Security Vulnerabilities of the NDEF Signature Record Type

Michael Roland
Upper Austria University of Applied Sciences, Hagenberg, Austria

3rd International Workshop on Near Field Communication
22 February 2011, Hagenberg, Austria

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

Outline

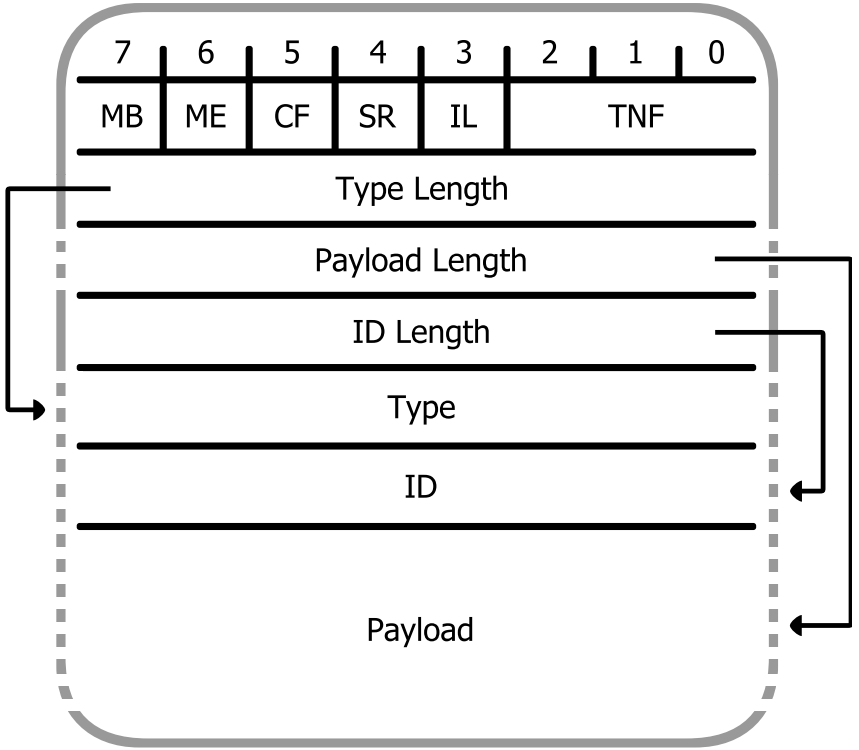
- Introduction and Motivation
  - What is the NFC Data Exchange Format?
  - What are potential attacks against NDEF applications?
  - How can digital signatures help?
- NDEF Signature Record Type
  - How does a signature record look like?
  - How to add a signature to an NDEF message?
- Weaknesses of the Signature RTD
  - Trust
  - Partial signatures
  - Record composition
  - Remote signatures and certificates
- Conclusion

NFC Data Exchange Format (NDEF)

- Standardized data format for NFC applications
- Enables the “it’s all in a touch” principle:
  - Upon touching an NFC-enabled object with an NFC device NDEF messages are exchanged and an action is triggered.
- Applications are:
  - Business cards
  - Smart posters (i.e. posters with active content like a website‘s URL or instructions to send an SMS message)
  - Enabler for wireless technologies (i.e. Bluetooth or WiFi pairing)
  - …

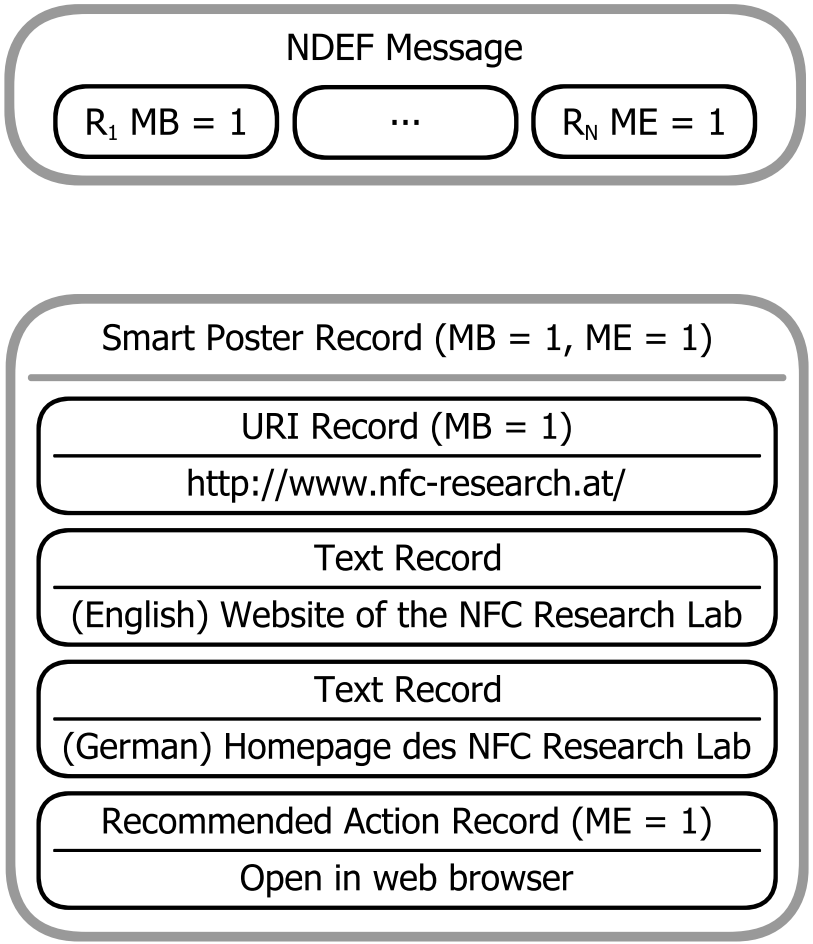
NDEF Record

- Header
  - Flags
    - Message Begin (MB)
    - Message End (ME)
    - Chunk Flag (CF)
    - Short Record (SR)
    - ID Length present (IL)
  - Type Name Format (TNF)
  - Length fields
  - Type
  - ID
- Payload



NDEF Message

- Sequence of one or more NDEF records
- First record has MB set
- Last record has ME set
- Records can contain NDEF messages as payload
  - E.g. Smart Poster Record



Vulnerabilities of NDEF applications

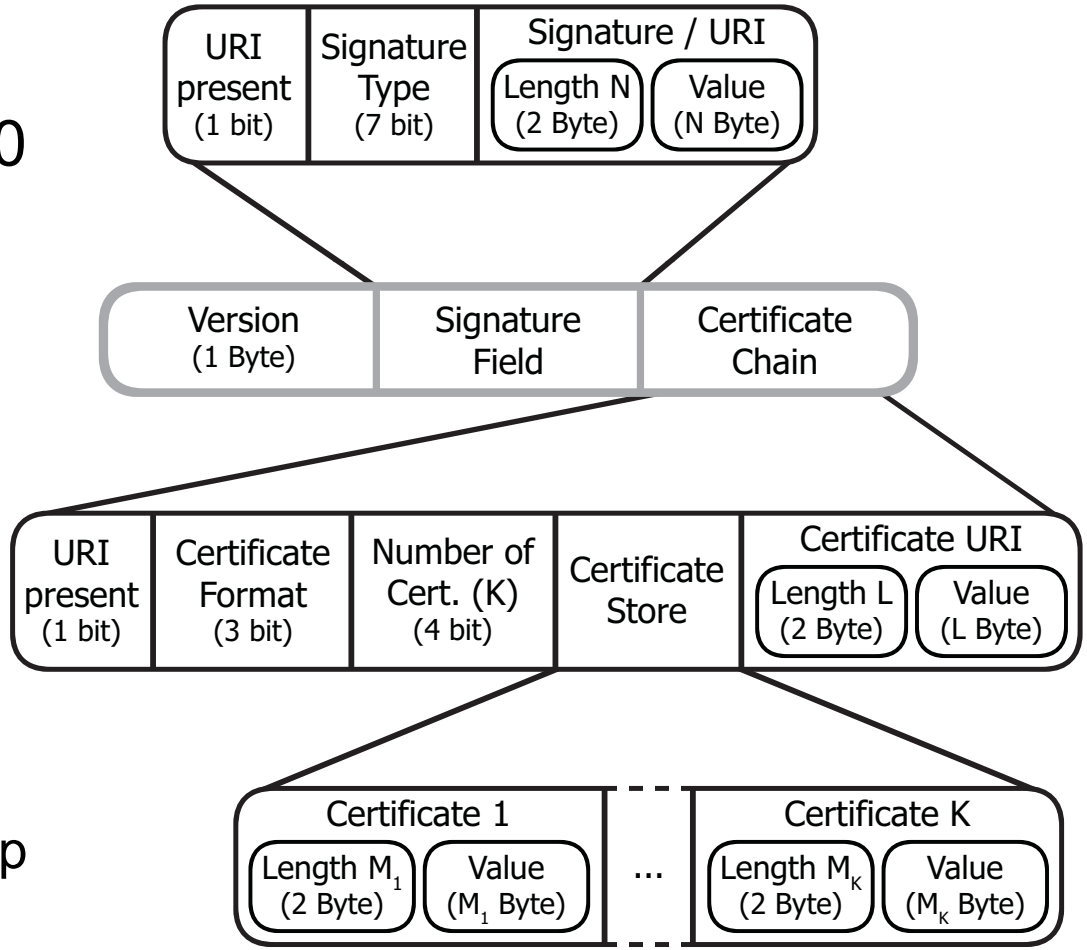
- Manipulation/replacement of NFC tags and their content
- Typical attack scenarios:
  - Replace a smart poster‘s URL
    - Redirect user to phishing site
    - Redirect user to malware
  - Replace a phone number (SMS or hotline)
    - Redirect user to premium rate service (typically owned the by attacker)
- The average user cannot distinguish forged from genuine tags

Digital Signatures

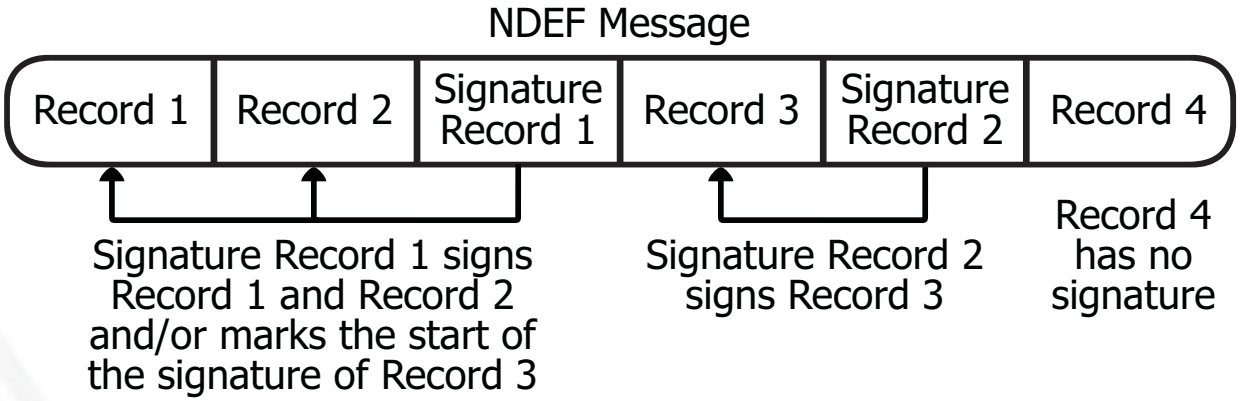
- What is a signature?
  1. A hash value is generated from the data.
     - Assures integrity of the signed data
  2. The hash value is encrypted with the signers secret key.
     - Assures authenticity of the signed data
- Properties of a digital signature:
  (based on a trustworthy certification infrastructure)
  - Authentic: The signer can be reliably identified.
  - Unforgeable: Only the owner of the signing key can produce a certain signature.
  - Non-reusable: The signature is only valid for the signed data.

NDEF Signature Record Type

- Final specification released in Nov. 2010
- Record structure
  - Signature field
    - Signature or URI reference to signature
  - Certificate chain
    - Chain of PKI certificates (embedded and referred by URI) up to a trusted root



NDEF Signature Record Type



- Signature record is appended to a sequence of records
- Signature record signs every record between the previous signature record and itself (or the beginning of the NDEF message and itself)
- One NDEF message may contain more than one signature

Signing NDEF Records

- Message Begin (MB)/Message End (ME)
  - Must not be signed, otherwise the signature could not be appended to the signed NDEF message
- Type, ID, Payload
  - Data fields must be signed to assure data integrity
- Type Length, ID Length, Payload Length
  - Must be signed, otherwise the boundaries of the Type, ID, Payload fields can be arbitrarily chosen (→ voids data integrity)
  - Subsequent records could be integrated into a records payload
- Type Name Format (TNF)
  - When TNF is changed, the meaning of the record changes
  - Can be used to hide records (specify type as “unknown”)

Signing NDEF Records

Field name	Signature useful	Possible on top of JSR 257	NDEF Signature Record Type
Message Begin	Must not sign	No	Not signed
Message End	Must not sign	No	Not signed
Chunk Flag	Important	No	Not signed
Short Record Flag	Important	No	Not signed
ID Length Present Flag	Important	No	Not signed
Type Name Format	Necessary	No	Not signed
Type Length	Necessary	Yes	Not signed
Payload Length	Necessary	No	Not signed
ID Length	Necessary	Yes	Not signed
Type	Necessary	Yes	Signed
ID	Necessary	Yes	Signed
Payload	Necessary	Yes	Signed

Weaknesses of the Signature RTD

No methods to establish trust are defined in Signature RTD

- Who should be trusted to issue certificates?
  - Implementers / users have to decide on their own
  - Compatibility issues between NDEF-applications if no common infrastructure is established
- What should (and could) a certificate certify?
  - E.g. a certain issuer may use a specific domain name in URIs
  - E.g. a certain issuer may use specific record types

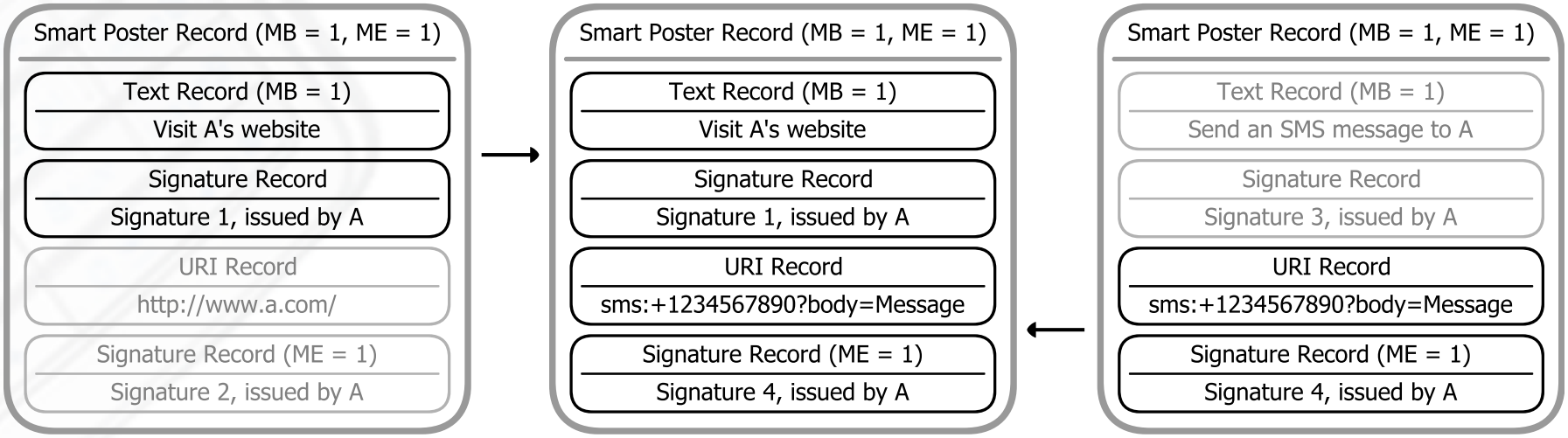
Weaknesses of the Signature RTD

Partially signed messages & records by multiple issuers

- One NDEF message can contain multiple individually signed (or unsigned) parts
  - No problem if record groups are independent of each other
  - BUT:
    - Can references between records issued by different parties be trusted?
- We propose:
  - Records within one context (e.g. smart poster) should be signed by exactly one party

Vulnerability → Record Composition

- Record Composition Attack
  - Choose multiple unrelated NDEF records that were signed by a single trusted party
  - Combine these records into a single context to create a new meaning



legitimately signed Smart Poster Record

new (composed) Smart Poster Record

legitimately signed Smart Poster Record

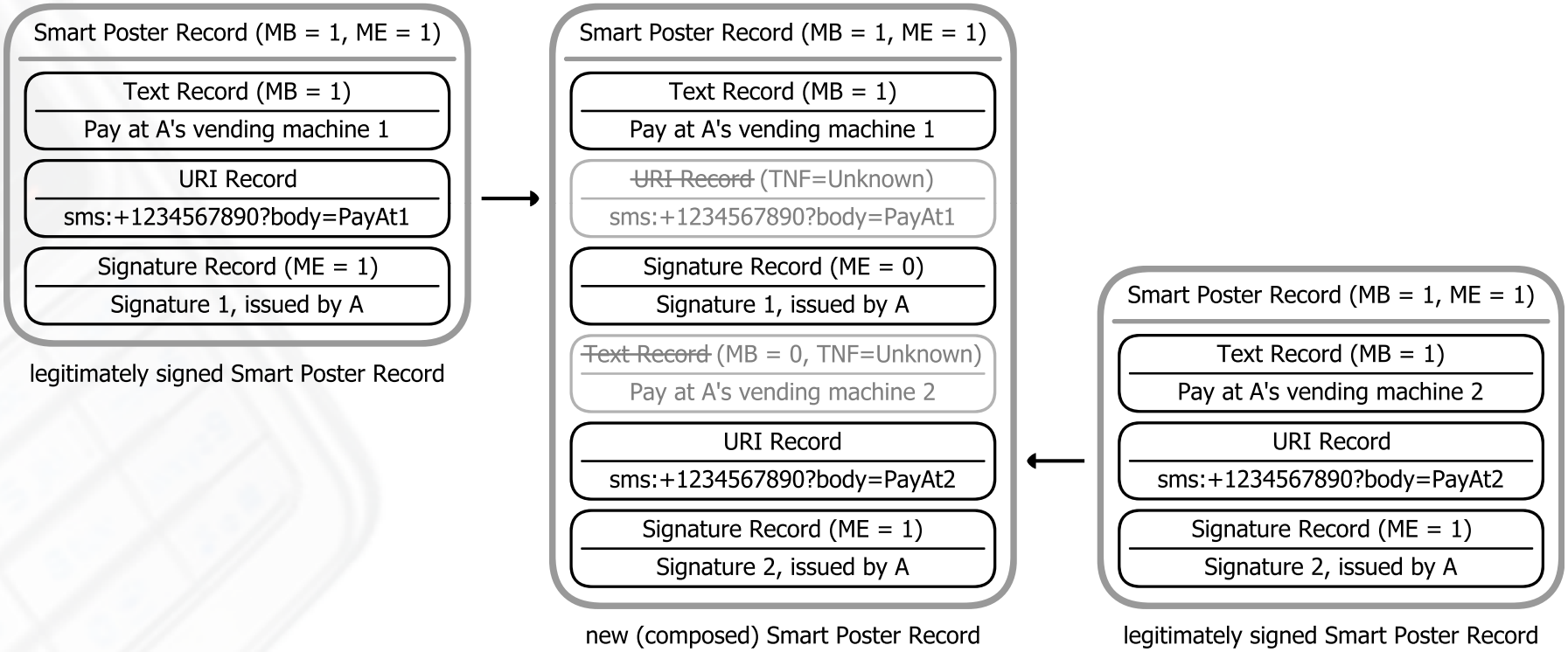
Record Composition Attack: Example

- Two snack vending machines (A & B) are equipped with NDEF tags containing ready-made SMS messages for payment
- The attacker exchanges the SMS message of the two NDEF tags but leaves the descriptive text inplace
- If a customer buys something at machine A the payment is registered at machine B where the attacker can retrieve the payed goods

Record Composition Attack: Advanced

- Record composition seems to be possible only if each sub-record has its own signature
- BUT: Records can be selectively hidden from signed NDEF messages
  - Type Name Field (TNF) can be set to “unknown” for every unwanted record
  - This is even possible if the smart poster record is signed as a whole (i.e. bytes before and after the wanted record can be put into own records)

Record Composition Attack: Advanced Example



Record Composition Attack: Avoiding It

- A receiver of NDEF messages should only trust the relationship of records if they are signed by the same signature record
- An issuer of NDEF records should sign all related records with a single signature record
- An issuer of NDEF records should sign all unrelated record groups with separate signature records
- BUT: Even if these rules are followed an attacker can still hide specific parts of a signed NDEF message

Vulnerability → Information Disclosure

- Signature records may contain remote signatures and certificates referenced by URIs
  - These resources have to be retrieved prior to signature verification
  - URIs have no integrity and authenticity protection
  - URIs can be used to trigger maloperation
- Examples:
  - Access services/resources that are only available to the attacked user (cookies, location based authentication, closed networks, …)
  - Disclose sensitive data of the user (IP address, cookies, tag usage, …)
  - Trigger bugs in the URI retrieval engine to execute code

Conclusion

- Signature RTD is a first step towards adding integrity protection and authenticity to the NFC Data Exchange Format
- Additional specifications of the certification architecture and signature handling are necessary
- Signature RTD has several flaws in its current version
  - Record Hiding
  - Record Composition Attack

Thank You!

Michael Roland
Research Associate, NFC Research Lab Hagenberg
Upper Austria University of Applied Sciences, Hagenberg, Austria

michael.roland (at) fh-hagenberg.at

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