Near Field Communication
Research Lab
Hagenberg

© Michael Roland
www.mroland.at

Security & Privacy Issues of the Signature RTD

Michael Roland
FH OÖ Forschungs & Entwicklungs GmbH

8 February 2012
TWG Security, NFC Forum Member Meeting

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).

© Michael Roland
www.mroland.at

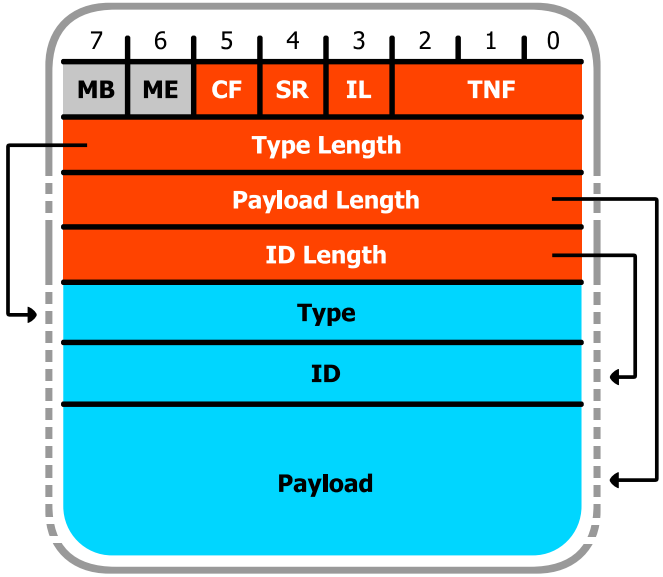
Content

- Partial Signature
- URIs for Certificate and Signature Retrieval
- Missing Framework

© Michael Roland
www.mroland.at

Vulnerability: Partial Signature

- Only Type, ID, Payload fields of NDEF records are signed
- Remaining fields not signed: TNF, IL, SR, CF, length fields
- It is possible to change the semantics of a signed record without invalidating the signature
  - 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 seperate records
  - Multiple signed NDEF messages can be combined into a new NDEF message



© Michael Roland
www.mroland.at

Moving data between fields

MB	ME	CF	SR	IL	TNF
X	0	0	1	0	external
Type Length 16					
Payload Length 10					
Type “mroland.at:myapp”					
Payload “1234567890”					

original record

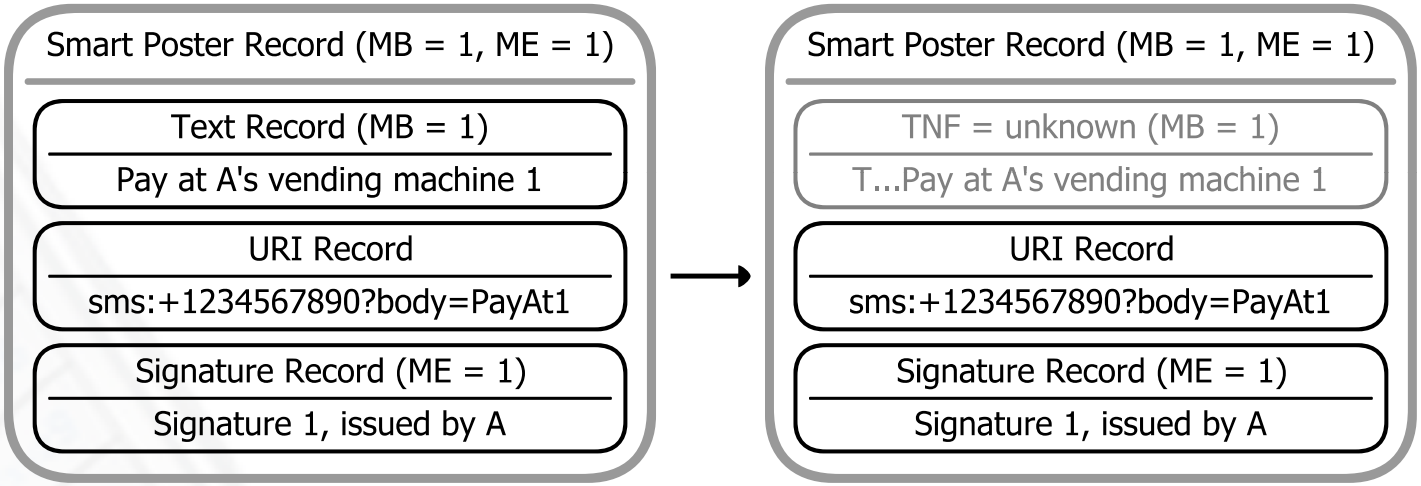
MB	ME	CF	SR	IL	TNF
X	0	0	1	1	external
Type Length 13					
ID Length 3					
Payload Length 10					
Type “mroland.at:my”					
ID “app”					
Payload “1234567890”					

after moving data

- The string “app” is moved from the Type field to the ID field
- The signature remains valid!

© Michael Roland
www.mroland.at

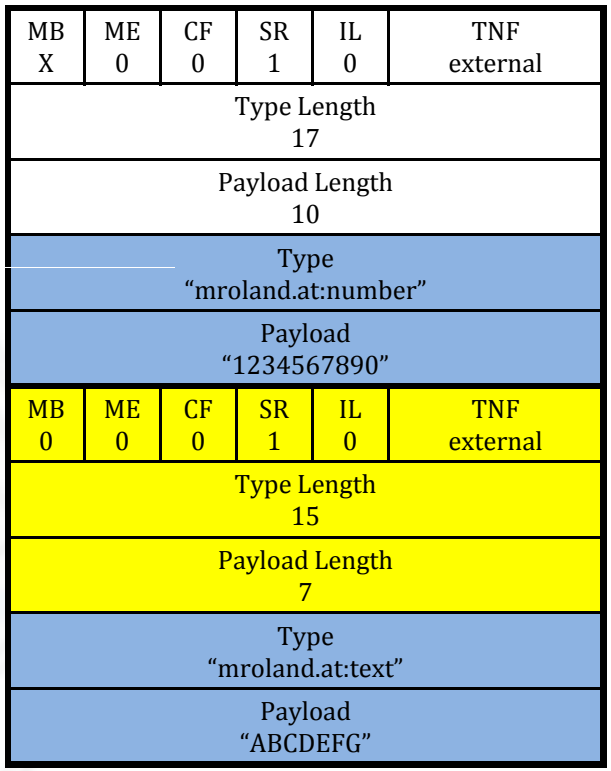
Record hiding



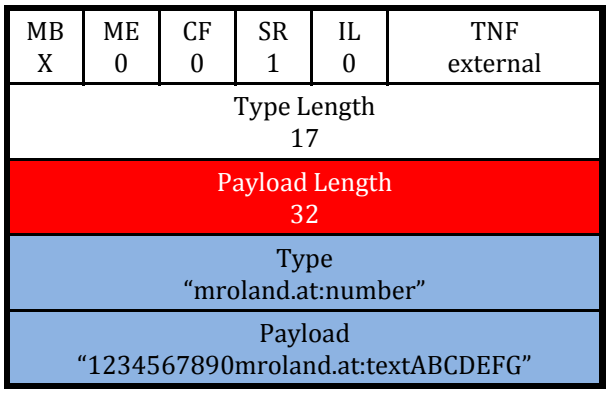
- A record can be hidden from processing by setting a records TNF (Type Name Field) to “unknown” (0x5)
- The signature remains valid!

© Michael Roland
www.mroland.at

Joining records



original record



after joining data

- The second record's signed fields are merged into the first record's payload field
- The signature remains valid!

© Michael Roland
www.mroland.at

Extracting records

MB	ME	CF	SR	IL	TNF
1	0	0	1	0	well-known
Type Length: 2					
Payload Length: 61					
Type: “Sp”					
Payload					

MB	ME	CF	SR	IL	TNF
1	0	0	1	0	well-known
Type Length: 1					
Payload Length: 26					
Type: “U”					
Payload: 0x00 “sms:+1234567890?body=Pay1”					

MB	ME	CF	SR	IL	TNF
0	1	0	1	0	well-known
Type Length: 1					
Payload Length: 27					
Type: “T”					
Payload: 0x02 “en” “Pay at vending machine 1”					

Signature Record

MB	ME	CF	SR	IL	TNF
1	1	0	1	0	well-known
Type Length: 2					
Payload Length: 69 + size(Signature Record)					
Type: “Sp”					
Payload					

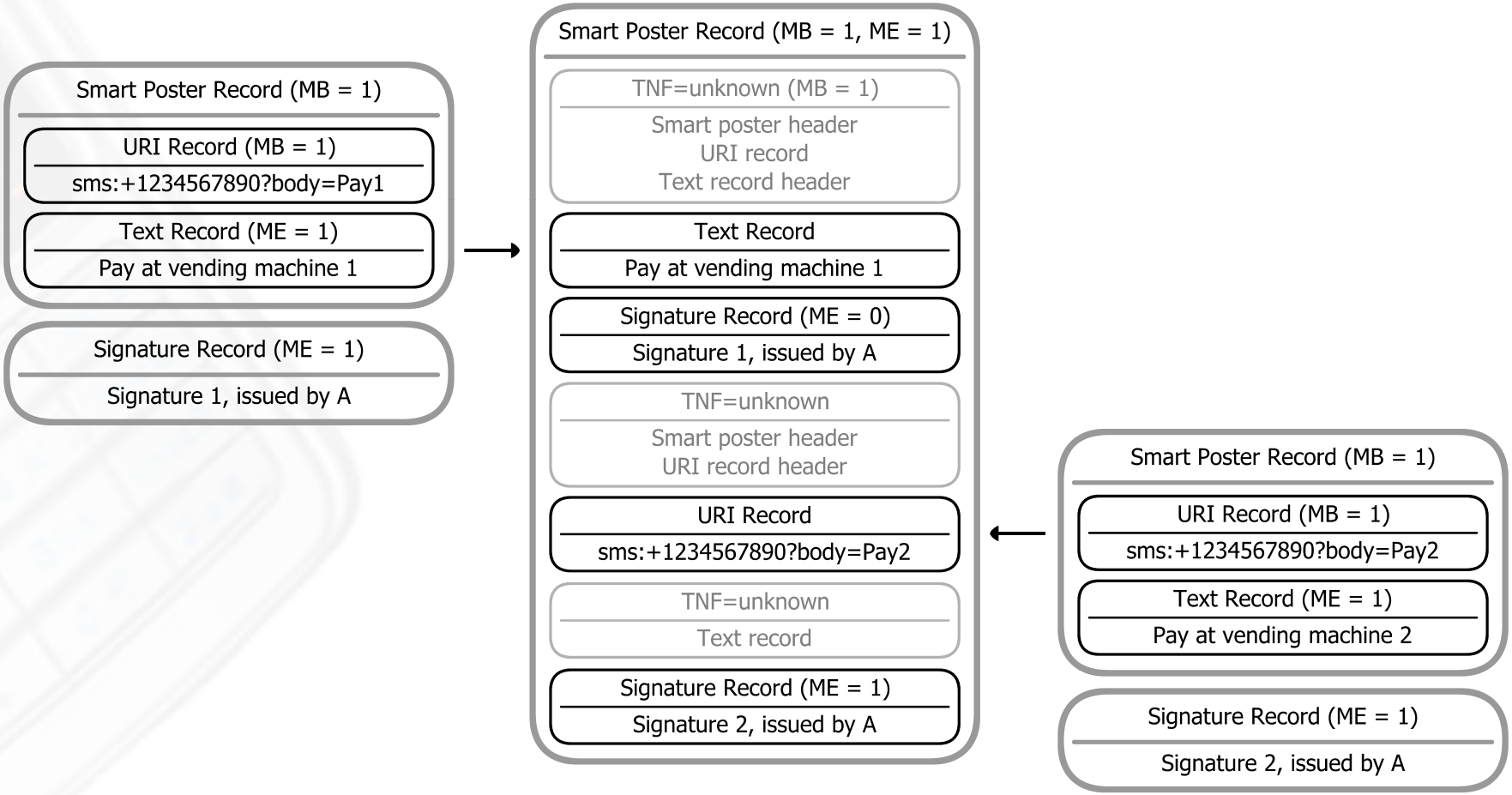
MB	ME	CF	SR	IL	TNF
1	0	0	1	0	unknown
Type Length: 0					
Payload Length: 35					
Payload: “Sp” 0x91 0x01 0x1A “U” 0x00 “sms:+1234567890?body=Pay1” 0x51 0x01 0x1B					

MB	ME	CF	SR	IL	TNF
0	1	0	1	0	well-known
Type Length: 1					
Payload Length: 27					
Type: “T”					
Payload: 0x02 “en” “Pay at vending machine 1”					

Signature Record

© Michael Roland
www.mroland.at

Record composition



© Michael Roland
www.mroland.at

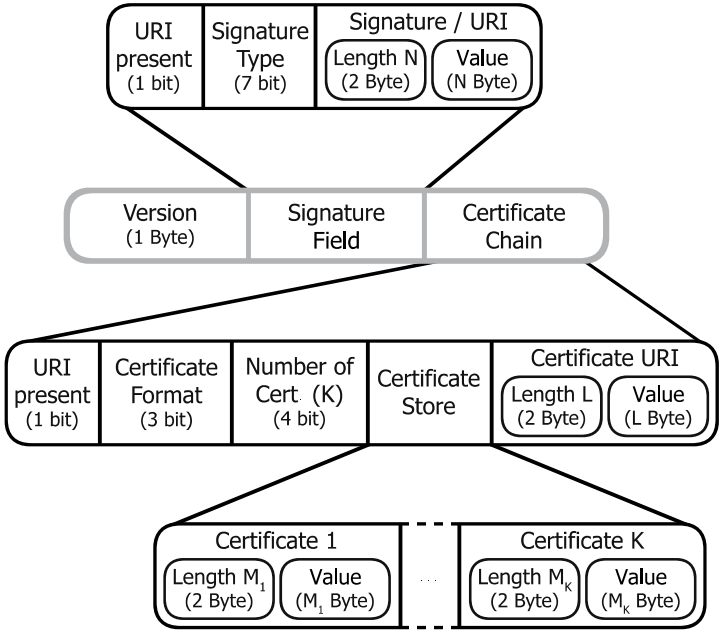
Proposed solution/workaround

- Include header fields (except MB, ME) into signature
  - \+ Prevents record hiding & manipulation
  - − No rearrangement of record chunks
  - − No conversion between short and normal-length records
- Sign accumulated length fields of all record chunks after the record payload
  - \+ Allows rearrangement of record chunks
  - \+ Can be independent of short record flag
- Enforce a “one signature per context” policy (e.g. one smart poster == one signature record)
  - \+ Prevents record composition
  - − Less dynamic?

© Michael Roland
www.mroland.at

Vulnerability: URIs in Signature Record

- Signature RTD uses URIs to reference signatures and certificates stored in remote locations
- Privacy risk!
  - If URLs are accessed without notification, the user's privacy can be invaded by collecting user data (IP addresses, cookies …)
  - **No need to actually use the service offered by the tag!**
- URIs have no integrity/authenticity protection
  - URIs are retrieved prior to signature verification!
  - **More evil scenarios possible ;-)** *(→ see next slide)*



URIs in Signature Record (cont'd)

- Collection of usage & user data by an attacker
  - Replace URLs of the signature record with URLs controlled by the attacker
  - When request is received:
    - Collect data
    - Redirect request to original URL (user will not notice this attack)
- Access locations that are only accessible by the user
  - Locations protected by IP based access control, local network segments …
  - An attacker can use specially crafted URLs to trigger operations in the context of the user
    - E.g. send Facebook message, issue HTTP GET request on user's LAN
- Trigger URL parsing vulnerabilities of the underlying operating system

© Michael Roland
www.mroland.at

Proposed solution/workaround

- Disallow URI references in signature records
  - \+ Prevents URI abuse
  - − May significantly increase signature size
- Authorize specific URIs based on the installed root certificate (i.e. root certificate carries set of allowed URIs)
  - \+ Prevents URI abuse
  - − Tag usage can still be tracked by URI owner
  - − URIs can only be managed by the root CA
    - CA must manage URIs / a scheme for delegating URIs to issued certificates is necessary

© Michael Roland
www.mroland.at

Missing Framework

- Signature RTD only defines the data structure of the signature record
  - Digital signature guarantees that issuer posesses a certain signing key
  - BUT: No information about trustworthiness of issuer
- Usable digital signatures requre a certificate infrastructure
  - Set of ultimately trusted third parties issue certificates
    - Certificate: a certain issuer **possesses** a **specific secret** signing key and is allowed to issue **trusted** signatures for **specific actions/records**
- Framework needs to give answers to several questions:
    - Who is allowed to issue trusted certificates? (Who are the root CAs?)
    - What does a certificate certify?
    - How are certificates linked to content? (Should every issuer be allowed to sign any records? Link to record type, URIs …)

© Michael Roland
www.mroland.at

Michael Roland
Research Associate, NFC Research Lab Hagenberg
FH Oberösterreich, Campus 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).