Enhancement of Network Slicing Phase 2 (eNS_Ph2) – Rel-17

George Foti

Handling for some outstanding issues

Agend

- EAC flag, Suppression Flag.
- Support for NSCAF Instances
- Distributed Architecture

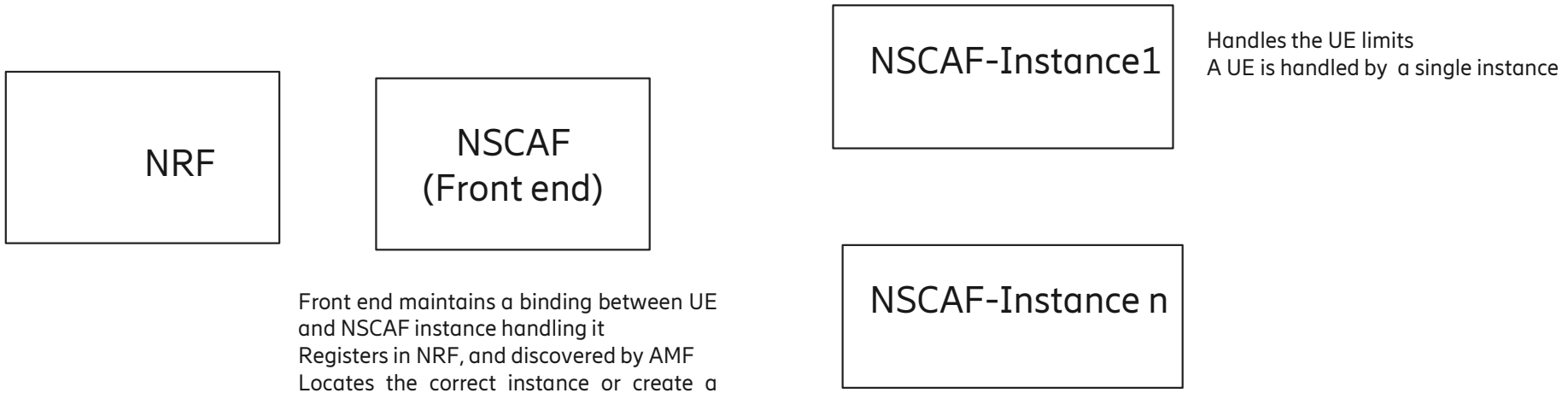
KI #1 : Number of Registered UEs - EAC Flag, Suppression Flag

- For EAC, there are 2 proposals; none of them are acceptable to all companies:
  - Currently in the TS but is incomplete: Implement a SUB/NOT framework in NSACF.
    - To complete this requires broadcasting the EAC flag to all AMFs since the NSCAF does not which AMF supports the S-NSSAI
    - This defeats the original intent of the EAC flag to reduce signaling.
  - Ericsson solution : piggyback the EAC flag status for all Slices supported by AMF in every Registration response. Technically sound solution.
    - Objection was that it is a UE operation, which is rather artificial reason.

  Way Forward: A completely new Approach to be proposed next meeting using existing NRF NSCAF discovery procedure:
    - The NSACF to register in its profile the EAC flag status. This enables an AMF to acquire the info. Any time it changes.
    - Minimize impacts to NSACF and AMF, eliminates the need for the SUB/NOT framework solution in the NSCAF, and fulfill the requirements in a generic way.
- Support for signalling suppression in case of S-NSSAI congestion. No proposal in the TS.
    - Proposal: The NSACF to register in its profile suppression flag which can be enabled and disabled on demand. This enables an AMF to be notified and act accordingly.
  - This proposal solves 2 outstanding issues in a unified , consistent fashion with existing procedures.

KI#1, KI#2: Support for NSCAF Instances

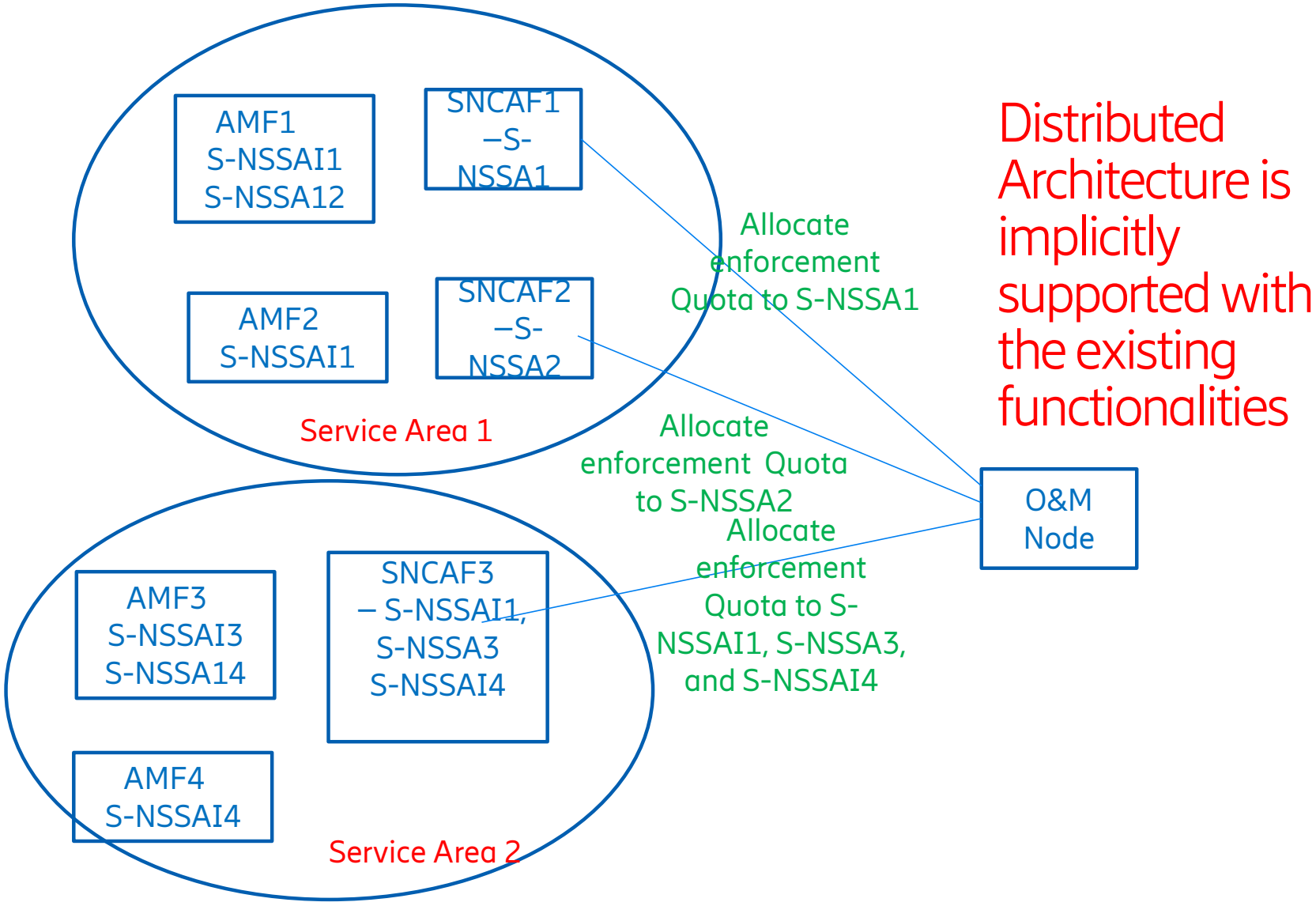
- Even though a service area can have one AMF which reduces scalability to a non-issue, there is some call for support of NSCAF Instances. This will require passing the NSCAF instance during AMF Mobility as well as storing the instance used by an AMF per UE.
- The current proposal provides a simple way to support NSCAF instances optionally and transparently to AMFs.



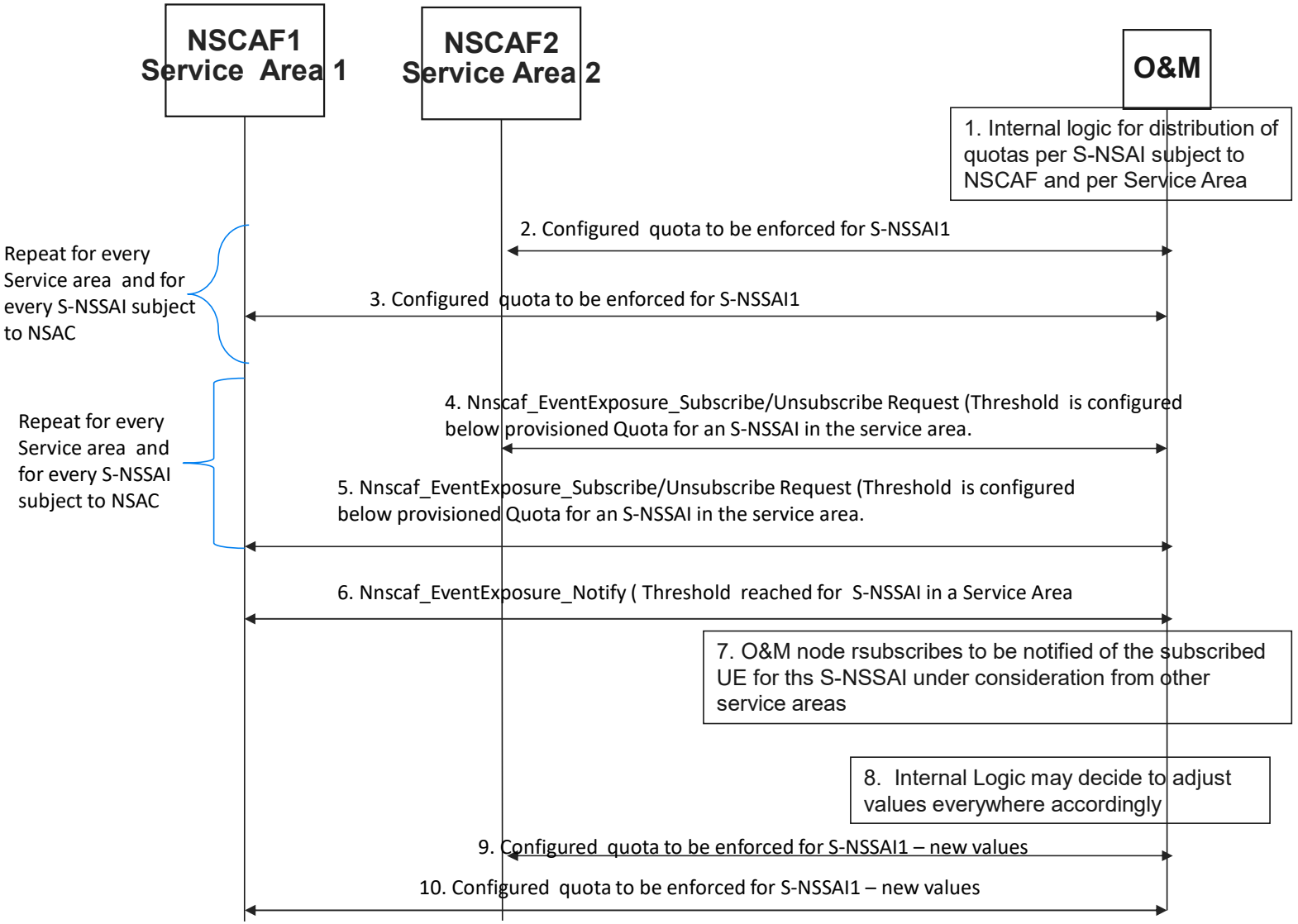
KI#1, KI#2: Support for NSCAF Instances - Summary

AMF discovers a NSCAF front-end and it can allocate instances per UE and store that association.

- This limits impacts to NSACF that would like to support instances.
- The actual verification is done in the NSACF instances.
- The front end NSCAF acts s a proxy while maintaining association between a UE and the NSCAF instance handling it
- Completely transparent to the AMF.
- Works as well in inter-AMF mobility cases.
- Provides all needed scalability to eliminate the need for an S-NSSAI to ne handled by more than a single NSCAF (instance).



Distributed Architecture is implicitly supported with the existing functionalities


NSCAF1
Service Area 1
NSCAF2
Service Area 2
O&M
1. Internal logic for distribution of quotas per S-NSAI subject to NSCAF and per Service Area
2. Configured quota to be enforced for S-NSSAI1
Repeat for every Service area and for every S-NSSAI subject to NSAC
3. Configured quota to be enforced for S-NSSAI1
Repeat for every Service area and for every S-NSSAI subject to NSAC
4. Nnscaf_EventExposure_Subscribe/Unsubscribe Request (Threshold is configured below provisioned Quota for an S-NSSAI in the service area.
5. Nnscaf_EventExposure_Subscribe/Unsubscribe Request (Threshold is configured below provisioned Quota for an S-NSSAI in the service area.
6. Nnscaf_EventExposure_Notify (Threshold reached for S-NSSAI in a Service Area
7. O&M node rsubscribes to be notified of the subscribed UE for ths S-NSSAI under consideration from other service areas
8. Internal Logic may decide to adjust values everywhere accordingly
9. Configured quota to be enforced for S-NSSAI1 – new values
10. Configured quota to be enforced for S-NSSAI1 – new values