IETF 100 参加報告

東芝研究開発センター
安次富大介
daisuke.ajitomi@Toshiba.co.jp

自己紹介：安次富 大介 (あじとみ だいすけ)

- (株)東芝 研究開発センター ネットワークシステムラボラトリ 所属
- もともと組込み機器向けの通信プロトコル・システム技術の開発や国内標準化などに従事
  - 組込み機器向けHTTP/1.1, SIPクライアントを自製したり

- 最近は, コンシューマ機器だけでなく, 社会インフラ, HEMS, メモリなど幅広い事業領域を対象に, IaaSを活用した通信・データ処理基盤を開発中
  - **OAuth2.0**/OIDC 認可サーバを自製したり, WebSocketブローカのクラスタシステム作ったり

- 対外活動: W3C HTTPS in Local Network CG
  - ローカルネットワーク(とは何ぞや)上の機器に, Webから読み込んだSecure Context からクロスオリジンアクセスしたい → ローカル機器にちゃんとした(ブラウザが認めてくれる)証明書発行したい(**ACME**?)

Index

- OAuth: Web Authorization Protocol
  - Webベースのアクセス認可フレームワーク
  - PoP(Proof of Possession)トークン関連、ベストプラクティスが主要トピック
  - 幾つか新規提案

- ACME: Automatic Certificate Management Environment
  - Let's Encryptのサーバ証明書発行プロトコル
  - 基本仕様については前回IESGに送られRFC化待ちの状態から幾つか問題が
  - 基本仕様を前提とした拡張仕様提案

OAuth

- ★ Mutual TLS Profile for OAuth 2.0
- ★ OAuth 2.0 Token Binding
- OAuth 2.0 Authorization Server Discovery Metadata
- ★ JSON Web Token Best Current Practices
- ★ OAuth 2.0 Device Flow
- ★ OAuth 2.0 Device Posture Signals
- ★ Security Topics
- ★ Mutual OAuth
- ★ Distributed OAuth
- Raw-Public-Key and Pre-Shared-Key as OAuth client credentials
- A Public Identity Infrastructure for the Internet

Mutual TLS Profile for OAuth 2.0
https://tools.ietf.org/html/draft-ietf-oauth-mtls-05

- ポイントは２つ
  - クライアント認証をTLS相互認証ベース(PKI-based or self-signed cert-based)に
    - Tokenエンドポイントで, クライアントのtls_client_auth_subject_dn”属性と証明書のDNで認証
  - クライント証明書をひもづけたsender constrained access token
    - tokenにクライアント証明書のハッシュを入れておく
    - クライアントとRS間もTLS相互認証, RSはトークン内のハッシュと, 使われたクライアント証明書を突合
- 背景：銀行系でのニーズ
  - FAPI (OpenID Financial API) の “Read and Write API Security Profile”
  - Open Banking API Security Profile
  - 銀行系はロードバランサでTLS終端とかしてないんですかね
- ステータス
  - 12/BにWGLCの計画

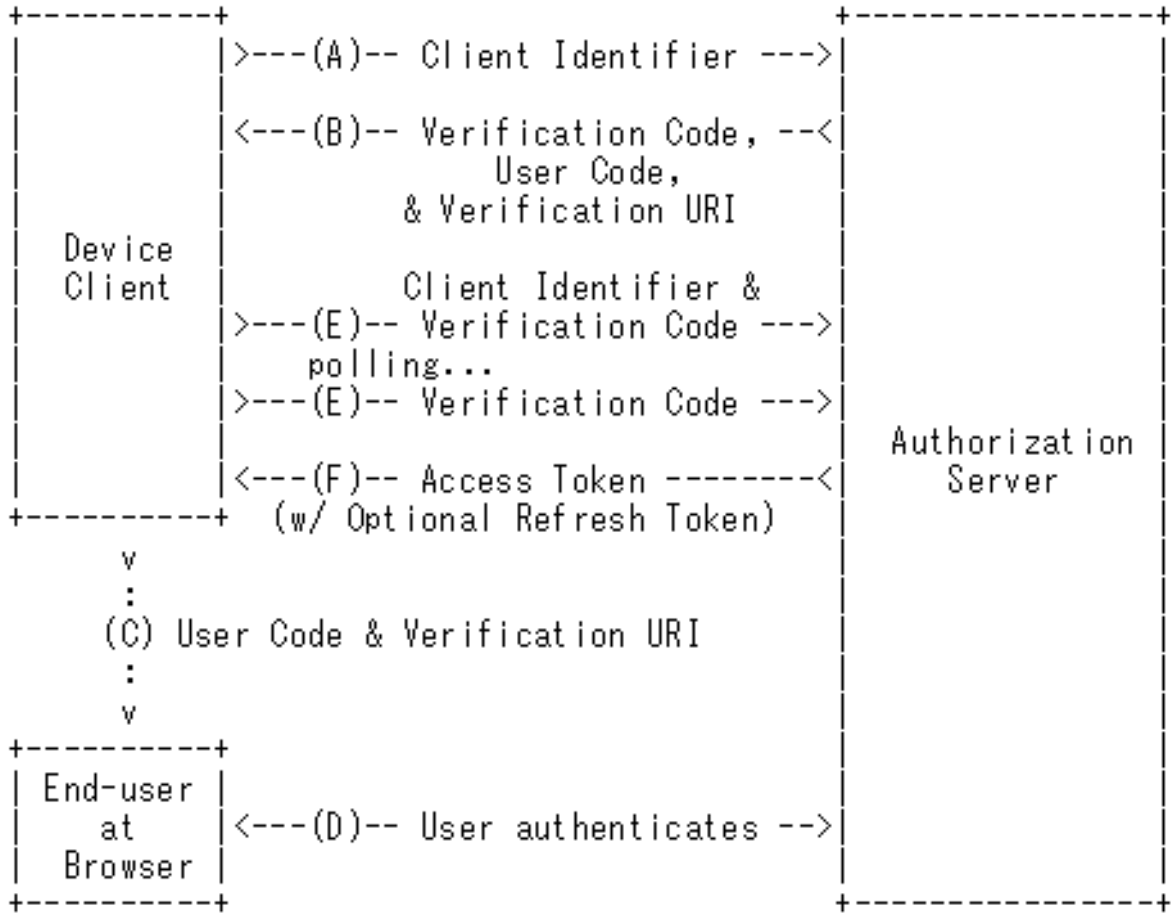
OAuth 2.0 Token Binding

https://tools.ietf.org/html/draft-ietf-oauth-token-binding-05

- Token Binding
  - サーバにアクセスするためのトークンを，TLSセッションに暗号論的に紐づけ，PoP(Proof of Possession)トークン化するための仕様。TLSネゴシエーション時に共有できる暗号論的乱数(EKM)に秘密鍵に署名することで実現
- OAuth 2.0 Token Binding
  - OAuthのトークンをToken Bindingを使ってPoPトークン化する方法を規定
  - 今回，明示的な指定がない限りrefresh_tokenをバインドしないようにした，JWT Authorization Grants向けtoken binding関連パラメータを追加したなど諸々修正
- ステータス
  - Token Bindingの主要3規格が全てIESGに送られており，もうじきRFC化
    - draft-ietf-tokbind-{protocol, negotiation, https}
  - 実装者からのフィードバック待ち

OAuth 2.0 Device Flow
https://tools.ietf.org/html/draft-ietf-oauth-device-flow-07

- UIを持たない機器に対してトークンを発行するフロー
- 前回(IETF99)の議論を反映し, (C)で渡すパラメータとして以下を追加
  - verification_uri_complete: Verification URIが, user_codeを含んでいるか否かを表す
- ステータス
  - 再びWGLCへ



ベストプラクティス関連

- JSON Web Token Best Current Practices
  - https://tools.ietf.org/html/draft-ietf-oauth-jwt-bcp-00
  - JWTはいろいろ罠がある(alg:noneなど)
  - ベストプラクティス： alg:noneを指定して良いのはしたでTLS等セキュア通信を使っている場合だけ, HS256にヒューマンリーダブルなキーは使わない, IssuerとSubjectはバリデーションしましょう等, 現状10項目ほど
  - ステータス: WGドラフトにはなったがフィードバックが皆無とのこと, 絶賛募集中
- Security Topics
  - https://tools.ietf.org/html/draft-hardt-mutual-oauth-00
  - OAuthのオープンなセキュリティトピックを総覧したドキュメント
  - ベストプラクティス：リダイレクトURIはexactマッチせよ, クエリパラメータ化されたURLへはリダイレクトするな, stateにはワンタイムトークンを入れよ, authorization_codeは, PKCEと合わせて使うべし, など
  - IETF100での変更は, RSでのtoken leakageの記載, TLS終端プロキシでの脅威に関する記載の追加など
  - ステータス: コメント募集中

[NEW]

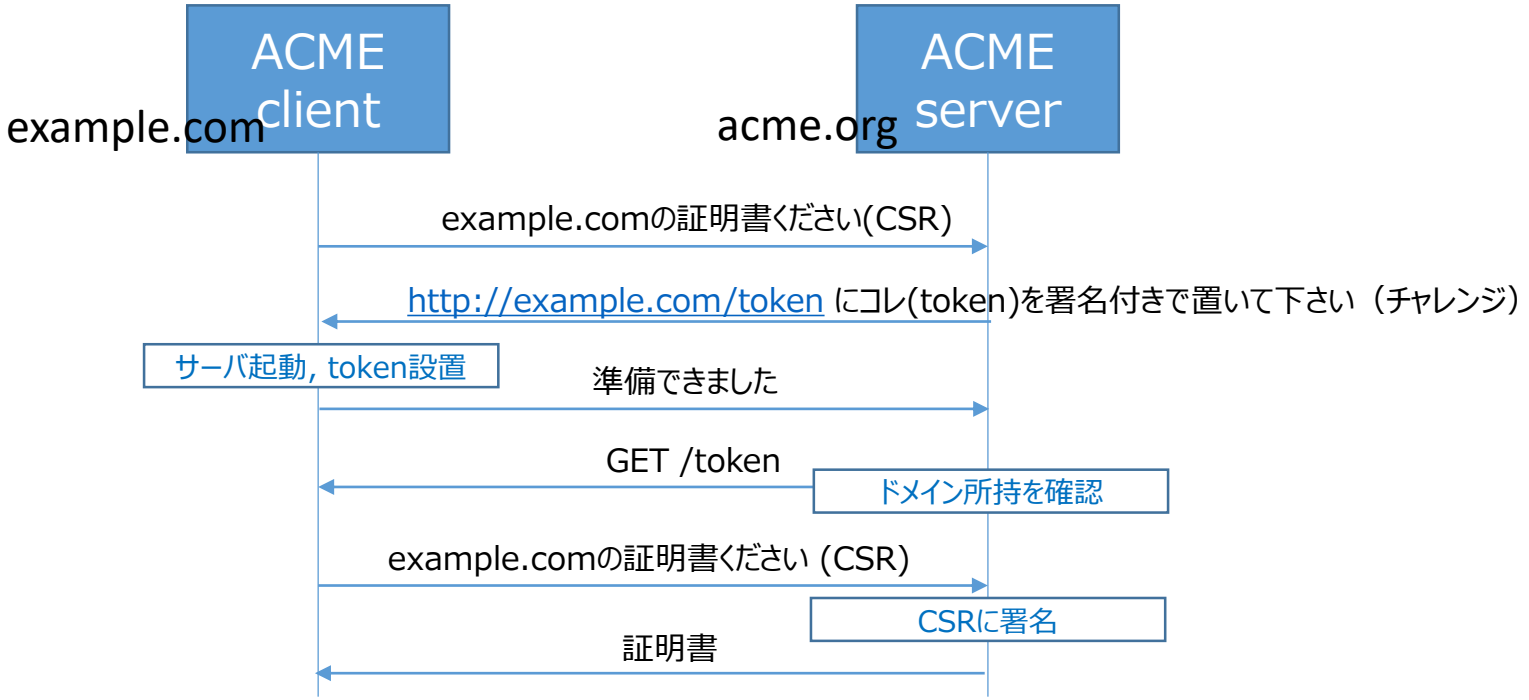
- OAuth 2.0 Device Posture Signals
  - https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01
  - W. Denniss (Google) ほか
  - Authorize時に, ユーザ端末情報(OS, バージョン, ルート権限があるか, スクリーンロックがONか等を送り, 与える権限範囲のヒント情報に使う
- Mutual OAuth
  - https://tools.ietf.org/html/draft-hardt-mutual-oauth-00
  - D. Hardt (Amazon)
  - 相互にアクセスし合うアプリケーションに認可を与える場合，２回認可フローを走らせなければならい。これを１回で済ませる方法を提案。新たなgrant_typeとして, mutual_authentication_codeを定義。
- Distributed OAuth
  - https://tools.ietf.org/html/draft-hardt-distributed-oauth-00
  - D. Hardt (Amazon)
  - 多数のRS, ASが存在する環境において, client_credentialsなクライアントがRSにアクセスし, 対応するASのアドレスを得て, authorizeリクエストするための仕様

ACME

- ACME
- Extensions to ACME for email (TLS, S/MIME)
- STIR TNs for ACME (for telephony)
- ACME Token Identifier and Challenges
- ACME IP
- ACME STAR

ACME

- Let’s Encrypt：インターネット上のWebサーバに対して，自動でTLSサーバ証明書の発行・更新をおこなうサービス
- 証明書の発行を求めるWebサーバ(ACMEクライアント)に対して，”チャレンジ”と呼ばれるドメイン所有証明を課し，ACMEクライアントがこれをクリアした場合に証明書を発行する



ACME
https://tools.ietf.org/html/draft-ietf-acme-acme-08

- IESG提出後のトピック
  - Proactive Issuance
    - 現状,CSRを２回送る必要があるが, 本当に２回送らなければならないのか？
    - キャッシュできるならキャッシュして, 必要なときにだけCSRを求めるようにすればよいのでは？
    - ⇒ 結論としては現状維持（2回送る）
  - OOBチャレンジを仕様から外すか否か
    - Out-Of-Bandチャレンジ
      - チャレンジにhrefを入れて, 例えばユーザによるWebページを介した許諾プロセス等を噛ませられるようにする仕様
    - Boulderなど主要実装にインプリされていないので外す方向で
- ステータス
  - 上記が反映された09が今朝公開。ロンドンまでにRFCエディターキューに入れたい意向

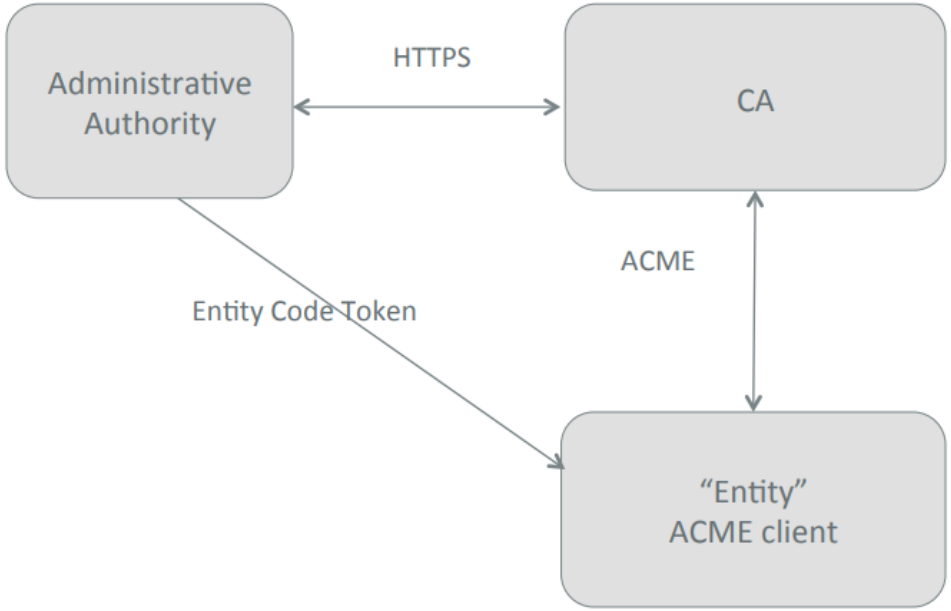
ACME拡張

- Extensions to ACME for email TLS
  - https://tools.ietf.org/html/draft-ietf-acme-email-tls-02
  - SMTPやIMAPサーバが証明書をACMEベースで動的に取得する
  - 拡張として, ポート番号属性, サービス: “smtp”, “imap”, チャレンジ: “dns-email-01”: ほぼ”dns-01”だが, TXTフィールドに入れるドメイン名にサービスとポートを入れたフォーマットを規定
- STIR TNs for ACME
  - https://tools.ietf.org/html/draft-ietf-acme-telephone-01
  - IP電話(&ゲートウェイ)で証明書を使う (STIR: Secure Telephony Identity (Revisited))
  - どのように電話番号の所有を証明するか？=> キャリアが端末にトークンを発行しておき、これを用いて発行
    - draft-peterson-acme-authority-token
- ACME IP Identifier Validation Extension
  - https://tools.ietf.org/html/draft-ietf-acme-ip-01
  - IPアドレスに対して証明書を出来るようにする
  - 拡張として, タイプ:”ip”, チャレンジ:“reverse-dns-00”

ACME Token Identifier and Challenges

https://tools.ietf.org/html/draft-barnes-acme-token-challenge-00
https://tools.ietf.org/html/draft-barnes-acme-service-provider-code-00

- “ACME Identifiers and Challenges for VoIP Service Providers”の汎用化の試み
  - https://tools.ietf.org/html/draft-ietf-acme-service-provider-02
  - タイプ:“tn”, チャレンジ:”spc-token-01”(<=これが汎用的)
- “spc-token-01”が名前のバリデーションをCAからCA以外のAuthorityに委譲する汎用的な枠組みになっていたので, この基本アイデアを, より汎用的なものにリバイズしたもの
- ステータス
  - ブラッシュアップ後、次回ロンドンにWGアイテムにするか判断



ACME STAR
https://tools.ietf.org/html/draft-ietf-acme-star-02

- STAR: Support for Short-Term, Automatically-Renewed (STAR) Certificates in ACME
- TLSサーバはロードバランサ等の中間ノードで終端されるケースがあり
- ドメイン制御ができるエンティティが，証明書の更新をロードバランサなどの別エンティティに委譲するための機構がSTAR
- ステータス
  - 前回会合(99)でWGアイテムに採用
  - TBDを埋める作業、Security Consideration