TEEP Working Group
Internet-Draft
Intended status: Informational
Expires: 1 January 2026

M. Chen
China Mobile
P. Yang
Dawning Information Industry Co., Ltd.
L. Su
China Mobile
T. Pang
Huawei Technology Co.,Ltd.

30 June 2025

TEEP Usecase for Confidential Computing in Network
draft-ietf-teep-usecase-for-cc-in-network-11

Abstract

Confidential computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. Confidential computing could provide integrity and confidentiality for users who want to run applications and process data in that environment. When confidential computing is used in scenarios which need network to provision user data and applications, TEEP architecture and protocol could be used. This usecase illustrates the steps of how to deploy applications, containers, VMs and data in different confidential computing hardware in network. This document is a use case and extension of TEEP architecture and could provide guidance for cloud computing, MEC (Multi-access Computing) and other scenarios to use confidential computing in network.

Table of Contents

1. Introduction

The Confidential Computing Consortium defined the concept of confidential computing as the protection of data in use by performing computation in a hardware-based Trusted Execution Environment [CCC-White-Paper]. In detail, computing unit with confidential computing feature could generate an isolated hardware-protected area, in which data and applications could be protected from illegal access or tampering. When using network to provision confidential computing, users need to choose appropriate steps to deploy their data and applications. This network could be in a cloud, MEC [MEC] or other network that provide confidential computing resource to users. For example in MEC, the autonomous vehicles could deploy private applications and data in confidential computing device to calculate on-vehicle and destination road information without knowing by MEC platform.

The TEEP WG defined the standardization of an architecture and protocol for managing the lifecycle of trusted applications running inside a TEE. In confidential computing, the TEE can also be provisioned and managed by TEEP architecture [I-D.ietf-teep-architecture] and protocol [I-D.ietf-teep-protocol]. By referring TEEP architecture and protocol, applications and data could be provisioned in confidential process, confidential container and confidential VM in different hardware architecture. The intended audiences for this use case are network users and operators who are interested in using confidential computing in network.

2. Terminology

2.1. Terms

The following terms are used in this document.

* Network Management/Orchestration Center(Network M/OC): M/OC exists in the management and orchestration layer of network. Network User uses the M/OC to request for computing resource. The TAM is inside the M/OC to provide management function to TEEP Agent via TEEP broker.

* Network User: Network User possesses personalization data and/or applications that need to be deployed on confidential computing device.

* Confidential Computing Device: Confidential Computing Device is connected by the network and can provide confidential computing service to Network User.

* Package: Package is a unit that is owned by Network User or TAM, and could be deployed on TEE/REE or treated as application data. If the TAM owns the Package, there must have no Personalization Data inside this Package. TA (Trusted Application) in confidential computing could be an application, or packaged with other components like library, TEE shim or even Guest OS. The specific package of confidential computing could refers to the white paper of [CCC_Common_Terminology] by CCC.

* Personalization Data(PD): Data that holds by Network User and needs to be protected by TEE during processing. Other terms like TAM, TEE, REE, TA will reuse the term definition defined in [I-D.ietf-teep-architecture].

2.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Notional Architecture of using confidential computing in network

Figure 1 is the architecture of confidential computing in network. Two new components Network User and Network M/OC are introduced in this document. The connection between Network User and Network M/OC depends on the implementation of specific network, and the network user requests for confidential computing resource is out of teep scope. The connection between Network User and UA (Untrusted Application) or TA depends on the implementation of application. The connection between TAM, TEEP Broker and TEEP Agent refers to the TEEP protocol. Interactions of all components in this scenario are described in the Usecase section. One real-world example could be expressed by this architecture. A company wants to process some personal data in a confidential cloud by network, in which it provides data analysis algorithm as TA, personal data as PD, and data transfer server as UA. When facing how to use confidential cloud, this architecture could provide specific steps based on different hardware architecture by the following usecases.

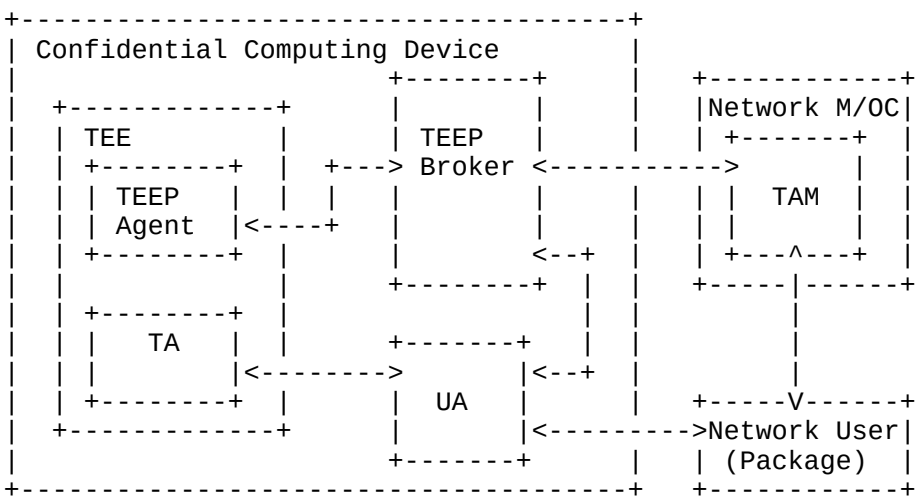

Figure 1: notional architecture of confidential computing in network

4. Confidential computing instances in different hardware architectures

Confidential computing is hardware-based technology, different hardware architectures support different instances like confidential process, confidential container and confidential VM. The following table illustrates this mapping relation. SGX and TrustZone only support process-based confidential computing, and could support confidential container by certain middleware like in the Appendix A. SEV-SNP, CSV, CCA and TDX support confidential VM, also support confidential container by certain middleware like Kata-container-runtime.

Supported Instance Type	Confidential Process in Physical or Virtual Machine	Confidential Container in Physical or Virtual Machine	Confidential VM
Hardware Architecture	TrustZone, SGX	TrustZone, SGX, SEV-SNP, CCA, TDX, CSV	SEV, CCA TDX, CSV

Figure 2: mapping relation between different instances and architectures

5. Use Cases

The basic process of how a Network User utilizes confidential computing is shown below. At present, the main confidential instances types exist in industry are confidential process, confidential container and confidential VM. The definition of these instances could be found at [CCC-White-Paper]. Since confidential computing is a hardware-based technology, different hardware could support different confidential instances. This document gathers the main hardware architectures that support confidential computing, which include [TrustZone], [SGX], [SEV-SNP], [CCA], [TDX] and [CSV]. The following use cases are possible packaging models and how to deploy them in different hardware architecture. In the following tables, the brace means the operation steps to deploy packages. The arrow means deploy package to a destination. The "att" means attestation challenge for the target. All these actions in the following use cases could be expressed by TEEP protocol.

5.1. Case 1: UA, TA and PD are bundled as a package

In this case, UA, TA and PD are bundled as a package. This package is bundled by Network User and sends to TAM by specific netwwork. Specific case, cloud tenant who wants to deploy its PAAS(Platform as a Service) software in a bare medel cloud by network. This PAAS software includes UA, TA and PD, in which UA is HYPERVISOR, TA is confidential VM OS. When TAM tries to deploy this package in confidential computing device, the process of TEEP is as follow.

1. Network User requests for confidential computing resource to Network M/OC.

2. M/OC orchestrates confidential computing device to undertake the request.

3. TAM requests remote attestation to TEEP Agent, TEEP Agent then sends the evidence to TAM. TAM works as Verifier in [RFC9334].

4. After verification, Network User works as Relying Party to receive the attestation result. If positive, Network User establishes secure channel [NIST-Special-Publication-800-133-V2] with TEEP Agent, and transfers this package to TEEP Agent.

5. TEEP Agent deploys TA and personalization data in TEE, then deploy UA in REE.

As for informing Network Users to develop their applications and data, the mapping of UA, TA and implementations are shown in figure 2.

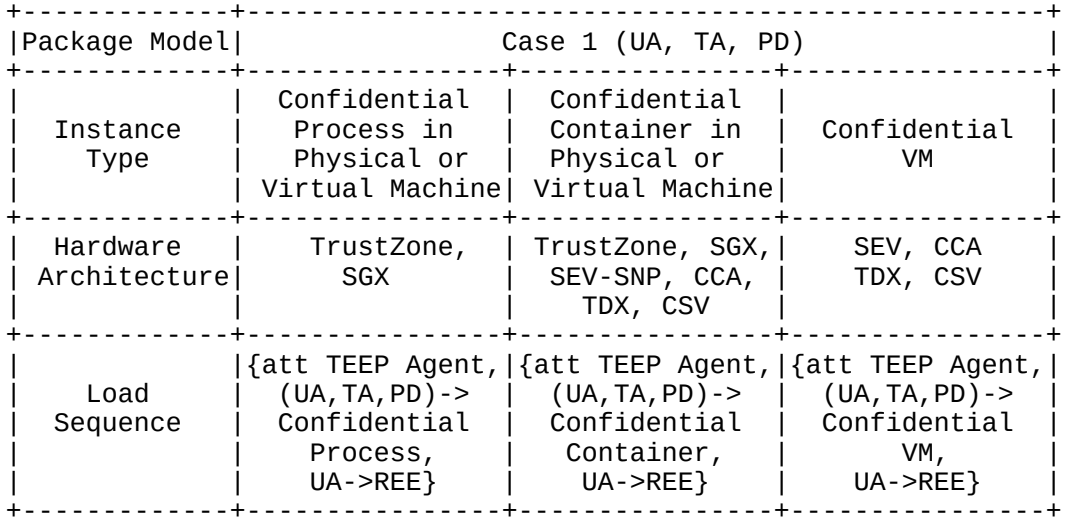

Figure 3: TEEP Implementation of Case 1

5.2. Case 2: PD is a separate package, TA and UA are integrated

In this use case, PD is a separate package, the UA and TA are integrated as a package. Specific case: K8s cluster would deploy working node in confidential computing devcie which includes confidential container, host OS. And confidential container and host OS are bundled as a image. If Network User provides packages like this, the process of TEEP is as follow.

1. Network User requests for confidential computing resource to Network M/OC.

2. M/OC orchestrates confidential computing device to undertake the request.

3. Network User transfers UA and TA to confidential computing device via TAM. TAM then deploys these two applications in REE and TEE respectively. (In SGX, UA must be deployed first, then let UA to load TA in SGX.)

4. TAM requests remote attestation to TEEP Agent, TEEP Agent then sends the evidence to TAM. TAM works as Verifier in RATs architecture.

5. After verification, Network User works as Relying Party to receive the attestation result. If positive, Network User establishes secure channel with TA, and deploys personalization data to TA.

The mapping of UA, TA and implementations are shown in figure 3.

Package Mode	Case 2 (UA, TA) (PD)		
Instance Type	Confidential Process in Physical or Virtual Machine	Confidential Container in Physical or Virtual Machine	Confidential VM
Hardware Architecture	TrustZone, SGX	TrustZone, SGX, SEV-SNP, CCA, TDX, CSV	SEV, CCA TDX, CSV
Load Sequence	{UA->REE, TA->Confidential Process, att TEEP Agent, PD->TA}	{UA->REE, TA->Confidential Container, att TEEP Agent, PD->TA}	{UA->REE, TA->Confidential VM, att TEEP Agent, PD->TA}

Figure 4: TEEP Implementation of Case 2

5.3. Case 3: TA and PD are separate packages, with or without UA

In this case, Network User provides TA and PD as separate packages with or without UA. Specific case: cloud tenant deploys its SAAS(Software as a Servcie) software in cloud. This SAAS software are confidential VM, and PD is a separete package. The process of TEEP in this case is as follow.

1. Network User requests for confidential computing resource to Network M/OC.

2. TAM in M/OC orchestrates confidential computing device to undertake the request.

3. Network User transfers UA to TAM, then TAM deploys UA in REE.

4. Network User transfers TA to TEEP Agent.

5. TAM requests remote attestation to TEEP Agent, TEEP Agent then sends the evidence to TAM. TAM works as Verifier in RATs architecture.

6. After verification, Network User works as Relying Party to receive the attestation result. If positive, Network User establishes secure channel with TA and transfers PD to it.

Package Mode	Case 3 (TA),(PD) or (TA),(PD),(UA)		
Instance Type	Confidential Process in Physical or Virtual Machine	Confidential Container in Physical or Virtual Machine	Confidential VM
Hardware Architecture	TrustZone, SGX	TrustZone, SGX, SEV-SNP, CCA, TDX, CSV	SEV, CCA TDX, CSV
Load Sequence	{UA->REE, TA->Confidential Process, att TEEP Agent, PD->TA}	{UA->REE, TA->Confidential Container att TEEP Agent, PD->TA}	{UA->REE, TA->Confidential VM, att TEEP Agent, PD->TA}

Figure 5: TEEP Implementation of Case 3

5.4. Case 4: TA and PD are bundled as a package, with or without UA

As in case 3, cloud tenant who wants to protect its data and TA and package them as a VM image. In this case, the process of TEEP is as follow.

1. Network User requests for confidential computing resource to Network M/OC.

2. TAM in M/OC orchestrates confidential computing device to undertake the request.

3. If there has UA, Network User deploys UA in REE.

4. TAM requests remote attestation to TEEP Agent, TEEP Agent then sends the evidence to TAM. The TAM works as Verifier in RATs architecture.

5. After verification, Network User works as Relying Party to receive the attestation result. If positive, Network User establishes secure channel with TEEP Agent and transfers TA and PD package to TEEP Agent.

Package Mode	Case 4 (TA, PD) (UA) or (TA, PD)		
Instance Type	Confidential Process in Physical or Virtual Machine	Confidential Container in Physical or Virtual Machine	Confidential VM
Hardware Architecture	TrustZone, SGX	TrustZone, SGX, SEV-SNP, CCA, TDX, CSV	SEV, CCA TDX, CSV
Load Sequence	{UA->REE, att TEEP Agent, (TA,PD)-> Confidential Process}	{UA->REE, att TEEP Agent, (TA,PD)-> Confidential Container}	{UA->REE, att TEEP Agent, (TA,PD)-> Confidential VM}

Figure 6: TEEP Implementation of Case 4

6. IANA Considerations

This document does not require actions by IANA.

7. Security Considerations

Besides the security considerations in TEEP architecture, there is no more security and privacy issues in this document.

8. Acknowledgements

Many thanks to Dave Thaler, Eric Voit, Hannes Tschofenig, the CCC TAC meeting and other people who provide comments and suggestions.

9. References

9.1. Normative Reference

[I-D.ietf-teep-architecture]
Pei, M., Tschofenig, H., Thaler, D., and D. M. Wheeler, "Trusted Execution Environment Provisioning (TEEP) Architecture", Work in Progress, Internet-Draft, draft-

ietf-teep-architecture-19, 24 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-teep-architecture-19>.

[I-D.ietf-teep-protocol] Tschofenig, H., Pei, M., Wheeler, D. M., Thaler, D., and A. Tsukamoto, "Trusted Execution Environment Provisioning (TEEP) Protocol", Work in Progress, Internet-Draft, draft-ietf-teep-protocol-21, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-teep-protocol-21>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/info/rfc9334>.

9.2. Informative Reference

[CCA] ARM, "Arm Confidential Computing Architecture", March 2022, <https://www.arm.com/architecture/security-features/arm-confidential-compute-architecture>.

[CCC-White-Paper] Confidential Computing Consortium, "Confidential Computing: Hardware-Based Trusted Execution for Applications and Data", January 2021, <https://confidentialcomputing.io/wp-content/uploads/sites/ 10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf/>.

[CCC_Common_Terminology] Confidential Computing Consortium, "Common Terminology for Confidential Computing", October 2022, <https://github.com/confidentialcomputing/governance/blob/main/terminology/commonterminology.md>.

[CSV] HYGON, "HYGON China Secure Virtualization", May 2023, <https://gitee.com/anolis/cloud-kernel/blob/devel-5.10/Documentation/x86/hygon-secure-virtualization.rst>.

[MEC] ETSI, "Multi-access Edge Computing (MEC);Framework and Reference Architecture", March 2022, <https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_MEC003v030101p.pdf>.

[NIST-Special-Publication-800-133-V2] NIST, "Recommendation for Cryptographic Key Generation", June 2020, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf>.

[SEV-SNP] Advanced Micro Devices, "AMD SEV-SNP: Strengthening VM-isolation-with-integrity-protection-and-more", January 2020, <https://www.amd.com/system/files/TechDocs/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf>.

[SGX] Intel, "Overview of Intel Software Guard Extension", June 2016, <https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html>.

[TDX] Intel, "Intel Trust Domain Extensions", August 2021, <https://www.intel.com/content/www/us/en/developer/articles/technical/intel-trust-domain-extensions.html>.

[TrustZone] HUAWEI Technologies, "Kunpeng BoostKit for Confidential Computing TrustZone Kit", January 2022, <https://www.hikunpeng.com/document/detail/en/kunpengcctrustzone/overview/kunpengcctrustzone.html>.

Appendix A. Submodules in TEEP Agent

The original design of TEEP only includes TEEP Agent and TA inside TEE. While in confidential computing implementation, other submodules may also be involved in the TEE. In TEEP, these submodules could be covered by TEEP Agent.

In SGX based confidential computing, submodule could provide convenient environment or API in which TA does not have to modify its source code to fit into SGX instructions. Submodules like Gramine and Occlum .etc are examples that could be included in TEEP Agent. If there is no submodule in TEEP Agent, the TA and UA need to be customized applications which fit into the SGX architecture.

In SEV and other architectures that support whole guest VM as a TEE, TEEP Agent doesn’t have to use extra submodule to work as a middleware or API. However with some submodules like Enarx which works as a runtime JIT compiler, TA could be deployed in a hardware independent way. In this scenario, TA could be deployed in different hardware architecture without re-compiling.

Authors’ Addresses

Meiling Chen
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing
100053
China
Email: chenmeiling@chinamobile.com

Penglin Yang
Dawning Information Industry Co., Ltd.
No. 36, Zhongguancun Software Park, No.8, West Dongbeiwang Road, Haidian District
Beijing
100193
China
Email: ypl_ietf@163.com

Li Su
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing
100053
China
Email: suli@chinamobile.com

Ting Pang
Huawei Technology Co.,Ltd.
127 Jinye Road, Yanta District
Xi’an
710077
China
Email: pangting@huawei.com