RFC 9310
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.

Copyright Notice
Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.
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


8.2. Informative References


Appendix A. NFType Strings

Table 6.1.6.3-1 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.
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 NType, 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-----
MIIC0DCCAlagAwIBAgIUDD5o44zEdfSghT2hHMk+P/EjGHlowCgYIKoZIzj0EAwMwFTEMTBEGAIUEglwXbZBSBDQTAFw3yMjxExMjxOED0NThaMdxCzAJBgNVYATAIyVTMSo kwAARQkVEA1Z2w5ubW5jNDAwLm1jYzMxM5s423bwv8029yay5sucmcdjAQBgckhjjoPQI8BqUrQQAiGhAT6IF1683q/1JjsUFeIRqQ5WWhjKqipB6EhRauvEyzSo5pRm/7Mze1s1qcnPu9mo1vriWwrjxKhb/Hm8H9TPv MachinesMQwCRCtvKvDC9h0东路wv/G8qybCpCms3ZkN0J1iCjFgBMIIBFTABg3rEgbF8c8b1gQMAUAWE8F3rNkAJXbgNHVSAEDAOMwGCMcGSAF1wIBMawDgYDVQR8PAQ/h/BADQArqBWMGMA1d0JQQMMGQGAQUBFBwMCMB0GA1wDgQLWBRMZ5gwYx08855KD5L5ZoGz9A/f8gNHVSEMDGAWBSIf6IE6tqjXR2/p/xCtRh4PqzNTAxgNhVR8KEKjAoMcajJKAihiBo4HReWII4ez8bpjhhWYxLmNsdXN0ZXIxLm5iDGuW1MmJ1vYyy5thmM0MDubWNjMzEljNnHBuXR3b3JrLM9yZY4yTdxJuOnV1aWQ6Zjg9ZDRmYWUtN2Ry8xMWQwLW3UjUtMdBhMG5M0MW2yM2AMaOCCqGSM49AMBADA2gAGMUCMTQEut9ceik1iM3R+QrzSNGIUr38Lr23ftr19wMpz3ZRIJYQaAw6gMf3VMAp7Q1xAKMoYatw5srKnJz+Ez6CqEk9f2banFltRupBt4B0Xraz5z/jn3NDP9ata SHUQQ==
-----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).
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER 2
    }
  }
  INTEGER
    0C 3E 68 E3 8C C4 75 F4 A0 85 3D A1 30 AF 8F FC
    48 C6 1E 5A
  SEQUENCE {
    OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
  }
  SEQUENCE {
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationName (2 5 4 10)
        UTF8String 'Example CA'
      }
    }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER countryName (2 5 4 6)
        PrintableString 'US'
      }
    }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationName (2 5 4 10)
        PrintableString '5gc.mnc400.mcc311.3gppnetwork.org'
      }
    }
  }
  SEQUENCE {
    SEQUENCE {
      OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
      OBJECT IDENTIFIER secp384r1 (1 3 132 0 34)
    }
    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 C9 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
    }
  }
  [3] {
  }
  SEQUENCE {
    OBJECT IDENTIFIER nfTypes (1 3 6 1 5 5 7 1 34)
    OCTET STRING, encapsulates {
    }
  }
}
IA5String 'AMF'

OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
OCTET STRING, encapsulates
  OBJECT IDENTIFIER '2 16 840 1 101 3 2 1 48 48'

OBJECT IDENTIFIER keyUsage (2 5 29 15)
BOOLEAN TRUE
OCTET STRING, encapsulates
  BIT STRING 7 unused bits
    '1'B (bit 0)

OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
OCTET STRING, encapsulates
  OBJECT IDENTIFIER clientAuth (1 3 6 1 5 5 7 3 2)

OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
OCTET STRING, encapsulates
  OCTET STRING
    4C 67 92 A0 C1 89 58 9F CF 39 98 A2 03 E7 96 5C
    13 39 C8 07

OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
OCTET STRING, encapsulates
  OCTET STRING
    [0]
      88 7F A2 04 E9 0B 6A 8D 74 76 FA 9F F1 0A D4 61
      E8 FA B3 35
    

OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
OCTET STRING, encapsulates
  OCTET STRING
    [0]
      [0]
      

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