明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

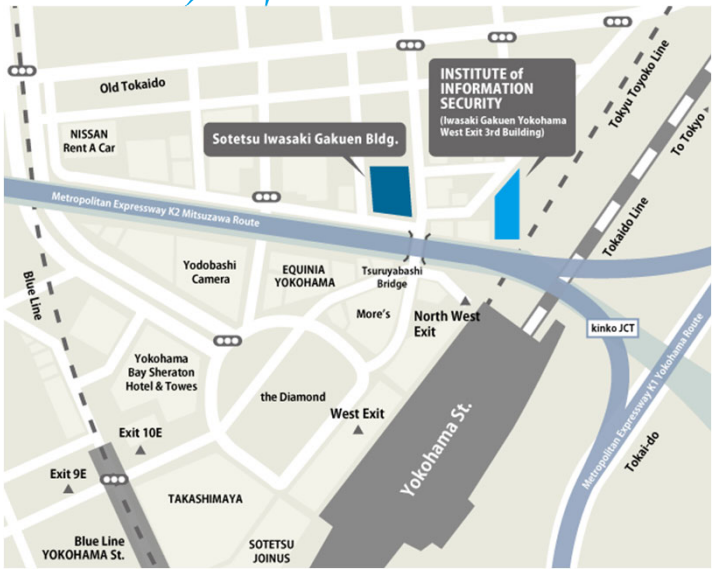
Security 101
Root of Trust と RISC-V TEE の概観

RISC-V Day Tokyo Autumn 2025
4/Dec/2025

IISEC: Institute of Information Security（情報セキュリティ大学院大学）
Kuniyasu Suzaki（須崎 有康）

Who am I ? (Kuniyasu Suzaki)

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

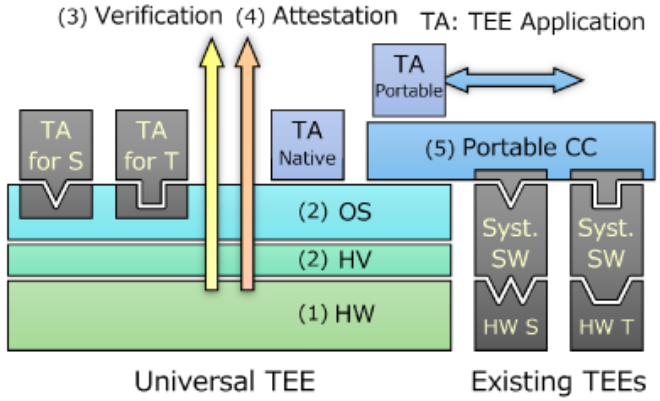


■ 情報セキュリティ大学院大学に　2022/9/1　着任

- 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(AIST)
  - ◆NEDOプロジェクト (2018-2023) RISC-V TEE の研究をセキュアオープンアーキテクチャ・エッジ基盤技術研究組合 TRASIO で行う

■ 現在のプロジェクト

- 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
  - ◆**Cloud(Azure, AWS, GCP)のConfidential Computing(Intel SGX, TDX, AMD SEV-SNP, AWS Nitro)で使えるRemote Attestation Sample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

- Why do we need hardware security?
- Hardware based Security
  - TEE (Trusted Execution Environment)　機密処理を隔離して安全に実行する。
  - Remote Attestation　隔離実行が意図したものであるかを確認する。
  - Root of Trust　Remote Attestationの信頼の起点となる。
- RISC-V Status
- Community/Standard/Certificate
- Conclusion

Why do we need hardware security?

■ データはどのような状態でも保護されなければならない。

種類	データがある場所	対処技術
Data at Rest（保存データ）	ストレージ（SSD,HDD）	Full Disk Encryption, BitLocker, dm-crypt
Data in transit（転送中のデータ）	ネットワーク上の移動（Internet）	TLS, SSH
Data in use（使用中のデータ）	Memory, Cache, Register	TEE, Hardware Root of Trust

■ Memoryは覗き見られる。Memory Forensicsなど。

■ Cacheの覗きはSpectre/Meltdownで実証済み。

■ RegisterもContext Switchする際にメモリに置かれるので覗き見できる

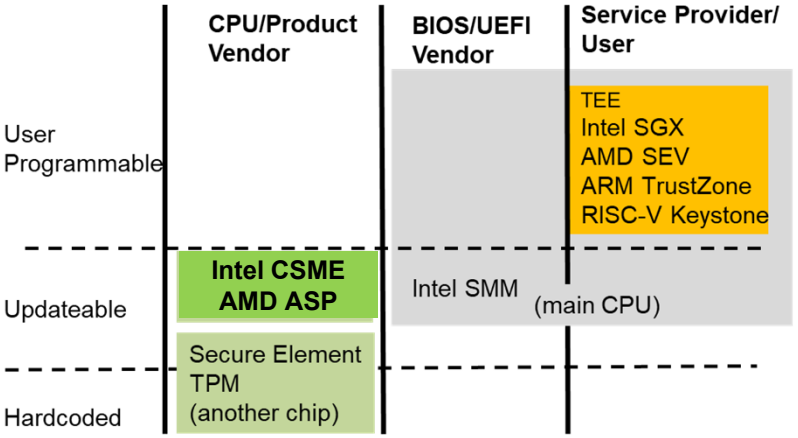
- “Analysis of Encryption Key Zeroization from System-wide Perspective”, ACSAC 2025でFPGAによる高速メモリ覗き見を発表します。

■ 覗き見されない仕組み

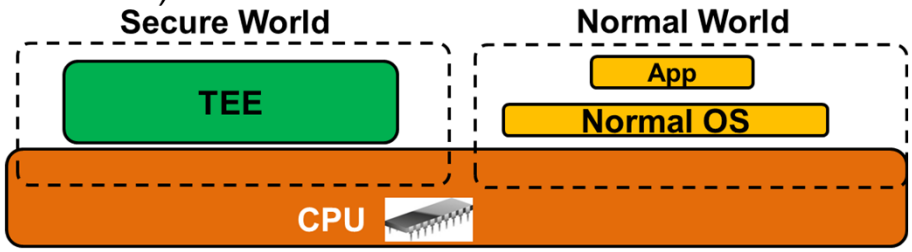
- TEEではアクセス制御／メモリ暗号。しかし、Cacheは共有されている脆弱性がある。
- Hardware Root of Trustでは耐タンパーハードウェアで保護。

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

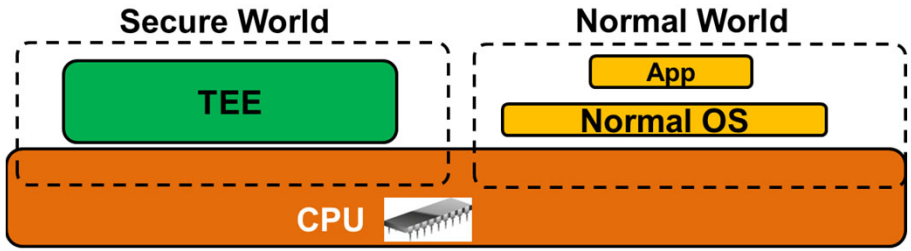


この図はあくまでTEEの一例

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?)



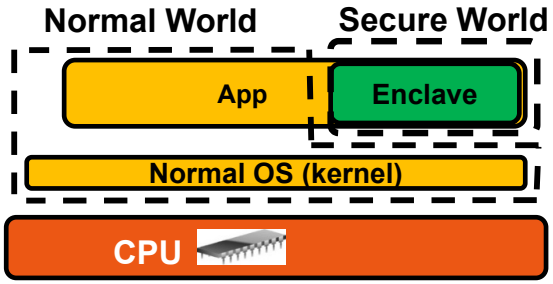
この図はあくまでTEEの一例
（Arm TrustZoneが一番近い）

■ 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 TEE/Confidential Computing

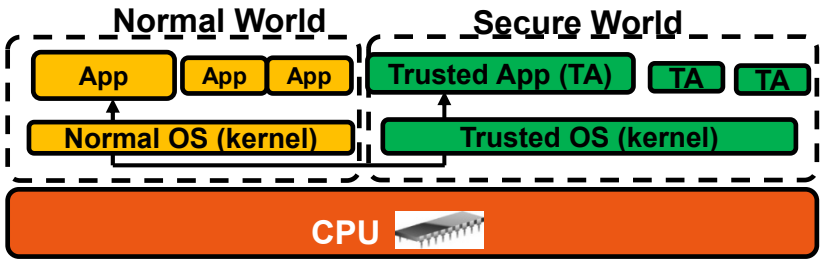
Library Type

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



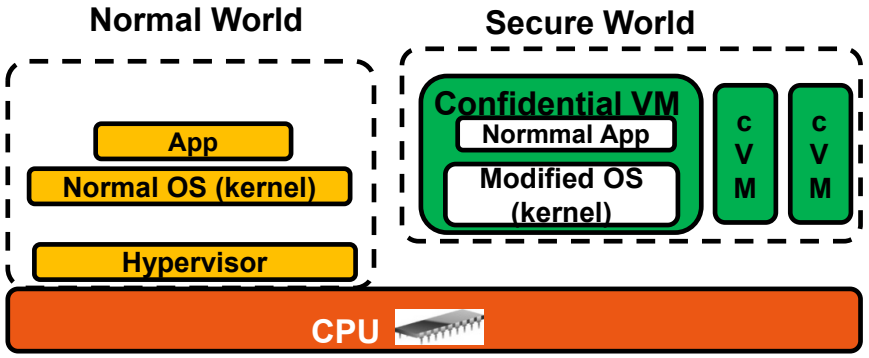
Process Type

- 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 (Confidential Computing)

- 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

	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 SEV (EPYC)					Azure, GCP, etc
AMD PSP			Playstation5		
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。

RISC-V?

サーバでのキラーアプリ候補？

RISC-V TEE

- TEE based on RISC-V

Academia
- Sanctum [MIT,USENIX Sec'16]
- TIMBER-V [Graz University of Technology, NDSS'19]
- MI6 [MIT,MICRO'19]
- Keystone [UC Berkeley, EuroSys'20]
- HECTOR-V [Graz University of Technology, arXiv'21]
- uTango [University of Minho, arXiv'21]
- Cure [Darmstadt University of Technology, USENIX Sec'21]
- CHERI-TrEE [University of Cambridge, IEEE S&P'23]
- Penglai [Shanghai Jiao Tong University, EuroSys'21]
- HPMP (Hybrid Physical Memory Protection) [Shanghai Jiao Tong University, MICRO'23]

Industry
- MultiZone [HexFive]
- SiFive Shield / World Guard [SiFive]
- AP-TEE（Application Processor –TEE) [RISC-V International TEE WG]
- CoVE (Confidential Virtual Machine for RISC-V) [Rivos Inc., arXiv'23]
  - ◆ RivosがMetaに買収される [2025/10]

VM Type TEE

TEEは信頼できるか？

- 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)

- Remote AttestationではIntegrityを確認する

Remote Attestation is NOT for TEE only

- インターネットは信頼できる？「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

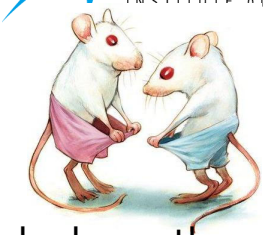
- これではインターネットで商取引ができないが、解消するために個人認証、サーバ認証などの技術(TLS)が進んだ。

- 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である

- 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.
- 最近はTLSにRemote Attestationを入れる研究が進んでいる。

Remote Attestation

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



RATS Logo

■ IETF RFC 9334 RATS(Remote Attestation ProcedureS)

- **Attester（信頼したいデバイス。証拠を渡す。証拠には署名秘密鍵で署名を付ける）**

  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（デバイスから情報を取りたい、あるいは情報を渡したい）**

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

- **Verifier正しいデバイスやソフトを知っている機関。証拠を判断する。署名公開鍵で検証。）**

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

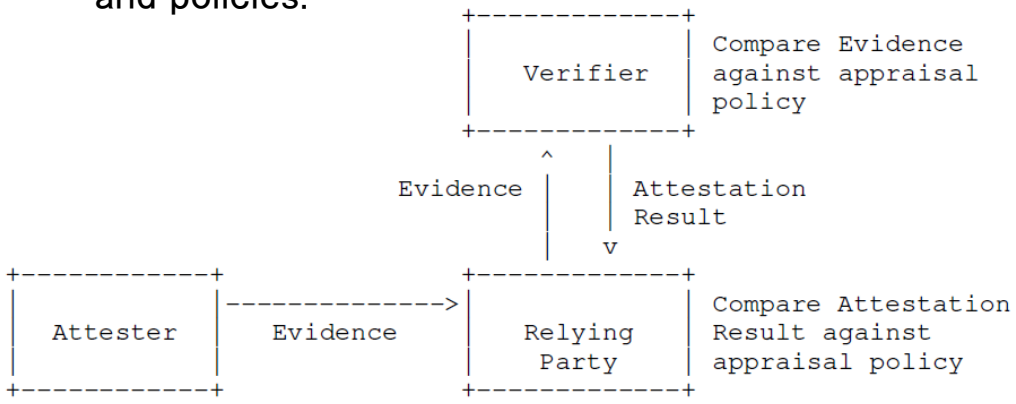
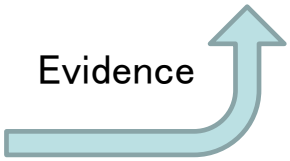


Figure 6: Background-Check Model

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

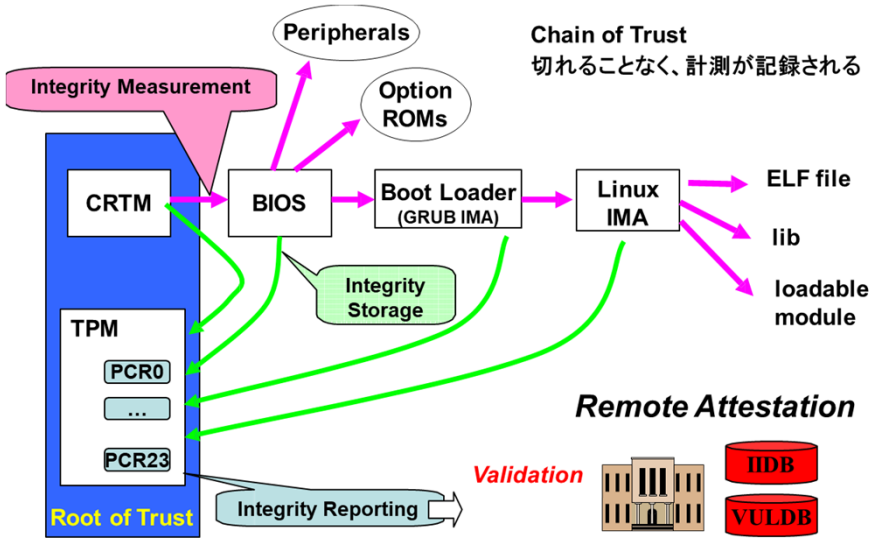
③ Verifier has the certificate of Attestation Public Key and reference values (ex: hashes of applications).
Verifier judges the Evidence with them and send the result.

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



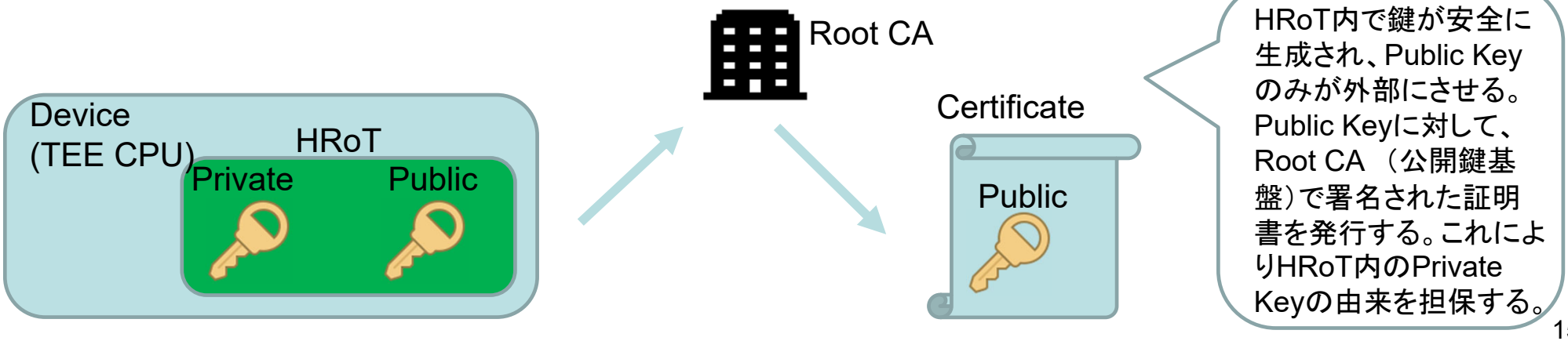
Attestationの種類

- Key Attestation (鍵構成証明)
  - 鍵がHRoT内に保存されている
- ID Attestation (ID構成証明)
  - IDがRoT内に保存されている
- Platform Integrity Attestation (プラットフォーム構成証明)
  - TEEではTEEが信頼できるハードなのか、意図したソフトウェアなのかの確認
  - TPMではTrusted Bootしたことの証明



Remote Attestationに必要な鍵

- Remote AttestationではEvidence（証拠）に対して、正しいことを保証する署名を付ける。
- 署名にはAttestation Key（Private/Public）をベースとする。
  - 署名の秘密鍵（Private Key）は個別のデバイスで安全に守れている。
  - 署名の公開鍵（Public Key）は公開鍵基盤(PKI)で証明書(Certificate)を取っていることが多い。
    - ◆Remote AttestationのVerifierに登録される。
- 鍵を安全に管理するためにTEEを有するCPUやTPMではHardware Root of Trust (HRoT)が求められる。



Hardware Root of Trustの要件

- 信頼の基点 (Verifiable Origin)
  - 攻撃者が介入する前に全体の信頼基点となる。鍵を設定するプロビジョニングが安全であること。
- 耐タンパ性 (Tamper Resistance)
  - 攻撃者が物理的にアクセスしても内部情報が得られない設計。
- 鍵管理の安全性 (Secure Key Management)
  - 安全に生成・格納・アクセス制御 できること。
- 識別と認証 (Device Identity)
  - デバイス固有 ID を持ち、外部に対して信頼性を証明可能。

- 秘密鍵を担保するためにデバイスが安全であることFIPS140を取っている。
  - FIPS140とは米国政府調達のための暗号セキュリティモジュール
- 公開鍵に対してベンダーはPKIベースの証明書を発行してもらう。
  - CPUベンダーはRoot CAの証明書を公開。

Current TEE CPU Vendor offers certificate

- 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

- 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

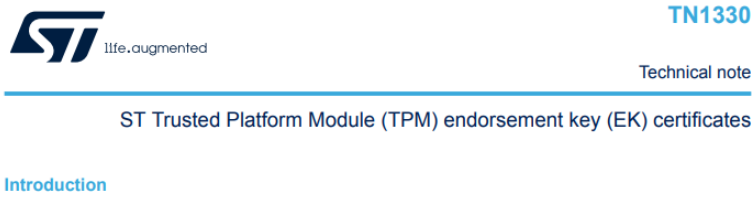
TPM FIPS140 and Root Certificate

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date	Status
5057	Nuvoton Technology Corporation	Nuvoton NPCT7xx TPM 2.0 Cryptographic Engine	Hardware	09/15/2025	Active
4737	STMicroelectronics	Trusted Platform Module ST33KTPM2XSPI / ST33KTPM2X / ST33KTPM2A / ST33KTPM2I	Hardware	07/25/2024	Active
4702	STMicroelectronics	Trusted Platform Module ST33KTPM2XSPI / ST33KTPM2XI2C	Hardware	06/04/2024	Active
4686	Microsoft Corporation	Virtual TPM	Software-Hybrid	04/03/2024	Active
4622	Nuvoton Technology Corporation	NPCT7xx TPM 2.0 rev 1.38	Hardware	10/02/2023	Active
4537	Microsoft Corporation	Virtual TPM	Software	06/20/2023	Active
4411	Nuvoton Technology Corporation	NPCT7xx TPM 2.0 rev 1.59	Hardware	01/12/2023	Active

Microsoft!

- 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/


life.augmented

TN1330

Technical note

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

Introduction

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

OPTIGA™ TPM & OPTIGA™ Trust certificates

Please find below the certificates for the Infineon intermediate CAs. The Intermediate CAs create certificates for the respective product and firmware version.

Further certificates for TPM 2.0 can be downloaded as required from the following URLs (**replace xxx with 3-digit CA number**):

https://pki.infineon.com/OptigaRsaMfrCAxxx/OptigaRsaMfrCAxxx.crt

https://pki.infineon.com/OptigaEccMfrCAxxx/OptigaEccMfrCAxxx.crt

RISC-V Hardware Root of Trust *this table is not complete.

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

	Commercial		Open	
	Rambus RISC-V CryptoManager	Silex Insight (Secure IC) eSecure	Open Titan	Caliptra
Core	Custom (RV32IMC) M/S/U Mode	Andes N22 (RV32IMAC/EMAC) M or M/U mode	lowRISC Ibex (RV32IMC/EMC) M/U Mode	Custom (RV32IMC) M mode
OS	Zephyr	---	Tock OS	Caliptra Firmware
Comm to Main	GPIO/SPI	---	SPI	Mailbox
Accelerator	AES, SHA Timer, RNG	AES, SHA RNG	AES/SHA/ECC/HMAC Timer, RNG	SHA/ECC/HMAC Timer, RNG
Anti-tampering	Yes	Yes	???	???
Target	Key Management, Secure Boot	Key Management, Secure Boot	Key Management, Secure Boot	Key Management, Secure Boot, Attestation
Misc.	FIPS 140-2 Level 2 FIPS 140-3 Level 2	FIPS 140 2 level 3 PUF for Unique Key	Data Center, etc.	SoC based on Open Compute Project

Hardware Security関連組織・規格

- GlobalPlatform
  - TEE関係のAPI規格。スマートフォンで採用が多い。
  - Secure Element規格。スマートフォンで採用が多い。
  - 認証制度：SESIP: Security Evaluation Standard for IoT Platforms
- TCG (Trusted Computing Group)
  - TPM (Trusted Platform Module) PC/Server向け
  - DICE (Device Identifier Composition Engine)　組込み向けAttestation
  - MARS (Measurement and Attestation RootS)　組込み向けAttestation
- FIPS (federal information processing standards) 140　米国政府調達基準
- Arm PSA(Platform Security Architecture) Certificate
- IETF Protocol
  - TEEP: Trusted Execution Environment Provisioning
  - RATS: Remote Attestation Procedures
- CCC: Confidential Computing Consortium

まとめ

- ハードウェアベースセキュリティ。
  - TEE (Trusted Execution Environment)　機密処理を隔離して安全に実行する。
  - Remote Attestation　隔離実行が意図したものであるかを確認する。
  - Root of Trust　Remote Attestationの信頼の起点となる。
- RISC-V の状況
- 関連組織・規格

- Cloud(Azure, AWS, GCP)のConfidential Computing(Intel SGX, TDX, AMD SEV-SNP, AWS Nitro)で使えるRemote Attestation Sample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