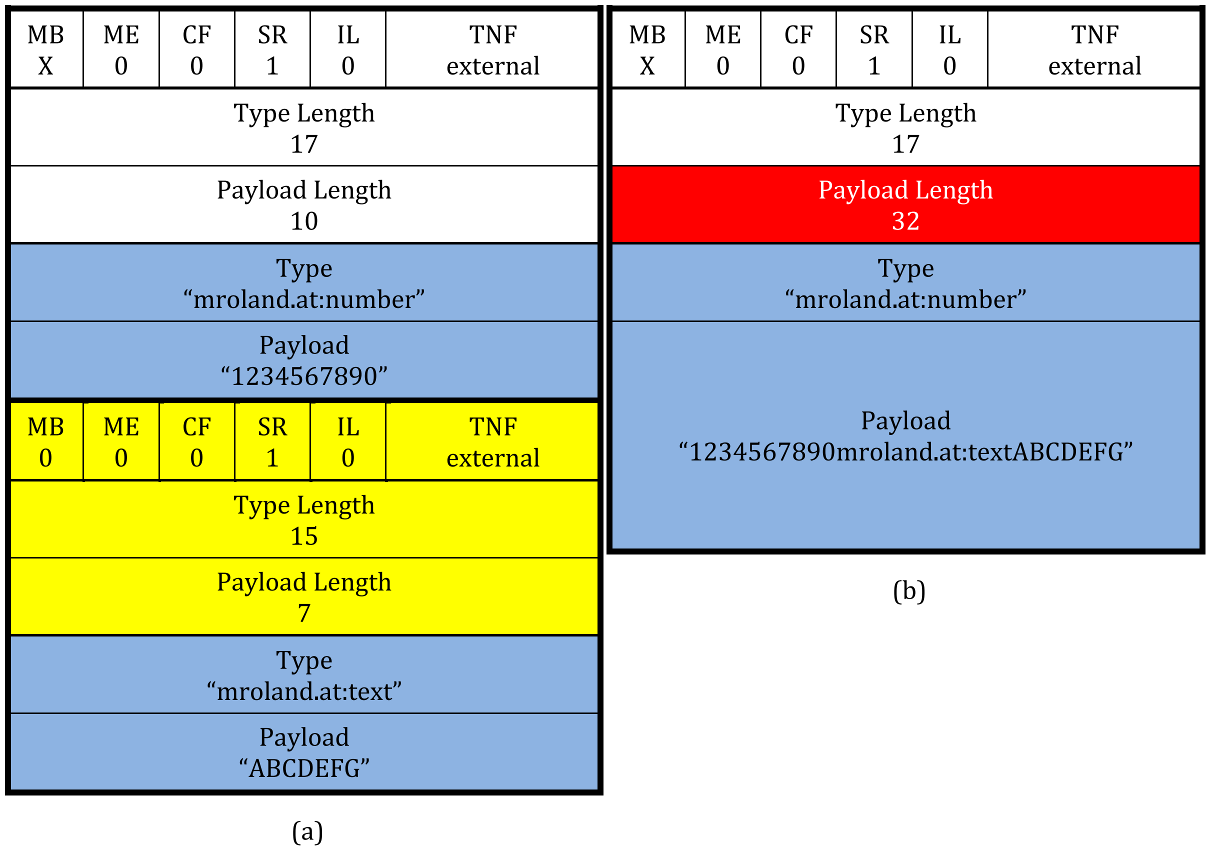

Fig. 4 Joining consecutive records: (a) is the original message, (b) is after joining (**blue**: covered by signature, **red**: modified header fields, **yellow**: removed header fields)

record with the external type "mroland.at:number", an empty ID and the payload "1234567890mroland.at:textABCDEFG". In both cases the signed data is "mroland.at:number1234567890mroland.at:textABCDEFG" (Fig. 4).

Extracting Records

Using these methods, it is possible to extract parts of a signed record's payload without voiding the signature. Unused parts can be suppressed with record hiding. Fig. 5 shows an example: A signed smart poster record is decomposed into sub-records. One sub-record hides all unwanted parts of the original smart poster record and one record is the remaining Text record. The signature is still valid.

Record Composition

Record composition can be achieved by collecting several signed NDEF messages (e.g. smart posters) and by assembling a new NDEF message from them. The new NDEF message still contains the old messages' signatures and will, therefore, still be regarded as validly signed. This is possible as multiple signatures are allowed in one NDEF message (or more precisely in one context.) I.e. a smart poster's URI record and Text record may have their own signature record (even if both signatures were issued with the same signing key.)

Practical Attack Scenario

The combination of the above vulnerabilities leads to a practical attack scenario (see Fig. 6):

Smart poster records contain ready-made SMS messages for payment at vending machines. Each message contains a text record "Pay at vending machine X" and a URI record "sms:+1234567890?body=PayX". Each smart poster record is signed.

Now, an adversary takes the legitimately signed smart poster NDEF messages of two vending machines (machine 1 & machine 2). The unwanted parts of each smart poster (i.e. the URI record of machine 1 and

Downloaded from www.mroland.at

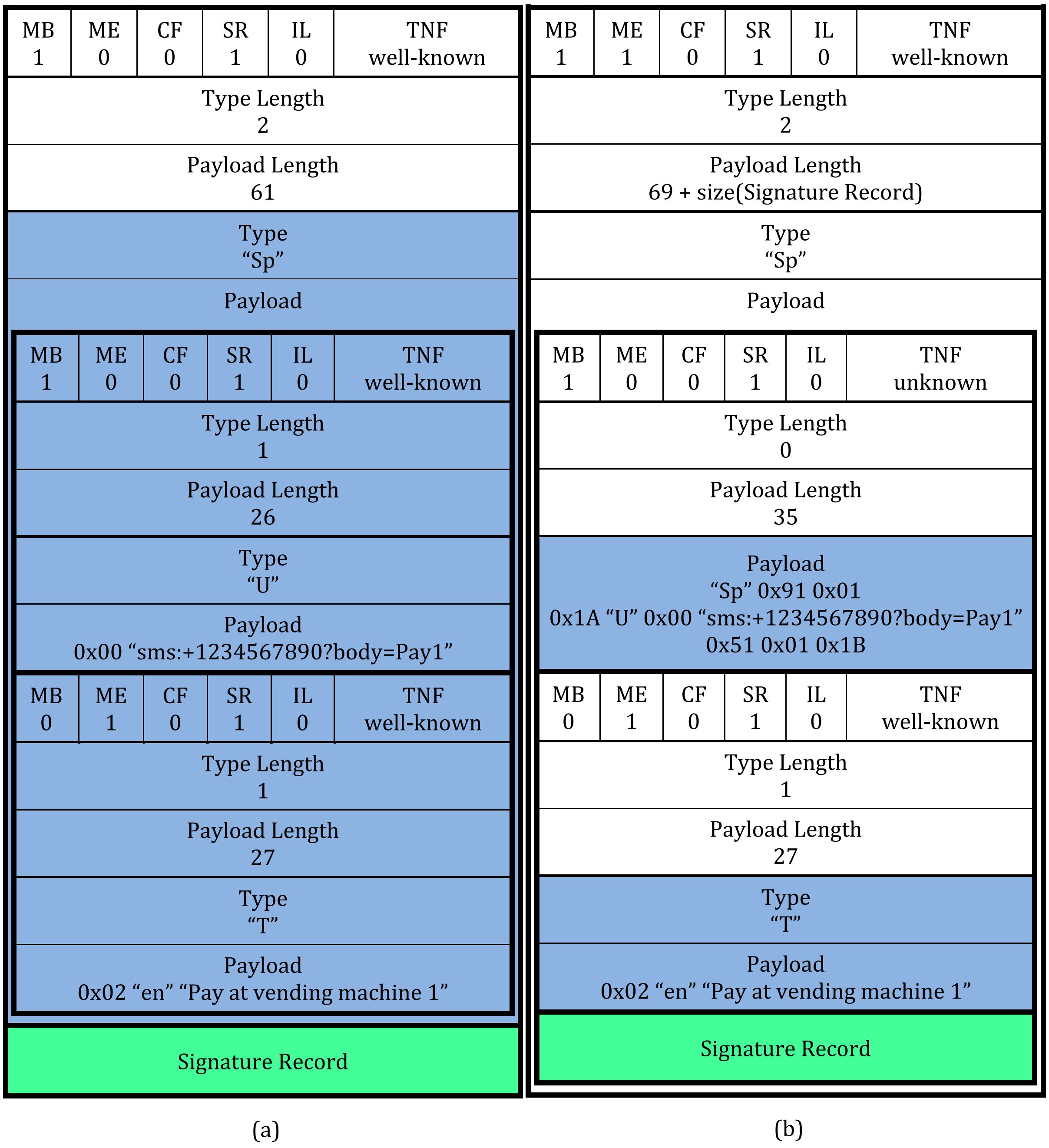

Fig. 5 Extracting parts of signed records: (a) original message, (b) extracted parts are embedded into a new smart poster record (blue: covered by signature)

the Text record of machine 2) are hidden by setting their TNF field to 0x5 ("unknown"). The resulting messages are then combined into a new smart poster record. The new smart poster's payload is now an unknown record, a Text record "Pay at vending machine 1", a valid signature over the previous two records, an unknown record, a URI record "sms:+1234567890?body=Pay2", an unknown record and again a valid signature over the previous three records.

As a result, the receiver of the NDEF message will see a smart poster record containing a Text record and a URI record, both with a valid signature. The attacker can now replace the NFC tag at vending machine 1 with a new tag containing this message. The user will still see the expected text "Pay at vending machine 1", but when sending the SMS message, the payment is actually processed for vending machine 2. There, the adversary could wait until the paid-for product is released.

Downloaded from www.mroland.at

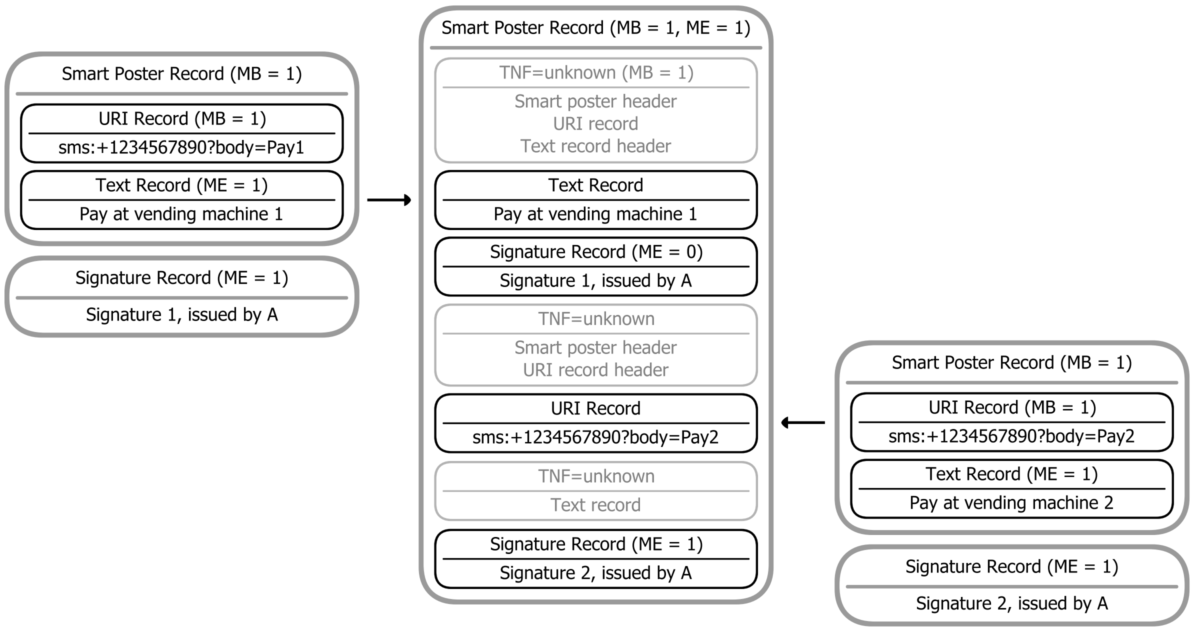

Fig. 6 Record Composition Attack: Two signed smart poster records are merged into a new signed(!) smart poster record

Proposed Solution

Record hiding and manipulation of header fields can be prevented by including record header fields (except for MB and ME flags) into the signature. However, this would prevent rearrangement of chunked records and recoding of the short record flag. A possible solution to this would be to sign the accumulated length field of all record chunks after the accumulated record payload. Additionally, the length field used for the signature could have a size that is independent of the short record flag.

Record composition can be prevented by enforcing a one signature per context policy. Where "context" refers to the sum of records that are in some way related to each other (e.g. all records in a smart poster's payload; records referencing other records by their ID field and the referenced records ...)

Vulnerability 2: URIs for Certificate and Signature Retrieval

The Signature RTD [1] allows signatures and certificates to be included directly or through URI references (Fig. 7). When signatures and certificate chains are referenced through URLs, these URLs themselves have no integrity and authenticity protection as they are required to be retrieved prior to any signature verification.

We identified several possible scenarios for abuse [6]:

- If the URLs are accessed without notifying the user, there is a possibility of invading the user's privacy by collecting user data (IP addresses, cookies ...) at the moment a tag is touched. Usage information can even be collected without the user actually accessing the offered service.
- Even an attacker could use this to collect usage & user data. The attacker would simply need to replace the tag with a tag where the certificate/signature URLs point to a location that is controlled by the attacker. The attacker would then collect data and forward the request to the original location (or the certificates/signature) extracted from the original tag. Therefore, the user would not even notice this attack.
- The URLs may reference locations only accessible by the user (controlled by cookies, IP based access control, local network segments ...). An attacker may use this to trigger operations that can only be started by the user. Examples would be to send a Facebook message in the context of the user or to issue a HTTP GET request to a service on the user's LAN.

Downloaded from
www.mroland.at

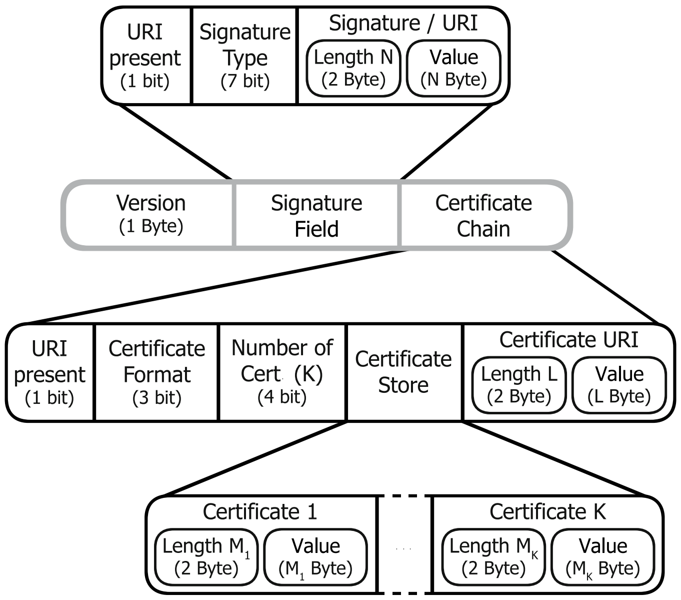

Fig. 7 Signature Record

- Vulnerabilities of the underlying operating system could be triggered (e.g. buffer overflows, execution of program code …)

Proposed Solution

The most restrictive solution would be to completely disallow the use of URI references in the signature record. Another (partial) solution would be to restrict the URIs to locations specified by the installed root certificates (not within the scope of the Signature RTD). With this partial solution the root certification authority would still be able to track tag usage.

Weakness 1: Missing Framework

Methods for establishing trust in the legitimacy of signed data are out of the scope of the Signature RTD [1]. 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 [7]:

> *"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 link an issuer with certain URIs and type names, or with the issuer's name.

Proposed Solution

A framework for certification needs to be defined:

- Who is allowed to issue trusted certificates?
- What does a certificate certify?
- How are certificates linked to content?
- Who is allowed to sign what content?

Downloaded from
www.mroland.at

References

[1] NFC Forum: *Signature Record Type Definition*. Technical Specification, Version 1.0.

[2] NFC Forum: *NFC Data Exchange Format (NDEF)*. Technical Specification, Version 1.0.

[3] M. Roland, J. Langer: *Digital Signature Records for the NFC Data Exchange Format*. In: Proceedings of the 2nd International Workshop on Near Field Communication, Monaco, Apr. 2010, pp. 71–76.

[4] M. Roland, J. Langer, J. Scharinger: *Security Vulnerabilities of the NDEF Signature Record Type*. In: Proceedings of the 3rd International Workshop on Near Field Communication, Hagenberg, Austria, Feb. 2011, pp. 75–84.

[5] NFC Forum TC Input Paper: *Comment #00652 - Record hiding and record composition*. Public comment on NFCForum-TS-Signature_RTD-1.0.
TC-SEC-00008R000-Signature_RTD_Comment_652_Record_hiding_and_record_composition.zip

[6] NFC Forum TC Input Paper: *Comment #00653 - Privacy issues and vulnerabilities with remote URIs for certificates*. Public comment on NFCForum-TS-Signature_RTD-1.0.
TC-SEC-00009R000-Signature_RTD_Comment_653_Privacy_issues_and_vulnerabilities.docx

[7] B. Gladman, C. Ellison, N. Bohm: *Digital Signatures, Certificates and Electronic Commerce*. Jun. 1999. Online: ftp://ftp.fh-wolfenbuettel.de/pub/security/dfn-cert/docs/PCA/misc/digsig.pdf

Downloaded from
www.mroland.at