**3GPP TSG-SA3 Meeting #108e *draft\_S3-221852-r3***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Key issue 2 update with solution and conclusion on trust domain**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

*The intention of the key issue was to introduce a trust domain as a superset of several SCP domain operated under the same trust assumption. The KI is updated accordingly.*

# 4 Detailed proposal

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[3] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2".

[4] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[5] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3"

[6] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3"

[7] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 3".

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE*

5.2 Key issue #2: Need for additional security at operational level among SCP domains

5.2.1 Key issue details

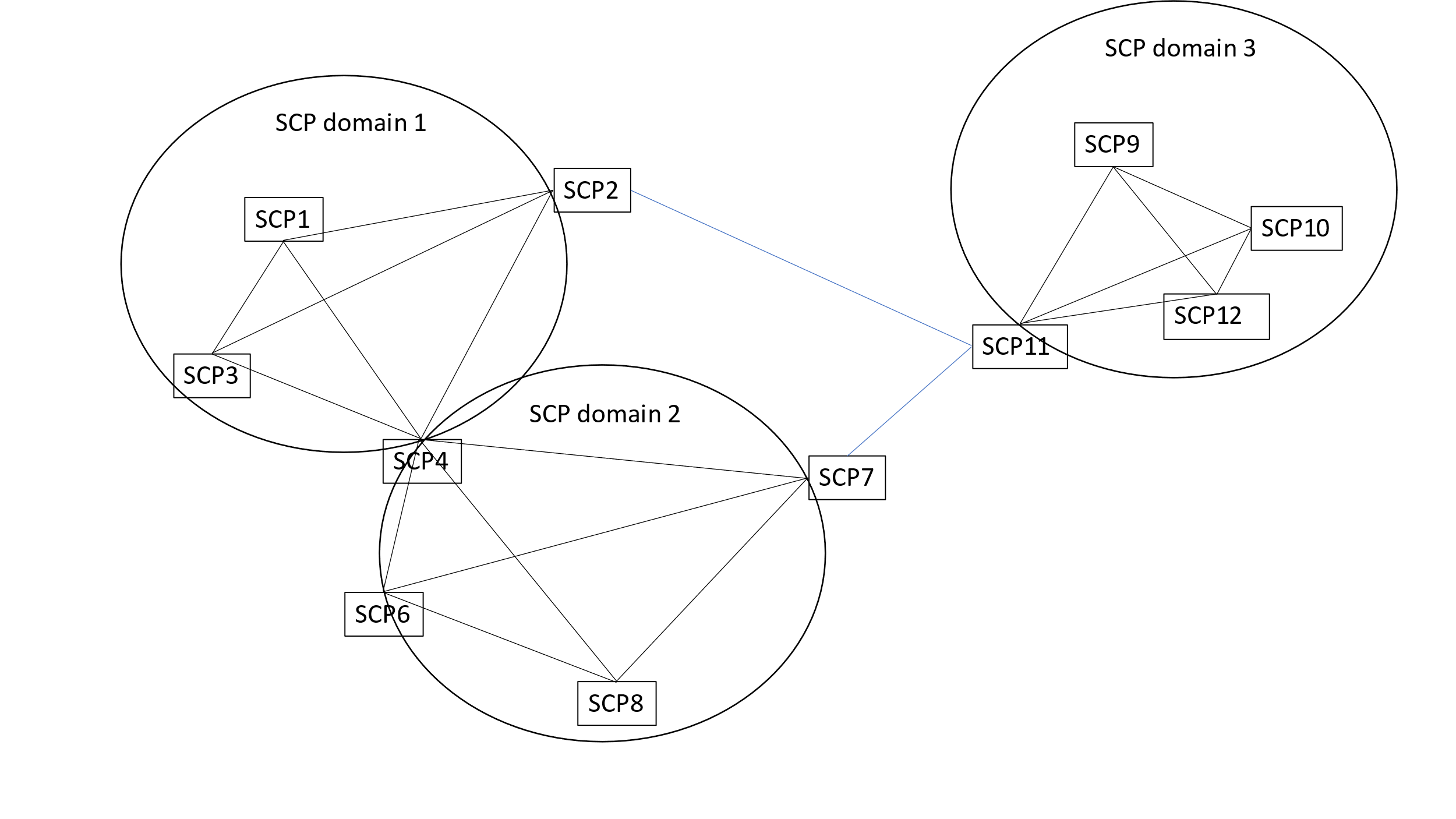
TS 23.501 [3] addresses the aspects of handling multiple SCPs in indirect communication without and with delegated discovery. With Rel-16 a SCP domain is introduced, which comprises a configured group of one or multiple SCPs that can reach certain NF instances or SCPs directly.

SCPs can register a SCP profile in NRF. 3GPP TS 23.502 [7] describes in the SCP profile SCP domain registration details about interconnected SCPs and also identifies SCPs that interconnect domains. Table 6.1.6.2.2-1 of 3GPP TS 29.510 [6] provides a detailed decription. SCPs need to request NRF to discover the next hop SCP to route a service request from the NF Service Consumer to a NF Service Producer via multiple SCPs.

The primary purpose of SCP domains is to describe the connectivity topology within a network. All SCPs within an SCP domain can directly interconnect. One SCP can be part of multiple SCP domains. In fact, the primary purpose of intermediate SCPs in the path is to interconnect SCP domains, thus, there are boundaries between SCP domains at each SCP in the path.

PLMN-wide trust between NFs and SCPs is an option, but more restrictions could be desirable in complex networks with SCP domains, e.g., if SCPs are operated in different regions/provinces, the domain concept could be used for establishing operational restrictions by defining SCP domains. Or, there can be several technical SCP domains within a PLMN, where equipment with different capabilities is deployed and signalling also varies in some respects, e.g., if equipment upgrade is performed in a stepwise manner. Such technical domains can be defined based on computer centre boundaries, based on operators of subnetworks, based on regions/provinces, etc.

The figure below gives an idea of structuring or grouping a PLMN in several SCP domains, possibly interconnecting with other SCP domains via dedicated SCPs.



**Figure 5.2.1-1: Illustration of SCP domains connecting via dedicated SCPs**

This key issue is to study the concept of one or several SCP domains becoming regions of trust of finer granularity than PLMN and whether there is a necessity of trust and policing of communication within or among such domains, i.e., for the case that request messages traverse a boundary between trust domains.

5.2.2 Security threats

In large PLMNs operated by different organizations in different regions/provinces or by slices operated by a tenant, PLMN wide trust between NFs and SCPs could result in messages traversing over several SCP domain boundaries, even though this is not wanted. It could be not possible to shield, e.g., regions or organizations against each other, resulting in availability of information to unauthorized parts of the network.

If an access token has been requested by one SCP on behalf of the NF Service Consumer and granted by NRF, it is not guaranteed that the same SCP is forwarding the service request to the NF Service Producer. Instead, the SCP could forward the service request including the access token to another SCP first. If the new SCP is not be part of the same SCP domain, the trust in this SCP could be less than in SCPs within the same SCP domain.

5.2.3 Potential security requirements

N/A.

NOTE: If it is decided to further develop the solutions of this key issue, potential security requirements can be discussed.

5.2.4 Potential architectural/operational security requirements

The 5G system shall allow restricting network topology so that requests between certain NFs or SCPs or SCP domains are not allowed.

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE*

*\*\*\*\* under 6. Potential Solutions*

6.X SCP trust domain or technical domain grouping

### 6.Y.1 Introduction

This solution is addressing key issue #2. It provides an optimization for SCP domain operation in trusted environments.

### 6.Y.2 Solution details

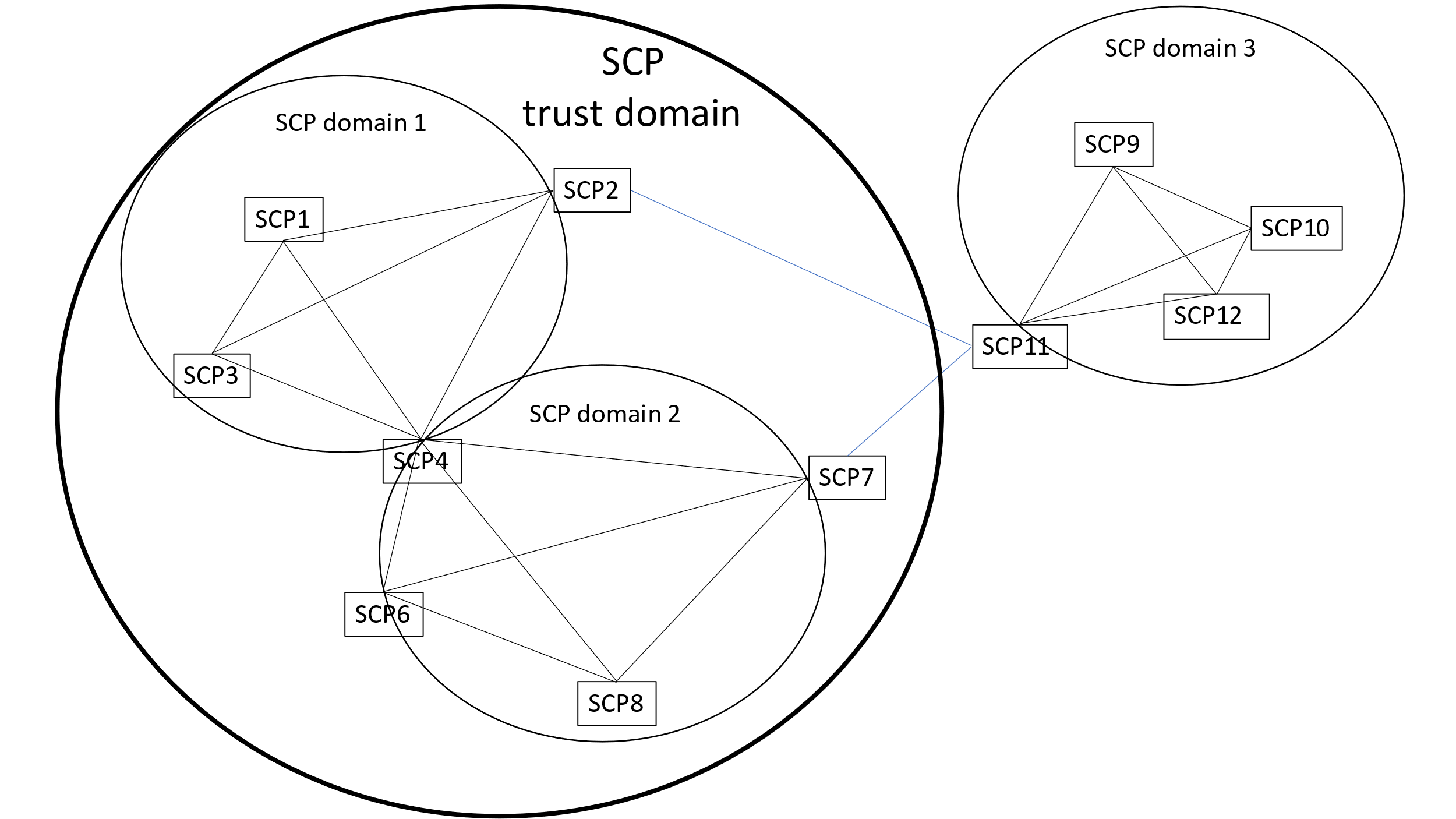
According to 23.502 [7], SCP domains can be registered at the NRF. A NF Service Producer can register within its profile its SCP domain.

A SCP domain is called trusted if it is a group or subset of available SCPs within one PLMN that includes several SCPs operated in the same trust environment according to a security policy. Such technical SCP trust domains can be defined in large PLMNs, for example, based on computer centre boundaries, operators of subnetworks, regions/provinces, etc.

SCP trust domains could also be formed equipment-specific or release-specific. Large operators could have involved different organizations to operate the complete network and hence, structure their regional availability by SCP domains, where additional security means between these organizations could be needed for achieving trust.

For a SCP trust domain, one or several SCP domains can be grouped, i.e., a SCP trust domain is a superset of a distinct set of SCP domains. A SCP trust domain could be isolated from other SCP domains. It could be registered or configured together with a set of policies at NRF.

If the SCP is part of several SCP domains, all SCP domains have to be part of the same SCP trust domain as illustrated in the figure below.



**Figure 6.X-1: Illustration of SCP trust domain**

SCPs can discover boundaries of trust or technical domains based on

* the SCP domain, from which a request is received from and is forwarded to, and
* the configured knowledge of the relationship of trust or technical domains and SCP domains.

Policies for a SCP trust domain could include information such as which domain can communicate with which domain or whether NFs from one SCP trust domain can access NFs of another SCP trust domain.

The policies are related to restriction in the communication between trust domains that the SCP enforces, as outlined in the examples below.

Some examples of policies for a SCP trust domain are as follows:

- Only SCPs from a particular (usually the same) SCP trust domain would be allowed to discover the NF Service Producer.

- An access token could be provided for all NFs of the same SCP trust domain.

- A service is provided only for NFs of a distinct NF Type within a specific SCP trust domain.

- The SCP domain of NF Service Consumer and SCP are the same as of the NF Service Producer.

- Access to certain services is not permitted over trust domain boundaries.

If the SCP discovers that a request message traverses a boundary between trust/technical domain, it can perform also policing on traffic between SCP trust domains, for example:

- Checking target URIs

- Checking delegated discovery parameters

- Checking routing binding indications

- Checking whether a request contains a CCA

The following are examples of using SCP trust domains:

- The access from NF or SCP to the SCPs of a SCP trust domain can be limited to this domain only. Hence, all SCPs forming a trust domain could be allowed to communicate with NRF and with NF Service Producers on behalf of a NF Service Consumer from the same trust domain. By this, SCPs forwarding a request to another SCP, e.g., for load balancing, have a mean to check whether the forwarding SCP is a member of the same SCP trust domain.

- If a policy for SCP trust domain is registered and the NF profile includes SCP trust domain information in the NRF, the NRF can authorize or reject a discovery request from NF or SCP based on whether the expected NF Service Producer or another SCP instance is part of the same SCP trust domain as the NF Service Consumer.

- If a NF Service Consumer has included in its request a target SCP trust domain, the NRF can provide an access token that provides authorization for all NFs within this domain.

- If the NF Service Producer receives a service request, it could provide the service only, when contacted by an SCP of the trust domain indicated in the access token (e.g., AMF getting a token from NRF granting access to any SMF in the same SCP domain).

- If domain information of the NF Service Consumer is included in the token, it enables the NF Service Producer or SCP to verify whether the requesting NF Service Consumer is part of the same SCP trust domain.

SCPs of a trust domain connecting to another SCP domain outside the trust domain shall provide confidentiality, integrity and replay protection.

### 6.Y.3 Evaluation

The solution addresses SCP domains in particular. Trust domains do not need to be necessarily identical to SCP domains. Restricting network topology so that requests between certain elelments are not allowed could be generalized as provided by the potential security requirement in clause 5.2.3.

Further evaluation is needed for deciding on the usefulness of the concept in general, such as addressing the moving of UEs between regions with different trust requirements.

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE*

*\*\*\*\* under 7. Conclusions*

## 7.2 KI#2: Need for additional security at operational level among SCP domains

### 7.2.1 Analysis

The key issue provides for operational aspects of SCP domains. Usually within an SCP domain, trust is assumed. If several SCP domains form a wider SCP trust domain, additional means for securing such trust domain against other SCP domains could be considered. However, further elaboratation would be needed, whether such operational concept is useful.

### 7.2.2 Conclusion

The topic is not followed up normatively.

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