Automated Certificate Management Environment (ACME) WGの動向

Masaki SHIMAOKA
as ISOC-JP Program Committee
(Intelligent Systems Lab., SECOM Co., Ltd.)

WGの概要

- WG co-chairs
  - Ted Hardie(Google) & Rich Salz(Akamai)
- 目的
  - X.509証明書の管理(身元確認、発行、更新、失効など)を自動化する
  - 当面は、いわゆるDV証明書を対象とする
  - CP/CPSなどの検討は対象外
- WG Draft
  - draft-ietf-acme-acme-01 (2015-10-04)
    - 目標：Proposed Standardとして2016-03 までにIESGレビュー

背景

- Let's Encrypt Project
  - TLSサーバ認証用証明書の無償自動発行を提供するプロジェクト
  - MozillaやEFF(Electronic Frontier Foundation)が主導
  - 元IETF ChairのRuss Housleyらもオブザーバ(いずれもindependent)
  - 2015-09 証明書発行開始(本格的な提供は10月以降。そろそろ?)
- SCEP(Simple Certificate Enrollment Protocol)
  - CiscoによるHTTPベースの証明書発行プロトコル
  - 2000-01にindividual I-D初版、2011年まで更新され続けた
    - 最後はHistorical RFCを目標としていた
- RFC7030 EST(Enrollment over Secure Transport)
  - やはりCiscoによる証明書発行プロトコル
  - SCEPとの違い/住み分けは未確認
  - PKIX WGで標準化された

現状

- draft-ietf-acme-acme
  - 証明書発行プロトコルを策定
- draft-mattson-acme-use-cases
  - ACMEのユースケース
- draft-gutmann-scep
  - 2015-09 何とSCEPがPeter Gutmannにより復活
  - 今度はStandard Track狙い
  - ただし現時点でACME WGでは議論なし
  - 何故このタイミング?? ACMEを意識しているとしか。。。

キーパーソン

- Richard Barnes
  - draft-ietf-acme-acmeのauthor
- Phillip Hallam Baker

- Eric Rescorla