**3GPP TSG-SA3 Meeting #108-e *draft\_S3-222001-r1***

**e-meeting, 22 - 26 August 2022**

**Source: Ericsson**

**Title:** **Combined certificate and profile solution for NRF validation of NFc for access token requests**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***Approve the pCR to TR 33.875***

# 2 References

[1] 3GPP TR 33.875: "Study on enhanced security aspects of the 5G Service Based Architecture (SBA)"

[2] S3-221999 "Discussion regarding issues for NRF validation of NFc for access token requests", Ericsson

# 3 Rationale

Approve the following changes to TR 33.875 [1].

Additional background information is found in a discussion paper "Discussion regarding issues for NRF validation of NFc for access token requests" [2].

# 4 Detailed proposal

#### \*\*\* Start of 1st Change \*\*\*

## 6.Y Solution #Y: Combined certificate and profile solution for NRF validation of NFc for access token requests

### 6.Y.1 Introduction

This potential solution addresses the KI #11, NRF validation of NFc for access token requests. It describes what entities that need to be validated, what needs to be in place from a provisioning perspective, and finally some additional details how the validation is performed.

The basic idea of the solution is that the NRF uses the information in the NF Consumer's certificate and additional information in the NF profile as basis for its authorization decision.

### 6.Y.2 Solution details

#### 6.Y.2.1 NF consumer information to validate at Service Request Authorization

The authorization of a NF consumer needs to be performed by validating verified information about the NF consumer stored in NRF. This solution proposes that the NRF validates NF Type, NF Instance ID, PLMN-ID, and FQDN.

#### 6.Y.2.2 O&M Provisioning solution

Any Network Function is allowed to use the NF management API to register its profile at the NRF. However, it can happen that NF consumers do not use the NF management API to register their profile at the NRF. In this case, this solution proposes that the NRF is provisioned with the NF profiles for these NF consumers, containing the NF consumer information described in clause 6.Y.2.1, by an O&M provisioning operation.

The O&M provisioning operation need not to be standardized

#### 6.Y.2.3 Certificates

In this solution, the public key certificate can be the TLS certificate of the NF Consumer, if the NF Consumer itself requests the access token, or the certificate used to sign the CCA of the NF Consumer, if the SCP requests the access token on behalf of the NF Consumer.

If the TLS certificate of the NF Consumer is used, this solution requires that the NF instance ID is available in the TLS certificate, so that the certificate can be linked to the NF profile.

Having the NF instance ID present in the certificate can be reached in different ways. It could either be mandated in the specification or required to be present in deployments in order for this procedure to work. If it is not mandated that the information is present in the certificates, this may lead to interoperability problems between different vendor implementations.

#### 6.Y.2.4 NRF validation solution

The NRF checks whether the NF Service Consumer is authorized to access the requested service(s) by performing the following validation(s):

1. The NRF retrieves the available NF consumer information in the public key certificate of the NF Service Consumer.

2. The NRF uses the NF instance ID of the NF Consumer that was obtained during authentication of the NF Consumer to retrieve the NF profile.

3. The NRF uses the information about the NF Consumer obtained in steps 1 and 2 to decide whether the NF Consumer is authorized to invoke the NF Producer's service.

In deployment scenarios with only one NRF, the NRF does not use the information about the NF Consumer in the access token request to base its authorization decision on, since this information is provided by the NF Consumer itself and therefore not reliable.

In hierarchical NRF deployments, additional measures are necessary. The NRF that receives the access token request needs to verify the information about the NF Consumer in the access token request with the certificate and/or the NF profile. The NRF that issues the token can then base its authorization decision on the information about the NF Consumer in the access token request, since the NRF that received the access token request has validated the information.

### 6.Y.3 Evaluation

TBD

Editor's Note: This solution assumes that it is not clearly specified for all releases including Rel-17 which mechanism the NRF uses to validate whether the NF service consumer is authorized to receive the requested service. It is ffs whether the mechanism in this solution is needed, or whether the NRF can use the NF Service Consumer profile to validate the NF Service Consumer in the process of authorization of requested services including access token request.

\*\*\* End of 1st Change \*\*\*