「IETF 105 での TEEP の動向」

National Institute of Advanced Industrial Science and Technology(AIST)

National Institute of
Advanced Industrial Science
and Technology
AIST

Akira Tsukamoto, Kuniyasu Suzaki

2019/08/30

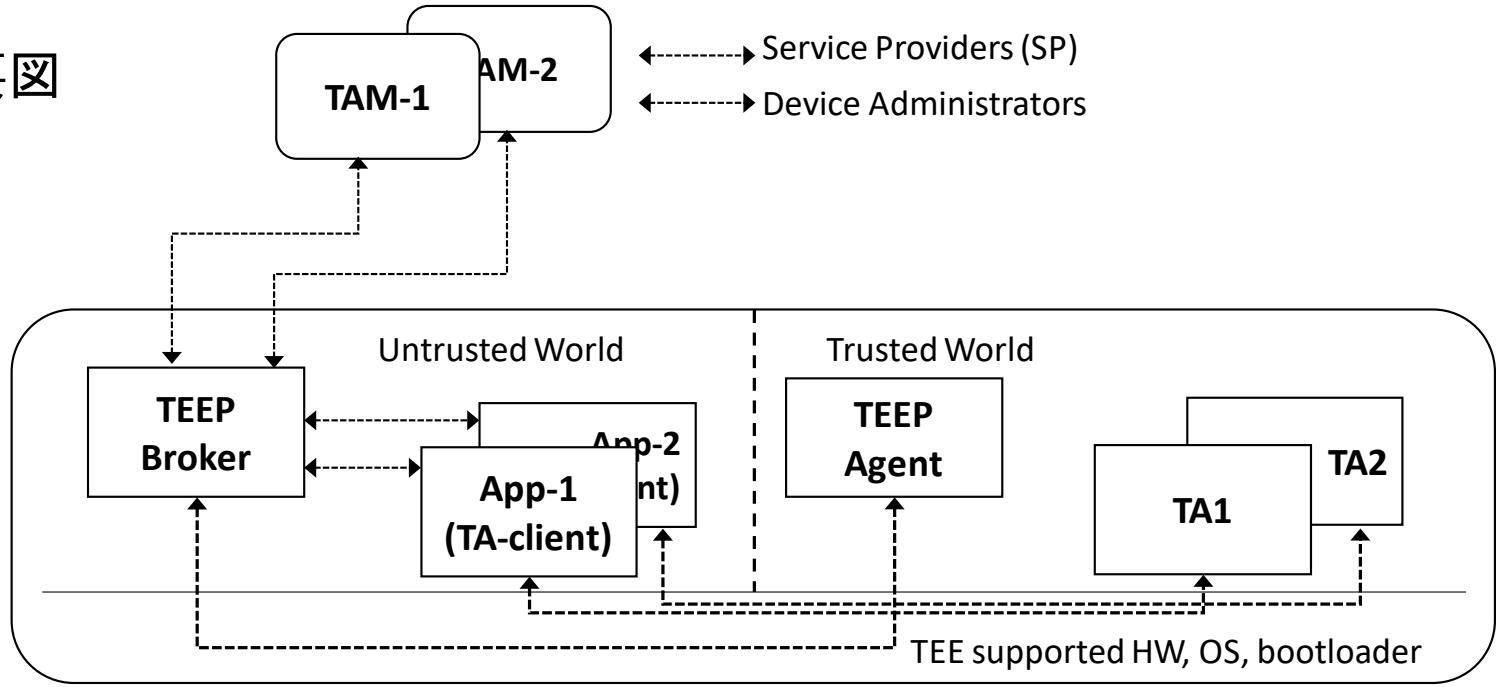
目次

- TEEP とは
- TEEP での OTrPの関係
- 前回の IETF 104 から 105 の間の進捗
- TEEP Hackathon とセッションの議論と進捗
  - OTrPv2 の変更点
  - RATS WG との協業について
- 次回の IETF106 に向けて
- まとめ

Trusted Execution Environment Provisioning(TEEP) とは

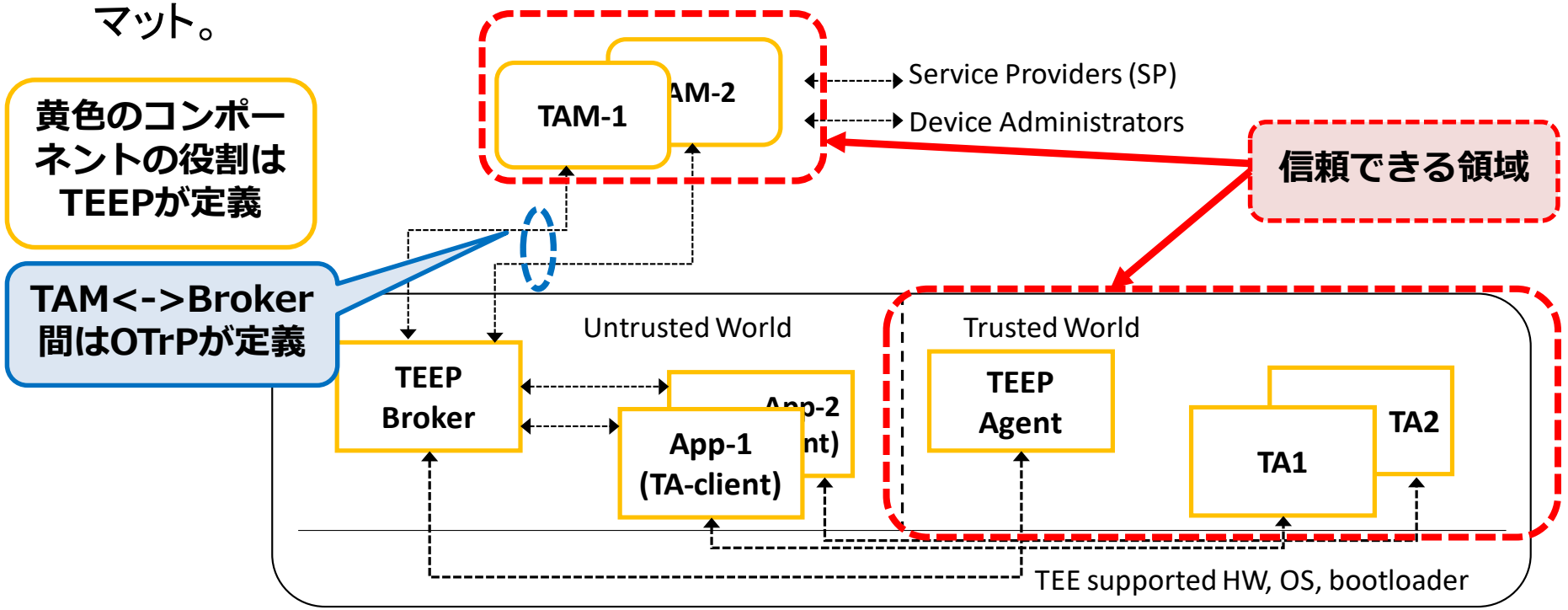
- 信用できないかもしれないデバイスで、Service Provider が開発したTrusted Application (TA)をインストール・ 実行・削除（TAのライフサイクル管理）のセキュリティーを担保する方式の定義と標準化を目的としている。
- 本目的のためにハード的に TA を隔離実行できるTrusted Execution Environment (TEE) 機能を活用する。

概要図



TEEP と OTrPの各ドラフトの関係

- TEEP のドラフトと OTrP (Open Trust Protocol) のドラフトを策定している
  - TEEPのドラフトで策定するのは、TAM(Trusted Application Manager), TEE broker, TEE Agent, App, TA などの役割。下図のボックス部分
  - OTrPのドラフトで策定するのは上記のTAMとTEEP Broker間がやり取りするバイナリーフォーマット。



前回の IETF 104 から 105 までの間

- ドラフト OTrPv2 が大幅更新
  - 111ページから、トータル18ページに削減
  - メッセージフォーマットを簡略化
    - OTrPで大きなページをしめていた Secure Domain に関するメッセージが削除された。
    - Query Request, TrustedAppInstall, TrustedAppDelete の3メッセージのみに。
    - TEE が複数ある場合の記述がなくなった。
- ドラフト TEEP に微修正
  - TEEP Agent が追加される

- 変更理由の背景
  - Secure Domain の削除は Intel SGX で TEEP の実装を容易にするため。また、Secure Domain の用途があまりない。
  - TEEPでTEE に追加で求められる機能(JSON, CBORパーサー機能など)を、TEEP Agent に機能追加分を担当させることで実装を容易にするため。TEE自体を拡張せずにすむ。

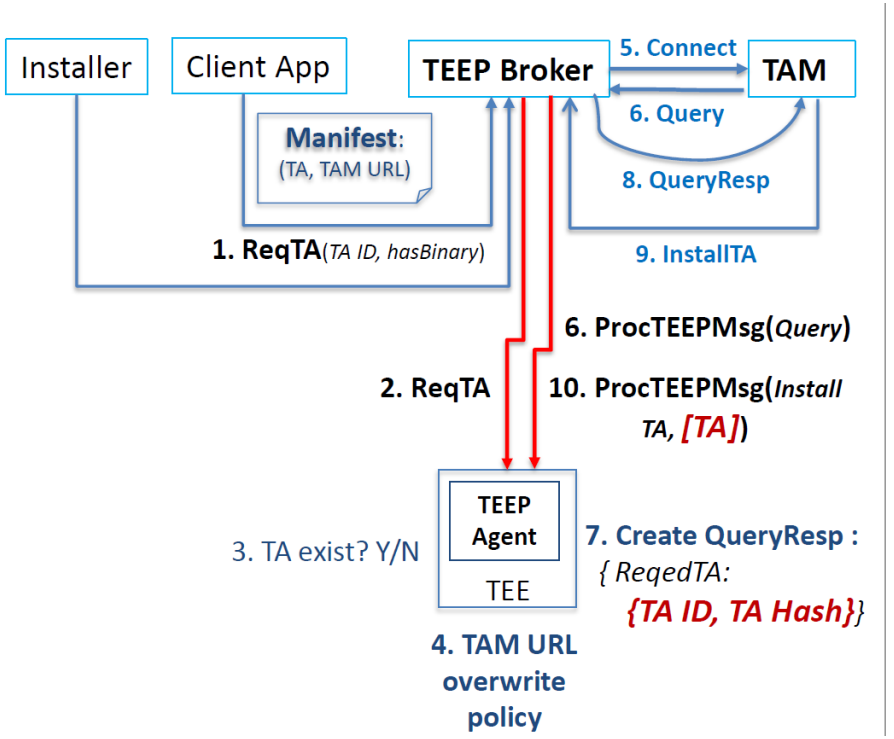
TEEP Hackathon とセッションの主な参加者

- IETF 105 TEEP 参加者
  - Dave Thaler (Microsoft)　TEEP WG の Chair, Open Enclave 開発リーダー
  - Mingliang Pei (Symantec)　teep-draft の Author
  - Hannes Tschofenig (ARM)　teep-draft の Author
  - Henk Birkholz (Fraunhofer SIT)　RATS WG の立場で参加
  - Dave Wheeler (Intel)　RATS WGがメインだが、今回 Intel版 TEEP を担当
  - 磯部さん（セコム）
  - 須崎、塚本（産総研）

- 土曜日と日曜日の Hackathon に主要メンバーが全員集まる

Hackathon とセッションでの議論と成果 (1/4)

- TEEP のTAのライフサイクル管理のシーケンスについて明確化
  - TEEP と OTrPのドラフトを読んだだけでは、どのようなステップで TA がインストールされるか判断が付きにくい。
  - IETF のドラフトでよくみられるシーケンス図が少ない。
  - 産総研とMingliang Peiで議論してシーケンスを明確化。
  - TEEP セッションの資料に反映

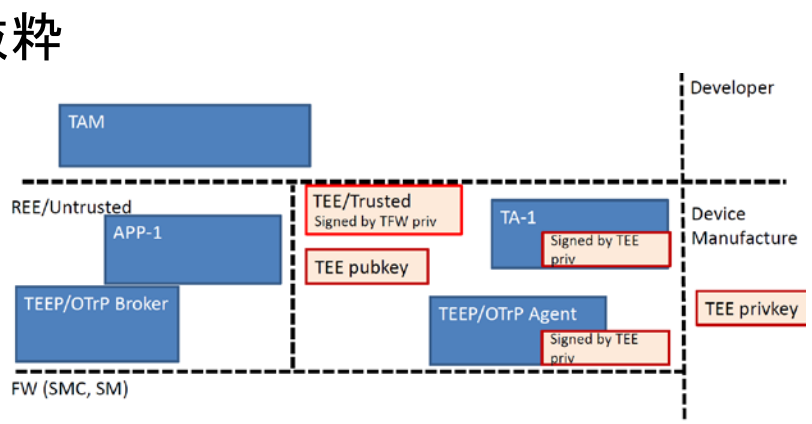


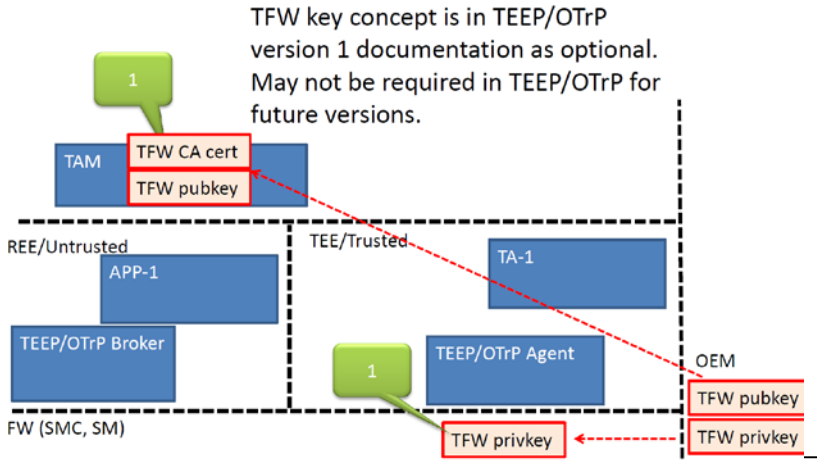
- TEEP セッション資料、ページ11
- https://datatracker.ietf.org/meeting/105/materials/slides-105-teep-sessa-teep-architecture-draft-00

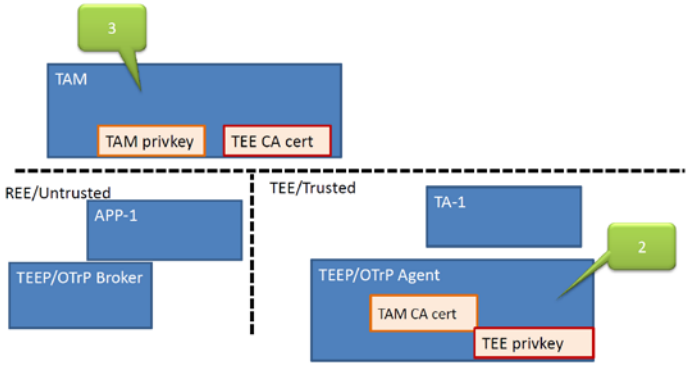
Hackathon とセッションでの議論と成果 (2/4)

- 鍵、証明書、CA について明確化
  - TEEP のドラフトのページ19 Figure 5に、TEEP実装時の各コンポーネントが保持すべき鍵と証明書とCAの図があるが、各々の具体的な明示がなかった。
  - TEEP で必要とされる鍵と証明書とCAの一覧表がページ21 Figure 6にあるが単語が上記の表とすべて一致しておらず照らし合わせが困難。
  - 産総研と磯部さん(セコム)とDave ThalerとHannes Tschofenig で実装時の位置を明確化。
  - TEEP セッションの資料に反映。月曜日のTEEPセッションで塚本が発表。
    - https://datatracker.ietf.org/meeting/105/materials/slides-105-teep-sessa-otrp-locations-of-keys

抜粋

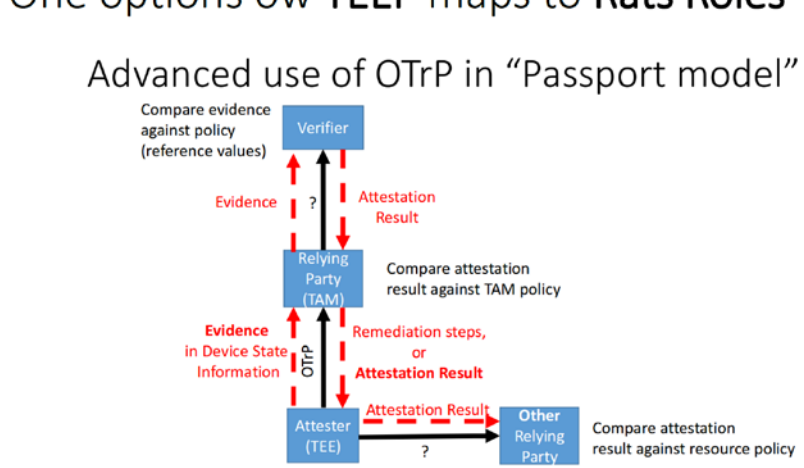






Hackathon とセッションでの議論と成果 (3/4)

- TEEP WGと RATS WG の協業
  - IETF では RATS WG にてリモートアテステーションが検討されている。TEEPで独自のリモートアテステーション方法を策定するのではなく、RATS WG の検討結果を活用することになった。
  - 一番のポイントであるリモートアテステーションの Verifier として働くコンポーネントを、TEEP の構成でどこの位置にするかについて議論が進んだ。
  - Dave Thalerと Henk Birkholz がメインとなり、RATSのセッションの資料に反映。
    - https://datatracker.ietf.org/meeting/105/materials/slides-105-rats-sessb-rats-architecture-interaction-model-challange-response-yang-module-information-module



Hackathon とセッションでの議論と成果 (4/4)

- その他の議論
  - ta-id について明確化
    - TEEP では TA のバージョン管理を行う。OTrPv2 のドラフトのページ7にOTrP メッセージの ta_id の記述がある。TAの名前情報のみ格納するようになっておりバージョン情報がない。
    - hash 値やバージョン情報の追加を検討することに。
  - 用語の統一
    - いままで TEEP と OTrP のドラフトでは、TEEP Brokerと OTrP Boker など同じコンポーネントがが二つのドラフトで別の名前になっていた。今回の顔合わせで TEEP Brokerのように接頭語は TEEP に統一することに。
  - Intel SGX に対する配慮
    - 今回のIETF 105に向けて更新されたTEEPドラフトでは Intel SGX での実装時の例などが明示的に記述された。それまでのTEEPのドラフトはARMで使われている Global Platform 準拠のTEEの議論に強く影響を受けている印象があった。そのため Intel SGXで TEEP を実装の困難が予想されたが改善中である。RATS WG のDave Wheeler (Intel)が議論に参加された影響が大きい。
  - SUIT WG との協業
    - パッケージ名やバージョン情報などのTAの manifest ファイルにSUIT WG の成果を使うことになっている。OTrPv2 に SUIT フォーマットが追加された。

次回の IETF106 に向けて

- プロトタイピングの活発化
  - Dave Thalerが率いるチームは TEE 上でデバッグなどを行える開発環境を MS Visual Studio で実現する Open Enclave プロジェクトを進めている。8月21日にIntel, Microsoft, Red Hatを主要メンバーとするコンソーシアムである Confidential Computing Consortium (CCC)を Linux Foundation で立ち上げた。CCCはIoT以外にデータセンターやPC領域でもTEEの活用範囲を広げることを意図しており、TEEPの技術開発が活発化すると予想される。
- リモートアテステーションのプロトコルの詳細化
  - RATS WGとはまだ基本構成でしか同意できておらず、プロトコルの詳細の議論を進める必要有り。
  - 09/10 にテレコンによる TEEP と RATS の合同による Virtual meeting を予定。
- OTrPv2のフォーマットのブラッシュアップ
  - 今回の大幅改訂でCBOR のみのフォーマットになってしまった。JSON対応が必要。すでに議論中。
  - OTrPv2 でSUIT フォーマット対応の詳細化。

まとめ

- TEEP の策定が大きく前進した。TEEP のメッセージプロトコルである OTrPv2 の策定が始まり、CPUの違いに依存しにくくなり、Security Domain 機能などが削除され実装も簡素化することになった。

- TEEPで必要なリモートアテステーション機能について RATS WG と実務的な議論が始まった。SUIT WG の成果はほぼそのまま活用する方向に。

- 前回の IETF 104 は初参加であり人とのネットワーク作りから始めることになったが、IETF 105 では鍵・証明書・CAの位置の議論など産総研の TEEの研究開発に必須な事項の議論をほかのメンバーと一緒に進め発表することができた。

- この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（ＮＥＤＯ）の委託業務「高効率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発/革新的AIエッジコンピューティング技術の開発/セキュアオープンアーキテクチャ基盤技術とそのAIエッジ応用研究開発」の結果得られたものです。

用語集

- IETF - Internet Engineering Task Force
- TEEP - Trusted Execution Environment Provisioning
  - https://datatracker.ietf.org/doc/draft-ietf-teep-architecture/
- OTrP - Open Trust Protocol
  - https://tools.ietf.org/html/draft-tschofenig-teep-otrp-v2-00
- TEE - Trusted Execution Environment
- リモートアテステーション – Remote Attestation
- CA - Certificate Authority
- RATS - Remote ATtestation ProcedureS
  - https://datatracker.ietf.org/wg/rats/documents/
- SUIT - Software Updates for Internet of Things
  - https://datatracker.ietf.org/wg/suit/about/
- JSON - JavaScript Object Notation
- CBOR - Concise Binary Object Representation
  - https://datatracker.ietf.org/doc/rfc7049/
- Intel SGX (Software Guard Extensions)
- ARM TrustZone
- Global Platform