PKIとトラスト

Attestationの観点から

PKI 相互運用性技術WG　伊藤忠彦（セコム株式会社）

本日の目次

- PKI相互運用技術WGの活動についてのご紹介
- 「Attestation」とは？
  - IETFにおける「Attestation」
  - AttestationとCertification
  - EAAにおけるAttestationとCertification
  - 何故、今Attestationが盛り上がっているのか？（考察）
- トラストのモデルを理解する上で、意識した方が良さそうな用語の使い分け
  - Acknowledgement、Confirmation、Validation、Vetting、Inspection
  - AuditとAssessment
- その他、考察（時間があれば）

PKI相互運用性技術WGの活動

■情報交換を目的に、報告会を開催（年3回程度）
- ■2025年1月23日　IETF121参加報告会
- ■2025年5月28日　IETF122参加報告＋CAB開催報告＋NIST Agility Workshop発表報告会
- ■2025年9月　2日　IETF123報告会

■発表内容
- ■IETF全体報告・初参加報告・ハッカソン報告
- ■Web PKI関係の動向報告
- ■暗号アルゴリズム/プロトコルの標準化に関する報告
- ■TEEP / Remote Attestation 関係の活動報告
- ■PQC関連報告（最近は、全体の半分くらいがPQC関連）

参加をお待ちしております。

IETFにおけるAttestation（1）

■（device）Attestation

■Attestation: the process of generating, conveying and appraising claims, backed by evidence, about device trustworthiness characteristics, including supply chain trust, identity, device provenance, software configuration, device composition, compliance to test suites, functional and assurance evaluations, etc.

■draft-ietf-rats-tpm-based-network-device-attest-14

■（日本語機械翻訳）証拠に基づいて、デバイスの信頼性に関する特性（サプライチェーンの信頼性、アイデンティティ、デバイスの由来、ソフトウェア構成、デバイス構成、テストスイートへの適合性、機能および保証評価など）についての主張を生成し、伝達し、評価するプロセス。

※ Device Attestationを前提とした定義

※ 対象となる機器が信用できるか評価するためのもの、機器に対するAttestation

IETFにおけるAttestation（2）

- Remote Attestation
  - In Remote ATtestation procedureS (RATS), one peer (the "Attester") produces believable information about itself ("Evidence") to enable a remote peer (the "Relying Party") to decide whether or not to consider that Attester a trustworthy peer. Remote attestation procedures are facilitated by an additional vital party (the "Verifier").
  - RFC 9334 - Remote ATtestation procedureS (RATS) Architecture

  - （日本語機械翻訳）Remote ATtestation procedureS（RATS）においては、あるピア（Attester）が、自身に関する信頼できる情報（Evidence）を生成し、リモートのピア（Relying Party）がそのAttesterを信頼できるピアと見なすかどうかを判断できるようにします。リモートアテステーション手続きは、もう一つの重要な関係者（Verifier）によって支援されます。

- IETFでは相手を信頼するために利用するM2Mの仕組みをAttestationと呼んでいる。

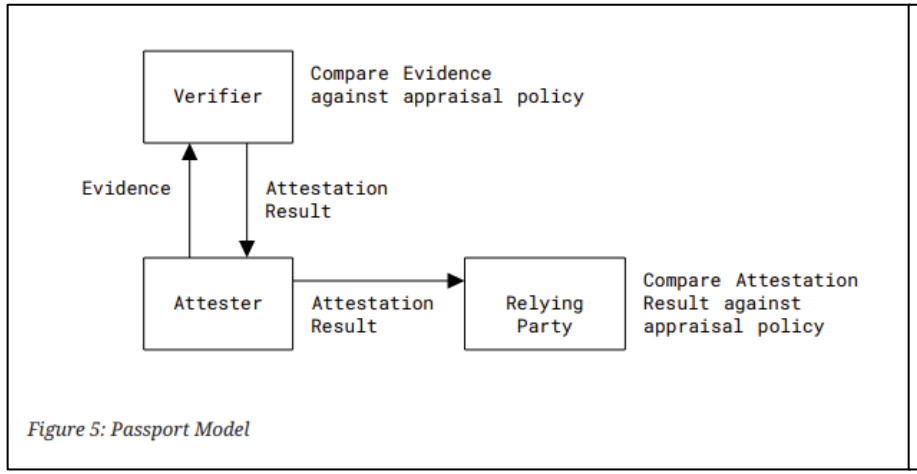


Figure 5: Passport Model

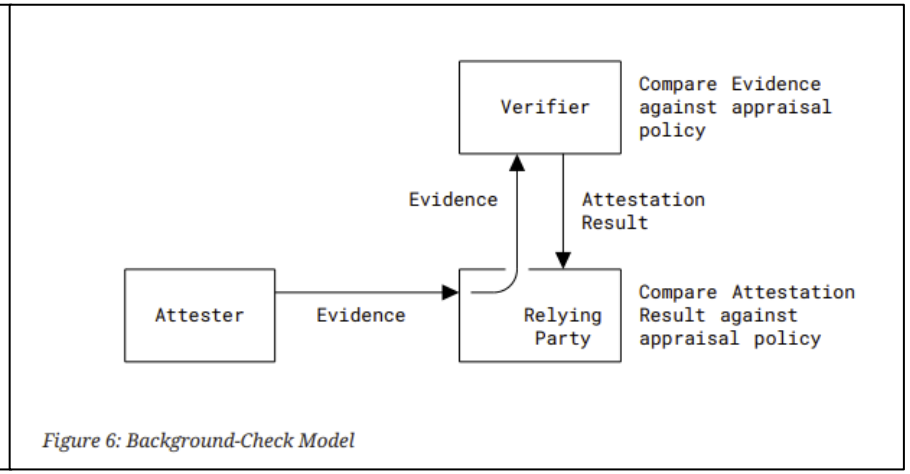


Figure 6: Background-Check Model

Information on RFC 9334 ≫ RFC Editor

IETFにおけるAttestation（3）

- draft-ietf-lamps-csr-attestation　（提案段階）
  - CAが、プライベート鍵の保管場所を確認するためのもの（ちゃんとしたHWの中に格納されているかなど）。
- draft-ietf-acme-client　（提案段階）
  - アカウント認証を行うプロセスを「Attestation」とし、自動化。短期間での定期的な認証ができる。
- draft-lui-acme-rats　（提案段階）
  - 特定バージョンのソフトウェアで動作していることを確認したい。

ところでEAA（Electronic Attestation of Attribute）の「Attestation」って、
IETFで話題のAttestationと同じもの？

多分違っていてですね…
最初に自然言語としての「Attestation」を理解する必要がありそうです。

- AttestationとCertificationの違いってなんなの？
  - 誰が発行するかの違い？
  - 鍵を持つか否かの違い？
  - 取得時/利用時におけるルールやポリシーの違い？
  - 発行プロセス等が標準化されているか否かの違い？
  - 失効可能か否かの違い？
  - 過去に達成したことに関する証明か、その時点での属性の証明かの違い？

AttestationとCertification使い分けない人もいる。
業界や技術ごとに使い分けの形態も違うが…

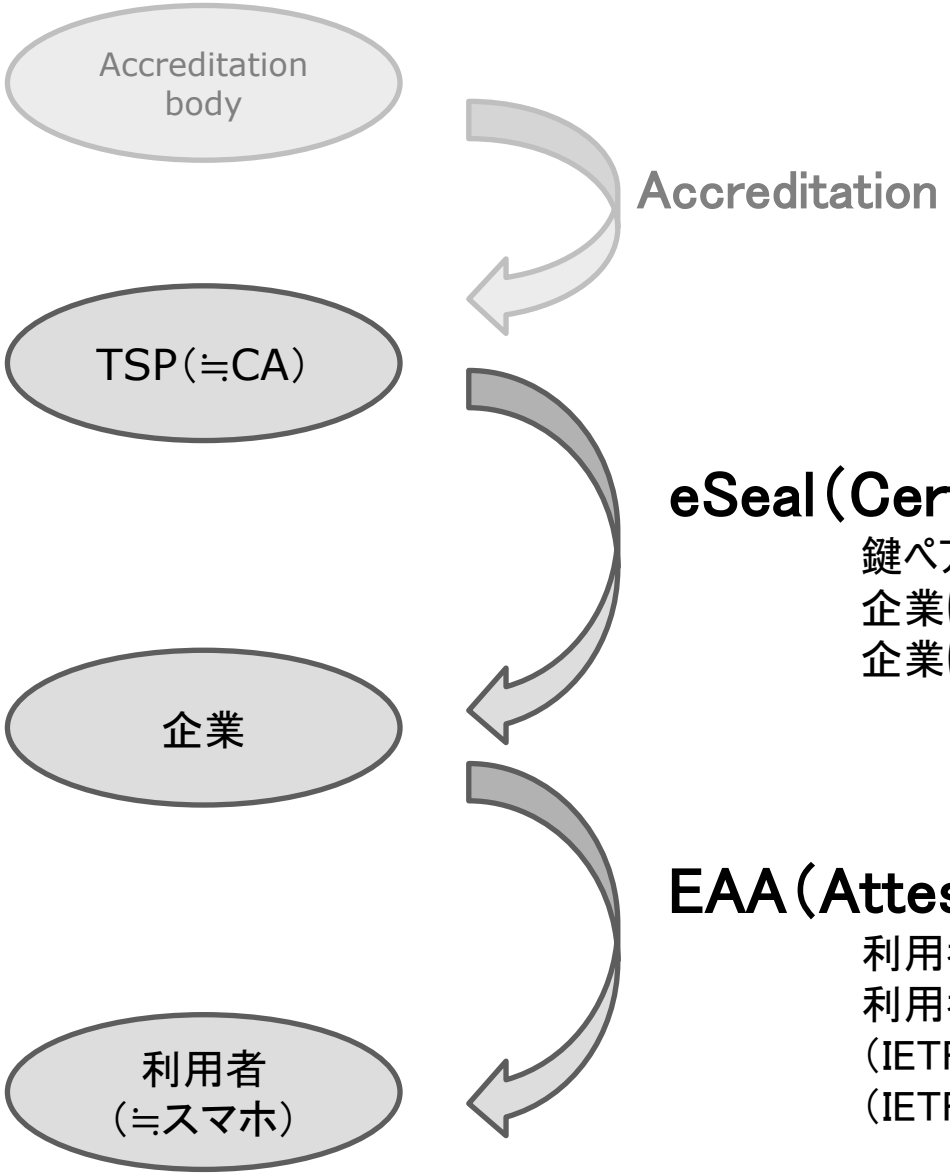
EAAの“Attestation”を理解することを目的に、
本日はPoint in Time と Period of Timeの違いに注目
（他の違いは例外が多い印象）

CertificationとAttestation

- Certification
  - 証明書に記載されている属性が、ある期間で成立することを示す（ことが多い）。
    - 有効期間がない資格等もある。
  - 紙しか使わない運用と相性が良さそう。
    - 利用のたびに属性が成立しているか確認するのは面倒/不可能なので、Authorityからの「証明書」の確認で代替するアプローチ。

- Attestation
  - 有る時点で、記載されていた情報が成立していたことを確認できる仕組み（であることが多い）。
  - 紙文化では効率が悪そう。
    - 効率部分は、デジタル技術で改善可能に見える（確認行為を自動化できれば、コストは低下し、毎回の確認も現実的に）。
  - 使い捨てができるので、名寄せ等のプライバシ上の懸念への対応と相性が良さそう。

EAAにおけるCertificationとAttestation



eSeal（Certificate/Certification）

鍵ペアに対しての署名
企業は、鍵ペアを利用してEAAを発行できる
企業は、名寄せできたほうが良い

EAA（Attestation）

利用者は鍵ペアを持たない
利用者を名寄せできない方が、プライバシ上有利
（IETFと異なり）「人」に対するもの
（IETFと異なり）M2Mだけなく、**PDFにも対応？**

物理世界と相性が悪そうだったAttestationが、デジタルの力で物理世界でも現実的に？？

（考察）

ということは、Attestationの価値は今後上がる？

⇒　多分Yesだが…

Web界隈のデジタル証明書の機能変化とAttestationとの比較

- 有効期間の観点
  - 一般的に、Certificateの有効期間　＞　Attestationが有効な期間
    - Attestationは使い捨てのこともある。
  - Certificateも有効期間が短縮されている…**境界がより曖昧になるかも？**
    - 過去：有効期間5年とか10年の証明書もあった。25年のコードサイン証明書ととかもあったらしい
    - その後（TLS向け）：3年⇒2年（825）⇒1年（398日）
    - 今後（TLS向け）：200日⇒100日⇒47日**（自動化必須）**
  - 一方で、証明書発行前のValidationもAttestationの一種とも言え、「有効期間短縮によりAttestation実行回数は増え、Attestationの重要度も上がる」とも言える。

- 自由度の観点
  - 一般的に、用途の自由度では、Certificateの方がAttestationより広い。
  - Certificateは様々なプロトコル/機能/用途に利用でき、Attestationは特定用途に使うという印象だったが…現在は各証明書ができることを制約していく方向（サーバ認証のみ、SMIMEのみ、コードサインのみ、etc）
  - ここでも、**境界がより曖昧になるかも**

（考察）

属性証明は、eSeal ＋ EAAではなく、**高機能暗号**を使うアプローチもあるのでは？

⇒　PQC移行のためには、**耐量子計算機性を持つ高機能暗号**が必要になる
PQC移行も意識すると、eSeal ＋ EAAの方が順当に見える。

（以下、時間があまれば）

Q: じゃぁ、一般的に、Attestationの方がいいの？

【私見】 一概にも言えなく...「確認」や「監査」のプロセスの程度や深さも考慮に入れたほうが良さそうで、難しそうです。

本日、多数の「確認」が出てきましたが、確認にも色々とありますよね

■どの程度の深さまで確認する（できる）かも、トラストモデルを理解する上で重要
（使い分けていない人もいますが…使い分けている人と会話を成立させるためには重要）

■Acknowledgement

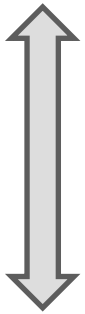
■Confirmation

■Validation

■Vetting

■Inspection

そういえばNotaryで
定型文として出てきたりしますよね



Certificationではこのあたりをする印象

■AuditとAssessmentは使い分けてます？

- ■Self AuditとSelf Assessmentは同じ？
  - ■多くの人は同じような使い方をしているかもしれませんが、、、

- ■人によっては（金融系は？）以下のように使い分け
  - ■Auditは、過去の特定の期間において、要件を満たしていたかの確認（Period of Time）
    （PKI文脈における、WebTrust系監査はこのような行為）
    （多くの場合は、第三者が実施するが、Self Auditという用語もある）

  - ■Assessmentは、その時点において所定の機能を持つかの確認(Point in Time)
    （PKI文脈における、ETSI系の監査はこのような行為）
    （なお、第三者によるAssessmentは（決められたプロセスでないこと等に起因し）高額になることもある）

Q:　EAAは、X.500（X.520　Attribute）の再来？

【私見】 X.500は複雑さゆえに実現しなかったが…LDAPやADは機能を縮退させて実現した。

EAAはさらに少機能みたいなので、実現性はあり、車輪の再発明ではなさそう（でも、あまり複雑にしない方が良さそうに見える。）。

X.500シリーズの中で、全く違う用途に適合しつつ生き残ったX.509だが… eSealとなり、そこからEAAが発行されるというのは興味深い。

Q:　PQC対応的にどっちがいいの？

【私見】 ハーベスト攻撃は考慮しなくて良さそうなので、証明書（or鍵）やAttestationの有効期間と、インフラを移行する期間による。

- WebPKIだと、証明書が47日で鍵の再利用禁止なので、証明書有効期間が長いものに比べたら楽。
- Attestationも、RPがどんな使い方をしているかによる。
- EAA方式なら、証明書方式と相性はそれほど変わらなそう。

-分からなかったりすると、インフラ移行が大変そう。