**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212880-r1***

**e-meeting, 16 - 27 August 2021** Revision of S3-21xxxx

**Source: Nokia, Nokia Shanghai Bell**

**Title: Way forward eSBA**

**Document for: Endorsement**

**Agenda Item: 5.20**

# 1 Decision/action requested

**Discussion on way forward, eSBA study and normative work**

# 2 References

[1] 3GPP 33.875

# 3 Rationale

**Introduction**

The work on eSBA study was initiated to address open points after Rel-16 freezing and allow for a thorough analysis of key issues and solutions, which can lead to conscious decisions on whether security requirements need to be fulfilled and require an update of existing specification text or the addition of new features.

Several key issues and solution have been added so far. But Rel-17 is ending fast and decision on how to continue with the study need to be made.

The purpose of this discussion document is as follows:

* Identify key issues for urgent treatment in Rel-17 and establish a WID for those
* Allow for further analysis of key issues in Rel-18 and potential other eSBA aspects that need to be addressed and do not need immediate treatment or are still in a stage of analysis, i.e. continue eSBA study in Rel-18.

-r1 includes all inputs from this meeting 🡪 6 new KIs(!)

**Status of eSBA study and proposed way forward for KI resolution**

|  |  |  |  |
| --- | --- | --- | --- |
| **Key issues** | **KI/Solutions details** | **Comments**  | **Way forward** |
| #1: Authentication of NRF and NF Service Producer in indirect communication | Threat scenario: MitM cooperating with NFp2 solution candidates#1: Service response verification in indirect communication without delegated discovery (Nokia)#6: Verification of Service Response from a NF Service Producer at the expected NF Set (Samsung) | Several concerns were raised for the Nokia solution Samsung solution updates / generalizes the solution for introduction of CCA\_NFpCan we agree on intro of CCA\_NFp in normative work?HW: Ensure the authenticity of NFpNokia: thinks it is covered, whether Reselection case is important, this is achieved by including NF Set id (if also part of the certificate)MVNR: not needed, no need to carry over to rel-18 | Samsung prefers Rel-17Bo, no need to postpone, but technical problems. |
| #2: SCP security domains | Trust assumptions not yet clear, list of ENs to be resolved in KINo solution so far | Solution pending | Postpone analysis to Rel-18, also depending on trust assumptions |
| #3: Service access authorization in the “Subscribe-Notify” scenarios | No requirement yetNo solution so far accepted in TR, but several proposals under discussion (but not yet included in TR) Threat – URI not authorized  | KI clarifications & solution pendingNokia: Despite KI clarifications and solution pending, it is suggested to address this KI in Rel-17, since the threat of URI being not authorized should be addressed.MVNR prefers to finalize either way in Rel-17, no carry over |  |
| #4: Authorization of SCP to act on behalf of an NF or another SCP | Threat: SCP acting without authorization and thus, compromising a NFc2 solution candidates#2: Authorization between NFs and SCP (Nokia)#3: Using existing procedures for authorization of SCP to act on behalf of an NF Consumer (Ericsson) | KI & solutions availableNokia: Important to address this KI, since otherwise SCP could be malicious and act on behalf of NFcs that have not requested an access token or service. Resolve in Rel-17.Existing mechanisms are not sufficient. Propose to conclude with sol. #2ERI prefers #3Discussion on whether authentication between NF and SCP is sufficient as authorization of SCP to act on behalf of NFc (ERI/MVNR say yes)Nokia: maybe okay in service mesh, but in SCP standalone case not true |  |
| #5: End-to-end integrity protection of HTTP messages | #4: Service request authenticity verification in indirect communication#5: End-to-end integrity protection of HTTP body and methodNew proposed in this meeting:LS reply by CT4: S3-212418S3-212928 - Integrity protection of HTTP message in consideration of update by SCP | 2 solution candidatesPending CT4 responseNeed to address backwards compatibility with Rel-16 MVNR: Stop this KIDCM: In general, it should be SA3 to decide on, not CT  | Propose to postpone to Rel-18 ORLS response from CT4 to discourage ie. it suggests to stop this activityAny views? |
| #6: Access token usage by all NFs of an NF set | #7: Access token request for NF Set | Existing concept, for which the access token usage has not been clarified | Propose to address in Rel-17 |
| **Tdocs / KIs brought up for this meeting** |
| **Key issues** | **KI/Solutions details** | **Comments** | **Way forward** |
| NEW #C**[S3-212879](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_104e/Docs/S3-212879.zip) (Nokia)**vNRF – hNRF mutual authentication in service access authorization | KI was proposed in last meeting, here updated and resubmitted by Nokia in this meetinghow to ensure the trust in the information provided by the vNRF to the hNRF during the access token get request | Pending acceptance of KI/solvNRF hNRF mutual authentication is not possible via SEPP, clarification is needed if trust via SEPP can be achieved better | Rel-17? |
| Also roamingNEW #B ???**[S3-212651](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_104e/Docs/S3-212651.zip)** (HW)New Key issue on authorization mechanism negotiation | KI / solution (2652) proposedProposal: HPLMN decides on authorization method. if the Final authorization mechanism indicates static authorization, then the NFc could use the static authorization to access the NFp service. If the Final authorization mechanism indicates OAuth authorization, then the NFc could get the token from the NRF before consuming the service from the NFp.NFc could get the token from the NRF before consuming the service from the NFp . | Nokia comment: Static authorization as described in 33.501 is based on local authorization policy at the NRF and the NF Service Producer if token-based authorization is not used within one PLMN from 13.3.0:“During the Nnrf\_NFDiscovery procedure, the NRF ensures that the NF Service Consumer is authorized to discover the NF Service Producer service(s)” 🡪 i.e. without presenting an OAuth tokenIsn’t this against the concept of 5G SBA in core? | ?? KI/Sol suggest usage of non-roaming concept in roaming ??? |
| NEW #Y: Proposal for KI on NRF deployment / handling S3-212878 (Nokia) | KI / solution presented in this meeting Deployment options for NRFs:- one NRF can serve the entire PLMN- one NRF can serve a set of network slices- one NRF can serve a single network slice- several NRFs can be deployed in a PLMN, optionally using a hierarchical structure • Proposal to add in TS 33.501 clarification text for NF Service Consumer behaviour along the lines*The NF Service Consumer may have discovered a specific NRF in advance, e.g. a slice specific NRF, and can send its request directly to that NRF.* *If the NF Service Consumer requests an NRF, where the NF Service Producer is not registered (see NRF deployment options in 13.4.1.1.1a), the requested NRF needs to redirect/forward the service request to that NRF.*• Proposal to add in TS 33.501 clarification text for local NRF deployments along the lines*NOTE: In a local NRF deployment, the NF Service Producer only gets the certificate of the local NRF. Thus, the local NRF would need to check if the NF Service Consumer is authorized and the NRF where the NF Service Producer is registered would need to trust the NRF which has verified the NF Service Consumer.* | Pending acceptance of KI/sol There is an ambiguous understanding among companies about hierarchical deployments / client registration & token issuing instances | Clarification needed in Rel-17, because NRF deployments in intra-PLMN need to be addressed.  |
| Earlier discussed KI, not yet agreed:**[S3-212641](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_104e/Docs/S3-212641.zip)** (HW)New KI #Z: NF Domain granularity authorization | resubmission Issue: An attacker may control an NF Service Consumer to request a token using the real FQDN of the NF Service Consumer.EG. A stateless UDM sends its FQDN as the callbackReference URI to UDR for subscribe to the notifications. If the UDM as Consumer sends a tamper FQDN in the subscription request to the UDR, and the UDR doesn’t check the authentic of the FQDN, the UDR may response the notification to the malicious FQDN, resulting sensitive information leaked to unauthorized NFs. | Pending acceptance of KI/solMerge with 2890? | Rel 17? |
| NEW #W:**[S3-212890](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_104e/Docs/S3-212890.zip) (Nokia)**KI and Solution for verification of NFc by NF producers | New KI/sol proposal Threat: If the requester fqdn/domain in the service request is tampered, the NF Service Producer can return a service response or a service notification to the malicious FQDN, resulting sensitive information leaked to unauthorized NFs.Sol: The NF Service Consumer adds fqdn or domain in the CCA. This guarantees that the consumer fqdn/domain is not manipulated while “travelling” to the NF Service Producer. | Pending acceptance of KI/sol Same threat as above??? Merge with 2641? | Rel17? |
| NEW KI: #AProposed in this meeting**[S3-212519](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_104e/Docs/S3-212519.zip)** (CableLabs)Authorization of IPX by PLMN in indirect roaming | New KI/sol proposalProposes: Authorization of IPX to represent PLMN in indirect roaming Proposed requirement:The 5GS should provide a mechanism for a PLMN to verify that an IPX has been authorized by another PLMN as its roaming proxy.  | Pending acceptance of KI/solNokia comment: Usage of indirect comm term is different than in SBA/SCP.If iPX is used, each PLMN has a dedicated contract with an IPX, one per other PLMN. This is the reason for having only 2 IPX in the PRINS protocol that can modify (on for outgoing PLMN, one for incoming PLMN), all other IPX on the route would just proxy the traffic. | IPX has not been in focus of 3GPP. Guidance for this provided in GSMA?? |
| KI NEW #VS3-212916 (Samsung)Authorization for Inter-Slice Access | New KI/solution proposalsIssue: NSSAI is neither a part of the certificate profile of NF Service Consumer, nor can it be assured that the NRF receiving the access token request contains the profile of the NF Service Consumer from which the request is received.S3-212917 - New Solution to KI #X: Authorization for Inter-Slice Access Solution proposed:The 5GS should provide a mechanism that allows NRF validate the S-NSSAIs of the NF-Service Producer that an NF-Service-Consumer is allowed to access.Using individual or combination of IEs like allowedNfTypes and allowedNssais, NRF can already filter the requests from NF Service Consumers not allowed to access any services of an NF Service Producer.Additionally, to allow NF Service Producers (themselves) validate the “Inter-Slice” access requests from the NF Service consumers, it is proposed to include “Requester-NSSAI” in the access-grant, indicating the NRF validated NF-Consumer’s S-NSSAIs. | Pending acceptance of KI/sol | Opinions? which release to address? |

**Proposed way forward**

* eSBA WID for key issues

OPEN DISCUSSION / Initial proposal

* + #3: Service access authorization in the “Subscribe-Notify” scenarios
	+ #4: Authorization of SCP to act on behalf of an NF or another SCP
	+ #6: Access token usage by all NFs of an NF set
	+ NEW#C: vNRF – hNRF mutual authentication in service access authorization
	+ NEW#Y: Proposal for KI on NRF deployment / handling
* eSBA SID continuation for Rel-18 to allow for further analysis and providing a proper finalization of the study.

# 4 Proposal

It is proposed to follow the way forward for eSBA SID and eSABA WID as discussed in the Rational.