lamps WG（PKI分野）+α報告

セコム株式会社　IS研究所
（兼）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)

伊藤 忠彦

2020/5/11

lamps WGのCharterが変わりました。

Limited Additional Mechanisms for PKIX and SMIME (lamps)

(略)

1. Specify the use of **short-lived X.509 certificates** for which no revocation information (略)
2. Update the specification for the **cryptographic protection of email headers** -- both for signatures and encryption (略)
3. The Certificate Management Protocol (**CMP**) is specified in RFC 4210,(略)

In addition, the LAMPS WG may investigate other updates to documents produced by the PKIX and S/MIME WG. The LAMPS WG **may produce clarifications where needed**, but the LAMPS WG shall not adopt anything beyond clarifications without rechartering.

（私見）PKIの標準化は、国やステークホルダの法制度・文化・ポリシ等が絡むから面倒。
また、主体数も多い。譲歩しない主体も多い。技術を理解している人がそこまで多くない。

今回のLAMPS WG

- CMP(RFC4210)の整備
- KU問題（今回は、ほんの少しだけ。伊藤が活動中）

CMP(RFC4210)の整備

- 用途
  - LWIG関連、eIDAS関係で使われているのも影響？
- 提案
  - EKUのOID割り振り
    - CABとかでEKUが必須化されているので必要
  - Alg-IDについて
    - コンテンツ用のハッシュアルゴリズムと、署名用のハッシュアルゴリズムは同じとしたい
    - 違う実装は存在するのか？
  - lightweight-cmp-profile
    - まだまだ先は長そう？

PKIがより広く使われるようになり、自動化が進み、CMPの重要性が高まった？

KU問題

背景:

- RFC5480(楕円暗号の標準)における鍵のメタデータの記載方法が不明瞭
  - 暗号理論的に不適切なメタデータを記載可能だった
    - そのような証明書や実装が一定数存在した。
    - 意図しない挙動の可能性。深刻な脆弱性に繋がる可能性。
    - IoT向けに、楕円曲線暗合の利用は増加しそう。修正するなら今しかない？
- どこで禁止するか
  - 各認証局のポリシ？、CABForum？、WebTrust？、CCADB？、IETF?、OpenSSL?
  - Standard? 、Erratta?、Guideline?、実装？
- 各関連団体の知人と話し合った結果、IETFでの議論が適切であろうということに。

- なお、将来ECAIS等が標準化される時に、それを妨げないような文章にするため、一般的なRFCとは違う表現を採用した。
  (その点を理解してもらうのには時間がかかった)

KU問題（経緯等）

[2019/02-06] 各所で情報交換•根回し、文案レビュー依頼
[2019/07] （伊藤＋Seanで）IETFで発表、WGの合意
[2019/11] Charter変更 （Clarificationもスコープに）
[2019/12-02] 大きな影響を受けそうな数十の団体に情報提供
（窓口が分かりにくい団体も多かった）
（対応速度や精度の差が興味深かった）
[2020/01] WG Adaption
[2020/02] WG LC 通過
[2020/03] IESG LC (交渉とか微修正アリ)
[2020/04] Submitted to IESG for Publication
[現在] RFC Ed Queue

順調にいけば、近いうちにRFC化されると思う（もう一波乱ないと願ってます）。
Seanの交渉力により、随分早く進んだ。
あと1件出す予定だが、そちらはもう少し早く進むかも。

まとめ

CMPの（再）標準化は、PKIの自動化が進んでいる影響だと考えられる。

実在の明確な課題に対しては、標準化団体は親身に対応してくれる。

おまけ（teep Virtual Hackathon）

【背景】IETF107HackathonもVirtualでやるかと思い、1箇所に集まり実施する準備はしていた。
公式ではやらないことになったので、有志でリモートhackathonを行った。

- **開催日：**
  - 3/27（1日間）
- **場所、インフラ：**
  - オンライン開催
  - ビデオ会議：V-CUBE）
  - ネットワーク：VPN (l2tp/ipsec)
- **参加者（敬称略、10人）：**
  - 須崎、塚本（産総研）
  - 大居（TRASIO）
  - 永田、森田（レピダム）
  - Dave Thaler（Microsoft）
  - 伊藤（ロボック）
  - 磯部、宮澤、瀧田（セコム）
- **目的：**
  - Virtual Hackathonの環境整備、TEEP Protocolの試作実装

詳細は、https://datatracker.ietf.org/meeting/interim-2020-teep-02/materials/slides-interim-2020-teep-02-sessa-teep-hackathon-report