Internet Engineering Task Force (IETF)
Request for Comments: 9310
Category: Standards Track
ISSN: 2070-1721

R. Housley
Vigil Security
S. Turner
sn3rd
J. Preuß Mattsson
D. Migault
Ericsson

January 2023

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.509 v3 public key certificates as profiled in RFC 5280.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9310.

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. There are 56 NF Types defined for 3GPP Release 17; they are 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.509 v3 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 to support role-based access control decisions by providing a list of NF Types associated with the certificate subject. The NFTypes certificate extension can be used by operators of 5G Systems or later.

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. Network Function Types 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 certificate extension MUST be identified by the following object identifier:

```
id-pe-nftype  OBJECT IDENTIFIER ::=
   { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) id-pe(1) 34 }
```

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 at least one NFType.

Each NFType MUST contain only an ASCII string; however, the string MUST NOT include control characters (values 0 through 31), the space character (value 32), or the delete character (value 127).

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

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

If the NFTypes contain more than one NFType, the NFTypes MUST appear in ascending lexicographic order using the ASCII values.

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

4. 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(106) }

  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) 34 }
```

```
  -- NFTypes Certificate Extension Syntax

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

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

  END
<CODE ENDS>
```

5. Security Considerations

The security considerations of [RFC5280] are applicable to this document.

Some of the ASCII strings that specify the NF Types are standard. See Appendix A for values defined in 3GPP Release 17. Additionally, an operator MAY assign its own NF Types for use in their own network. Since the NF Type is used for role-based access control decisions, an operator-assigned NF Type MUST NOT overlap with a value already defined in the commonly defined set. Use of the same ASCII string by two different operators for different roles could lead to confusion or incorrect access control decisions. The mechanism for an operator to determine whether an ASCII string associated with a NF Type is unique across operators is outside the scope of this document.

The certificate extension supports many different forms of role-based access control to support the diversity of activities that NFs are trusted to perform in the overall system. Different levels of confidence that the NFTypes were properly assigned might be needed to contribute to the overall security of the 5G System. For example, more confidence might be needed to make access control decisions related to a scarce resource than implementation of filtering policies. As a result, different operators might have different trust models for the NFTypes certificate extension.

6. 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 the NFTypes certificate extension can help an observer determine which systems are of most interest based on the plaintext certificate transmission.

7. IANA Considerations

For the NFTypes certificate extension defined in Section 3, IANA has assigned an object identifier (OID) for the certificate extension. The OID for the certificate extension has been allocated in the "SMI Security for PKIX Certificate Extension" registry (1.3.6.1.5.5.7.1).

For the ASN.1 Module defined in Section 4, IANA has assigned an OID for the module identifier. The OID for the module has been allocated in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0).

8. References

8.1. 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, "Technical Specification Group Core Network and Terminals; 5G System; Network Function Repository Services; Stage 3 (Release 17)", 3GPP TS:29.510 V17.8.0, December 2022, <https://www.3gpp.org/ftp/Specs/archive/29_series/29.510/29510-h80.zip>.

[TS33.310] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF) (Release 17)", 3GPP TS:33.310 V17.5.0, December 2022, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.310/33310-h50.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>.

8.2. 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>.

[TS29.571] 3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; 5G System; Common Data Types for Service Based Interfaces; Stage 3 (Release 17)", 3GPP TS:29.571 V17.8.0, December 2022, <https://www.3gpp.org/ftp/Specs/archive/29_series/29.571/29571-h80.zip>.

Appendix A. NFType Strings

Table 6.1.6.3.3-1 of [TS29.510] defines the ASCII strings for the NF Types specified in 3GPP documents; these enumeration values in 3GPP Release 17 are listed below in ascending lexicographic order. This list is not exhaustive.

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

Appendix B. Example Certificate Containing a NFTypes Extension

The example certificate conforms to the certificate profile in Table 6.1.3c.3-1 of [TS33.310]. In addition, the NFTypes certificate is included with only one NFType, and it is "AMF". The SubjectAltName certificate extension contains a fully qualified domain name (FQDN) and a uniformResourceIdentifier, which carries the NF Instance ID as specified in Clause 5.3.2 of [TS29.571].

-----BEGIN CERTIFICATE-----
MIIC0DCCAlagAwIBAgIUDD5o44zEdfSghT2hMK+P/EjGHlowCgYIKoZIzj0EAwMw
FTETMBEGA1UECgwKRXhhbXBsZSBDQTAeFw0yMjExMjkxODE0NThaFw0yMzExMjkx
ODE0NThaMDkxCzAJBgNVBAYTAlVTMSowKAYDVQQKEyE1Z2MubW5jNDAwLm1jYzMx
MS4zZ3BwbmV0d29yay5vcmcwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAATJ6IFHI683
q/JJjsJUfEiRFqGQ6uKDGJ0oqDP6wEhRAuvyEyz5pgRmz/7Mze1+s1qcnPU9mo1v
rIW9rjKhb/Hm8H9TPvnMQwCRCtKvCD90MkWvc/G8qyCBpCms3zNOJOijggFBMIIB
PTATBggrBgEFBQcBIgQHMAUWA0FNRjAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMDAw
DgYDVR0PAQH/BAQDAgeAMBMGA1UdJQQMMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBRM

```
Z5KgwYlYn885mKID55ZcEznIBzAfBgNVHSMEGDAWgBSIf6IE6QtqjXR2+p/xCtRh
4PqzNTAxBgNVHR8EKjAoMCagJKAihiBodHRwOi8vZXhhbXBsZS5jb20vZXhhbXBs
ZWNhLmNybDB1BgNVHREBAf8EazBpgjhhbWYxLmNsdXN0ZXIxLm5ldDIuYW1mLjVn
Yy5tbmM0MDAubWNjMzExLjNncHBuZXR3b3JrLm9yZ4YtdXJuOnV1aWQ6ZjgxZDRm
YWUtN2RlYy0xMWQwLWE3NjUtMDBhMGM5MWU2YmY2MAoGCCqGSM49BAMDA2gAMGUC
MEtQEut9kelkiMIMR+QzkSNGIuR30Lr23ftarLi9wMp3ZRIJYQgaAWc6gmf3MVAp
7QIxAKMoYAtw5srkNjE+Zg6CqEkf9f2banFltRuPbTp4B0Xraz5z/jn3NDPM9ata
SHUxOQ==
-----END CERTIFICATE-----

The following shows the example certificate.  The values on the left
are the ASN.1 tag (in hexadecimal) and the length (in decimal).

30 720: SEQUENCE {
30 598:  SEQUENCE {
A0   3:   [0] {
02   1:    INTEGER 2
       :     }
02  20:   INTEGER
       :    0C 3E 68 E3 8C C4 75 F4 A0 85 3D A1 30 AF 8F FC
       :    48 C6 1E 5A
30  10:   SEQUENCE {
06   8:    OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
       :     }
30  21:   SEQUENCE {
31  19:    SET {
30  17:     SEQUENCE {
06   3:      OBJECT IDENTIFIER organizationName (2 5 4 10)
0C  10:      UTF8String 'Example CA'
       :       }
       :      }
       :     }
30  30:   SEQUENCE {
17  13:    UTCTime 29/11/2022 18:14:58 GMT
17  13:    UTCTime 29/11/2023 18:14:58 GMT
       :     }
30  57:   SEQUENCE {
31  11:    SET {
30   9:     SEQUENCE {
06   3:      OBJECT IDENTIFIER countryName (2 5 4 6)
13   2:      PrintableString 'US'
       :       }
       :      }
31  42:    SET {
30  40:     SEQUENCE {
06   3:      OBJECT IDENTIFIER organizationName (2 5 4 10)
13  33:      PrintableString '5gc.mnc400.mcc311.3gppnetwork.org'
       :       }
       :      }
       :     }
30 118:   SEQUENCE {
30  16:    SEQUENCE {
06   7:     OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
06   5:     OBJECT IDENTIFIER secp384r1 (1 3 132 0 34)
       :      }
03  98:    BIT STRING
```

```
      :     04 C9 E8 81 47 23 AF 37 AB F2 49 8E C2 54 7C 48
      :     91 16 A1 90 EA E2 83 18 9D 28 A8 33 FA C0 48 51
      :     02 EB F2 13 2C F9 A6 04 66 CF FE CC CD ED 7E B3
      :     5A 9C 9C F5 3D 9A 8D 6F AC 85 BD AE 32 A1 6F F1
      :     E6 F0 7F 53 3E F9 CC 43 00 91 0A D2 AF 08 3F 74
      :     32 45 AF 73 F1 BC AB 20 81 A4 29 AC DF 33 4E 24
      :     E8
      :     }
A3 321:   [3] {
30 317:    SEQUENCE {
30  19:     SEQUENCE {
06   8:      OBJECT IDENTIFIER nfTypes (1 3 6 1 5 5 7 1 34)
04   7:      OCTET STRING, encapsulates {
30   5:       SEQUENCE {
16   3:        IA5String 'AMF'
      :        }
      :       }
      :      }
30  23:     SEQUENCE {
06   3:      OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
04  16:      OCTET STRING, encapsulates {
30  14:       SEQUENCE {
30  12:        SEQUENCE {
06  10:         OBJECT IDENTIFIER '2 16 840 1 101 3 2 1 48 48'
      :        }
      :       }
      :      }
      :     }
30  14:     SEQUENCE {
06   3:      OBJECT IDENTIFIER keyUsage (2 5 29 15)
01   1:      BOOLEAN TRUE
04   4:      OCTET STRING, encapsulates {
03   2:       BIT STRING 7 unused bits
      :        '1'B (bit 0)
      :       }
      :      }
30  19:     SEQUENCE {
06   3:      OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
04  12:      OCTET STRING, encapsulates {
30  10:       SEQUENCE {
06   8:        OBJECT IDENTIFIER clientAuth (1 3 6 1 5 5 7 3 2)
      :        }
      :       }
      :      }
30  29:     SEQUENCE {
06   3:      OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
04  22:      OCTET STRING, encapsulates {
04  20:       OCTET STRING
      :        4C 67 92 A0 C1 89 58 9F CF 39 98 A2 03 E7 96 5C
      :        13 39 C8 07
      :       }
      :      }
30  31:     SEQUENCE {
06   3:      OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
04  24:      OCTET STRING, encapsulates {
30  22:       SEQUENCE {
```

```
   80  20:         [0]
         :         88 7F A2 04 E9 0B 6A 8D 74 76 FA 9F F1 0A D4 61
         :         E0 FA B3 35
         :          }
         :         }
         :        }
   30  49:      SEQUENCE {
   06   3:       OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
   04  42:       OCTET STRING, encapsulates {
   30  40:        SEQUENCE {
   30  38:         SEQUENCE {
   A0  36:          [0] {
   A0  34:           [0] {
   86  32:            [6] 'http://example.com/exampleca.crl'
         :             }
         :            }
         :           }
         :          }
         :         }
         :        }
   30 117:      SEQUENCE {
   06   3:       OBJECT IDENTIFIER subjectAltName (2 5 29 17)
   01   1:       BOOLEAN TRUE
   04 107:       OCTET STRING, encapsulates {
   30 105:        SEQUENCE {
   82  56:         [2]
         :          'amf1.cluster1.net2.amf.5gc.mnc400.mcc311.3gppnet'
         :          'work.org'
   86  45:         [6]
         :          'urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6'
         :          }
         :         }
         :        }
         :       }
         :      }
         :     }
   30  10:   SEQUENCE {
   06   8:    OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
         :    }
   03 104:   BIT STRING, encapsulates {
   30 101:    SEQUENCE {
   02  48:     INTEGER
         :      4B 50 12 EB 7D 91 E9 64 88 C2 0C 47 E4 33 91 23
         :      46 22 E4 77 D0 BA F6 DD FB 5A AC B8 BD C0 CA 77
         :      65 12 09 61 08 1A 01 67 3A 82 67 F7 31 50 29 ED
   02  49:     INTEGER
         :      00 A3 28 60 0B 70 E6 CA E4 36 31 3E 66 0E 82 A8
         :      49 1F F5 FD 9B 6A 71 65 B5 1B 8F 6D 3A 78 07 45
         :      EB 6B 3E 73 FE 39 F7 34 33 CC F5 AB 5A 48 75 31
         :      39
         :     }
         :    }
         :   }
```

Acknowledgements

Many thanks to Ben Smeets, Michael Li, Tim Hollebeek, Roman Danyliw, Bernie Volz, and Éric Vyncke for their review, comments, and assistance.

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