**3GPP TSG-SA3 Meeting #124** **S3-253759-r4**

**Merger of S3-253555, S3-253597, S3-253309**

**Wuhan, China, 13-17 October**

**Source: China Telecom, Nokia, Ericsson**

**Title:** **New KI on open discover service API**

**Document for: Approval**

**Agenda Item: 5.2.10**

# 1 Decision/action requested

***It is proposed to approve this pCR about New KI on open discover service API.***

# 2 References

[1] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

# 3 Rationale

It is proposed to approve this pCR about New KI on open discover service API.

# 4 Detailed proposal

\* \* \* First Change \* \* \* \*

# 5 Key issues

## 5.X Key issue #X: Security for open discover service API

### 5.X.1 Key issue details

As specified in TS 23.222[x], the requestor which doesn’t register to the CAPIF can discover service API from CCF. There is an EN:

NOTE: The security aspects of this procedure are unspecified in this release of the specification.

The existing security mechanism specified in TS 33.122[x] does not discuss the security aspects of the new feature of open discover service API, which may cause information leakage. This key issue aims to address the security aspects of open discover service API.

### 5.X.2 Threats

Without proper protection mechanism, the API invoker may obtain sensitive service API information beyond its permission.

An attacker impersonating the CCF can send wrong information to the Requestor about the service APIs.

An attacker between the CCF and the Requestor can access to the information about the service APIs.

An attacker between the CCF and the Requestor can modify the information about the service APIs.

An attacker between the CCF and the Requestor can replay the outdated information about the service APIs.

### 5.X.3 Potential security requirements

CAPIF should support authentication of CCF by the requestor.

CAPIF should support authorization for the requestor not recognized by CAPIF to discover sensitive API information through service API from CCF.

CAPIF should support confidentiality, integrity protection, and replay protection for the secure communication between the CCF and the Requestor.

Editor’s note: The interface between Requestor and CCF will be described by SA6 and the potential security impacts are FFS.

\* \* \* End of Change \* \* \* \*