**3GPP TSG-SA3 Meeting #108e-Adhoc** ***S3-222614***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Solution based on OCSP Stapling addressing Key Issues #5 and #6**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

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

# 2 References

[1] RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions"

[2] RFC 6961: "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension

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

# 3 Rationale

This contribution provides a solution addressing some of the requirements of key issue #5 (related to revocation procedures) and key issue #6 (related to the relation of certificate management lifecycle and NF management lifecycle). It provides an approach to reconcile the NF lifecycle processes with the validity period of the certificates by introducing standard OCSP stapling as part of the NF profile.

# 4 Detailed proposal

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

## 6.X Solution #X: OCSP Stapling addressing Key Issues #5 and #6

### 6.X.1 Introduction

This solution addresses key issue #5 by introducing, within the context of 5GC SBA, the revocation procedures associated to standard OCSP stapling [1][2], whose profile can be found in clause 6.1b of TS 33.310 [3]. The use of the Certificate Status extension, commonly referred to as "OCSP stapling", aims to offload the consumption of client resources and the contact with the OCSP server. OCSP stapling makes the server responsible of performing OCSP requests, thus reducing the latency and increasing the availability of the revocation service, i.e., the server timestamps and caches the most recent OCSP responses, so that those can be attached (“stapled”) to the clients TLS handshakes responses together with the certificates, even during short CA and/or OCSP server outages. Every NF should get the OCSP stapling of its end entity (EE) certificate from OCSP periodically.

The solution addresses the relation of the certificate management lifecycle and NF management lifecycle described in key issue #6, specifically the reconcialitation of certain NF lifecycle proceses such as the discovery procedure performed by the NRF with the validity period of the certificates, by adding the OCSP stapling of the NF EE certificate in the NF profile. Consequently, every NF should register and update its profile with OCSP stapling of its EE certificate in the NRF. The NRF should check the NF producer’s (NFp) OCSP stapling from its profile and accordingly responds to the NF consumers discovery, access token or subscription requests by including only the NFps with valid stapling.

### 6.X.2 Solution details

Before the first registration of the NFp in the NRF, the NFp should get the OCSP stapling for its EE certificate from the OCSP server, and then embed this information as part of the NF profile registered in the NRF.

The OCSP stapling contains the validity and recovation status of the EE certificate provided by the OCSP server, despite its initial validity availed from the CA. The OCSP server will always have the latest information about the NF certificate status. The OCSP stapling of the EE certificate can be updated by the periodic requests from the NF to the OCSP server, or by preconfigured OCSP server policies. The OCSP stapling updates should trigger the corresponding update of the information in the NF profile within the NRF.

Figure 6.X.2-1 illustrates the procedure:



Figure 6.X.2-1: OCSP stapling procedure for NFp validation in NRF

1) NFp sends a OCSP stapling request for its EE certificate to OCSP server.

2) OCSP server sends the OCSP stapling response to NFp with the latest status of the EE certificate.

NOTE: Alternatively, OCSP server may push stapling updates to the NFp based on operator security policy.

3) NFp registers or updates its NF profile in the NRF including the latest status of the EE certificate.

4a) NRF register the NFp profile, which contains the OCSP stapling information, i.e., the latest status of the EE certificate.

4b) NRF validates the OCSP stapling message and updates the NF profile.

5) NFc sends a request to NRF for a NFp, e.g., discovery request, access token request, subscription request.

6a) Checks the OCSP stapling information of the candidate NFps (along with other parameters in the profile)

6b) If the status of the EE certificate is OK, the NFp is considered in the response.

7) NRF response to NFc request with a NFp whose EE certificate is valid.

If the NFp instance is removed from the insfrastructure by the corresponding management function, the NF profile is deactivated from the NRF, and the management function and/or NRF should inform the operator RA/CA to proceed with the revocation of the certificate. This procedure is left to implementation.

### 6.X.3 Evaluation

TBD

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