DNSとSSLの新しい関係

- DNSSECはSSLを置き換えるのか？-

DNSSEC 2011 スプリングフォーラム

2011-04-20

クロストラスト株式会社 代表取締役 秋山卓司

SSLの2つの機能

- 「第三者による実在証明」
- 「通信経路の暗号化」

CrossTrust

認証レベルの違い

レベル	ドメイン認証	実在審査	グリーンバー
EV	Y	国際標準	Y
OV	Y	各CA基準	N
DV	Y	N	N
自己署名	N	N	N

当初のSSL証明書

いわゆるオレオレ証明書

CrossTrust

EV SSL

- 世界的に標準化された審査プロセス
- 審査発行に関して外部監査が必須
- 最新版の主要なブラウザ（IE, Firefox, Opera, Safari, Google Chrome）で採用
- アドレスバーが緑に表示される

CrossTrust

DV証明書とは？

- サーバ運営組織の身元が第三者によって確認されているわけではない

- 既に信頼関係のあるサーバとクライアント間の通信経路を暗号化する

- SMTP over SSL, POP over SSL, SSL-VPN

オレオレじゃだめなの？

- オレオレだと鍵配送問題が解決できない
- ブラウザ・OSが信頼しているルート
  を使うためにDV証明書がある
- CAがドメイン所有者を確認して発行
  →よく使われる方法はメール到達性

CrossTrust

鍵配送問題の例

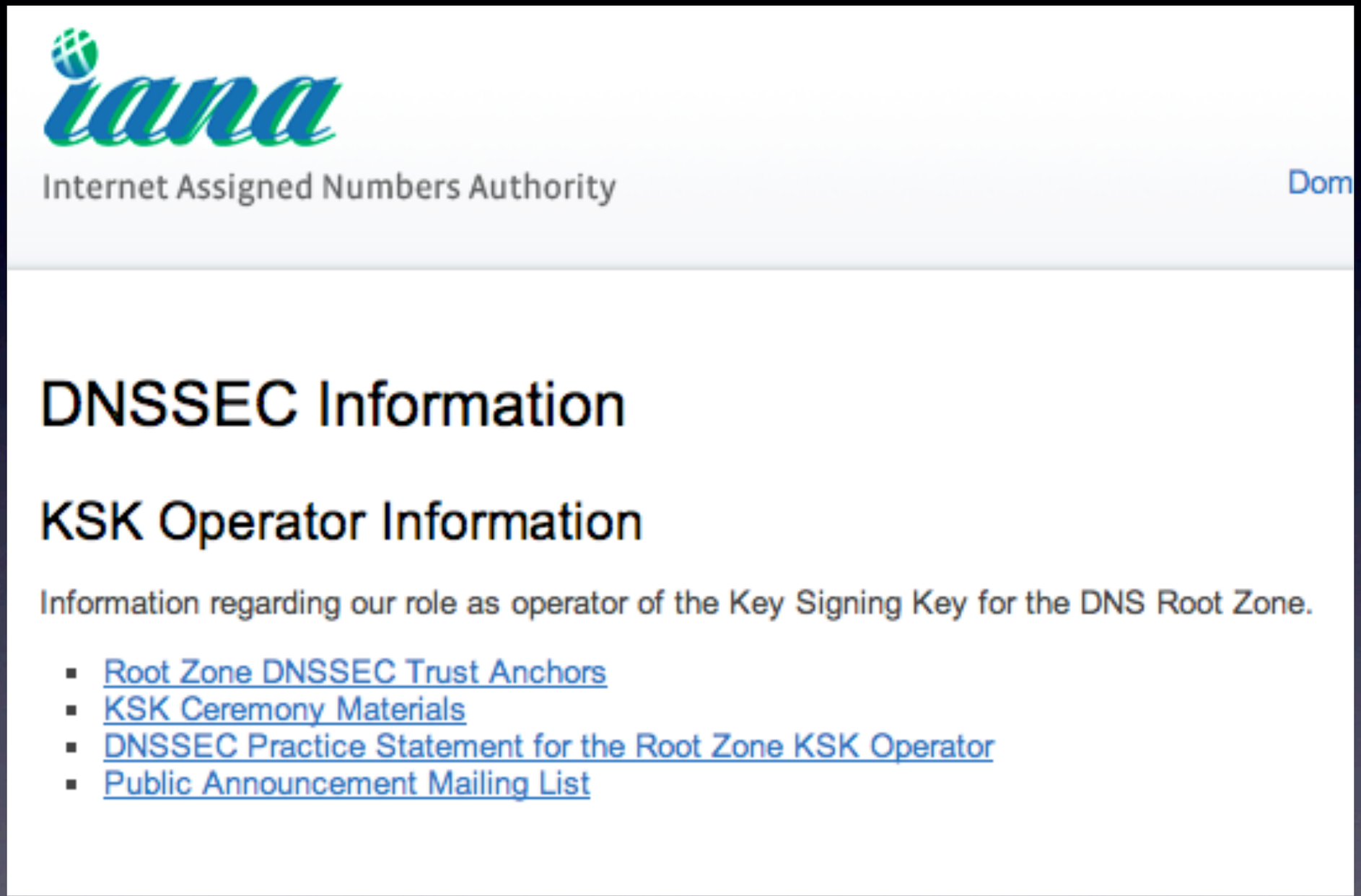
DNSSEC を利用するリゾルバーのための
トラストアンカーの設定方法について

“ 執筆段階では、ルートゾーンのKSKに対する署名に使われているOpenPGPの鍵やS/MIMEの証明書がICANNのものであることを確認できず、厳密に配布元を確認する手段がありません。”

http://dnssec.jp/wp-content/uploads/2011/02/20110124-techwg-dnssec-trustanchor-install-howto-2.pdf

CrossTrust

探してみた



https://www.iana.org/dnssec/

CrossTrust

あれ？

CrossTrust

閑話休題

話はもどって...

- ドメイン所有者を確認するのにいちいちメールを使うのって、どうだろう...
- そもそも鍵配送問題が解決できるならオレオレ証明書でもいいよね？

CrossTrust

DANE/TLSA

- DNS-based Authentication of Named Entities
- 証明書もしくはハッシュ値を返す
- DNSSEC経由で配ると、ドメインと証明書の関係性が保証できる！
- 今年の夏くらいには？

http://tools.ietf.org/html/draft-ietf-dane-protocol-06

CrossTrust

CAA

- DNS Certification Authority Authorization (CAA) Resource Record
- 認証局(CA)の情報を返す
- DNSSECが推奨されるが必須ではない

http://tools.ietf.org/html/draft-hallambaker-donotissue-03

CrossTrust

DANEで可能になること

- オレオレ証明書の鍵配送問題の解決
  →DV証明書と同等なことが可能に
- ドメイン所有者が信頼できるかどうか
  は別問題 → EV/OV証明書は今後も必要

CrossTrust

SSL不正発行問題

- 証明書を不正に取得できただけでは攻撃は成立しない
- DNSもしくは経路情報の偽装が必要
- DNSSECが信頼性を補完できるか？

問題点？

- DNSSECでもSSLと同様な攻撃が可能？
- 問題があった場合に、それを取り除く

ことが容易ではない

http://blog.thoughtcrime.org/ssl-and-the-future-of-authenticity

to be continued...

- 証明書屋さんはあんまりDNSのことに詳しくないし多分その逆もまた真かと
- 本件に興味のある方は、ぜひ今後も継続的に情報交換させて下さい

twitter: @yet2come

CrossTrust