Web-related WG Report (IETF90)

株式会社レピダム

前田 薫 (@mad_p)

IETF90報告会 2014/08/25

Agenda

- 自己紹介
- 参加の背景・経緯
- httpbis WG
- httpauth WG
- oauth WG

- IETF90
  - Toronto, Canada
  - July 20-25

自己紹介

- 名前
  - 前田 薫
- 所属
  - 株式会社レピダム
シニアプログラマ
マネージャ
- コミュニティー活動
  - Lightweight Language
  - Identity Conference
  - http2勉強会

- 業務領域
  - 認証・認可、デジタルアイデンティティー、プライバシー
  - 標準化支援
  - ソフトウェアセキュリティー、脆弱性

経緯・背景

- 「HTTP相互認証プロトコル」の標準化支援
  - httpauth WG(Sec Area)
    - https://tools.ietf.org/html/draft-oiwa-http-mutualauth
  - (独)産業技術総合研究所様の研究成果
    - https://www.rcis.aist.go.jp/special/MutualAuth/
- IETFや標準化との関わり
  - IETF89から参加
  - HTTP/Webと認証を中心に
- 標準化支援や最新動向のコンサルテーション等をしています

httpbis WG (Mon Jul 21, Tue Jul 22)

- Hypertext Transfer Protocol Bis
- HTTP/2 WGLC秒読み → 8/1 WGLC
  - 仕様はML上でほぼ固まった
  - プロキシについて議論
- HTTP/1.1 update
  - RFC7230-7235

HTTP/2

- HTTP/2

  8/1付でWorking Group Last Call

- 目的
  - 環境を限定しないパフォーマンス改善
  - ネットワーク資源の効率的な使用
  - 現代的なセキュリティ要件および慣習の反映
  - いくつかの提案の中からGoogleのSPDYプロトコルをスタートポイントに策定を開始

HTTP/1.1とHTTP/2の違い

- HTTPヘッダーのバイナリ化
- HTTPヘッダーの効率化(圧縮)
- 多重化(Multiplexing)
- 優先制御(Prioritizing)
- 通信の開始方法
- TCPコネクションの利用方針
- etc...

HTTP/2 draftの最近の歴史

- draft-ietf-httpbis-http2 (h2)
  - 日本語訳
    - http://summerwind.jp/docs/draft-ietf-httpbis-http2-14/
- draft-ietf-httpbis-header-compression (HPACK)

Date	h2	HPACK	WG Activity	備考
2014/02/13	10	06	Interim 2014/1 Zurich	
2014/04/03	11	07	IETF89	
2014/04/23	12			HPACK更新なし
2014/06/17	13	08	Interim 2014/6 New York	
2014/07/30	14	09	IETF 90	WG Last Call

HTTP/2 最新仕様の主な変更点

- 拡張性が復活
  - 誰でもが使うものでない機能は拡張機能へ
    - content gzip, ALTSVCなど
- フレームサイズを2**24-1 (16M)まで拡大可能
  - フレームサイズは3オクテットで表現
- pseudo headers(「:」で始まるもの)は最初に
- HPACK
  - 簡略化: reference setの削除、ヘッダの順序保存
  - 「ヘッダテーブルに追加しない」リテラル
    - 圧縮率観測攻撃の対象になるヘッダで使用、プロキシへの指示
  - ハフマンテーブルの更新

HPACK reference set削除

- reference setとは
  - 前回のHEADERSの中身を覚えておき、差分だけ送信
  - 同一のヘッダフィールドは送らない
    - まったく同一の場合は空のHEADERSフレームを送る
- reference setの問題点
  - 最後まで読まないと中身がわからない
    - 接続先(:authority, :scheme)が不明
  - ヘッダの順番が保たれない
  - 圧縮率に貢献するというデータがない
  - 実装がややこしくなりバグの元
- 山本和彦さんの指摘により再検討され、削除に至る

HTTP/2今後の予定

- 8月いっぱい WG Last Call
- 11月中旬、 IETF 91 Honolulu
  - http/3の仕様検討?
- 2014内(?) IETF Last Callをめざす

プロキシについて

- HTTP/2でend-to-end TLS encryptionの普及が進む
  - TLSのALPN拡張によるHTTP/2への切りかえ
  - 暗号化のmandateはされなかった
- end-to-end暗号化世界でのプロキシの役割
  - 現状分析
  - Trusted Proxyが使われている例
  - HTTP/1.1でのプロキシ定義振り返り

プロキシの現状について

- HTTP/2におけるプロキシについて(Adam)
  - SPDYでは間にプロキシがあるために接続できない人がいる
  - コンテンツfilteringはクライアントでやるべき
- Trusted Proxyとコスト(Peter)
  - ネットが遅い地域ではOpera Miniが普及
  - サーバー側でTLSをほどき、高圧縮で送信
  - CDNではラストマイルはサポートできない

Explicitly Authenticated Proxy(Salvatore)

- userのexplicit consent下で動くプロキシ
- これまでとは別のカテゴリのプロキシ
  - reduce data usage
  - content filtering
  - accessには干渉しないが、optional servicesを提供するもの
- Proxy Certificate
  - opt outの必要性
  - per requestではなくブラウザ設定で

そもそもProxyって何だ(mnot)

- HTTP/1.1ではどう定義されているか
  - explicitly allows transformation and cache
  - explicitly configured by clients
  - HTTPS request is end-to-end
- これらのプロキシの定義を変えるのは大変
  - 機能追加ではなく現在のコンセンサスの変更である
  - IETFは政治的にはサイドを取らないが、↑を選ぶとサイドを取ることになる
- What can we do?
  - publish "proxy problem" draft
  - standardize proxy.pac
  - find other ways to address underlying use cases

プロキシのディスカッション

- MITMプロキシの問題
  - オリジンサーバーの証明書を渡せない
  - end-2-endセキュリティーではない
  - 「HTTPがMITMを許容」なんて見出し見たいか?
- 保護の必要なコンテンツの分離
  - サーバーが秘匿性を表明したい
  - ムービーだから内容は秘密じゃない
- フレームごと暗号化は考えたけど複雑すぎ
- トレードオフと選択は選択者によって違う
- 検閲は分けて考えないといけない
- アフォーダンスが必要だ。選択肢だけではダメ

プロキシディスカッションまとめ

- Mark
  - HTTPS is inviolate
  - Maybe some interest in opt in to soften that
  - Some interest in adorning TLS
  - Interest in normalizing what an intercepting proxy is
  - Interest in encrypted caching.
  - Open issue on how opportunistic security interacts with a proxy

HTTP/2以外の仕様

- HTTP/1.1 → RFC7230-7235
  - RFC2616を分割、6つのRFCになった。http/2ではそのうちの1つだけを置きかえる(wire format)
  - goals: wire formatとそれ以外を分離
  - 他の仕様にあったものでbase RFCにあるべきだったものをcherry-pickingした
- RFC7238: 308 permanent redirect
  - expirimental → proposed standard
- RFC5987: character set
  - UTF-8だけを要求すればよく、ISO-8859-1 必須はドロップしてよい
- RFC6266: Use of the Content-Disposition Header Field
  - Proposed Standard → Internet Standard.

その他の文書の検討

- draft-nakajima-httpbis-http2-interop-survey
- draft-ietf-httpbis-alt-svc
  - 拡張になったAltSvcのissuesについて
- draft-ietf-http2-encryption
  - 日和見暗号とHTTP/2の関係
- draft-hutton-httpbis-connect-protocol
  - WebRTCがHTTPトンネルを使って送信されていることがわかるようにしてほしい → 炎上

httpauth WG (Mon Jul 21)

- Hypertext Transport Protocol Authentication
- 現在の機能の不足や安全性等、課題の多いHTTPプロトコルの認証機構を、新しく安全にすることを目指す
  - TLSを用いる方法やHTMLのフォーム認証はスコープ外
- 新しい認証をExperimental RFCとして策定
  - 現在ある複数の提案を統合したり選んだりするのではなく相互にレビューする形
  - 仕様と実装とどっちが先かの問題を避ける
- BasicおよびDigestの国際化、Digestのアルゴリズム更新もスコープ
  - こちらはStandard Track RFCを目指す

Basic認証、Digest認証、SCRAM

- Basic認証、Digest認証はWGLCが近い
- Digest認証
  - ユーザ名ハッシュ化: 前回のリベンジ
    - セキュリティーのためではなくプライバシー
- Basic認証
  - パラメータ「charset」を追加
  - 拡張パラメータの可能性を検討
- ユーザ名、パスワードの国際化
  - UTF-8 NFCとする
  - realmの国際化はoverkill
- SCRAM: 1-round-trip reauthenticationなど

mutual認証

- ドラフトはわかりやすさのための修正が中心
- password strengthening function
  - MLで提案が多くあったが、標準でないので見送った。将来入れることができる
- NIST curvesでよいのか問題
  - ここでは難しい
  - tls WGでの動向を見て合わせる方向

oauth WG (Thu July 24)

- Web Authorization Protocol
  - OAuth 2.0とその周辺仕様を検討
- IETF90でのトピック
  - Dynamic Client Registration
  - Token Introspection
  - Proof-of-Possession Security
  - OAuth Symmetric Proof of Possession for Code Extension
  - Providing User Authentication Information to OAuth 2.0 Clients
  - OAuth 2.0 Token Exchange
  - Request by JWS ver.1.0 for OAuth 2.0

oauth WGの議論

- Dynamic Client Registration
  - 文書構造をリファクタ
  - application_type: nativeの定義を書きたくない
  - management API
    - 人によってめざす方向が違いすぎる → experimental?
- Proof-of-Posession Security: 後述
- Token Introspection
  - トークン検証をAuth Serverに聞くAPI

oauth WGの議論 (cont'd)

- OAuth Symmetric Proof of Posession for Code Extension
  - code interception attack対策
  - clientでone-time credentialを作成
    - authorization request と token request で送信
    - ASでは2つのリクエストの送信者が同一であると検証
- OAuth 2.0 Token Exchange
  - act_as, on_behalf_of関連を表わすため、token endpointで別のaccess_tokenに交換してもらう

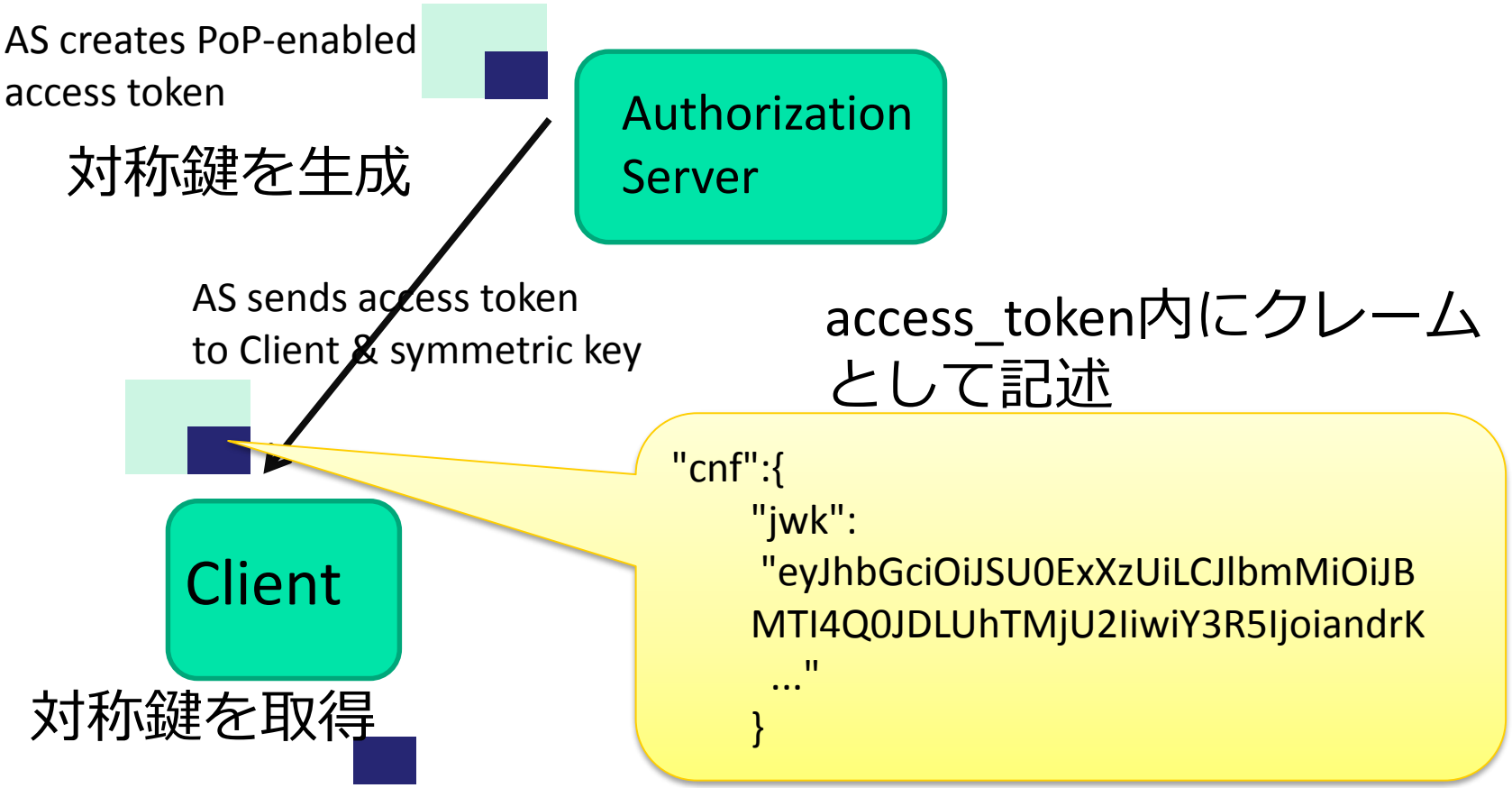
oauth WGの議論 (cont'd)

- Request by JWS ver.1.0 for OAuth 2.0
  - Authorization リクエストをJWTで表現
    - x-www-form-urlencodedの代わりにJSONを使い、JWTにパッケージ
    - JWSで署名またはJWEで暗号化
  - またはそのJWTのURIを送信
  - → この方法をHTTPリクエスト一般に拡張するとIoT向けリクエスト署名などに使えそう

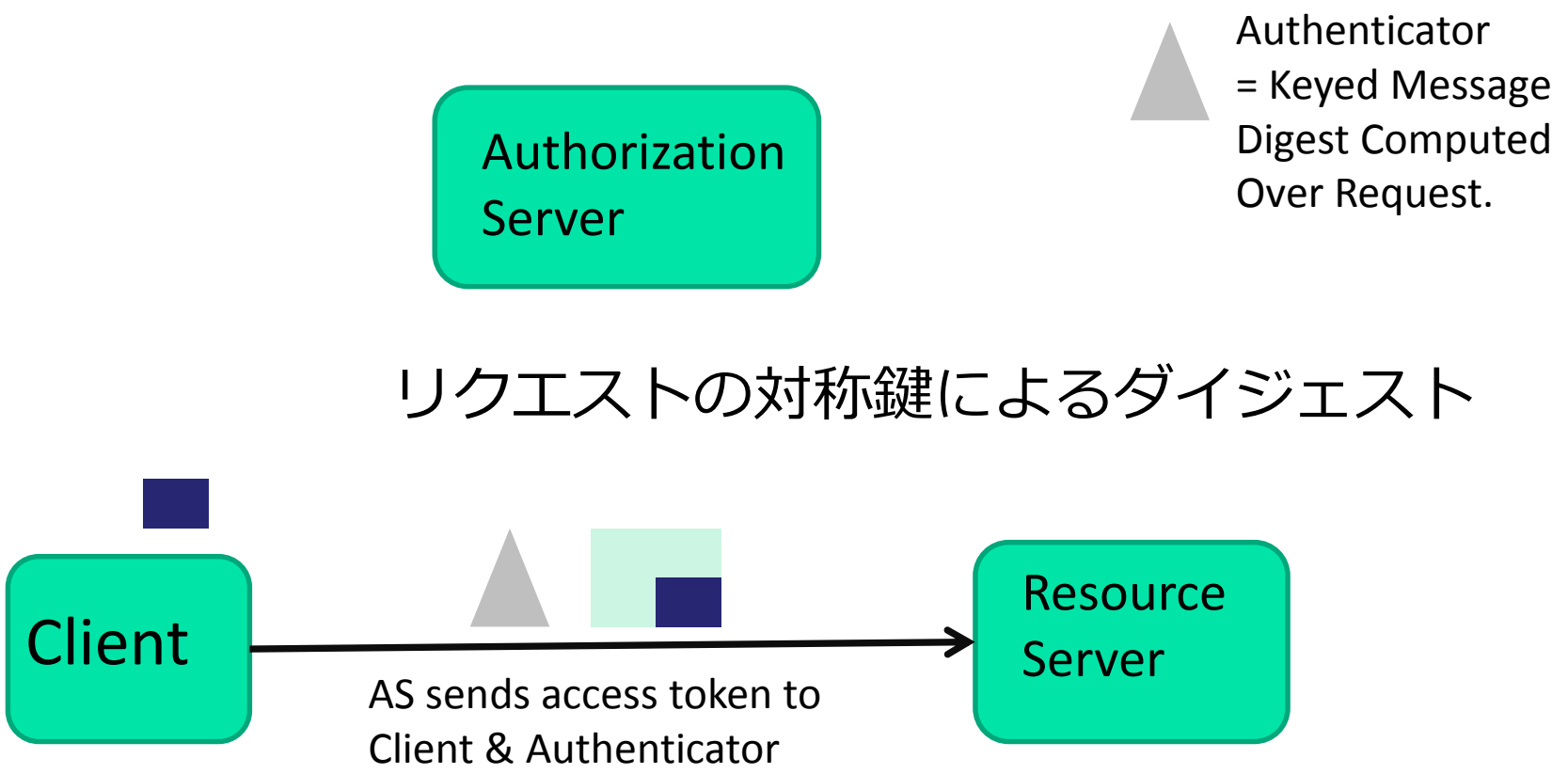
Proof-of-Possession Security

- http://www.ietf.org/proceedings/90/slides/slides-90-oauth-7.pptx
- 複数のリクエストにおいて、クライアントが鍵を持っていることを以て同一であることを証明
  - 例: authorization request 送信者とresource access request 送信者が同一である
- draft bundle
  - draft-richer-oauth-signed-http-request
  - draft-bradley-oauth-pop-key-distribution
  - draft-hunt-oauth-pop-architecture
  - draft-jones-oauth-proof-of-possession
- 実装が必要!

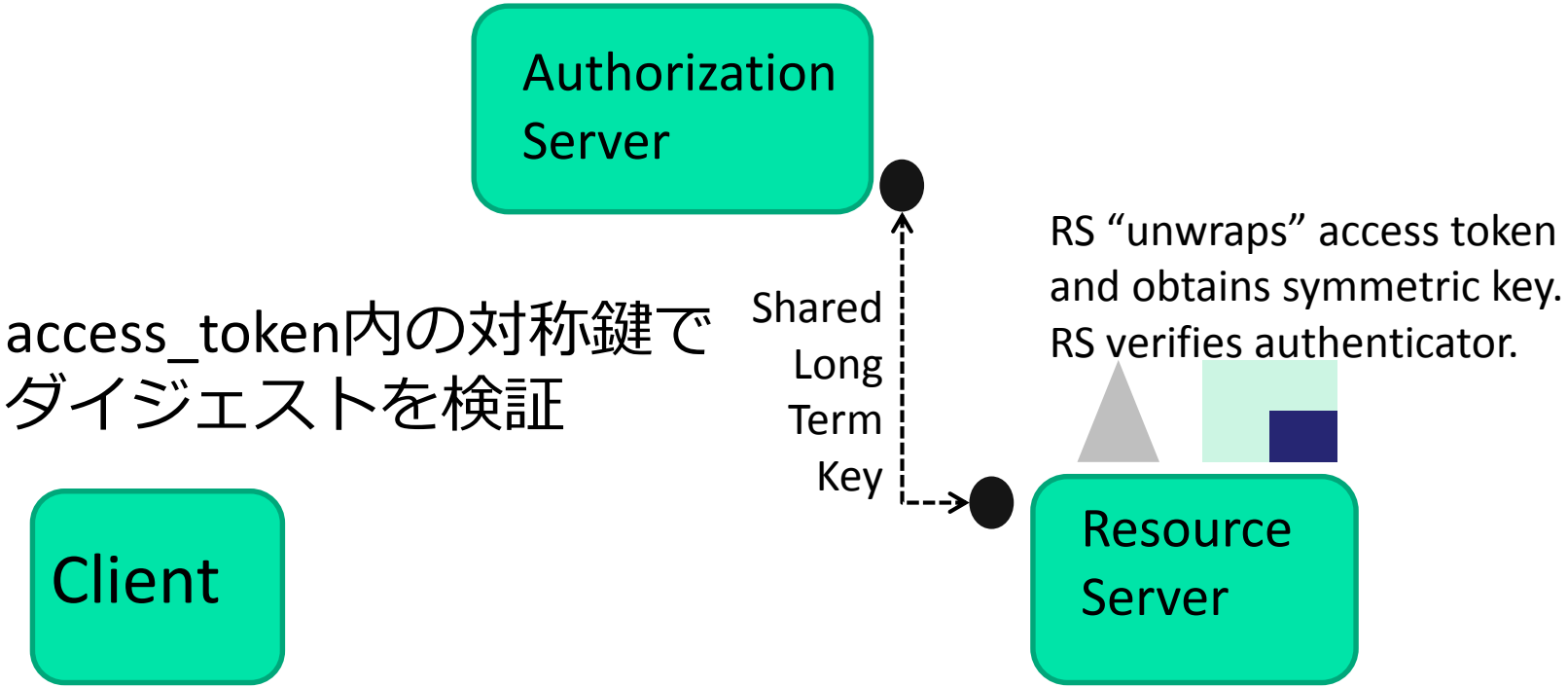
AS <-> Client Interaction Example: Symmetric Key



AS <-> Client Interaction
Example: Symmetric Key



AS <-> Client Interaction Example: Symmetric Key



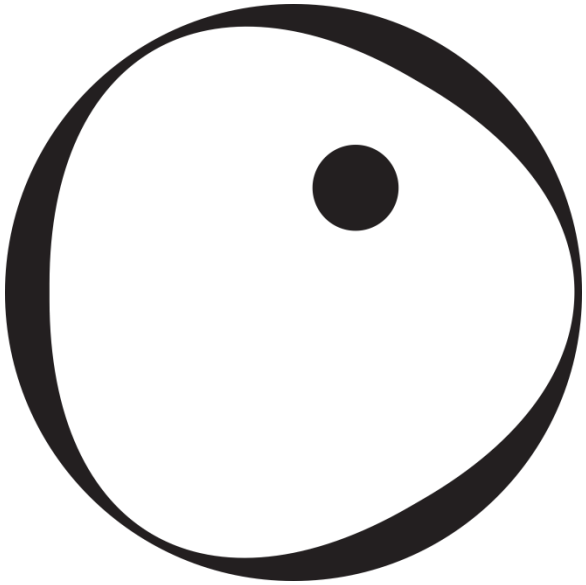
却下された提案

- Providing User Authentication Information to OAuth 2.0 Clients
  - 「OAuth2認証」→ 必要性不明
  - OpenID Connectでいいじゃん

まとめ

- HTTP/2 がWGLCに
  - 実装も増え、interopも活発に
- httpauth
  - Basic, Digest認証の修正がWGLC真近
- oauth
  - proof-of-possession, HTTP request signingなどIoTに応用の効く提案も

Any Questions? / Please Feedback!



lepidum

https://lepidum.co.jp/

mailto:maeda@lepidum.co.jp / twitter: @mad_p