DNS関連技術動向
～KIDNS（Keys In DNS）について～

JPRS 白井 出

2010/11/25 DNSOPS.JP BoF

KIDNS (Keys In DNS)とは

- 簡単にいえば
  - デジタル証明書をDNSのレコードの中に格納する技術に関して現在行われている検討
  - 基本的にはRFC 4398 (2006年)でCERT RRとして規定されているもの

話としては古くからある

- RFC 2538 (1999年 obsoleted by 4398)
  - Storing Certificates in the Domain Name System (DNS)
  - X.509やPGPの証明書や指紋を格納するためのCERT RRというものを定義したRFC

なぜ今話題になっているのか？

- 一言でいえば「DNSSECの普及が本格化」したため
  - デジタル証明書をDNS経由で配布するとして、そのDNSは安全な配布手段と言えるのか？
    - 最初（RFC 2538の時点）からDNSSECが前提となっていた
  - 今年、rootゾーンの署名で「DNSSECの普及が本格化」したことにより、CERT RRの実用化を望む声が増えた
    - 同時多発的に発生していたようだが、CENTR(*)方面でまとめる話が出て、IETFで議論をする流れとなった
    - 8月17日 IETF Non-WG ML Keyassureとして立ち上がった
      - https://www.ietf.org/mailman/listinfo/keyassure
    - 10月26日 KIDNS WGというWG Proposalが出ている
      - IETF80の前には立ち上がる見込み

(*) ヨーロッパ地域におけるccTLDレジストリの連合体

この技術の背景

- 既存のモデルの問題
  - あるCA局を信用すると、そのCA局によって証明される全ての証明書が信用されてしまう
  - 特定のCA局で証明された特定の証明書を信用するということができない
- 一つの考え方
  - ドメイン名の一致を重要な目的とする証明書では、DNSで自己署名証明書を配布するほうがリーズナブル？
    - そうすれば個々のドメインごとに信用情報をコントロールできる
    - ドメイン以外の証明を目的としたければ、既存CA局の証明書を使えば良い

CERT RRとは具体的にどんなもの？

RFC 4398の中での定義

RRの形式

```
EXAMPLE.JP.   IN CERT <type> <key tag> <algorithm> <Certificate or CRL>
                      16bit   16bit      8bit            Binary
     <type>:      Certificate Type Values
     <key tag>:   RRSIG Key Tag algorithm
     <algorithm>: same meaning in DNSKEY and RRSIG RRs
```

RFC 4398におけるCertificate Type Values

Value	Mnemonic	Certificate Type
0		Reserved
1	PKIX	X.509 as per PKIX
2	SPKI	SPKI certificate
3	PGP	OpenPGP packet
4	IPKIX	The URL of an X.509 data object
5	ISPKI	The URL of an SPKI certificate
6	IPGP	The fingerprint and URL of an OpenPGP packet
7	ACPKIX	Attribute Certificate
8	IACPKIX	The URL of an Attribute Certificate
9-252		Available for IANA assignment
253	URI	URI private
254	OID	OID private
255		Reserved
256-65279		Available for IANA assignment
65280-65534		Experimental
65535		Reserved

CERT RRの設定例

```
www.example.jp.          86400 IN CERT PKIX 0 RSAMD5 (
                                MIIDajCCAlICQDcJa4wW3oEDjANBgkqhkiG9w0BAQQF
                                ADB3MQswCQYDVQQGEwJKUDEOMAwGA1UECAwFVG9reW8x
                                EDAOBgNVBAcMB0NoaXlvZGExDTALBgNVBAoMBEpQUlMx
                                FTATBgNVBAMMDEl6dXJ1IFNoaXJhaTEgMB4GCSqGSIb3
                                DQEJARYRc2hpcmFpQGpwcnMuY28uanAwHhcNMTAxMTE4
                                MDUOMDQyWhcNMTAxMjE4MDUOMDQyWjB3MQswCQYDVQQG
                                EwJKUDEOMAwGA1UECAwFVG9reW8xEDAOBgNVBAcMB0No
                                aXlvZGExDTALBgNVBAoMBEpQUlMxFTATBgNVBAMMDEl6
                                dXJ1IFNoaXJhaTEgMB4GCSqGSIb3DQEJARYRc2hpcmFp
                                QGpwcnMuY28uanAwggEiMA0GCSqGSIb3DQEBAQUAA4IB
                                DwAwggEKAoIBAQDftsnvDxmLLNx7uoiUTjo/QDDOPYoh
                                b1tXySUGZLabIqQvNLptQZL2fZTgK9buACDMXoGvxCLQ
                                jDdikeojCFwxCVSFfcTf1E1IVb1QOdvJFvpkIrbF2VZf
                                R2x6Z2p/DrX/21aRImtemfN95uAtFX4oNMSxLKjanIZp
                                7TbD6hFFg5+Nw9CLDvygE6dA7KIm/kr+KpgAtYaHdt8R
                                oNafQWSIJIaeTxn01vjVfF6Pa8yBII2jh3osXEABg6HP
                                8uVZnvN3qZzydwBoREMFOm5YxcJ1rt1skrCfGFFK3eo/
                                ma+3RoB9ZpJBo+MHpI1VTGj9KB2taKOxHzOEk6YSBPHQ
                                Ivi7AgMBAAEwDQYJKoZIhvcNAQEEBQADggEBAErdVRFw
                                kLaAz8+Q9NOSmWgqOZMoxgKS89nDwUMg29grFKtbhjwU
                                ZdzdMC6vyM/3v1MzzizFdqrrgDLAwDG+aPVTn9OfpSMi
                                qZjkUZHrRmgLNwWcv1LXsVdmRLKr6OOmGjpFAEFJYff7
                                tQj+QftaYLkGOBUtc2yT9+Z+NPGBXZJvcLVBZwxzJs0e
                                nWnz4bdOnzxOH4kAxOoNTOCaBOH4ftr5qXtbuKVKIisT
                                b+vFqgchazHF1wUOcDZdsOxIXFH5ueOhbfbBXUOTbbhM
                                JSkjwuGPm6vR1OcL2GnHmnPKN19Jv7bsN2AJrk0193rY
                                sejFAvRAPsd2ODEGvs4ygPyUKkE= )
```

大きな応答が返ってくる。
DNSSEC対応により、大きなパケットが通るようになったことも実用化への大きな一歩となっている。

アプリケーションでの実装例

- アプリケーション
  - GnuPGは以前から対応している
    - “—auto-key-locate”オプションがそれに該当する
    - 使い方は以下によくまとまっている
      - http://www.gushi.org/make-dns-cert/HOWTO.html

KIDNS WGの対象

- 目的
  - RFC 4398で定義されているCERT RRの実用化に向けて足りない部分を検討
  - 利用方法についても対象（WEBSEC WGとの境界領域になる）
- Keyassure MLでの検討
  - 以下のI-DのAppendix A.に過去の経緯がまとめられている
    - http://tools.ietf.org/html/draft-hoffman-keys-linkage-from-dns
  - 最初はTLSFP RRなどというものを定義しようとしていた
    - TXT RR形式なども議論されていた
    - が、とりあえずCertificate Type Valuesの追加を行っている

- RFC 4398でAvailable for IANA assignmentな部分の定義
- 利用方法やポリシー定義方法について

参照先

- Keyassure ML
  - https://www.ietf.org/mailman/listinfo/keyassure
- Keyassure Wiki
  - http://trac.tools.ietf.org/area/sec/trac/wiki/Keyassure
- IETF79 Beijing KIDNS BoF資料
  - https://datatracker.ietf.org/meeting/79/materials.html#wg-kidns

参考：現在のInternet Draft

- Certificate Type Valuesの拡張
  - http://tools.ietf.org/html/draft-hallambaker-certhash
    - DPKIX, DPTR
  - http://tools.ietf.org/html/draft-hoffman-keys-linkage-from-dns
    - TLSFP, TLSRQ
  - http://tools.ietf.org/html/draft-josefsson-keyassure-tls
    - TLSCERT
- ポリシー定義について
  - http://tools.ietf.org/html/draft-turner-dnssec-centric-pki
  - http://tools.ietf.org/html/draft-hallambaker-donotissue

参考：類似話題

- RFC 4255で定義されているSSHFP
  - これはSSHのホスト公開鍵のfingerprintをDNS経由で提供するもの
    - SSHを使う場面ではドメイン名が確定しているので、メリットがより明確となっている
  - RRの設定方法はCERT RRと似たような形式
  - ssh_configで”VerifyHostKeyDNS ask”などと指定することで対応できる