PKI便り
– IETFの方から –

2023年11月21日(火)

木村泰司

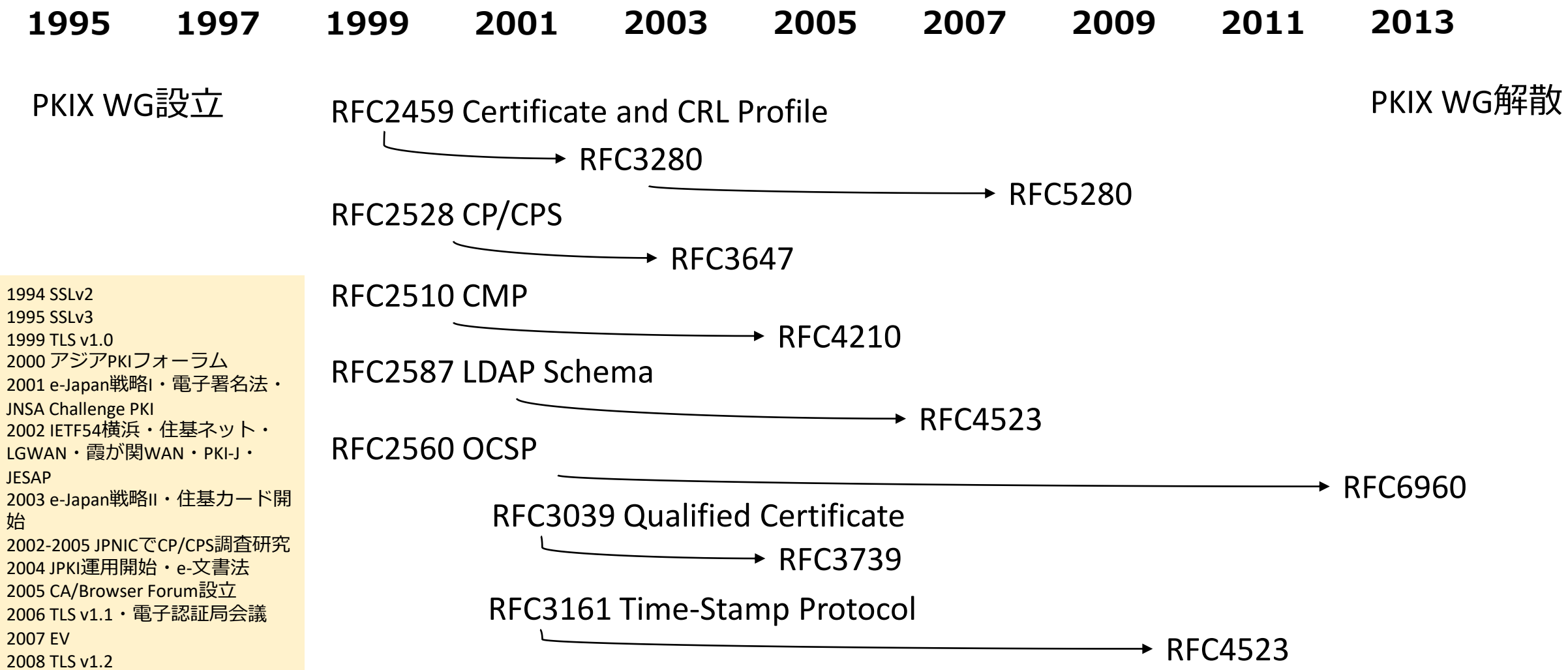
一般社団法人 日本ネットワークインフォメーションセンター

この発表について

- **「PKI、最近どうしてるかな...」というあなたに、あの頃のPKIとイマ時のPKIをIETFを中心にお知らせするメッセージ**

  - あの頃　＝　PKIX WGのころ
  - イマ時　＝　lamps WGのころ

Public-Key Infrastructure (X.509) WG (pkix)



1994 SSLv2
1995 SSLv3
1999 TLS v1.0
2000 アジアPKIフォーラム
2001 e-Japan戦略I・電子署名法・JNSA Challenge PKI
2002 IETF54横浜・住基ネット・LGWAN・霞が関WAN・PKI-J・JESAP
2003 e-Japan戦略II・住基カード開始
2002-2005 JPNICでCP/CPS調査研究
2004 JPKI運用開始・e-文書法
2005 CA/Browser Forum設立
2006 TLS v1.1・電子認証局会議
2007 EV
2008 TLS v1.2
2008 iPhone 3G・MD5危殆化
2009 政府CIO制度
2010 ECOM解散

※すべて話者選

Limited Additional Mechanisms for PKIX and SMIME (lamps)

2016 2017 2018 2019 2020 2021 2022 2023

lamps WG設立

RFC8399 Internationalization *

RFC8550 S/MIME v4.0

RFC8659 DNS CAA Record (6844bis)

RFC8813 KeyUsage for ECC

RFC8954 OCSP Nonce Extension *

Ryan Sleevi氏によるSAAGでの発表
「Requirements for Building a PKI」

RFC9045 Alg. Requirement update on CRMF

RFC9216 S/MIME Example *

RFC9295 Ed Algorithm ID

RFC9310 5G NF types extension *

RFC9399 Logotypes (3709bis)

RFC9480 CMP Updates

RFC9495 CAA for Email *

※すべて話者選

アクティブなInternet-Drafts(一部)

draft-ietf-lamps-rfc5019bis
OCSP for High Volume Env.
draft-ietf-lamps-keyber-certificates
Algorithm ID for KYBER
draft-ietf-lamps-csr-attestation
Remote Attestation with CSR
draft-ietf-lamps-nf-eku
EKU for 5G Network Functions
draft-ietf-lamps-dilithium-certificates
Dilithium (耐量子署名アルゴリズム)
draft-ietf-lamps-x509-policy-graph
Updates to X.509 Policy Validation

まとめ

- 活躍中です。
- リモートアテステーション・耐量子暗号・5Gなどのイマ時の話題にも関わっているようです。

- 目立たないけど気になる話題
  - Updates to X.509 Policy Validation

おわり