**3GPP TSG-SA3 Meeting #107-e *S3-220644-r1***

**e-meeting, 16 - 20 May 2022**

**Source: Deutsche Telekom, Lenovo**

**Title: New KI on Post-Quantum Secure Subscription Concealed Identifier**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***SA3 is kindly requested to approve the proposed changes to TR 33.870.***

# 2 References

[1] 3GPP TR33.870, Study on privacy of identifiers over radio access

[2] S3-220601, DP on Post-Quantum Secure Subscription Concealed Identifier

# 3 Rationale

This contribution adds a new KI to TR 33.870 section 5 Key issues

.

# 4 Detailed proposal

\*\*\* BEGIN OF 1st CHANGE \*\*\*

## 5.X Key issue #X: Post-Quantum Secure Subscription Concealed Identifier

### 5.X.1 Key issue details

This key issue covers both aspects of SUCI protection, resistance against quantum computing and forward secrecy.

In current 3GPP standards, the security of the public-key cryptography, that underpins the SUCI, relies on the hardness of the discrete logarithm problem. Using Shor’s algorithm, a quantum adversary could break the SUCI’s cryptography and once more gain the capability to track and identify users. Advancements in quantum computing are unpredictable, and a breakthrough might be only a decade away.

Given the lifetimes of cellular network deployments, it is thus necessary to already integrate now quantum-resistant cryptography into the current generation of cellular networks.

Additionally, the quantum threat is further aggravated by the design of the SUPI protection schemes. The current SUPI protection schemes do not provide forward secrecy. As a result, breaking an operator’s public key is sufficient to de-anonymize all SUPIs encrypted with that public key, without needing to solve additional discrete logarithm problems. More specifically, the current protection schemes derive the shared secret 𝑘 using a long-term public key instead of using an ephemeral public key also on the operator’s side. As a result, the protocol does not provide forward secrecy, and one invocation of Shor’s algorithm is sufficient to de-anonymize many (recorded) SUCIs. Consequently, an adversary can invest large resources into recording SUCIs now and breaking just a small number of operator public keys (and thus de-anonymize all collected SUCIs) later on.

Therefore, this key issue is about investigating if and how a modification of the existing SUPI protection schemes is needed so that the risk caused by quantum adversaries could be further minimized.

### 5.X.2 Threats

Lack of SUPI protection schemes that provide forward secrecy and are able to resist quantum computing could potentially have following impact:

- Enable to track and identify users

- Enable for large-scale de-anonymization attack(s). Such an attack can retroactively de-anonymize and track users with packets captured today.

Such a large-scale de-anonymization attack would proceed as follows:

1. Given an operator’s public key 𝐻𝐴 = 𝑑𝐴 · 𝑃 and the curve’s base point 𝑃, an adversary equipped with a quantum computer can simply solve the discrete logarithm problem to obtain the operator’s private key 𝑑𝐴. Note that this only needs to be done once.
2. Once an attacker obtained the operator's private key, the adversary can deanonymize any subscriber for whom he captured a packet containing a subscriber’s ephemeral public key 𝐻𝐵 = 𝑑𝐵 · 𝑃 and the SUPI encrypted using the broken public key 𝐻𝐴. Such a packet is transferred over radio when registering to the network, for example. This packet is sufficient to de-anonymize the subscriber. Given the captured packet, the adversary can follow the decryption steps at the home network side to obtain a user’s SUPI. The only confidential information required to decrypt the SUCI is the respective home operator’s private key, which the attacker obtained in step (1).

### 5.X.3 Potential security requirements

The 5G system’s SUPI protection schemes should have support for privacy protection against the risk caused by quantum adversaries.

The 5G system’s SUPI protection schemes should provide means to ensure forward secrecy.

\*\*\* END OF 1nd CHANGE \*\*\*