**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222613-r1***

**e-meeting, 10 - 14 October 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Solution to indicate and validate the purpose of the certificate**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***It is requested to approve this proposal***

# 2 References

[3] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

# 3 Rationale

This contribution provides a solution addressing the requirements of key issue #7 related to the association of multiple certificates which are used for different purposes within a single Network Function. The solution provides a proposal for the indication of the purpose(s) of the certificate in the CSR (Certificate Signing Request) to the operator CA and the validation of the purpose(s) by the entity receiving the certificate.

# 4 Detailed proposal

*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES \*\*\*\*\*\*\*\*\*\*\*\**

## 6.X Solution #X: Solution to indicate and validate the purpose of the certificate

### 6.X.1 Introduction

This solution addresses the security requirements exposed in key issue #7 related to the association of multiple certificates which are used for different purposes within a single Network Function (NF) in the 5GC SBA context, namely:

* TLS client EE certificates
* TLS server EE certificates
* Certificates for signing the access tokens for authorization (for NRFs)
* Certificates for encrypting HTTP messages between SEPPs
* Certificates for signing Client credentials assertion (CCA) tokens

NOTE: Other purposes may be added for X.509 certificates in the context of 5GC SBA.

The basic concept is to provide the purpose(s) of the certificate to be used in 5GC SBA in the CSR (Certificate Signing Request) to the Certification Authority (CA). The CA should validate the request and add the purpose(s) in the certificate, specifically in the subjectAltname field.

When the NF consumer (NFc) request a service to a NF producer (NFp), SCP or SEPP, and sends its certificate for authentication (mutual TLS authentication), or when the NFc sends a CCA token that can be checked against the certificate by the NFp among other situations, the receiver of the certificate should check whether the received purpose in the certificate matches the content of the service request. If it does not match, the receiver of the certificate should reject the request with a corresponding error code.

### 6.X.2 Solution details

The first step of the procedure for the NF is to fetch a certificate that includes the purpose(s) of usage in the context of 5GC SBA (e.g., TLS authentication, CCA signing, etc.). The purpose(s) of the certificate should be added in subjectAltname field by the CA server:

* If an automated enrolment protocol is used by the NF to fetch the certificate, the NF should indicate the purpose(s) of the certificate in the certificate request message to the CA. E.g., “ir” or “cr” messages in CMPv2.
* The OAM fetches the certificate from the CA with indicated purpose and install it manually in the NF

The solution proposes to use subjectAltname field to indicate the purpose of the certificate in a string format. For example, <PURPOSE-LIST>NF\_TLS\_CLIENT, NF\_TLS\_SERVER, ACCESSTOKEN\_SIGNING, CCA\_SIGNING</PURPOSE-LIST>.

The receiver of the certificate should validate the purpose indicated in the subjectAltname of the certificate, with the actual purpose it is being used in the service request (e.g., TLS authentication, CCA signing, etc.).

Editor’s note: subjectAltname field is provided as an example. The field to place the purpose of the certificate is ffs.

Figure 6.X.2-1 illustrates the procedure with an example that combines a successful validation of the certificate to be used for TLS mutual authentication (NFc à SCP), but it is rejected when used for CCA signing (NFc à NFp).



Figure 6.X.2-1: Validation of the purpose of the certificate

1) The CA is configured with policies intended to validate the purpose of the certificate requests from NFs.

2) The NFc sends a certificate request to the CA with PURPOSE = NF\_TLS\_CLIENT, what indicates that the NFc is requesting a certificate in principle intented to be used only for TLS client authentication purposes.

3) The CA validates the purpose of the certificate with predefined policies and adds the purpose in the certificate (subjectAltname field).

4) The CA sends the certificate with purpose information in subjectAltname field to the NFc.

5) The NFc initiates a TLS connection with SCP, which requires mutual authentication.

6) The SCP validates the TLS client authentication with the purpose of the certificate and allows the TLS connection.

7) The NFc sends a service request to NFp with CCA token. Let’s assume that NFc misuses the single purpose TLS client certificate by signing with the associated private key the CCA token.

8) The purpose of the certificate used to verify the signature of the token does not include CCA\_SIGNING, so the service request is rejected by the NFp with a new error code.

9) The NFp sends the service response rejecting the request with a new error code.

### 6.X.3 Evaluation

TBD

*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES \*\*\*\*\*\*\*\*\*\*\*\**