Workgroup: Network Working Group
Internet-Draft: draft-ietf-lamps-5g-nftypes-03
Published: 26 September 2022
Intended Status: Standards Track
Expires: 30 March 2023
Authors: R. Housley
Vigil Security
S. Turner
sn3rd
J. P. Mattsson
Ericsson
D. Migault
Ericsson

X.509 Certificate Extension for 5G Network Function Types

Abstract

This document specifies the certificate extension for including Network Function Types (NFTypes) for the 5G System in X.509v3 public key certificates as profiled in RFC 5280.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 30 March 2023.

Table of Contents

1. Introduction

The 3rd Generation Partnership Project (3GPP) has specified several Network Functions (NFs) as part of the service-based architecture within the 5G System. The 49 NF types that are defined for 3GPP Release 17 listed in Table 6.1.6.3.3-1 of [TS29.510], and each NF type is identified by a short ASCII string.

Operators of 5G systems make use of an internal PKI to identify interface instances in the NFs in a 5G system. X.509v3 public key certificates [RFC5280] are used, and the primary function of a certificate is to bind a public key to the identity of an entity that holds the corresponding private key, known as the certificate subject. The certificate subject and the subjectAltName certificate extension can be used to support identity-based access control decisions.

This document specifies the NFTypes certificate extension, which provides a list of NF Types associated with the certificate subject. The NFTypes certificate extension can be used to support role-based access control decisions. The NFTypes certificate extension can be used by operators of 5G systems or later.

The certificate extension supports many different forms of role-based access control as the various types of NF are trusted to perform their activities in the overall system. An activity might include the implementation of filtering policies. Another activity might provide an access controlled resource. These example illustrate differing levels of confidence that are needed in the proper assignment of the NFType in the overall security of the 5G system.

2. Terminology

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Certificate Subject Identification

The Network Domain Security (NDS) Authentication Framework (AF) for 3GPP Release 17 [TS33.310] provides several patterns for certificate subject names. For example, the certificate subject name for an NF instance follows one of these patterns:

(c=<country>), o=<Organization Name>, cn=<Some distinguishing name>

cn=<hostname>, (ou=<servers>), dc=<domain>, dc=<domain>

When either pattern is used, the cn= portion is a DirectoryString; however, Section 4.1.2.6 of [RFC5280], limits the character set to either PrintableString or UTF8String. Note that the PrintableString has a much more limited set of characters that can be represented.

When the first pattern is used, the o= portion of the name contains the home domain as specified in [TS23.003] to identify the public land mobile network, and it takes the following form:

5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

where MNC designates the Mobile Network Code, and MCC designates the Mobile Country Code.

The certificates are expected to include the SubjectAltName certificate extension that contains a fully qualified domain name (FQDN), where the FQDN designates the NF as defined in [TS23.003]. For example, the SubjectAltName certificate extension for an NF instance implementing the AMF might include these FQDNs:

amf1.cluster1.net2.amf.5gc.mnc012.mcc345.3gppnetwork.org

amf1.callback.cluster1.net2.amf.5gc.mnc012.mcc345.3gppnetwork.org

The certificates for entities that can act as TLS clients or servers are also expected to include a uniformResourceIdentifier in the SubjectAltName certificate extension that contains the NF Instance ID as specified in Clause 5.3.2 of [TS29.571]. For example, the SubjectAltName certificate extension for an NF Instance ID might be:

urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6

Following these patterns facilitates the use of the certificate subject and the subjectAltName certificate extension to support identity-based access control decisions.

When the second pattern is used, the dc= portion of the name contains a single domain component. For example, hostname.example.net would appear in the certificate subject as:

```
cn=hostname, dc=example, dc=net
```

4. Network Functions Certificate Extension

This section specifies the NFTypes certificate extension, which provides a list of NF Types associated with the certificate subject.

The NFTypes certificate extension **MAY** be included in public key certificates [RFC5280]. The NFTypes extension **MUST** be identified by the following object identifier:

```
id-pe-nftypes  OBJECT IDENTIFIER  ::=
   { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) id-pe(1) TBD1 }
```

This extension **MUST NOT** be marked critical.

The NFTypes extension **MUST** have the following syntax:

```
NFTypes ::= SEQUENCE SIZE (1..MAX) OF NFType

NFType ::= IA5String (SIZE (1..32))
```

The NFTypes **MUST** contain only the ASCII strings.

The NFTypes **MUST** contain at least one NFType.

The NFTypes **MUST NOT** contain the same NFType more than once.

Each NFType **MUST** contain at least one ASCII character, and each NFType **MUST NOT** contain more than 32 ASCII characters.

The NFType is of type IA5String to permit inclusion of the character underscore character ('_'), which is not part of the PrintableString character set.

5. ASN.1 Module

This section provides an ASN.1 module [X.680] for the NFTypes certificate extension, and it follows the conventions established in [RFC5912] and [RFC6268].

```
<CODE BEGINS>
  NFTypeCertExtn
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-nftype(TBD2) }

  DEFINITIONS IMPLICIT TAGS ::=
  BEGIN

  IMPORTS
    EXTENSION
    FROM PKIX-CommonTypes-2009  -- RFC 5912
      { iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) id-mod(0)
        id-mod-pkixCommon-02(57) } ;


  -- NFTypes Certificate Extension

  ext-NFType EXTENSION ::= {
    SYNTAX NFTypes
    IDENTIFIED BY id-pe-nftype }

  -- NFTypes Certificate Extension OID

  id-pe-nftype  OBJECT IDENTIFIER  ::=
     { iso(1) identified-organization(3) dod(6) internet(1)
       security(5) mechanisms(5) pkix(7) id-pe(1) TBD1 }

  -- NFTypes Certificate Extension Syntax

  NFTypes ::= SEQUENCE SIZE (1..MAX) OF NFType

  NFType ::= IA5String (SIZE (1..32))

  END

<CODE ENDS>
```

6. Security Considerations

The Security Considerations of [RFC5280] are applicable to this document.

The ASCII strings that specify the NF Types are not standard; an operator **MAY** build its own NF Type. Since the NF Type is used for role-based access control decisions, the operator that specifies

their own ASCII string for an NF Type **MUST** ensure that the new NF Type does not match an existing one.

The NFType can be used for various purposes. For example, access to a particular resource might only be provided to a subset of NFTypes. In another example, the NFTypes might be an input to a filtering decision. These different uses of the NFType values have different requirements on the level of trust in the NFType values carried in the certificate extension. Granting access to a resource based on the NFType in the certificate extension requires a great deal of confidence that the NFType is set properly. On the other hand, filtering decisions primarily address misconfiguration, and they require less confidence. As a result, different trust models might apply to the NFTypes certificate extension.

7. Privacy Considerations

In some security protocols, such as TLS 1.2 [RFC5246], certificates are exchanged in the clear. In other security protocols, such as TLS 1.3 [RFC8446], the certificates are encrypted. The inclusion of NFType certificate extension can help an observer determine which systems are of most interest based on the plaintext certificate transmission.

8. IANA Considerations

For the NFType certificate extension in Section 4, IANA is requested to assign an object identifier (OID) for the certificate extension. The OID for the certificate extension should be allocated in the "SMI Security for PKIX Certificate Extension" registry (1.3.6.1.5.5.7.1).

For the ASN.1 Module in Section 5, IANA is requested to assign an object identifier (OID) for the module identifier. The OID for the module should be allocated in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0).

9. Acknowledgements

Many thanks to Ben Smeets and Michael Li for their review and comments.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[TS29.510] 3rd Generation Partnership Project, "5G System; Network Function Repository Services; Stage 3 (Release 17)", 3GPP TS:29.510 V17.5.0 , March 2022, <https://www.3gpp.org/ftp/Specs/archive/29_series/29.510/29510-h50.zip>.

[TS33.310] 3rd Generation Partnership Project, "Network Domain Security (NDS); Authentication Framework (AF) (Release 17)", 3GPP TS:33.310 V17.2.0 , March 2022, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.310/33310-h20.zip>.

[X.680] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.680>.

10.2. Informative References

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <https://www.rfc-editor.org/info/rfc5912>.

[RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", RFC 6268, DOI

10.17487/RFC6268, July 2011, <https://www.rfc-editor.org/info/rfc6268>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[TS23.003] 3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (Release 17)", 3GPP TS:23.003 V17.5.0 , March 2022, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.003/23003-h50.zip>.

[TS29.571] 3rd Generation Partnership Project, "5G System; Common Data Types for Service Based Interfaces; Stage 3 (Release 17)", 3GPP TS:29.571 V17.5.0 , March 2022, <https://www.3gpp.org/ftp/Specs/archive/29_series/29.571/29571-h50.zip>.

Appendix A. Appendix A. NFType Strings

Each NFType is identified by an ASCII string. Table 6.1.6.3.3-1 of [TS29.510] defines the ASCII strings for the NF Types specified in 3GPP documents, which are listed below in alphabetical order. This list is not exhaustive.

"5G_DDNMF"	"ICSCF"	"SCEF"
"5G_EIR"	"IMS_AS"	"SCP"
"AANF"	"LMF"	"SCSAS"
"ADRF"	"MB-SMF"	"SCSCF"
"AF"	"MB-UPF"	"SEPP"
"AMF"	"MFAF"	"SMF"
"AUSF"	"MME"	"SMSF"
"BSF"	"N3IWF"	"SOR_AF"
"CBCF"	"NEF"	"SPAF"
"CEF"	"NRF"	"TSCTSF"
"CHF"	"NSACF"	"UCMF"
"DCCF"	"NSSAAF"	"UDM"
"DRA"	"NSSF"	"UDR"
"EASDF"	"NSWOF"	"UDSF"
"GBA_BSF"	"NWDAF"	"UPF"
"GMLC"	"PCF"	
"HSS"	"PCSCF"	

Authors' Addresses

Russ Housley
Vigil Security, LLC
Herndon, VA,

United States of America

Email: housley@vigilsec.com

Sean Turner
sn3rd
Washington, DC,
United States of America

Email: sean@sn3rd.com

John Preuß Mattsson
Ericsson
Kista
Sweden

Email: john.mattsson@ericsson.com

Daniel Migault
Ericsson
Saint Laurent, QC
Canada

Email: daniel.migault@ericsson.com