

Draft new Recommendation ITU-T Y.CCO-req

Requirements of orchestration supporting confidential computing for network slices in IMT-2020 networks and beyond

Table of Contents

1.	Scope	2
2.	References.....	2
3.	Definitions.....	3
	3.1 Terms defined elsewhere	3
	3.2 Terms defined in this Recommendation.....	3
4.	Abbreviations and acronyms	3
5.	Conventions.....	4
6.	Overview.....	4
	6.1 Background and motivation.....	4
7.	Requirements of orchestration supporting confidential computing for network slices	5
8.	Architecture of orchestration supporting confidential computing for network slices	5
9.	Reference points of orchestration supporting confidential computing for network slices	6
10.	Procedures of orchestration supporting confidential computing for network slices	6
	10.1 Procedure of hardware based TEE property registration	6
	10.2 Procedure of confidential computing environment remote attestation	6
11.	Security considerations	6
	Appendix I Use cases of orchestration supporting confidential computing	6
	I.1 Use case template	6
	Bibliography.....	6

Draft new Recommendation ITU-T Y.CCO-req

Requirements of orchestration supporting confidential computing for network slices in IMT-2020 networks and beyond

1. Scope

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

The scope of the new work item is as follow:

- Requirements of orchestration supporting confidential computing for network slices in IMT-2020 networks and beyond;
- Architecture of orchestration supporting confidential computing for network slices in IMT-2020 networks and beyond.
- Reference points and procedures of orchestration supporting confidential computing for network slices in IMT-2020 networks and beyond.

Editor's Note: The security requirement regarding the hardware-based TEE and confidential computing themselves is out of the scope of the recommendation.

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.

- | | |
|----------------|--|
| [ITU-T Y.3010] | Recommendation ITU-T Y.3110(2017), <i>IMT-2020 network management and orchestration requirements</i> |
| [ITU-T Y.3011] | Recommendation ITU-T Y.3011 (2017), <i>Framework of network virtualization for future networks.</i> |
| [ITU-T Y.3111] | Recommendation ITU-T Y.3111 (2017), <i>IMT-2020 network management and orchestration framework</i> |
| [ITU-T Y.3154] | Recommendation ITU-T Y.3154(2020), <i>Resource pooling for scalable network slice service management and orchestration in the IMT-2020 network</i> |
| [ITU-T Y.3157] | Recommendation ITU-T Y.3157(2021), <i>IMT-2020 network slice configuration</i> |

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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Confidential computing: TBD

Note1-[b-ITU-T H.DLT.TEE] technology that realizes data operation on the premise of protecting the confidentiality and integrity of sensitive information.

3.2.2 Trusted execution environment: TBD

Note1-[b-ITU-T H.DLT.TEE] A secure area that ensures sensitive data is stored, processed and protected in an isolated and trusted environment.

Note2-[b-IETF TEEP Arc]-Trusted Execution Environment (TEE): An execution environment that enforces that only authorized code can execute within the TEE, and data used by that code cannot be read or tampered with by code outside the TEE. A TEE also generally has a device unique credential that cannot be cloned. There are multiple technologies that can be used to implement a TEE, and the level of security achieved varies accordingly. In addition, TEEs typically use an isolation mechanism between Trusted Applications to ensure that one TA cannot read, modify or delete the data and code of another TA.

Note3-[b-ITU-T J.1201] Trusted Execution Environment A secure area of the main processor in an IBB-capable cable STB and TV to ensure that sensitive data is stored, processed and protected in an isolated and trusted environment. It offers isolated safe execution of authorized security software providing end-to-end security by enforcement of protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights.

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
NFV	Network Function Virtualization
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

6.1 Background and motivation

As the deployment of IMT-2020 networks, the network slice has become one of the most important enabling technologies for mobile network operators to develop the network services for the enterprises and vertical industries. The network slices could provide the customers the customized services with URLLC, mMTC or eMBB capabilities leveraging the cross-domain orchestration of the virtual and physical network resource, and the slice-level control and self-provision services. The network slice satisfies the different requirements of the customers in terms of the service SLA/QoS, service isolation, visual management and so on, leading to the accelerated digital transformation of the enterprises and vertical industries.

The E2E network slice instance usually is over a complex network environment. To support an E2E network slice instance, a combination of networking technologies, such as SDN, NFV, cloud-native computing and hard slicing technology, are necessary to adapt the diverse features of multiple network domains. Furthermore, the multi-vendor and multi-stakeholder infrastructure increases the complexity of the network slice, specifically in the resource orchestration. The network slice faces the challenges regarding the inherent trust in the multi-domain, multi-vendor and multi-stakeholder environment, which mainly include as follows: 1) how to prevent the access/manipulate the sensitive data or code in the VMs/Dockers of the network slice instances running on the same physical infrastructure, from a malicious network slice stakeholder or third-party infrastructure providers; 2) how to protect the algorithm and underlying models of the digital technologies, e.g. AI/ML, along with privacy and intellectual property, especially in the virtualized network function in multi-tenant environments; 3) how to protect the connection key and configuration of network functions in the network slice instance which may cross heterogeneous networks and multiple administrative domains.

The hardware TEE-based confidential computing[b-CCC WP] could be used to meet the challenges associated with protecting data and code in use. Through this hardware-level isolation, the TEE provides a level of assurance of key properties including the data confidentiality, data integrity and code integrity. Through root-of-trust built-in from the hardware, the network slice can protect both the data and code in the VMs/Dockers from the malicious network slice stakeholder and even the infrastructure owner, and build inherent trust in a multi-domain, multi-vendor, multi-tenant, and multi-stakeholder environment.

However, the network slice orchestration can not identify and distinguish the confidential computing resource. The network slice orchestration regarding the network resource supporting the

confidential computing still faces some issues, which are mainly as follows: (1) how to register and update the enabling status for the infrastructure supporting the hardware-based TEE; (2) how to discover, describe and orchestrate the confidential computing resource, specifically in a hybrid resource orchestration scenarios; (3) how to provide the remote attestation and lifecycle management of the network applications running in the confidential computing environment, especially for the interworking of the applications executing in different vendor's TEEs.

7. Requirements of orchestration supporting confidential computing for network slices

Editor's Note: This section would provide the service requirements of orchestration supporting confidential computing for network slices.

8. Architecture of orchestration supporting confidential computing for network slices

Editor's Note: This section would provide the architecture and functional requirements of orchestration supporting confidential computing for network slices. The capabilities requirements of the network slice orchestrator also would be raised.

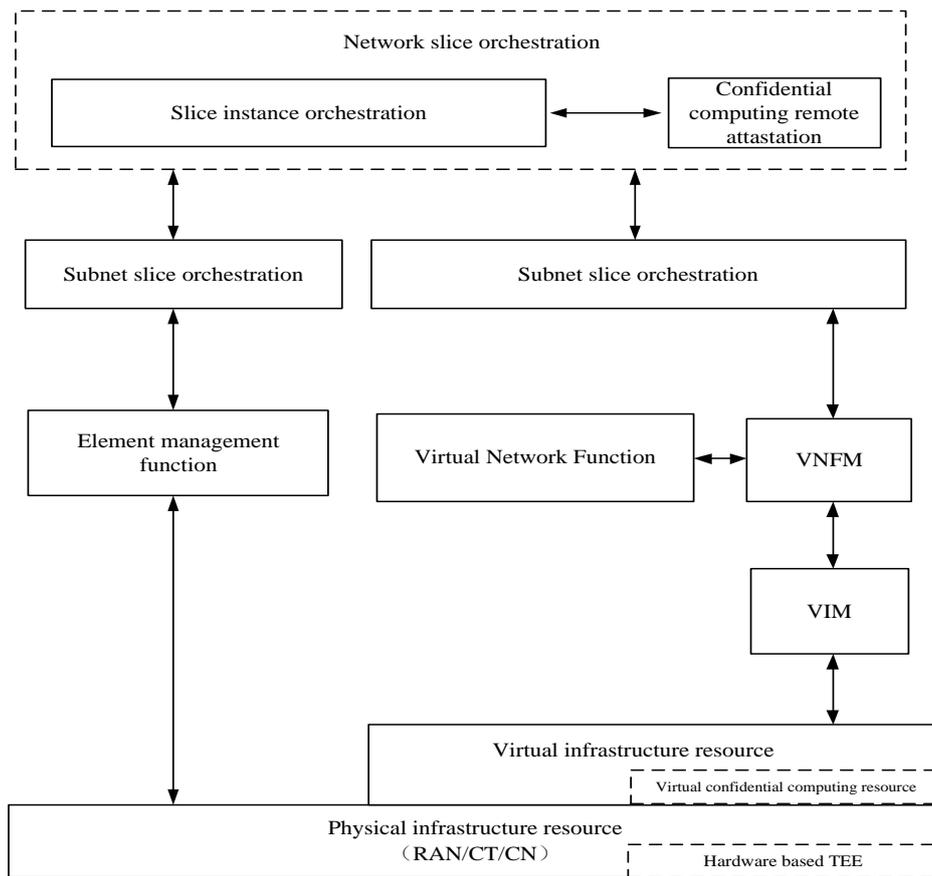


Figure 8-1. Architecture of orchestration supporting confidential computing for network slices

Editor's note: the Figure 8-1 aligns with the IMT-2020 network slice instance management functional architecture[ITU-T Y.3111]

9. Reference points of orchestration supporting confidential computing for network slices

Editor's Note: This section would describe the reference points of orchestration supporting confidential computing for network slices in IMT-2020 networks and beyond.

10. Procedures of orchestration supporting confidential computing for network slices

Editor's Note: This section would describe the essential procedures of orchestration supporting confidential computing for network slices in IMT-2020 networks and beyond.

10.1 Procedure of hardware based TEE property registration

10.2 Procedure of confidential computing environment remote attestation

11. Security considerations

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

Appendix I Use cases of orchestration supporting confidential computing

(This appendix does not form an integral part of this Recommendation.)

I.1 Use case template

The use cases developed in Appendix I should adopt the following unified format for better readability and convenient material organization.

Title	Note: The title of the use case
Description	Note: Scenario description of the use case
Pre-conditions (optional)	Note: The necessary pre-conditions should be achieved before starting the use case.
Post-conditions (optional)	Note: The post-condition that will be carried out after the termination of current use case.
Figure and operational flows (optional)	Note: Figures and operational flows to explain the use case if necessary
Derived requirements	Note: Requirements derived from the use cases, whose detailed description are presented in the dedicated chapter.

Bibliography

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*

[b-ITU-T H.DLT.TEE] Draft Recommendation H.DLT.TEE (under study) , *TEE based confidential computing on distributed ledger technology system*

[b-IETF TEEP Arc] draft-ietf-teep-architecture-18, *Trusted Execution Environment Provisioning (TEEP) Architecture*

[b-CCC WP] Confidential Computing Consortium, *Confidential Computing: Hardware-Based Trusted Execution for Applications and Data*

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

[b-ITU-T J.1201] Recommendation ITU-T J.1201 (2019), *Functional requirements of a smart TV operating system*

TBD
