This document is the initial baseline text of the draft Recommendation Q.CCONS “Signalling requirements and protocol for confidential computing orchestration of network slices in IMT-2020 networks and beyond” in Q6/11 meeting (Geneva, 1-10 May 2024).

This document is based on this meeting’s discussion and results on the following contribution:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Title</th>
<th>Discussion and results</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG11-C464R1</td>
<td>China Unicom, China Telecommunications Corporation, China Mobile Communications Co. Ltd.</td>
<td>Proposal to start a new work item - Q.CCONS “signalling requirements and protocol for confidential computing orchestration of network slices in IMT-2020 networks and beyond”</td>
<td>Accepted with modifications</td>
</tr>
</tbody>
</table>
Signalling requirements and protocol for confidential computing orchestration of network slices in IMT-2020 networks and beyond

Summary
This recommendation aims to specify the signalling requirements and protocol for confidential computing orchestration of network slices in IMT-2020 networks and beyond, which includes the signalling requirements, protocol procedures and message format.

Keywords
Confidential computing, orchestration, signalling requirements, protocol, network slice
# Table of Contents

1. Scope ................................................................................................................................. 4

2. References ........................................................................................................................... 4

3. Definitions ........................................................................................................................... 4

4. Abbreviations and acronyms .............................................................................................. 5

5. Conventions ........................................................................................................................ 5

6. Overview ............................................................................................................................. 6

7. Signalling requirements ....................................................................................................... 7

8. Protocol procedures ............................................................................................................ 7

9. Message format .................................................................................................................... 7

10. Security considerations ..................................................................................................... 7

Bibliography................................................................................................................................ 7

Annex xx A.1 justification for proposed draft new Recommendation Q.CCONS ................. Error! Bookmark not defined.
Signalling requirements and protocol for confidential computing orchestration of network slices in IMT-2020 networks and beyond

1. Scope

This Recommendation aims to specify the signalling requirements and protocol for confidential computing orchestration of network slices in IMT-2020 networks and beyond.

The scope of this Recommendation is as follows:

- Overview;
- Signalling requirements;
- Protocol procedures and message format;
- Security considerations.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.


TBD

3. Definitions

3.1 Terms defined elsewhere

3.1.1 network slice [b-ITU-T Y.3100]: A logical network that provides specific network capabilities and network characteristics.
3.1.2 network slice instance [b-ITU-T Y.3100]: An instance of network slice, which is created based on a network slice blueprint.

3.1.3 orchestration [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructures by optimization criteria.

3.1.4 Confidential computing [b-ITU-T F.751.9]: technology that realizes data operation on the premise of protecting the confidentiality and integrity of sensitive information.

3.1.5 Trusted execution environment [b-ITU-T F.751.9]: A secure area that ensures sensitive data is stored, processed and protected in an isolated and trusted environment.

3.2 Terms defined in this Recommendation
This Recommendation defines the following terms:
TBD

4. Abbreviations and acronyms
This Recommendation uses the following abbreviations and acronyms:

CC Confidential Computing
IMT-2020 International Mobile Telecommunications-2020
TEE Trusted Execution Environment
NSI Network Slice Instance

TBD

5. Conventions
In this Recommendation:
The keywords “is required to” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.
The keywords “is prohibited from” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.
The keywords “is recommended” indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.
The keywords “can optionally” indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor’s implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.
6. Overview

Figure 6-1 demonstrates the architecture of network slice orchestration supporting confidential computing, which aligns with the functional architecture of network slice management and orchestration [ITU-T Y.3153] and the high-level architecture of IMT-2020 network management and orchestration [ITU-T Y.3111]. The architecture consists of the functional blocks described in [ITU-T Y.3153][ITU-T Y.3150], and confidential computing remote attestation function which manages the remote attestation of the hardware-based TEE in the confidential computing orchestration. To support the hardware TEE based confidential computing resource orchestration, the enhanced capabilities are required to improve the functional architecture of network slice orchestration, such as the cross domain slice M&O function, the single domain M&O, the element management function and NFVO. The architecture focuses on the network slice instance level orchestration of the confidential computing resource. The resource orchestration in single domain is out of the scope of this Recommendation.

NOTE 1-In Figure 6-1 the confidential computing remote attestation function is shown as a separate function in the slice management and orchestration domain. However, it is a logical function that could be integrated with the single domain M&O.

The I1-I4 are logical interfaces enhanced based on the reference point Si and Ie defined in [ITU-T Y.3111], while I5-I6 are new interfaces for the verifying the TEE instances based on the remote attestation reports.

Figure 6-1. Architecture of orchestration supporting confidential computing for network slices
7. Signalling requirements

Editor’s Note: This section describes the signalling requirements of the interface II-I6.

7.1 Signalling requirements for Interface I1

7.2 Signalling requirements for Interface I2

7.3 Signalling requirements for Interface I3

7.4 Signalling requirements for Interface I4

7.5 Signalling requirements for Interface I5

7.6 Signalling requirements for Interface I6

8. Protocol procedures

Editor’s Note: This section describes the signalling protocol procedures of confidential computing orchestration of network slices in IMT-2020 networks and beyond.

9. Message format

Editor’s Note: This section describes the message format of the interfaces.

10. Security considerations

Editor’s Note: This section provides the security considerations of the signalling and protocol of the confidential computing orchestration of network slices in IMT-2020 networks and beyond.

Bibliography

[b-ITU-T F.751.9] Draft Recommendation F.751.9 (2023), Trusted execution environment based confidential computing on distributed ledger technology system


[b-ITU-T F.748.13] Recommendation F.748.13 (2021), *Technical framework for a shared machine learning system*