Signature Record Type Definition

Technical Specification

NFC Forum™

SIGNATURE 1.0

NFCForum-TS-Signature_RTD-1.0

2010-11-18

RESTRICTIONS ON USE

Contents

Figures

Tables

1 Introduction

Digital signing of NDEF data is a trustworthy method for providing information about the origin of NDEF data in an NFC Forum Tag and NFC Forum Device. It provides users with the possibility of verifying the authenticity and integrity of data within the NDEF message.

1.1 Objectives

The objective of this document is to function as a normative reference to the Signature RTD.

1.2 Purpose

1.2.1 Mission Statement and Goals

The Signature RTD specifies the format used when signing single or multiple NDEF records. The goal is to define the required and optional signature RTD fields, as well as provide a list of suitable signature algorithms and certificate types that can be used to create the signature.

The goal is not to define or mandate a specific PKI or certification system, or to define a new algorithm for use with the Signature RTD. Also, specification of the certificate verification and revocation process is out of scope.

1.3 Applicable Documents or References

[DSA]	Digital Signature Standard (DSS), FIPS PUB 186-2 with Change Notice 1, October 05, 2001 Information Technology Laboratory, National Institute of Standards and Technology
[ECDSA]	Digital Signature Standard (DSS), FIPS PUB 186-2 with Change Notice 1, October 05, 2001 Information Technology Laboratory, National Institute of Standards and Technology
[NDEF]	NFC Data Exchange Format, Version 1.0, July 2006, NFC Forum
[PKCS_1]	PKCS#1, RSA Cryptography Standard, Version 2.1, June 2002, RSA Laboratories
[RFC2119]	See [DIGITAL].
[RFC3280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, April 2002, Internet Engineering Task Force

[RFC3492] Punycode: A Bootstring Encoding of Unicode for Internationalized Domain Names in Applications (IDNA), RFC 3492, A. Costello: March 2003, Internet Engineering Task Force

[RFC3987] Internationalized Resource Identifiers (IRIs), RFC 3987, M. Duerst, M. Suignard, January 2005 Microsoft Corporation

[RTD] NFC Record Type Definition (RTD), Version 1.0, July 2006, NFC Forum

[URI_RTD] URI Record Type Definition, Version 1.0, July 2006, NFC Forum

[X_509] Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, ITU-T Recommendation, August 2005, International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T)

[X9_68] ASC/X9 X9.68 Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems: Part 2: Domain Certificate Syntax, January 2001, Accredited Standards Committee

1.4 Administration

The NFC Forum Data Exchange Format Specification is an open specification supported by the Near Field Communication Forum, Inc., located at:

401 Edgewater Place, Suite 600
Wakefield, MA, 01880

Tel.: +1 781-876-8955
Fax: +1 781-610-9864

http://www.nfc-forum.org/

The Security Technical Working Group maintains this specification.

1.5 Name and Logo Usage

The Near Field Communication Forum's policy regarding the use of the trademarks NFC Forum and the NFC Forum logo is as follows:

- Any company MAY claim compatibility with NFC Forum specifications, whether a member of the NFC Forum or not.
- Permission to use the NFC Forum logos is automatically granted to designated members only as stipulated on the most recent Membership Privileges document, during the period of time for which their membership dues are paid.
- Member's distributors and sales representatives MAY use the NFC Forum logo in promoting member's products sold under the name of the member.
- The logo SHALL be printed in black or in color as illustrated on the Logo Page that is available from the NFC Forum at the address above. The aspect ratio of the logo SHALL be maintained, but the size MAY be varied. Nothing MAY be added to or deleted from the logos.
- Since the NFC Forum name is a trademark of the Near Field Communication Forum, the following statement SHALL be included in all published literature and advertising material in which the name or logo appears:

  NFC Forum and the NFC Forum logo are trademarks of the Near Field Communication Forum.

1.6 Intellectual Property

The Signature Record Type Definition Specification conforms to the Intellectual Property guidelines specified in the NFC Forum's *Intellectual Property Rights Policy*, as outlined in the NFC Forum *Rules of Procedure*.

1.7 Special Word Usage

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.8 Acronyms and Definitions

Acronym	Definition
CA	Certificate Authority
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
NDEF	NFC Data Exchange Format
RFU	Reserved for Future Use
RSA	Rivest-Shamir-Adleman encryption algorithm (public key encryption algorithm)
RTD	Record Type Description
SHA-1	Secure Hash Algorithm, version 1
URI	Uniform Resource Identifier (e.g., http://, ftp://, mailto:, news:)
URL	Uniform Resource Locator (a special case of a URI)

2 Signature Record Overview

2.1 Introduction

The Signature record contains a digital signature related to one or more records within an NDEF message. The signature can be used to verify the integrity and authenticity of the content, i.e., the data records that have been signed.

2.2 Dependencies

There are no specific dependencies for the Signature RTD.

2.3 Security Considerations

The primary function of the signature record is to verify the integrity and authenticity of data (i.e., certain record(s) or the whole NDEF message) within an NFC Forum tag or device.

However, a malicious third party could delete the signature record from the NDEF message or attach a new signature record to prevent the user from noticing any malicious change of content. It must be understood that the verification is only as trustworthy as the tools (signature algorithm, certificate, etc.) and processes (e.g., security policies) that are being used. These risks, along with the use of the Signature record, should be taken into consideration in the development of applications.

3 Signature NDEF Structure

3.1 Messaging Sequence

There is no particular messaging sequence.

3.2 Use of RFU Fields and Values

This document defines some of the Signature and Certificate type values as Reserved for Future Use (RFU).

- An implementation of this version of the Signature RTD Specification MUST NOT send a Signature or Certificate type value defined as RFU.
- An implementation of this version of the Signature RTD Specification receiving a Signature or Certificate type value defined as RFU MUST ignore the Signature record in which the value was contained and consider the signature as invalid**.**

3.3 Records Mapping

3.3.1 Syntax

The NFC Forum Well Known Type [NDEF], [RTD] for the Signature record is "Sig" (0x53, 0x69, 0x67).

The contents of the payload of a Signature record consist of the following fields: *Version*, *Signature*, and *Certificate Chain*. The record is illustrated in Table 1.

Table 1: Signature Record

Signature Record		
Version	Signature	Certificate Chain

3.3.2 Version Field

The *Version* field, as shown in Table 2, is a 1-octet field indicating the version of this specification to which a signature is compliant.

Table 2: Signature Record Version Field

7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Version							

Because the current specification is the only version of Signature RTD, the only valid version number is 1. Devices implementing this specification to verify signatures must ignore all signature records with other version values.

Signatures created to be compliant with this specification SHALL have the Version field set to 0x01.

3.3.3 Signature Field

The *Signature* field contains either the actual signature or a reference to the location where the signature can be found. The Signature field contains up to four sub-fields and SHALL be formatted as shown in Table 3.

Table 3: Signature Field Sub-fields

Signature Field			
URI_Present	**Signature Type**	**Signature / URI Length**	**Signature / URI**
1 bit	7 bits	16 bits	*N* octets

The *URI_Present* flag SHALL be a 1-bit field indicating whether a signature or a reference to the signature is present in the record.

- If *URI_Present = 0* and *Signature_Type = 0*, then the Signature record SHALL NOT be used to verify the preceding record(s) from the beginning of the NDEF message or the previous signature record. In this case, the *Signature / URI Length* sub-field and the *Signature/URI* sub-fields SHALL NOT be present and the Certificate Chain field SHALL NOT be present. In this case, the record is used as a start marker to indicate the beginning of a collection of records to which a subsequent signature record will be applied. See Section 3.4.
- If *URI_Present* is set to 0 and the *Signature Type* is not set to 0, then the *Signature / URI* field SHALL contain the actual signature and the *Signature / URI Length* field SHALL contain a 16-bit unsigned number denoting the length, in octets, of that signature.
- If *URI_Present* is set to 1 and the *Signature Type* is not set to 0, the *Signature / URI* field SHALL contain a URI that is a reference to the signature location. The URI SHALL be in the format specified in Section 3.3.4.
- If *URI_Present* is set to 1, the *Signature Type* SHALL NOT be set to 0.

3.3.4 URI Format

The *Signature / URI* field provides the URI as per [RFC3987] (so it is actually an IRI, or Internationalized Resource Identifier, but for legacy reasons we use the term URI). This IRI can be a URL or URN. The encoding used MUST be UTF-8, unless the URI scheme specifies a particular encoding. Most modern applications support IRI.

The length is in octets, not in characters, because UTF-8 characters can occupy more than one byte.

URIs are defined only in the 7-bit US-ASCII space. Therefore, a compliant application SHOULD transform the UTF-8 IRI string to a 7-bit US-ASCII string by changing code points above 127 into the proper encoding. This coding has been defined in [RFC3987] and IDN [RFC3492]. For different schemes, the encoding might be different.

For example, if the URI contains the string “http://www.hääyö.com/”, it is transformed, as per standard IDN [RFC3492] rules, into “http://www.xn--hy-viaa5g.com” before acting on it. It is RECOMMENDED that implementations include support for IRI where display of the URI in human-readable form is anticipated.

Any character value within the URI between (and including) 0 and 31 SHALL be recorded as an error, and the URI record to be discarded. Any invalid UTF-8 sequence SHALL be considered an error, and the entire URI record SHALL be discarded.

The Signature Type SHALL be a 7-bit field indicating the type of the signature and SHALL use values defined in Table 4.

Table 4: Signature Type Values

Hex	Signature Type
0x00	No signature present
0x01	RSASSA-PSS SHA-1 [PKCS_1]
0x02	RSASSA-PKCS1-v1_5 (with SHA-1) [PKCS_1]
0x03	DSA [DSA]
0x04	ECDSA - P-192 SHA-1 [ECDSA]
0x05 – 0x7f	RFU

3.3.5 Certificate Chain Field

The Certificate Chain field contains mandatory and optional sub-fields as defined in Table 5.

Table 5: Certificate Chain Field Sub-fields

Certificate Chain Field						
URI_Present	Cert_Format	Nbr_of_Certs	Cert_Store			Cert_URI
1 bit	3 bits	4 bits	Certificate_0	…	Certificate_n	URI Field

The *URI_Present* flag SHALL be a 1-bit field indicating whether a certificate or a reference to the certificate is present in the record.

- If *URI_Present* is set to 1, the *Cert_URI* sub-field SHALL be present.
- If *URI_Present* is set to 0, the *Cert_URI* sub-field SHALL NOT be present.

The *Cert_Format* field SHALL be a 3-bit field that indicates the type of certificate present in the signature record and SHALL use one of the values defined in Table 6.

Table 6: Certificate Format Values

Hex	Certificate Format
0x00	X.509 [X_509]
0x01	X9.68 [X9_68]
0x02-0x07	RFU

The *Nbr_of_Certs* SHALL be a 4-bit integer that specifies only the number of certificate sub-fields that are present in the *Cert_Store* field and SHALL have a value in the range of 0 to 15.

- If the *Nbr_of_Certs* is greater than 0, then the first sub-field in *Cert_Store* SHALL be the signer's certificate and SHALL then be followed by zero or more certificates. Each following certificate MUST directly certify the one preceding it.

The *Cert_Store* sub-field SHALL NOT contain the top-most certificate in the certificate hierarchy (e.g., the root Certificate Authority certificate in an X.509 certificate chain).

The top-most certificate in the certificate hierarchy SHALL NOT be present in the chain referenced by the *Cert_URI* sub-field.

If present, the *Cert_URI* SHALL contain a URI that is a reference to the next certificate in the chain following the last certificate contained in the *Cert_Store*.

If a signature is given within the Signature field, either by inclusion or by reference, and the *URI_Present* and *Nbr_of_Certs* are set to 0 in the Certificate Chain field, then the identification and retrieval of the certificate chain is out of scope of this document.

Because certificate validation requires that the top-most certificate in the certificate hierarchy be distributed independently, this specification omits the top-most certificate from both the *Cert_Store* and *Cert_URI* sub-fields, under the assumption that the NFC Forum Device must already possess it in order to validate the chain.

3.3.6 Certificate Sub-field

The format for the Certificate sub-field in the *Cert_Store* field SHALL be as shown in Table 7.

Table 7: Certificate Format

Certificate	
Length, N	**Value**
16 bits	N octets

- The *Length* field SHALL be a 16-bit field that indicates the number of octets in the *Value* field.
- The *Value* field SHALL contain the certificate.

3.3.7 URI Sub-field

The format for the URI sub-field SHALL be as shown in Table 8.

Table 8: URI Sub-field Format

URI	
Length, N	**Value**
16 bits	N octets

- The *Length* field SHALL be a 16-bit field that indicates the number of octets in the *Value* field.
- The *Value* field SHALL contain a URI as defined in Section 3.3.4.

3.4 Use of the Signature Record within an NDEF Message

The Signature Record SHALL apply to all preceding records, starting either from the first record of the NDEF message or from the first record following the preceding Signature Record. The Signature Record itself is not signed.

The Signature Record SHALL apply to the Type, ID (if present), and Payload fields of all records to be signed. The first byte of the NDEF header (TNF, SR, etc.), Type Length, Payload Length, and ID Length fields SHALL NOT be included.

In the case where an application needs to sign only a selection of records within the NDEF message, an empty signature record MAY be inserted in the records to act as a start marker as illustrated in Figure 1. Also, see Section 3.3.3.

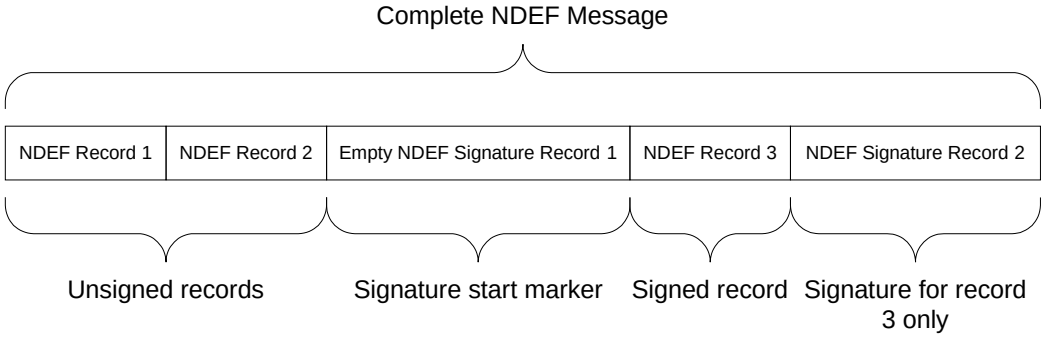

Figure 1: Example of the Use of an Empty Signature Record

When applying a signature to a record or selection of records, then the rules for concatenating NDEF records SHALL be followed, which might involve changing the state of MB, ME, SR, and length fields.

If any records included in a signature are changed or if the order of records is changed, then the signature will be affected.

3.5 Use of Signature Record with Data Other than an NDEF Message

While this specification does not preclude the use of the Signature Record outside the NDEF framework, its use in such applications is not specified in this document.

A. Examples

Figure 2 shows the format of a simple Smart Poster NDEF Message, in which the payload of the Smart Poster contains an NDEF URI message. Following the message is a Signature Record that signs the NDEF URI message. Note that typically, before the Signature Record was applied, the ME bit of the URI message would have been set to 1.

In the case where a Signature Record, along with other records, is carried in the payload of a record, such as shown in the Smart Poster example below, then the parent record (the Smart Poster) header, etc., is not included in the signature.

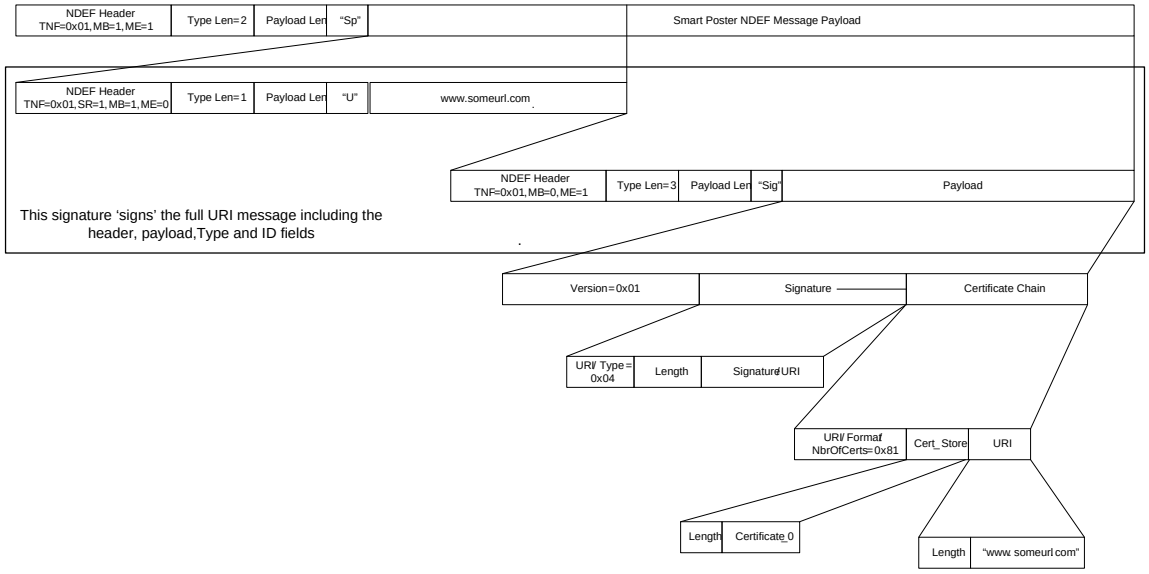

Figure 2: Simple Signed Smart Poster

The signature record contains a type 4 signature (ECDSA - P-192 SHA-1) and a type 0 (X.509) certificate chain; the certificate chain includes a URI.

Figure 3 shows the format of a Smart Poster NDEF Message, in which the payload of the Smart Poster contains a NDEF Text message ("Hello world") and a URI to a website. Following the Text message is a Signature Record that signs the NDEF Text message only, and following the URI record is a signature that signs only the URI record.

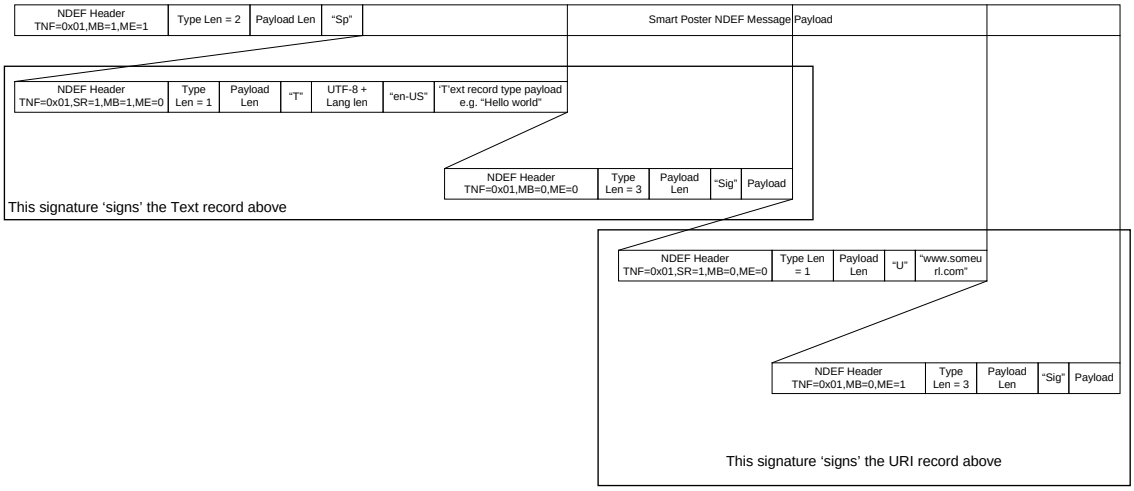

Figure 3: Smart Poster with Individual Signatures

Figure 4 shows the format of a NDEF Message in which there is an NDEF Text Message ("Hello world") and a URI to a website before a signature is applied.

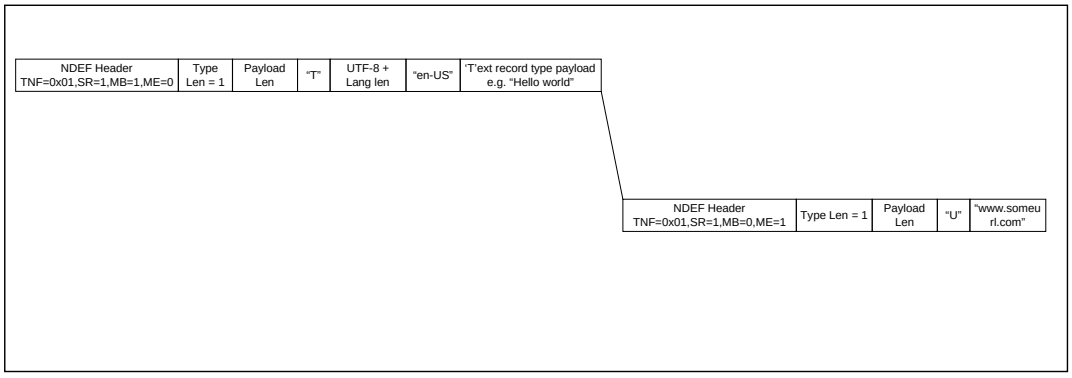

Figure 4: Unsigned Record Example

Figure 5 shows the same NDEF Message, but with a signature following the URI message that signs both the NDEF Text message and the URI record.

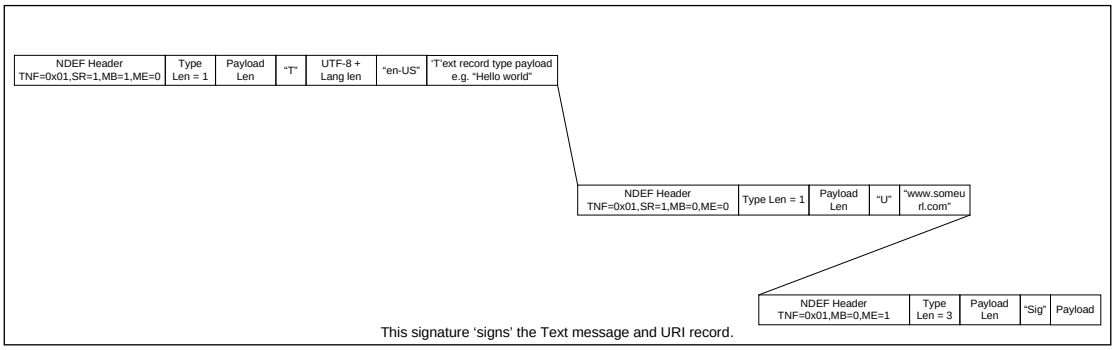

Figure 5: Signed Record Example

B. Revision History

The following table outlines the revision history of Signature Record Type Definition.

Table 9: Revision History

Document Name	Revision and Release Date	Status	Change Notice	Supersedes
Signature Record Type Definition	Version 1.0, November 2010	Final		