INSTITUTE of INFORMATION SECURITY

プライバシー保護技術に関する研究アイデア・成果、実装プラクティス

TEEとRemote Attestation（とZK）

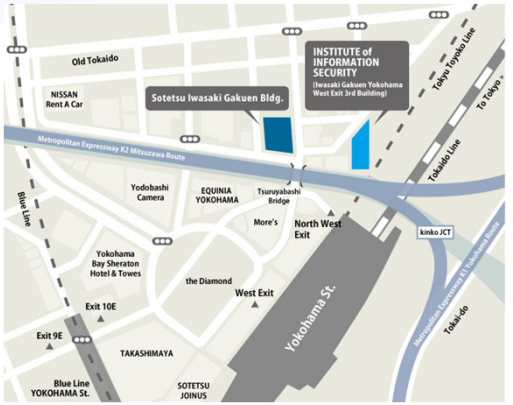
Zero Knowledge Frontier Japan vol.2 (2025/Nov/29)

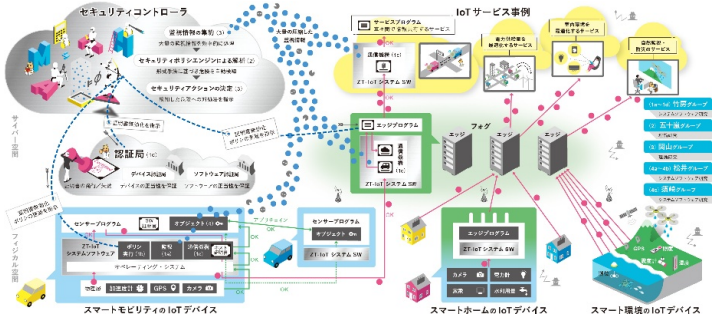
Institute of Information Security (情報セキュリティ大学院大学)
Kuniyasu Suzaki (須崎 有康)
https://lab.iisec.ac.jp/~suzaki_lab/

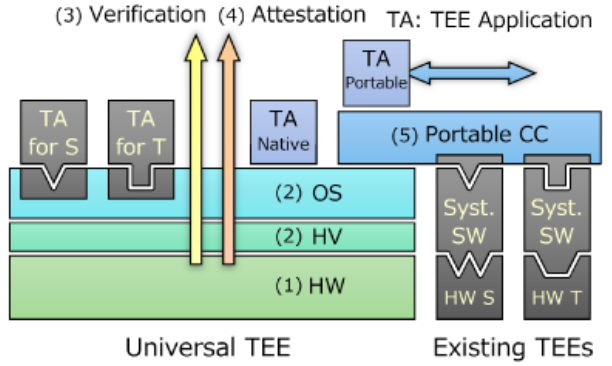
Who am I ? (Kuniyasu Suzaki)

INSTITUTE of INFORMATION SECURITY

- 情報セキュリティ大学院大学に　2022/9/1　着任
  - 横浜駅北西口にあります　https://lab.iisec.ac.jp/~suzaki_lab/
  - その前は産総研
    - 1CD Linux KNOPPIX Japanese Edition (2003-2013)
- TGC (Trusted Computing Group) Invited Expert 2019 –
  - TCG Award 2025を頂きました
- プライバシーテック協会アドバイザー　2024 –
- プロジェクト
  - JST CREST Zero Trust IoT 2021-26 https://zt-iot.nii.ac.jp/
  - JST Kプロ　2025-29 ハードウェア・ソフトウェア・理論の連携によるユニバーサルTEEアーキテクチャの実現　https://cradsec.rois.ac.jp/jp/index.html
- クラウドのConfidential Computing(Intel SGX, TDX, AMD SEV-SNP, AWS Nitro)で使えるRemote Attestationサンプルを公開
  - https://github.com/iisec-suzaki/cloud-ra-sample







参考資料

- AI時代の安全なデータ処理「Confidential Computing」: 機密コンピューティングの技術的特徴～低レイヤの開発課題とAI／機械学習等への適用が期待される新しい機能を解説～　2025/07　https://ipsj.ixsq.nii.ac.jp/records/2002747
- IoTデバイスにおけるTEE(Trusted Execution Environment)の実装, システム制御情報学会誌「システム／制御／情報」2024/5 https://www.jstage.jst.go.jp/article/isciesci/68/5/68_185/_pdf/-char/ja
- Trusted Execution Environmentの実装とそれを支える技術, 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review 2020/10 https://www.jstage.jst.go.jp/article/isciesci/67/9/67_379/_pdf/-char/ja

Contents

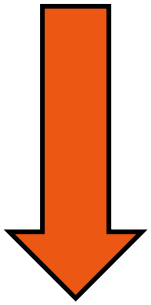
INSTITUTE of INFORMATION SECURITY

- TEEの簡単な特徴紹介
- Remote Attestation要件
  - ① 署名鍵が耐タンパなハードウェアで守られている
  - ② 署名鍵を使うソフトや完全性(Hash)を計測するソフトは信頼できる
- TEEのRemote Attestationパターン
  - （一例）AMD SEV-SNPのVM型TEEのRemote Attestation
    1. CPUベースのAttestation (VM起動前)
       1. Provisioning (鍵の設定)
       2. Initial Measurement (VM起動前イメージ)
       3. Making Attestation Evidence (署名付Attestation Evidence作成)
    2. vTPMベースのAttestation (VM起動後)
- Remote AttestationとZero Knowledge (私見)
  - 何がZero Knowledgeでできるか？
  - TikTokのTrustless Attestation (Circomを使っている）
- まとめ

ざっくばらんに確認してほしい課題

INSTITUTE of INFORMATION SECURITY

- Remote Attestation内でZero Trustに変えられるところ?
  - Quote?
    - ◆CPU・ハードウェア情報?
    - ◆バイナリ情報?
  - Verifier？
  - 署名鍵（Attestation Key）?
  - Hardware Root of Trust

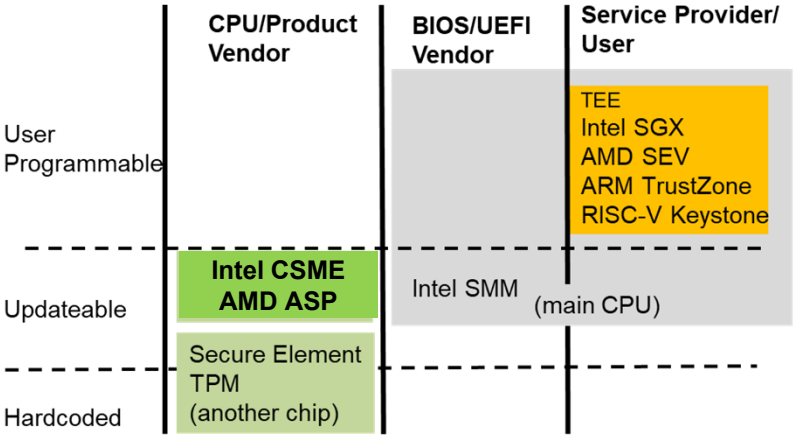


難易度？

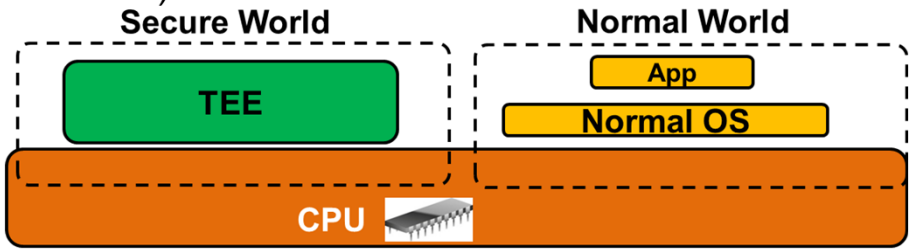
- Remote Attestation内で無くならないところ?
  - (予想)Hardware Root of Trustでの機密情報保護

TEEとは（1/2）

- ハードウェアが提供する隔離実行環境HIEE(Hardware-assisted Isolated Execution Environments)の一つ
  - HIEEにはBIOSが使うSMMやIntel CSME&AMD ASP、別チップのTPM & Apple Secure Enclaveがある
  - TEEは第三者がプログラミング可能であることを特徴とする



- TEEはCPUの状態を二つに分ける
  - ノーマルワールド (i.e., REE: Rich Execution Environment)
    - ◆通常のOS(Linux, Windows)が実行される
  - セキュアワールド(i.e., TEE: Trusted Execution Environment)
    - ◆OSやハイパーバイザーなどの脆弱性とは無縁の環境
    - ◆クリティカルな処理を行う

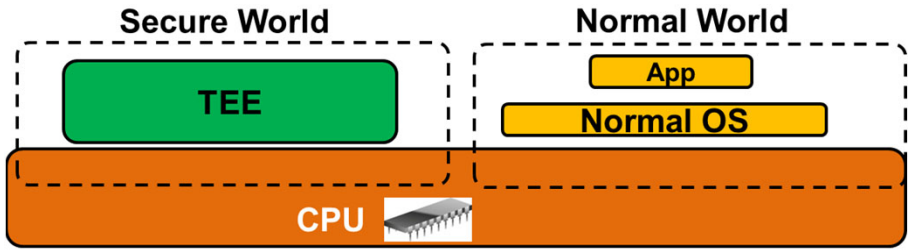


この図はあくまでTEEの一例

TEEとは（2/2）

■ 特徴：
- （極端に言えば）一時的に隔離実行されるのみ
- 長期的な鍵保存は別の手段が必要
  - ◆Root of Trustには安全に鍵・証明書を保存する耐タンパハードウェアが必要
  - ◆これを信頼の基点に外部からの健全性の検証（Remote Attestation）が行われる

■ 利用できるCPU
- ARM TrustZone （スマホ）
- Intel SGX (サーバ、PCはdeprecatd)
- Intel TDX (Xeon サーバ)
- AMD SEV (EPYC サーバ)
- Arm CCA (サーバ, スマホ?)



この図はあくまでTEEの一例
（Arm TrustZoneが一番近い）

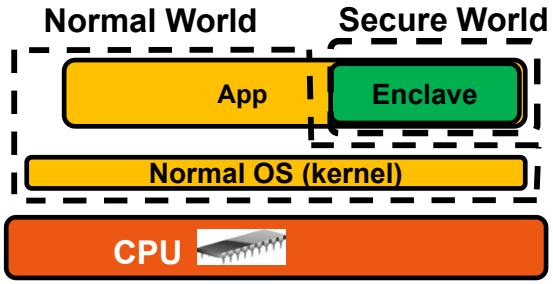
■ その他の実装
- GPU内 (Nvidia H100)
- AWS Nitroはハイパーバイザー＋セキュアハード(Nitro Card, Nitro Security Chip)

Type of Confidential Computing

INSTITUTE of INFORMATION SECURITY

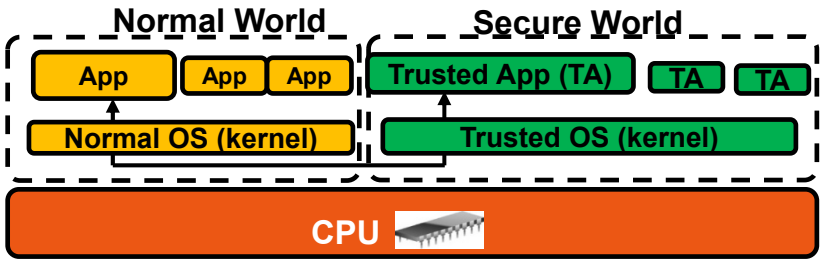
Library Type

- A part of process (library) is executed in TEE.
- CPU: Arm Cortex-M, Intel SGX



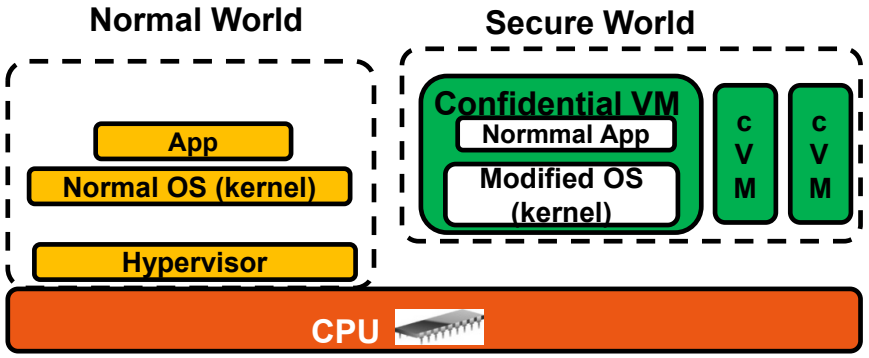
Process Type

- Secure World has an own OS and TA (Trusted Application) runs on it. Normal App calls TA.
- CPU: Arm Cortex-A, AMD PSP, Apple Secure Enclave



VM Type

- Secure World has VMs, namely confidential VM.
- The OS modified for secure world.
- CPU: Intel TDX, AMD SEV, Arm CCA



Current TEE-enabled CPUs and targets

INSTITUTE of INFORMATION SECURITY

	Embedded	Smartphone	Game	PC	Server/Cloud
Arm TrustZone (Cortex-M)	Raspberry Pi Poco				
Arm TrustZone (Cortex-A)	Raspberry Pi 3B+	Many	Nintendo Switch		
Arm CCA upcoming		?		?	?
Intel SGX (Core) deprecated				deprecated	
Intel SGX (Xeon Scalable)					Azure, GCP, etc
Intel TDX (Xeon)					Azure, GCP, etc
AMD PSP			Playstation5		
AMD SEV (EPYC)					Azure, GCP, etc
Apple Secure Enclave		iPhone		Mac	

TEEの応用

- 機密情報処理
  - 鍵管理
    - ◆AndroidのKeyMaster
  - DRM処理
    - ◆スマホのWidevine(Google)
    - ◆WindowsのUltra HD Blu-rayビューア
  - 個人情報管理
    - ◆指紋認証処理
    - ◆FIDO認証
    - ◆暗号資産ハードウェアウォレット
- コード・データの隠蔽
  - 機械学習の重み付けデータ
  - プライバシー保護
  - 遺伝子解析

スマホでTEEを普及させた
キラーアプリ

キラーアプリになれなかった

キラーアプリ候補？

- メモリ消費が少ない
- スマートフォン
- Arm TrustZone向き

- メモリ消費が大きい
- サーバ・クラウド
- Intel SGX、AMD SEV 向き
- **Confidential Computing**の
  ターゲットはこちら。

サーバでのキラーアプリ候補？

TEEではなぜRemote Attestationが必要か？

- TEEは色々なソフトが実行できるが隔離実行環境であり、REE(Secure World)からは何をしているのか分からない。
- TEEの実行を信頼できるのか？
  - TEEの実行をだれ（どのハードウェア、ソフトウェア）が担保するのか？
    - ◆信頼とはどう確立されるのか？
- TEEの処理
  - TEEのコードは安全でないREEからロードされる。コードは変更されない。
  - 初期データもREEからだが、TEE実行後の変化は見えない。
    - ◆TEEで担保されること

	Integrity	Confidentiality
Code	○	△(別の技術を使う)
Data	○	○(Remote Attestation後に渡す)

- AttestationではIntegrityを確認する

インターネットは信頼できる？

INSTITUTE of INFORMATION SECURITY

- 「インターネット上ではあなたが犬だと誰も知らない」
  ″On the Internet, nobody knows you're a dog″
  - New Yorker(1993年7月5日)でのインターネット匿名性に関する格言
  - https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you're_a_dog

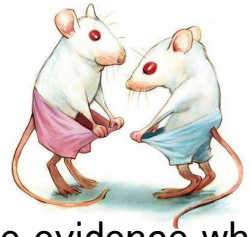
- これではインターネットで商取引ができないが、解消するために個人 認証、サーバ認証などの技術が進んだ。

- さらに進んで、あなたの使っているデバイス(PC,スマホ)は信頼できるのか(ハードは想定のものであるか、ソフトは改変されていないか、等)をリモートで確認する技術がRemote Attestation

- 現在の活用事例
  - Smartphone
  - TPM (Trusted Platform Module) on PC
  - FIDO (Fast IDentity Online)
  - Smart home protocol “Matter”
  - TEE
    - Because TEE is an isolated execution environment and hides the behavior.

Remote Attestation

INSTITUTE of INFORMATION SECURITY



RATS Logo

■ IETF RFC 9334 RATS(Remote Attestation ProcedureS)

- **Attester**

  wants to get data or service form Relying Party. The device offers the evidence which shows the soundness of devices, systems, applications, configurations, etc.

- **Relying Party**

  wants to confirm the Attester's soundness to provide data or service.

- **Verifier**

  judges the Attester's evidence based on registered endorsement (ex: attestation public key), reference values, and policies.

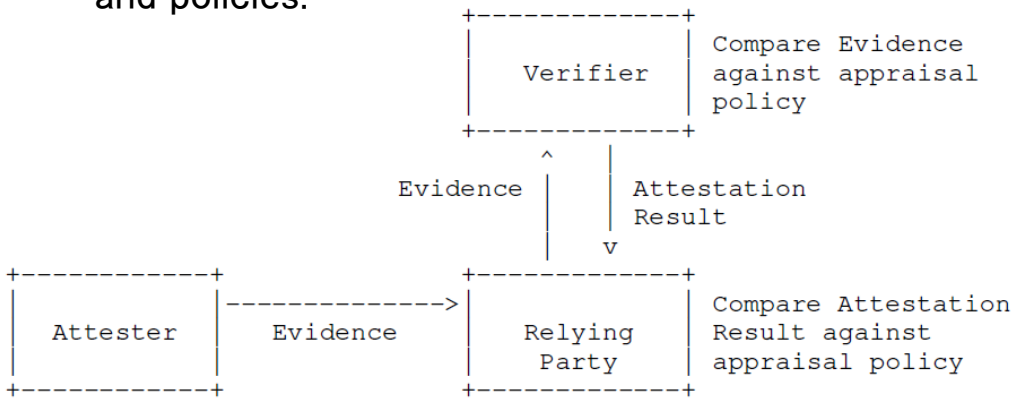
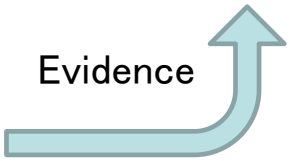


Figure 6: Background-Check Model

① Make "Attestation Evidence (Ex:hash values of applicatoins)" and sign it with Attestation Private Key.

③ Verifier has the certificate of Attestation Public Key and reference values (ex: hashes of applications).
Verifier judges the Evidence with them and send the result.

② Relying Parity cannot verify and ask Verifier with the evidence.



Remote Attestation 2Phases

INSTITUTE of INFORMATION SECURITY

■ 2 のフェーズ

1. Provisioning
2. Remote Attestation

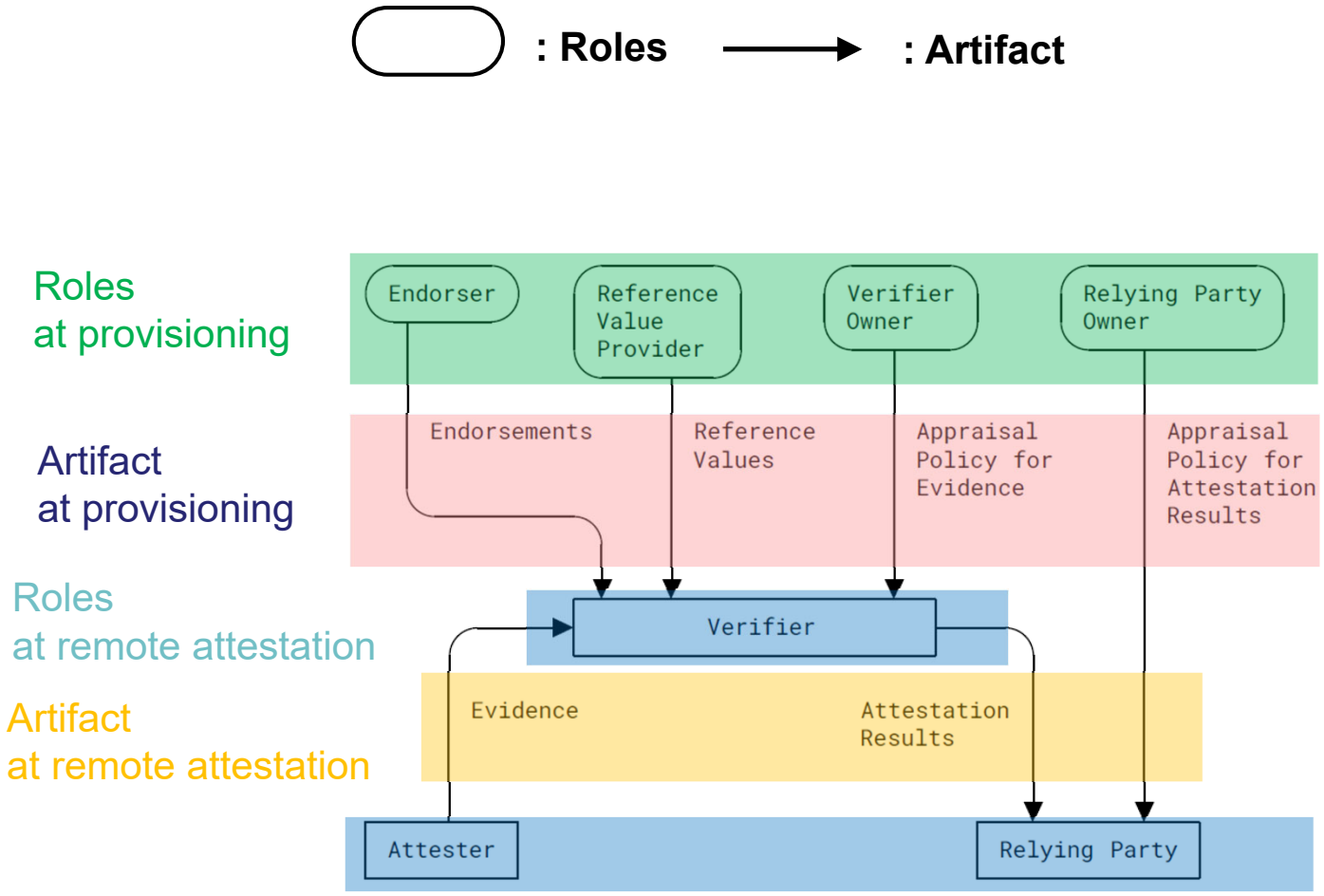


Figure 1: Conceptual Data Flow

Remote Attestation 要求事項

INSTITUTE of INFORMATION SECURITY

- 要求事項①: 署名鍵がハードウェア的に守られていること
  - 耐タンパーなハードウェアで守られていること
  - 署名鍵はベンダーがPKIベースの証明書を出すこと
- 要求事項②: 署名鍵を使うソフトや計測するソフトが信頼できること
  - ユーザが改ざんできない実装になっていること
  - ユーザが改ざんした場合検出できること
    - ◆TPMのMeasure Boot LogやSecure Boot時のみで使える署名鍵など。(本日は出て来ない)

要求事項 ①Attestation Private Key must be protected securely.

INSTITUTE of INFORMATION SECURITY

- CPU Vendors Key
  - AMD SEV-SNP (VECK: Versioned Chip Endorsement Key) protected by AMD-SP
    - ◆AMD SEV のCert情報　https://www.amd.com/ja/developer/sev.html
  - Intel TDX
    - ◆Intel TDX のCert情報　https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_TDX_DCAP_Quoting_Library_API.pdf
  - Intel SGX
    - ◆Intel SGX のCert情報　https://api.trustedservices.intel.com/documents/Intel_SGX_PCK_Certificate_CRL_Spec-1.5.pdf

- Vendors get the FIPS(Federal Information Processing Standards) 140-3 validation certificate.
  - https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date	Status
4749	Intel Corporation	Crypto Module for Intel® Alder Point PCH Converged Security and Manageability Engine (CSME)	Firmware-hybrid	08/02/2024	Active
4941	Advanced Micro Devices (AMD)	AMD ASP Cryptographic CoProcessor ("Genoa")	Firmware-hybrid	01/15/2025	Active
4915	Advanced Micro Devices (AMD)	AMD ASP Cryptographic CoProcessor ("Raphael")	Firmware-hybrid	12/12/2024	Active
4914	Advanced Micro Devices (AMD)	AMD ASP Cryptographic CoProcessor ("Storm Peak")	Firmware-hybrid	12/12/2024	Active

要求事項 ②の実装（CPU依存）

INSTITUTE of INFORMATION SECURITY

要求事項 ②： 署名鍵を使うソフトや計測するソフトが信頼できること

4つの実装カテゴリ

- Hardware Only
  - SGX
    - Architectural Enclave (Quoting Enclave)
- Hardware + Secure Boot
  - Arm Cortex-A TrustZone
- Hardware + Trusted Boot (vTPM)
  - AMD SEV
  - Intel TDX
  - Arm CCA
- Hardware + Trusted Boot (vTPM) + Secure Boot
  - RISC-V APTEE or CoVE

CPUの署名鍵によるアテステーション
はVM起動前まで。
VM起動後はTPMを使う。
つまり2段階になっている

VM型のTEEの2段階Remote Attestation

INSTITUTE of INFORMATION SECURITY

- VM型のTEE(Intel TDX, AMD SEV-SNP)の多くは2段階になっている。
  - 理由：CPUベースのAttestationではVM起動後まで追えない。CPUベースのAttestationではVMの起動前（BIOS,TPM）の状況までを保証する。
  - VM起動後はTPMベースのRemote Attestationを使う。

- 2段階Remote Attestation
  - 1st Step: CPU rooted Attestation
    - ◆要求事項① 署名鍵はCPUベンダーが提供し、Hardware Root of Trustで守る。
    - ◆要求事項② TEEの専用命令で計測することで担保する。
  - 2nd Step: VM内のvTPM Based Attestation
    - ◆要求事項① 仮想TPM(vTPM)を想定してきちんと鍵管理されいること。クラウドベンダ依存。
    - ◆要求事項② 計測はBIOS以前のCRTM(Core Root of Trust Measurement)から始まること。

AMD SEV-SNPのRemote Attestation

注意点

- 2つのAttestation Key
  - VCEK (Versioned Chip Endorsement Key): Chip ID を元に発行される署名鍵。
  - VLEK (Versioned Loaded Endorsement Key): AMD と CSP (Cloud Service Provider、例: AWS) が共有するシードから導出される署名鍵。AMD Key Derivation Service (KDS)から提供される。
- 2つのAttestation方式
  - Standard (Regular) Attestation (PKIの証明書なし)
  - Extended Attestation (PKIの証明書付)
- Migrationや古くなったVerifier対応も考慮されている

AMD SEV-SNPで使われる命令

INSTITUTE of INFORMATION SECURITY

■ AMD SEV-SNP用の命令

- アテステーションデータ設定用（ホストOS/ハイパーバイザ側） プロビジョニング
  - SET_CONFIG　　注：Standard (Regular) Attestation用
  - SET_EXT_CONFIG　注：Extended Attestation用
- 起動用（ホストOS/ハイパーバイザ側）
  - LAUNCH_START
  - LAUNCH_UPDATE_DATE & LAUNCH_UPDATE_VMSA
  - LAUNCH_MEASURE
  - LAUNCH_SECRET
  - LAUNCH_FINISH
- リモートアテステーション時（ゲストOS用）
  - GET_REPORT　　注：Standard (Regular) Attestation用
  - GET_EXT_REPORT　注：Extended Attestation用

The Definitive SEV Guest API Documentation
https://docs.kernel.org/virt/coco/sev-guest.html
にgust ioctolとhypervisor ioctl がある

AMD SEV-SNPで使われる鍵

INSTITUTE of INFORMATION SECURITY

- PKI用
  - ARK (AMD Root Key): AMD の最上位認証局 (Root of Trust) の鍵
  - ASK (AMD Sign Key): AMD が発行する中間認証局のような鍵
- チップ固有鍵
  - CEK (Chip Endorsement Key):チップ固有の秘密鍵。
  - PEK (Platform Endorsement Key):プラットフォーム固有の鍵。古い。チップとプラットフォームの違いは不明瞭。
- Attestation用
  - VCEK (Versioned Chip Endorsement Key): Chip ID を元に発行される署名鍵。
  - VLEK (Versioned Loaded Endorsement Key): AMD と CSP (Cloud Service Provider、例: AWS) が共有するシードから導出される署名鍵。AMD Key Derivation Service (KDS)から提供される。

- KDS: Key Distribution Service
  - KDSから取ることもキャッシュすることも可

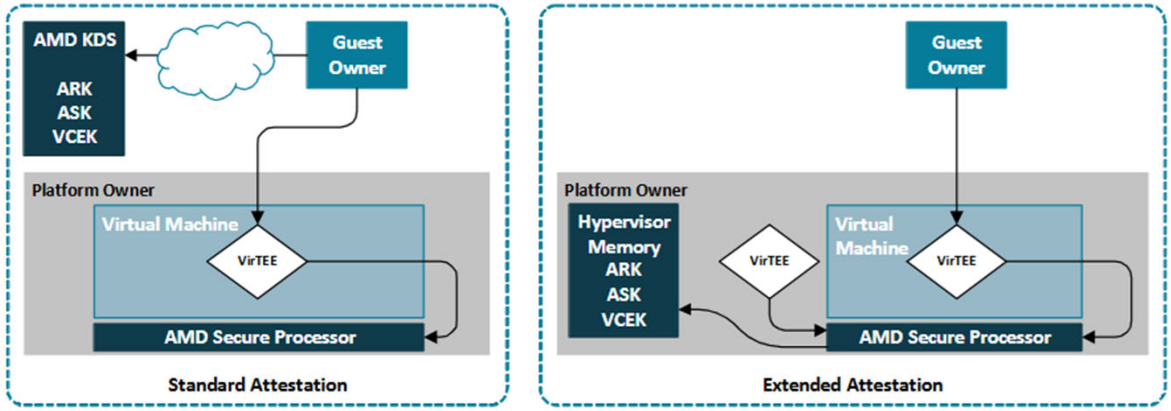


Figure 2-1: Standard (left) and extended (right) attestation flows

SEV-SNP Platform AttestationUsing VirTEE/SEV
https://www.amd.com/content/dam/amd/en/documents/developer/58217-epyc-9004-ug-platform-attestation-using-virtee-snp.pdf

Attestation手順

INSTITUTE of INFORMATION SECURITY

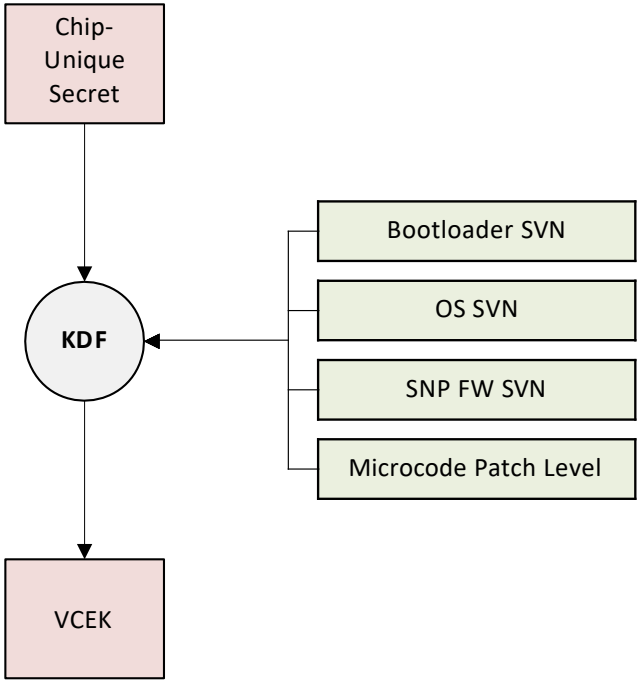
- AMD SEV-SNP
  - A) Attestationのための署名鍵が作られるまでの動作　(Provisioning)
  - B) バイナリロード時にAttestation用のデータ(Quote)を作るまでの動作 (VMの場合はGuestOS起動前)
  - C) Attestation時にCPUに由来する鍵でEvidenceを作るまでの動作

Authenticity of Attestation Report

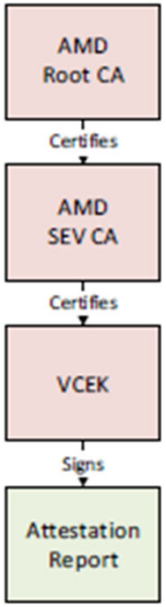
AMD SEV-SNP Attestation: Establishing Trust in Guests [Linux Security Summit Europe 2022]より
https://www.amd.com/content/dam/amd/en/documents/developer/lss-snp-attestation.pdf

INSTITUTE of INFORMATION SECURITY

■ 鍵導出KDF (Key Derivation Function)手順と証明書の連鎖



REPORTED_TCB is mixed into the chip unique secret to derive the Versioned Chip-Endorsement Key (VCEK), which is used as the attestation key



Certificates retrieved from AMD Key Distribution Service (KDS)

AMD Certificate Authority certifies the VCEK

VCEK signs the attestation report

Attestation手順

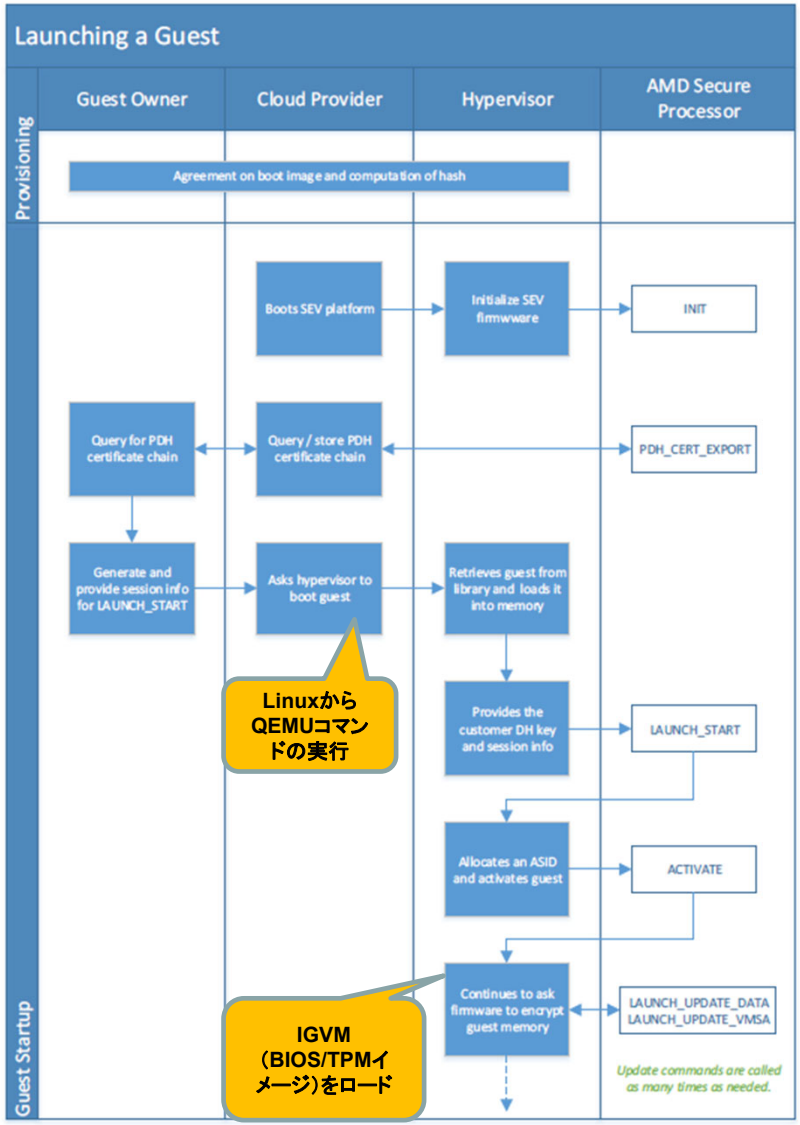
INSTITUTE of INFORMATION SECURITY

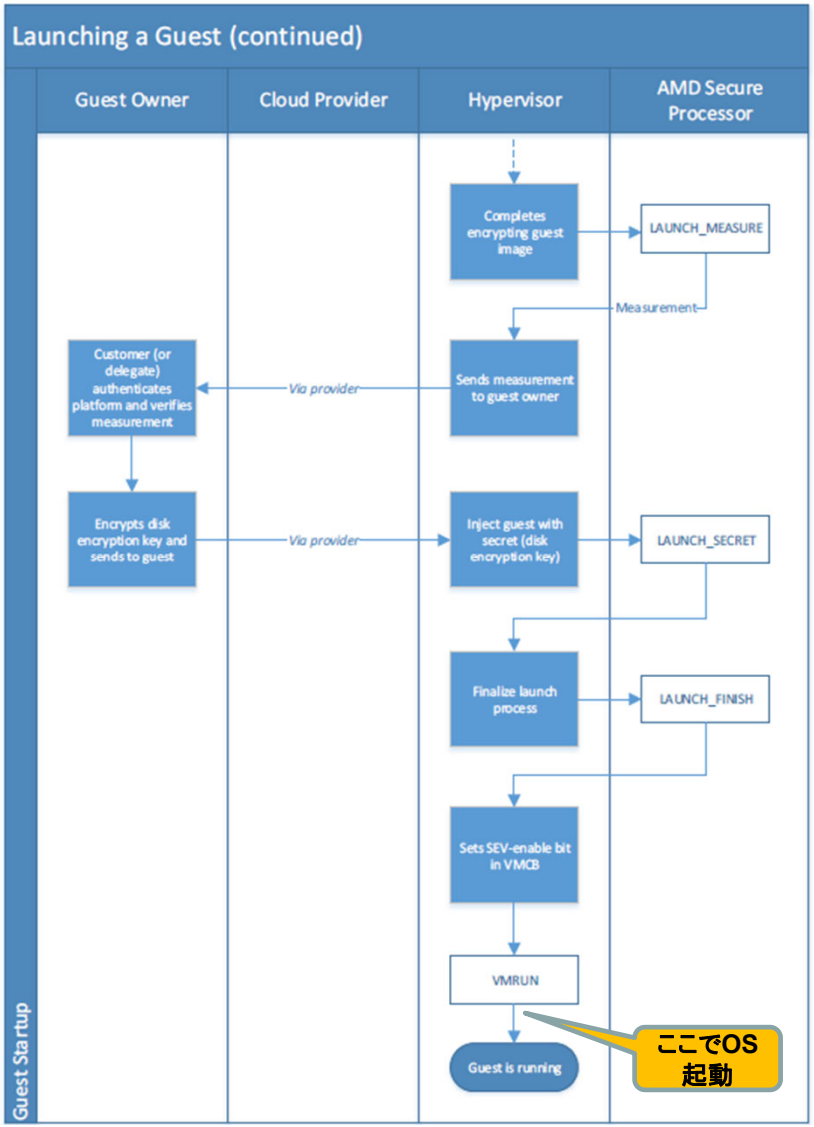
- AMD SEV-SNP
  - A) Attestationのための署名鍵が作られるまでの動作　(Provisioning)
  - B) バイナリロード時にAttestation用のデータ(Quote)を作るまでの動作 (VMの場合はGuestOS起動前)
  - C) Attestation時にCPUに由来する鍵でEvidenceを作るまでの動作

AMD Secure Encrypted Virtualization API Version 0.24より

https://www.amd.com/content/dam/amd/en/documents/epyc-technical-docs/programmer-references/55766_SEV-KM_API_Specification.pdf

■ cVMでOS起動以前





AMD SEV-SNPでの起動時計測

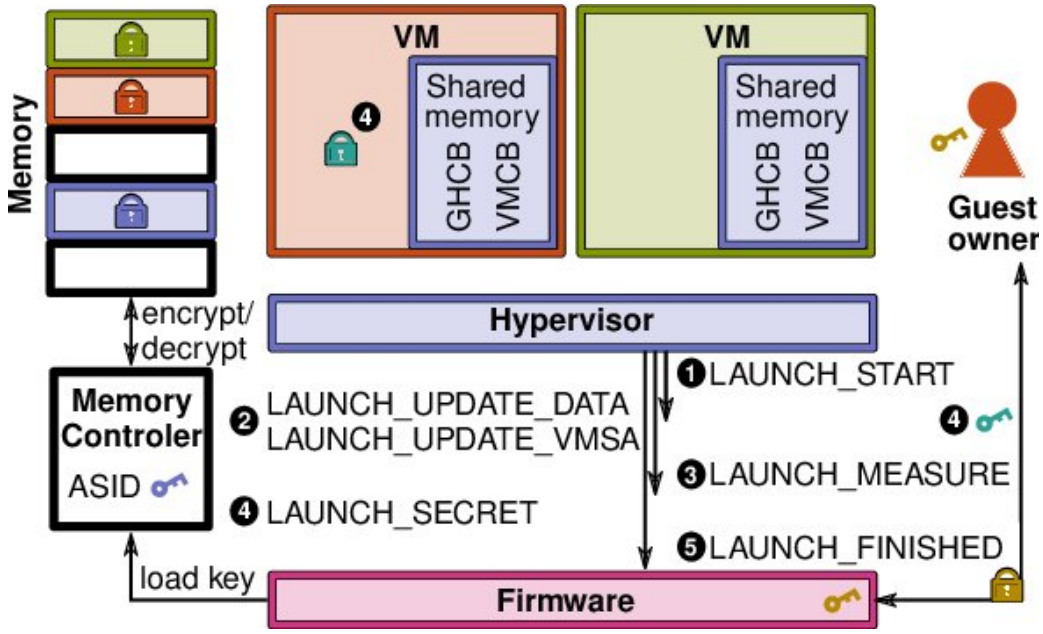
INSTITUTE of INFORMATION SECURITY

■ 起動時に使われる命令

1. LAUNCH_START
2. LAUNCH_UPDATE_DATE & LAUNCH_UPDATE_VMSA
3. LAUNCH_MEASURE
   - ◆ 起動されたゲストのメモリページ測定値を返す。ゲストが改ざんされることなく正常に起動されたことを確認。
4. LAUNCH_SECRET (オプション)
   - ◆ LAUNCH MEASUREMENTが成功すればSecure Processorが持つSecret(ディスク暗号鍵)を返す
5. LAUNCH_FINISH (これ以降でguestOS起動)

■ 状態の管理

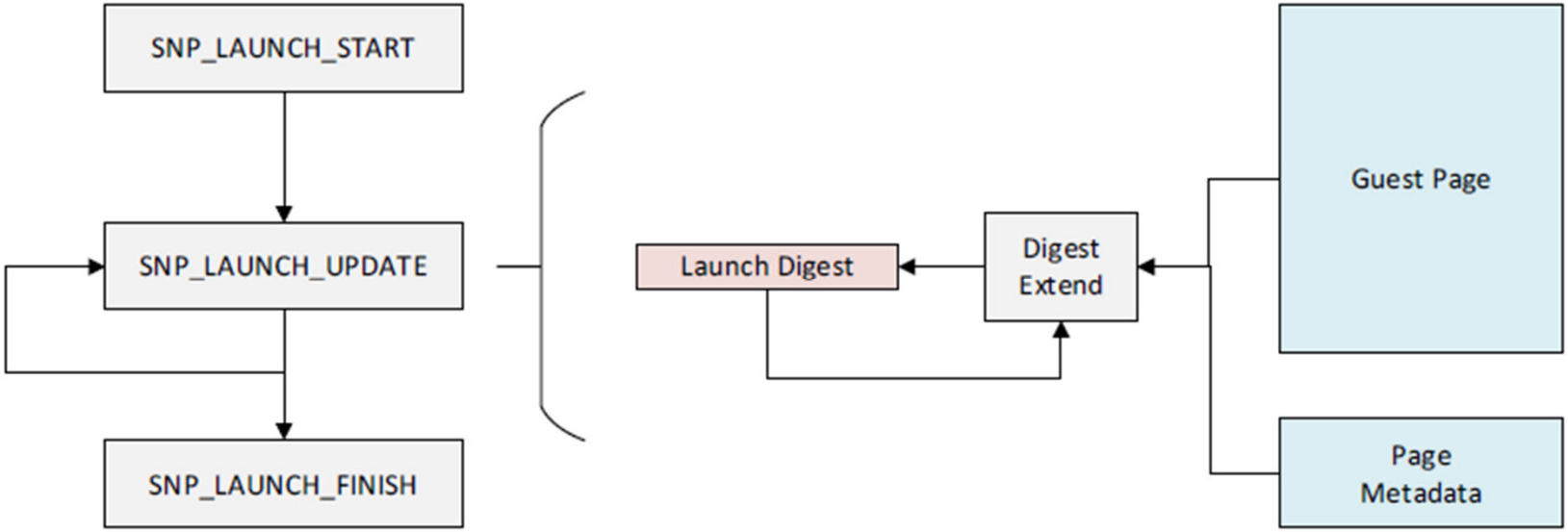
- SEV-ES で導入したVMSA (Virtual Machine Save Area)



Attestation Mechanisms for Trusted Execution Environments Demystified [arXiv22]

Attestation Report: Guest Measurements
アテステーションレポート: ゲスト計測

INSTITUTE of INFORMATION SECURITY



LD := Hash(LD || Page || Metadata)

(slight simplification)

計測されるのはVMの起動前。
つまり、BIOS・TPMのロードが計測される。

Attestation手順

INSTITUTE of INFORMATION SECURITY

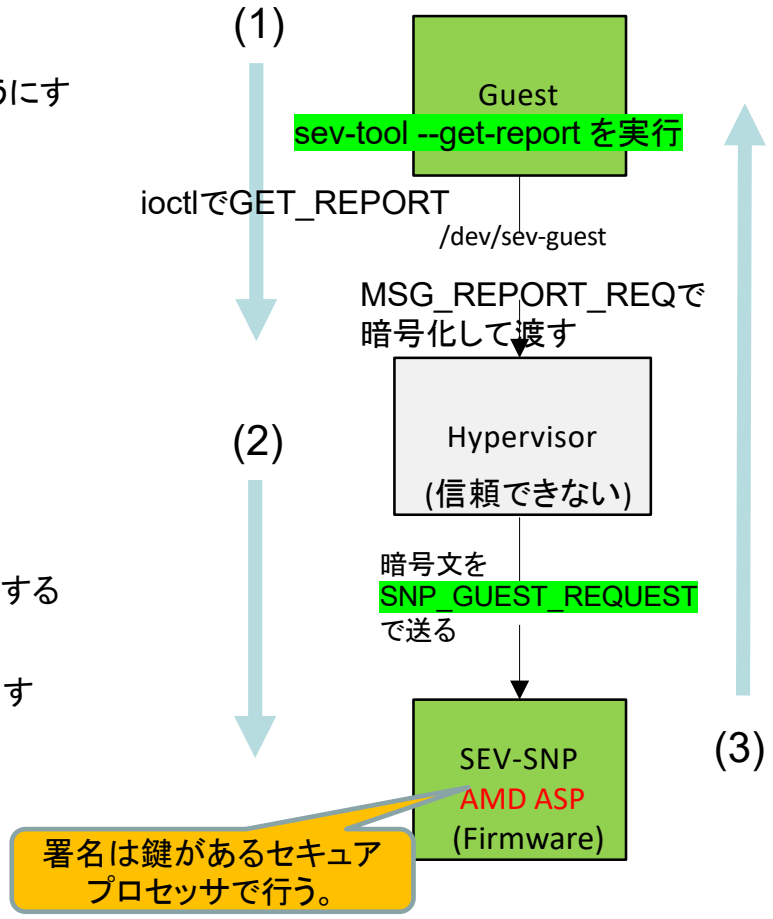
- AMD SEV-SNP
  - A) Attestationのための署名鍵が作られるまでの動作　(Provisioning)
  - B) バイナリロード時にAttestation用のデータ(Quote)を作るまでの動作 (VMの場合はGuestOS起動前)
  - C) Attestation時にCPUに由来する鍵でEvidenceを作るまでの動作

Retrieving Attestation Reports

INSTITUTE of INFORMATION SECURITY

■ アテステーションレポートの作成手順

- Linuxホストは/dev/sevのIOCTL経由で構成証明鍵証明書を提供できる (事前準備)
  - SNP_SET_EXT_CONFIG – 構成証明鍵証明書を保存し、/dev/sev-guestで取得できるようにする
- Linuxゲストは/dev/sev-guestのIOCTL経由でレポートを取得する
  - SNP_GET_REPORT – レポートを取得する
  - SNP_GET_EXT_REPORT – レポートと証明書を取得する
- 【手順】ゲストメッセージ経由でレポートを取得
  - (1)ゲストはMSG_REPORT_REQメッセージを構築
    - ゲストはゲスト起動時に共有された鍵を使用して***メッセージを暗号化***し、整合性を保護する
    - ゲストはラップされたリクエストをハイパーバイザーに送信する
  - (2)ハイパーバイザーはラップされたリクエストに対してSNP_GUEST_REQUESTを呼び出す
  - (3)SEV-SNPファームウェアは同じチャネル経由で構成証明レポートを返す



レポート作成命令

INSTITUTE of INFORMATION SECURITY

- GET_REPORT命令
  - Secure Processor の measurement を外部に証明書付きで取り出す
  - 作成されるAttestation Result
    - ◆Measurement Hash (LAUNCH_MEASURE で確定した値)
    - ◆ゲスト固有の情報 (Guest SVN, Policy, Family/Model/Stepping など)
    - ◆プラットフォーム情報 (Chip ID, TCB Version)
    - ◆AMD Chip Endorsement Key (CEK) による署名
- GET_EXT_REPORT命令
  - GET_REPORT命令の拡張版で証明書も付ける。

項目	GET_REPORT	GET_EXT_REPORT
主目的	ゲストの状態証明	ゲスト状態 + 証明書チェーンをまとめて提供
返却内容	Attestation Report のみ	Attestation Report + AMD証明書
検証に必要な外部要素	AMD 証明書を別途取得	追加不要（レポート内に含まれる）
主な用途	軽量・内部検証	クラウドでのリモートアテステーション（フル検証）

参照資料　SEV-SNP Platform Attestation Using VirTEE/SEV
https://www.amd.com/content/dam/amd/en/documents/developer/58217-epyc-9004-ug-platform-attestation-using-virtee-snp.pdf

Attestation Evidenceの作成と検証

https://knowledge.sakura.ad.jp/38508/

INSTITUTE of INFORMATION SECURITY

QEMUの起動

```
$ sudo qemu-system-x86_64 ¥
  -enable-kvm -cpu EPYC-v4 ¥
  -machine q35,confidential-guest-support=sev0,memory-backend=mem0 ¥
  -smp cpus=4 ¥
  -object memory-backend-memfd,size=8192M,id=mem0,share=true,prealloc=false,reserve=false ¥
  -object sev-snp-guest,id=sev0,cbitpos={cbit の値},reduced-phys-bits=1,init-flags=5,igvm-file=coconut-qemu.igvm ¥
  -no-reboot ¥
  -device virtio-scsi-pci,id=scsi0,disable-legacy=on,iommu_platform=on ¥
  -device scsi-hd,drive=disk0,bootindex=0 ¥
  -drive file=guest.qcow2,if=none,id=disk0,format=qcow2 ¥
  -netdev tap,id=nd0,ifname=tap0,script=no,downscript=no ¥
  -device virtio-net-pci,netdev=nd0 ¥
  -nographic ¥
  -monitor unix:/tmp/monitor.sock,server,nowait ¥
  -serial mon:stdio
```

起動後のAttestation Evidence作成

```
$ snpguest fetch vcek der milan certs report.bin
```

Reportに入るはずの値の計測

```
$ ./igvmmeasure coconut-qemu.igvm measure
================================================================================================================================
igvmmeasure 'coconut-qemu.igvm' Launch Digest:
A3A4D5E40A5D27FD5733930CC95813C861DD8D7077B12585E5E46F10192C679974B8B0AD5979F02E5867FEE41A576FCC
================================================================================================================================
```

Reoprt.binの中身

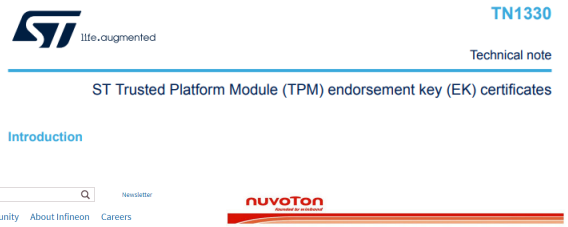
```
$ ./snpguest display report report.bin
---- (省略) ---- Measurement: a3 a4 d5 e4 0a 5d 27 fd 57 33 93 0c c9 58 13 c8 61 dd 8d 70 77 b1 25 85 e5 e4 6f 10 19 2c 67 99 74 b8 b0 ad 59
79 f0 2e 58 67 fe e4 1a 57 6f cc ---- (省略) ----
```

2nd Step: vTPM Attestation

- 1st Step: CPU rooted AttestationでvTPMがRemote Attestationで検証できる。
  - つまり、正しい仮想TPMとして確認できる。
- このvTPMをベースとしてVM内のOSのRemote Attestationを行う。
  - これは通常のOSで同じ。

- 注意点
  - vTPMは正しいかもしれないが、それを管理しているのはクラウドベンダー
  - vTPM内の鍵が正しいか不明。
    - ◆ハードウェアTPMの場合はTPMベンダーがEndorsement Keyの証明書を発行している。

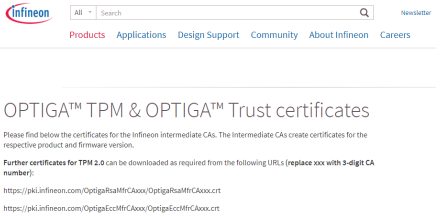
- ST Micro
  - https://www.st.com/content/ccc/resource/technical/document/technical_note/group0/aa/c5/c7/a2/61/9a/4d/13/DM00711714/files/DM00711714.pdf/jcr:content/translations/en.DM00711714.pdf
- Nuvoton
  - https://www.nuvoton.com/export/sites/nuvoton/files/security/Nuvoton_TPM_EK_Certificate_Chain.pdf
- Infineon
  - https://www.infineon.com/cms/en/product/promopages/optiga_tpm_certificates/

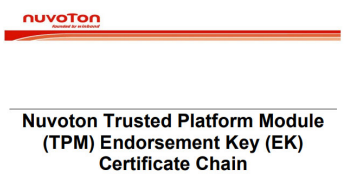

TN1330

Technical note

ST Trusted Platform Module (TPM) endorsement key (EK) certificates

Introduction


OPTIGA™ TPM & OPTIGA™ Trust certificates

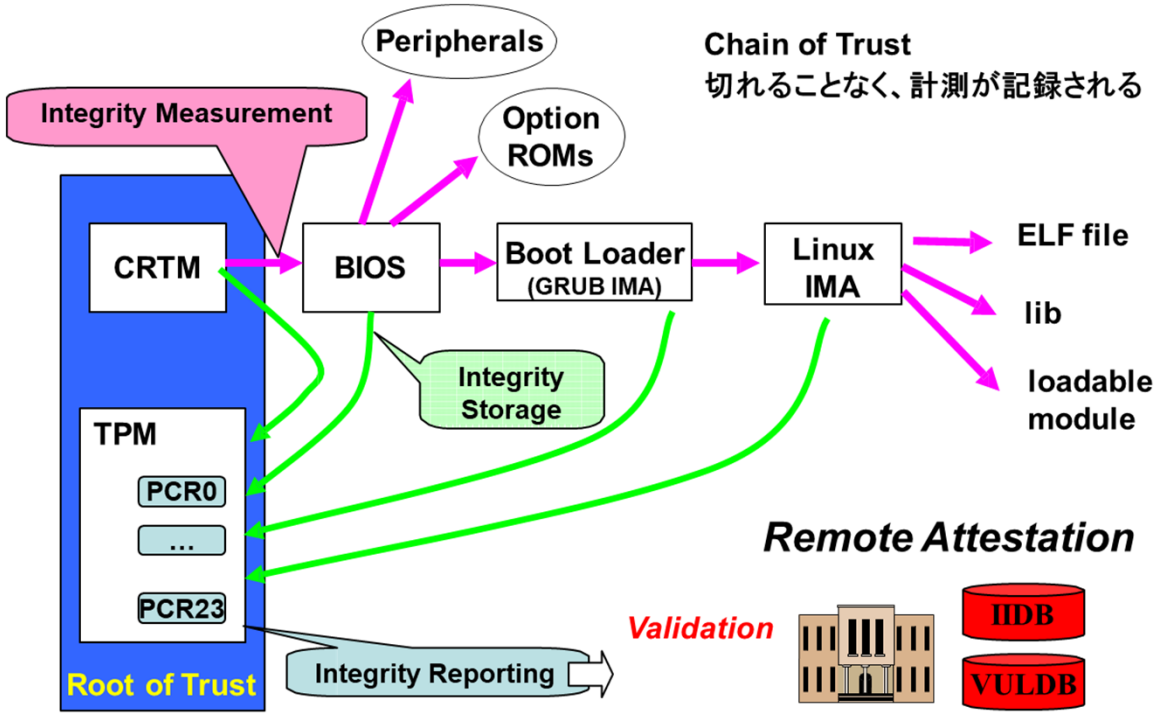

Nuvoton Trusted Platform Module (TPM) Endorsement Key (EK) Certificate Chain

2nd Step: vTPM Based Attestation

Trusted Boot と Remote Attestation

INSTITUTE of INFORMATION SECURITY

- TPM を基点とする高信頼な起動方法(Trusted Boot)
  - TPMはpassive deviceであり、TPM自体が能動的なセキュ リティを確保するものではない
  - 信頼できるソフトウエアからハッシュ値(SHA-1)をTPM内のPCR (Platform Configuration Register)にExtendする
  - 信頼できるソフトウェアはCRTM: Chain of Root of Trust Managementから始まり、Chain of Trustを作成する
  - **Chain of TrustのPCR値は外部の検証機関(Verifier)を通して、起動の完全性検 証が可能。(Remote Attestation)**



計測: Measurement

- 各デバイスやファイルは起動時に計測され、そのSHA1 digest をTPMのPCR (Platform Configuration Register)に “Extend” により記録する。
  - **Extend**
    - **PCR(i) = SHA1(PCR(i) +Digest)**
- PCR の利用法はTCGにより規格化されている。

TPM 1.1

PCR	Function
0	CRTM, BIOS, and Platform Extensions
1	Platform Configuration
2	Option ROM Code
3	Optional ROM Configurations and Data
4	IPL Code (Usually the MBR)
5	IPL Code Configuration and DATA (for use by the IPL code)
6	State Transition and Wake Events
7	Reserved for future usage. Don't use.
8-15	Flexible use

TPM 2.0

PCR Index	PCR Usage
0	SRTM, BIOS, Host Platform Extensions, Embedded Option ROMs and PI Drivers
1	Host Platform Configuration
2	UEFI driver and application Code
3	UEFI driver and application Configuration and Data
4	UEFI Boot Manager Code (usually the MBR) and Boot Attempts
5	Boot Manager Code Configuration and Data (for use by the Boot Manager Code) and GPT/Partition Table
6	Host Platform Manufacturer Specific
7	Secure Boot Policy
8-15	Defined for use by the Static OS
16	Debug
23	Application Support

Trusted Bootのログ

■ これはTPM1.2の例で古いですが、分かりやすいので使います。

– **/sys/kernel/security/tmp0/ascii_bios_mesurements**

PCR SHA1 Event

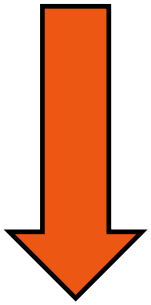
```
3 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
5 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
6 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
7 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 c1e25c3f6b0dc78d57296aa2870ca6f782ccf80f 05 [Calling INT 19h]
4 38f30a0a967fcf2bfee1e3b2971de540115048c8 05 [Returned INT 19h]
4 7ca42b22324927c400263bae94e1e7cc28655532 05 [Booting CD ROM]
4 5c3eb80066420002bc3dcc7ca4ab6efad7ed4ae5 01 [POST CODE]
4 1cdac212c5342627905cfcc4931972a8b4a09996 0d [IPL]/boot/grub/stage2_eltorito
4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []
4 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 f1f74d078d57197ee9cd9205995a6ba5e6a68cbf 0e [IPL Partition Data] /boot/grub/grub.conf
5 aed235d4ddb5fed00156f4991f2c1d1330c97694 1105 []
8 94c417906f8d383b811d918dce6bafdbc650ed42 1205 []  /boot/isolinux/linnux-ima
8 793eb4a591229afe35d60d5c2b66cee9dc33225c 1405 []  /boot/isolinux/minirt-ima.gz
5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 fac33a1fc0ad42c07d00322d64c23f67567f334a 1005 []
```

Measured files

確認してほしい課題

INSTITUTE of INFORMATION SECURITY

- Remote Attestation内でZero Trustに変えられるところ?
  - Quote?
    - ◆CPU・ハードウェア情報?
    - ◆バイナリ情報?
  - Verifier？
  - 署名鍵（Attestation Key）?
  - Hardware Root of Trust



難易度？

- Remote Attestation内で無くならないところ?
  - (予想)Hardware Root of Trustでの機密情報保護

ZTを使ったRemote Attestation

- TikTok Trustless Attestation Verification Circom
  - https://github.com/tiktok-privacy-innovation/trustless-attestation-verification-circom
  - Zero Knowledge ProofにCircomを使っている
  - Verifierを信頼せずにAttestation Resultが信頼できるようになる。
    - ◆信頼するものを少なくする。
  - ただし、SEV-SNP のVCEK（Versioned Chip Endorsement Key）の信頼チェーンは活用する。
    - ◆VCEKを通してこのチップ／ファームウェア構成が正規のものかを確認する。

Remote AttestationとZero Trust

INSTITUTE of INFORMATION SECURITY

既存のRemote Attestation

- Attester
  - Provisioning
    - 署名秘密鍵 (Root of Trustで保存が基本)
    - Verifierは絶対信頼
  - 構成情報(Quote)作成
    - Binary情報の計測
    - ハードウェア・CPU情報の確保
  - Attestation
    - 構成情報(Quote)に署名
- Verifier
  - Provisioning
    - 署名公開鍵 or 証明書
    - 正しい構成情報
  - Attestation

Zero Trustを適用したRemote Attestation

- Attester
  - Provisioning
  - 構成情報(Quote)作成
  - Attestation
- Verifier
  - Provisioning
  - Attestation

まとめ

- Remote Attestation要件
  - ① 署名鍵が耐タンパなハードウェアで守られている
  - ② 署名鍵を使うソフトや完全性(Hash)を計測するソフトは信頼できる
- TEEのRemote Attestationパターン
  - （一例）AMD SEV-SNPのVM型TEEのRemote Attestation
    1. CPUベースのAttestation (VM起動前)
       1. Provisioning (鍵の設定)
       2. Initial Measurement (VM起動前イメージ)
       3. Making Attestation Evidence (署名付Attestation Evidence作成)
    2. vTPMベースのAttestation (VM起動後)
- Remote AttestationとZero Knowledge (私見)
  - 何がZero Knowledgeでできるか？
  - TikTokのTrustless Attestation