**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222616-r2***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Proposal to complement KI#3 NF Certificate Update**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

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

# 2 References

# 3 Rationale

This contribution proposes to complement the scope of the KI#3 related to NF Certificate Update procedure by adding the use case / scenario where massive number of certificates required to be updated / renewed simultenaously (e.g., due to a compromise of a certain used crypto algorithm), leading to a potential service unavailability. The intention is to study potential approaches in the certificate management framework for 5GC which prevent unexpected overload situations in this security procedure of Certificate Update.

# 4 Detailed proposal

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

## 5.3 Key Issue #3: NF Certificate Update

### 5.3.1 Key issue details

NF certificate update is a necessary part of an automated certificate management mechanism because the long validity period certificate is considered not secure. Therefore, it is important that each certificate is set with an appropriate period of validity. Furthermore, it is necessary to update the NF certificate when the certificate is about to expire or has expired. Otherwise, NF communication can be disrupted in the middle of operation due to an unhandled certificate expiry.

If a vast number of NF instances and services simultenously require certificate updates, for example due to same expiration date, or a common CA certificate revocation, or the compromise of a crypto algorithm in use among other causes, the automated certificate management framework may trigger the certificate update procedure for all affected end entities at the same time. If there are no mechanisms to manage this situation, it can bring congestion and/or overload in the automated certificate management framework, leading to temporary service unavailability.

### 5.3.2 Security threats

If the NF certificate is not updated, or the certificate update procedure is not secured, the following problems can occur:

* An attacker misuses the update mechanism to get hold of valid certificates from CA and mount impersonation attacks.

In some implementations the simultaneous update / renewal of a vast number of certificates may lead to partial or complete disruption of the automated certificate management framework.

### 5.3.3 Potential security requirements

5GS should support to update the NF certificate securely.

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