IETF報告会（93rd プラハ）

SAAG/CFRG/TLS/SIDR/ACME

木村泰司
taiji-k at nic.ad.jp
協力：菅野哲さん

JPNIC 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

内容

- **セキュリティエリア全体会合の動向**
  - SAAG
- **Research Group (RG) の動向**
  - CFRG
- **Working Group (WG) の動向**
  - TLS
  - SIDR
  - ACME

発表者について

- **名前**
  - 木村泰司（きむらたいじ）
- **所属**
  - 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 (JPNIC)
    - CA / RPKI / DNSSEC / セキュリティ情報：
      調査 (執筆)・セミナー・企画・開発・運用・ユーザサポート
- **参加活動**
  - JNSA PKI関連 / WIDE / JANOG / WIT
- **IETF**
  - MLは1997年、ミーティングは2003年頃より

SAAG
(Security Area Advisory Group)

セキュリティエリアの全体会合

JPNIC 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

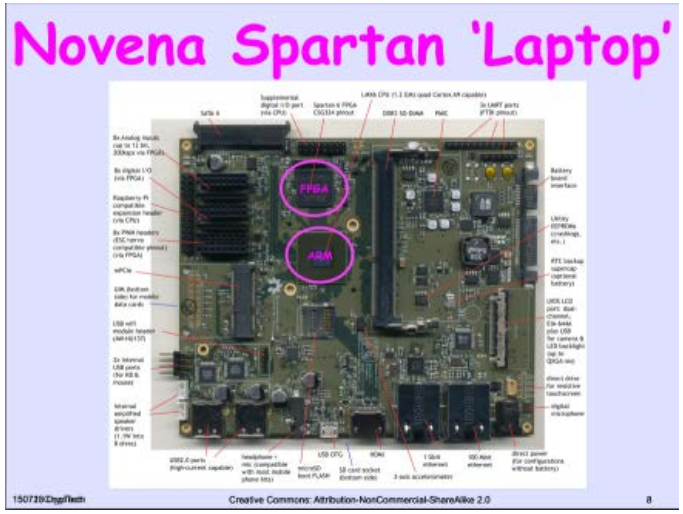
SAAG - 議題

- **WG/BoFレポート (18WG)**
- **招待講演**
  - CrypTech ★
  - トランスポート・セキュリティの状況 ★
    - Email / Web におけるSSL/TLSの暗号利用状況
  - EAP設定の自動化について
  - エンティティの鍵リカバリー
  - DHCPv6セキュリティの動向
  - Managing Radio Networks in an Encrypted World (MaRNEW) Workshop (IAB)
- **オープンマイク（意見交換）**

SAAG IETF 93
https://www.ietf.org/proceedings/93/slides/slides-93-saag-7.pdf

CrypTech - オープンソースのHSM

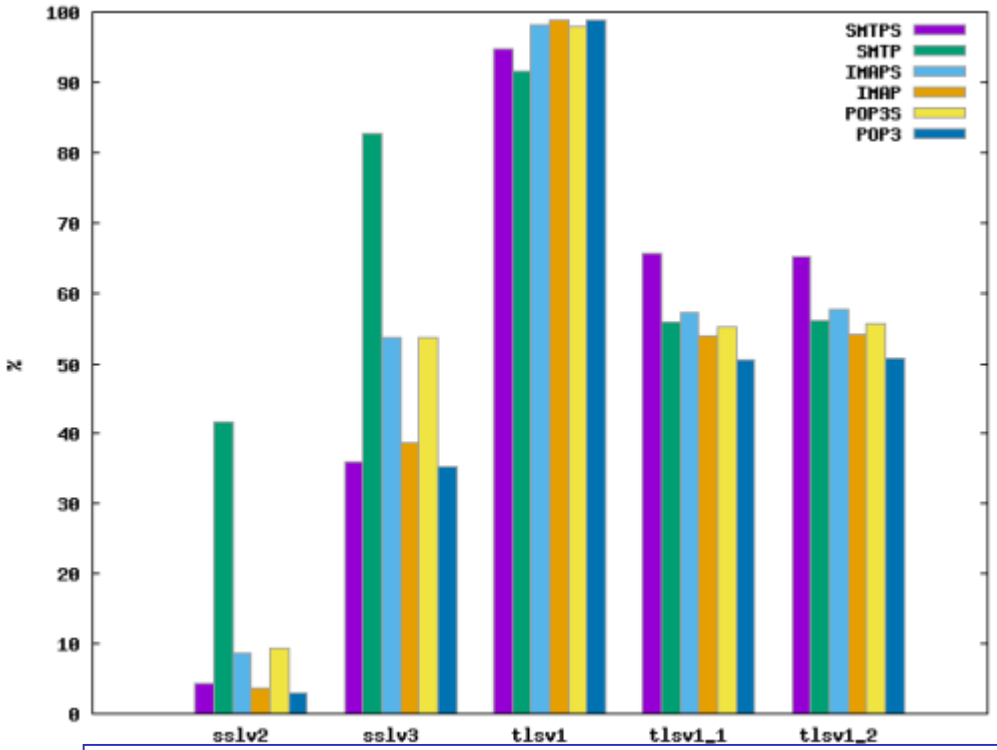
- 2013年末頃から活動しているソースコードや設計をオープンにしつつHSMのリファレンスデザインをするプロジェクト
- 2015年7月18日（土）「cryptech hackday」でソースコードやFPGAとARMを使ったハードウェアを公開



CrypTech
https://www.ietf.org/proceedings/93/slides/slides-93-saag-0.pdf

トランスポート・セキュリティの状況

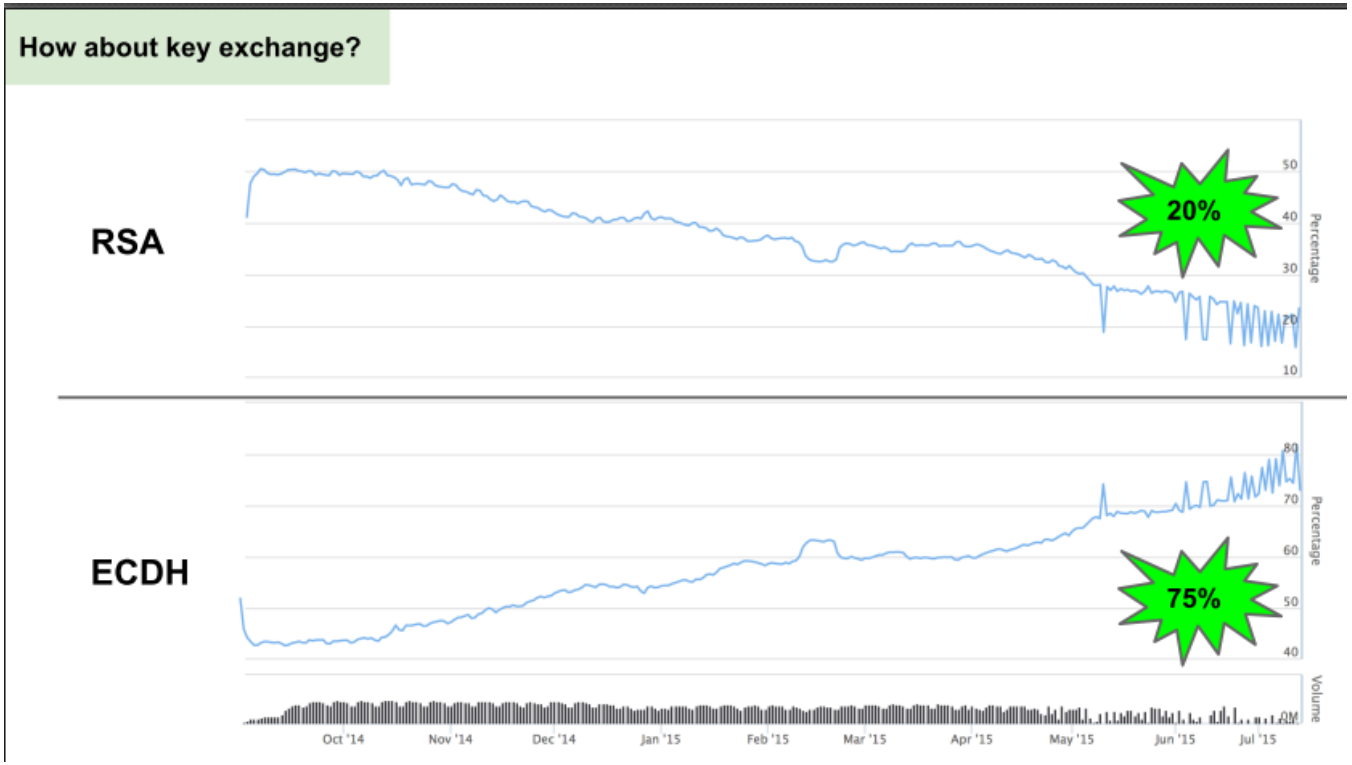
- **SSL/TLSの暗号利用状況調査 - E-mail**
  - 二か月に渡ってE-mail関連のポートをスキャン（SMTPS/SMTP/IMAPS/IMAP/POP3S/POP）



State of Transport Security in the E-mail Ecosystem
https://www.ietf.org/proceedings/93/slides/slides-93-saag-2.pdf

トランスポート・セキュリティの状況(1)

- **SSL/TLSの暗号利用状況調査 - Webブラウザ**
  - 大手Webサーバ(Mozilla?)にて計測



State of Transport Security for HTTP - browsers
https://www.ietf.org/proceedings/93/slides/slides-93-saag-3.pdf

トランスポート・セキュリティの状況(2)

- **SSL/TLSの暗号利用状況調査 - Webサーバ**
  - 100万サイトのスキャン結果にみる変遷

2014年5月	SHA2利用が4%から8%へ
2014年5月	TLS1.2利用が50%に
2014年9月	CAとサーバの証明書の96%以上がRSA2048に
2015年1月	サーバの70%がECDHE利用可
2015年6月	RSA with SHA256が60%超え

State of Transport Security for HTTP - Server
https://www.ietf.org/proceedings/93/slides/slides-93-saag-4.pdf

CFRG
(Crypto Forum Research Group)

IETFのプロトコルと一般的なネットワークセキュリティに関わる
暗号の利用メカニズムをレビューし議論するグループ

JPNIC 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

CFRG - 議題

- **チェア報告（I-Dの状況ほか）**
- **PAKEスキームの要件**
  - 小さなデバイスのためのパスワード認証スキーム提案
- **XMSS: 拡張されたハッシュベース署名**
  - 疑似乱数の鍵を付与するハッシュ関数利用の提案
- **TLSにおけるハイブリッド耐量子暗号 ★**
- **CrypTechプロジェクト**
  - オープンソースのHSM
- **楕円曲線暗号を使った署名方式の提案**
  - ECDSAやEdDSAの複数の改善案
- **DH/ECC鍵の強度**
  - 通信相手の鍵を使って鍵生成し、各ノードの弱い鍵利用を避ける手法の提案

CFRG - Crypto Forum Research Group (agenda)
https://datatracker.ietf.org/meeting/93/agenda/cfrg/

TLSにおけるハイブリッド耐量子暗号

- **耐量子暗号**
  - 量子コンピュータが登場すると、素因数分解問題(RSA)や楕円曲線離散対数問題(ECC)、離散対数問題(DH)が容易に解けるようになるため、これらを使った暗号は破られやすくなると言われている。
  - そこで量子コンピュータでも効率よく解けないことが期待される「最近ベクトル問題(Closest Vector Problem)」や「最短ベクトル問題(Shortest Vector Problem)」などを使った「耐量子暗号」が注目されている。

⇒ TLSにおける耐量子暗号の利用は？

参考：量子コンピュータによる解読に耐えうる『格子暗号』を巡る最新動向
http://www.imes.boj.or.jp/citecs/symp/16/ref3_seito.pdf

TLSにおけるハイブリッド耐量子暗号

- **TLSにおける耐量子暗号の利用**
  - 耐量子暗号を指定できるTLSのCiphersuiteはない。まだ議論が行われてもいない。適切な署名アルゴリズムはない。
  - そこで公開鍵暗号として耐量子暗号を使うハイブリッドの方式を提案
    - draft-whyte-qsh-tls12
    - draft-whyte-qsh-tls13
  - 実装　Quantum-Safe wolfSSL
    - https://www.wolfssl.com/wolfSSL/Blog/Entries/2015/7/13_Quantum-Safe_wolfSSL.html

⇒ 会場ではCFRGとしても取り組むことに賛成多数

William Whyte - Cheap quantum-safe cryptography without breaking anything
https://www.ietf.org/proceedings/93/slides/slides-93-cfrg-7.pdf

TLS WG
(Transport Layer Security)

トランスポート層セキュリティ
TLSの策定を行っているWG

TLS WG - 議題

- **WGやドキュメントのステータス報告**
- **TLS 1.3 ★**
  - 様々な検討事項の議論
- **楕円曲線暗号のCiphersuite (RFC4492の更新)**
  - Curve25519やEd448-Goldilocksの追加
- **DANEを使うDNSSECチェイン拡張 ★**
- **IEEE 1609 証明書への対応**
  - ITS(高度道路交通システム)などで使われる形式
- **TLSセッションキーを別ホストで扱える提案**
  - TLSセッションを張るホストの他に鍵を管理するホスト設置方式
- **事前共有鍵ECDHE_PSKのCiphersuite提案**
  - 事前共有鍵を使ったTLSのための提案
- **TLSにおけるハイブリッド耐量子暗号**
  - TLSで耐量子暗号を使うための提案

TLS WG @ IETF93
https://www.ietf.org/proceedings/93/slides/slides-93-tls-0.pdf

TLS 1.3

- **IETF92以降...(抜粋)**
  - DHベースのハンドシェイクの追加
  - PSKサポート
  - RC4を使うネゴシエーションの禁止
- **議論されるべき論点**
  - ハンドシェイクのメッセージ
    - ServerConfiguration／相対時間か絶対時間か
  - 0-RTT関連
    - PSKをどうするか／認証との連携／拒否する方式
  - クライアント認証の方式
    - HTTP/2との整合性
  - トラフィック鍵の生成
  - アラカルト方式のCiphersuite
  - パッディング

議論は継続中。IETF93で3時間近く議論してもまとまってきていない。

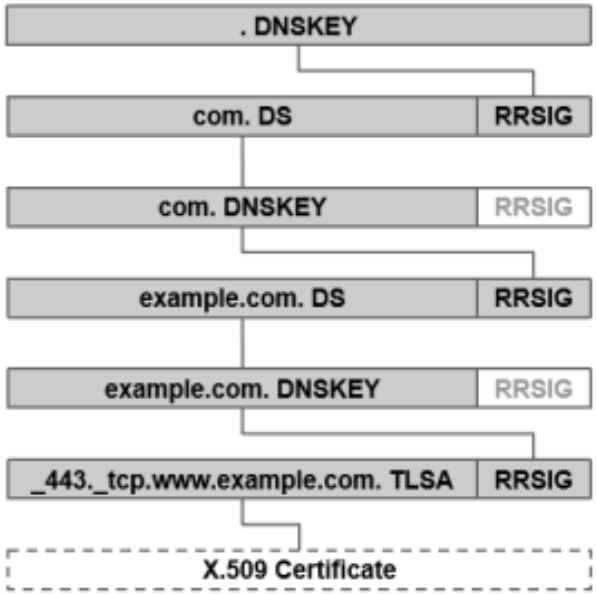
TLS 1.3
https://www.ietf.org/proceedings/93/slides/slides-93-tls-8.pdf

DANEを使うDNSSECチェイン拡張

- **TLSの拡張メッセージを使って、DANEのTLSAを使った署名検証に必要なリソースレコードを相手に伝える提案**
  - TLSクライアントのホストがTLSAの確認のために、必要な鍵と署名をDNSで引く必要がなくなる。

```
struct {
  opaque rrset<0..2^16-1>;
  opaque rrsig<0..2^16-1>;
} RRset

// MUST be in auth'n order
// Like cert chain
RRset AuthenticationChain<0..2^16-1>;
```



-dnssec-chain-extension
https://www.ietf.org/proceedings/93/slides/slides-93-tls-1.pdf

SIDR WG
(Secure Inter-Domain Routing)

"セキュア・ドメイン間ルーティング"

証明書を使ってインターネットの経路情報を
検証できる仕組みを検討しているWG

SIDR WG - 議題と内容(1)

- **WGやドキュメントのステータス報告**
  - BGPSECプロトコルがWGラストコール済
  - RFC6490bis(Trust Anchor Locator書式) IETFラストコール
- **RPKIリポジトリ差分転送プロトコル**
  - rsyncに代わるプロトコル
    コンセプト実装はあるものの同期方式などについて議論中
- **RPKIとアドレス移転**
  - リソース証明書にカバー範囲を超える場合が起きないかの確認
- **リポジトリやCAに向けた不正行為対策**
  - リポジトリやCAに対する攻撃行為の洗い出し

Chair slides - status and agenda
https://www.ietf.org/proceedings/93/slides/slides-93-sidr-9.pdf

SIDR WG - 議題と内容(2)

- **RPにおける例外処理SLURM**
  - Origin validationの結果のうち、特定のprefixの扱いを除外するなどの仕組み
- **中国におけるRPKI**
  - 調査研究を行っている旨の発表
- **RPKIビーコン**
  - BGPビーコンと同様に不正な経路情報を監視する仕組みの提案
- **RPKIブラウザ - RPKI MIROプロジェクト**
  - リソース証明書やROAを辿ることができる実装
- **BGPSECと経路漏えい**
  - BGPSECで検知できるかどうかのケース分け

Chair slides - status and agenda
https://www.ietf.org/proceedings/93/slides/slides-93-sidr-9.pdf

ACME WG (Automated Certificate Management Environment)

証明書管理環境の自動化

JPNIC 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

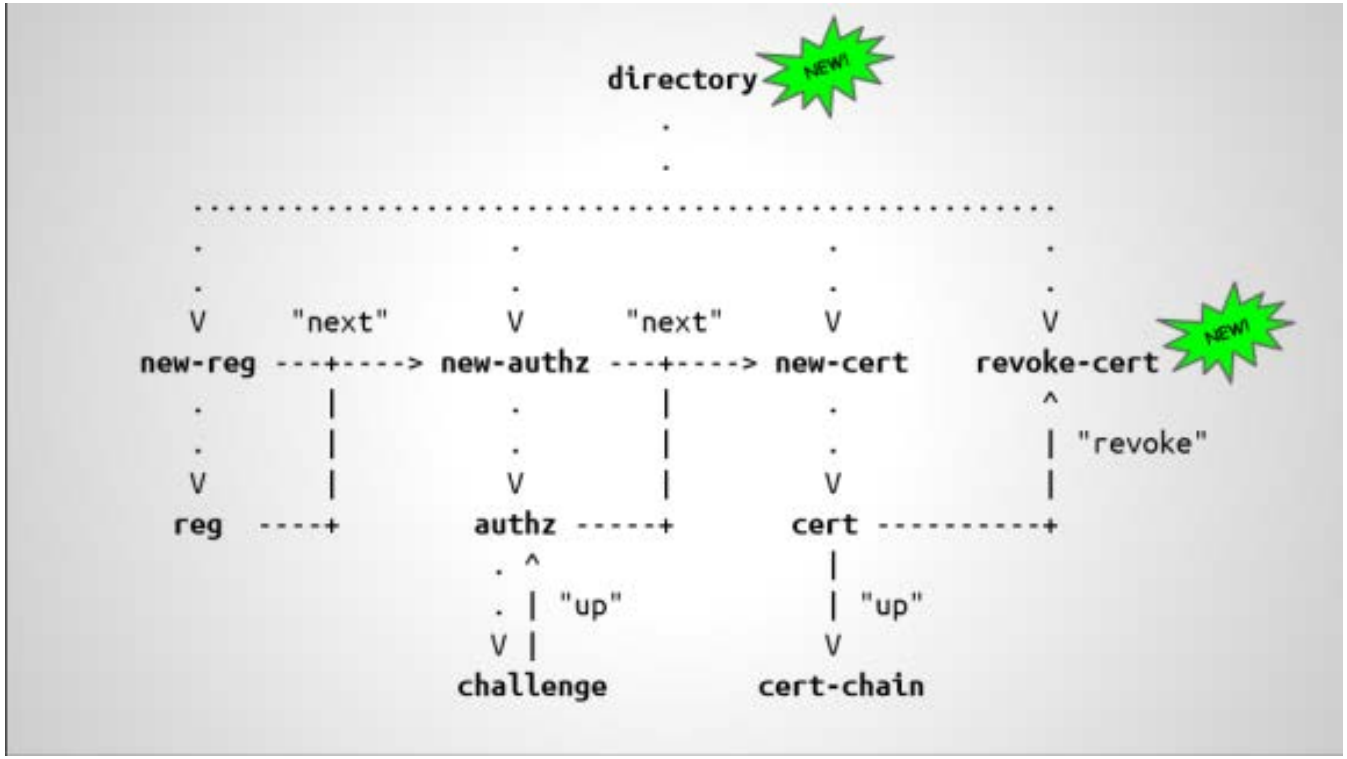
ACME WG - 議題

- **アジェンダの確認**
- **ACMEの基本的なプロトコル ★**
  - 今回、Individual draftからWG draftとして採用することについてコンセンサス
  - 無料のサーバ証明書発行プロジェクト「Let's Encrypt」で使われるプロトコル。Let's Encryptは2015年第４四半期にサービス開始を予定。
- **ユースケース**
  - Webサーバの代行をする"証明書管理サーバ"の形態を考察
- **JSON Web Signature の変更**
  - JWSの"detached content"をbase64エンコードしない提案
- **OmniPublish**
  - LocalRAの形態で汎用的な仕組み

WG設立後、最初の会合

ACMEの証明書管理とは(1)

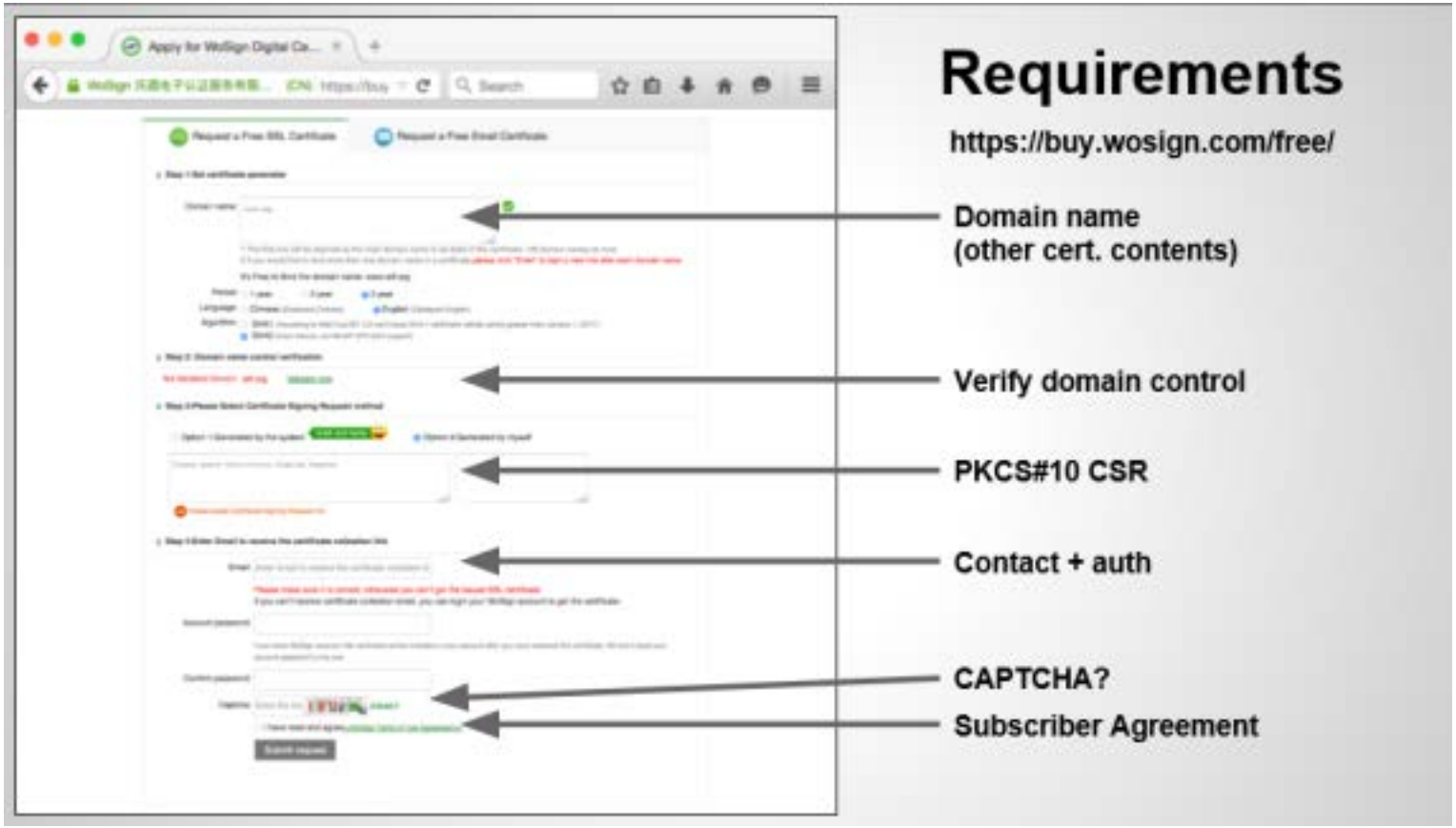
- ディレクトリを使って、(クライアントの)登録／発行認可／発行／失効の状態管理



draft-barnes-acme
https://www.ietf.org/proceedings/93/slides/slides-93-acme-1.pdf

ACMEの証明書管理とは(2)

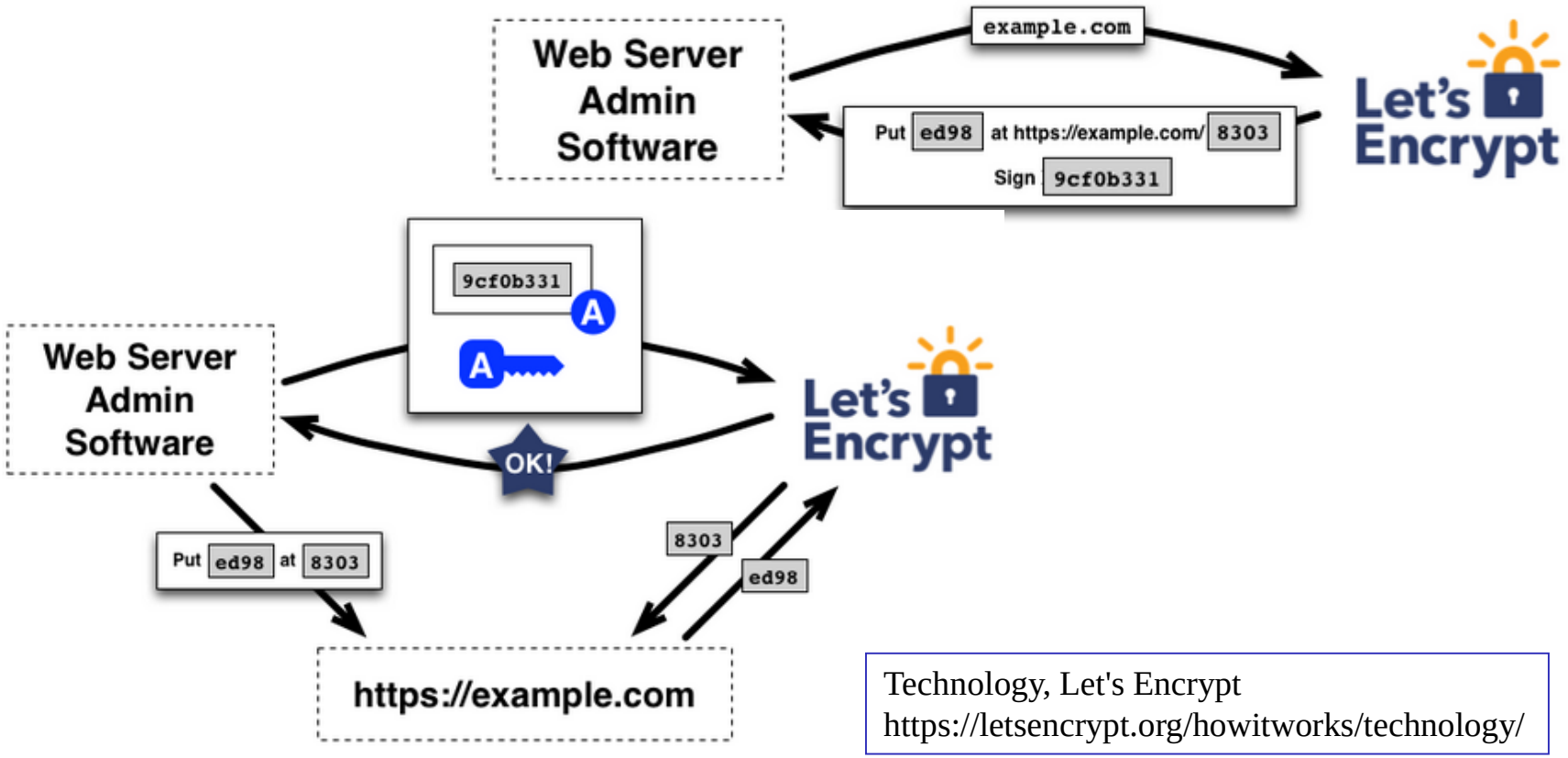
- クライアント要件（Web経由で証明書申請）



draft-barnes-acme
https://www.ietf.org/proceedings/93/slides/slides-93-acme-1.pdf

Let's EncryptのDomain Validation証明書

- Webサーバ上の管理ソフトウェアが、ドメイン名確認と証明書発行／失効の手続きを行う



Technology, Let's Encrypt
https://letsencrypt.org/howitworks/technology/

Let's Encryptの証明書

- **ルート証明書**
  - ISRG Root X1
    https://letsencrypt.org/certs/isrgrootx1.der
  - IdenTrustによるクロスルート証明書が発行される予定
  - HSM使用／RSA4096 SHA256
- **中間証明書**
  - Let’s Encrypt Authority X1
    https://letsencrypt.org/certs/letsencryptauthorityx1.der
    - 通常はこちらからサーバ証明書が発行される
  - Let’s Encrypt Authority X2
    https://letsencrypt.org/certs/letsencryptauthorityx2.der
  - RSA2048 SHA256
- **現在はRSA、今後ECDSAへ移行を計画**

Certificate, Let's Encrypt
https://letsencrypt.org/certificates/

まとめ(1)

- **オープンソースのHSM　CrypTech**
  - FPGAとARMを使ったボードやソースコードが公開
  - 協賛企業も多数
- **SSL/TLSの暗号利用状況調査**
  - SMTPS ECDH鍵交換が増加中
  - HTTPS RSA SHA256が主流か
- **耐量子暗号**
  - TLSで使えるようにする方向性の議論が始まる
- **DANEを使ったTLS**
  - 署名検証に必要なRRを伝える拡張の提案

まとめ(2)

- **BGPSEC**
  - ほぼ仕様が固まった
  - Rsyncに代わるリポジトリ差分転送プロトコルの議論も進む
- **ACME**
  - 無料のDVサーバ証明書の発行プロジェクト「Let's Encrypt」で使われるプロトコルの策定活動開始
  - Webサーバ上で証明書管理プログラムが動く形態

おわり

木村泰司
taiji-k at nic.ad.jp