Opportunités d'affaires pour DNSSEC

DNSSEC Roadshow,
Dakar, 21 March 2014

aalain@trstech.net

C’est quoi le DNS déjà ?

- Le DNS convertit les noms (www.nic.sn.) en des numéros (196.1.95.19)
- ..pour identifier des services comme le www and e-mail
- ..qui identifie et lie les clients aux fournisseurs et vice versa

+1-202-709-5262
VoIP

US-NSTIC effort

DNS fait partie de tous les écosystèmes IT

facebook

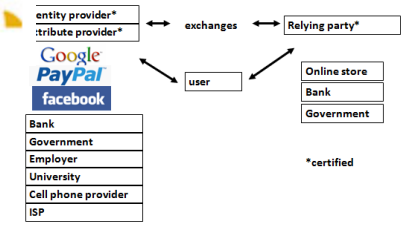
Google

OpenID

PayPal

ebay

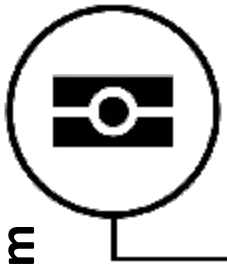
AADHAAR



OECS ID effort

amazon Prime

e-Passport symbol

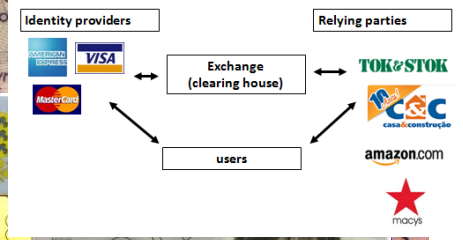


ICP Brasil
O Brasil na era da certificação digital

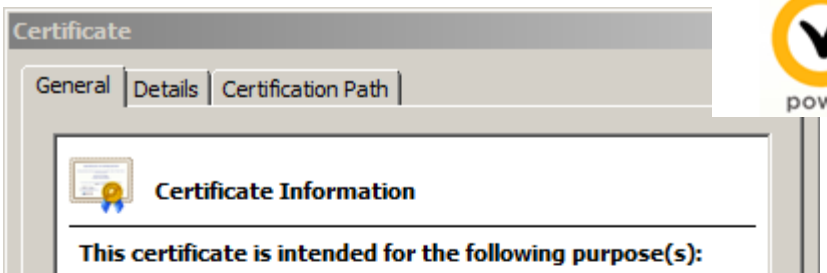
DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online

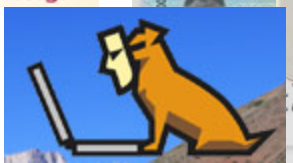
Trust frameworks are not new



Smart Electrical Grid



Norton SECURED
powered by VeriSign



lamb@xtcn.com

mydomainname.com

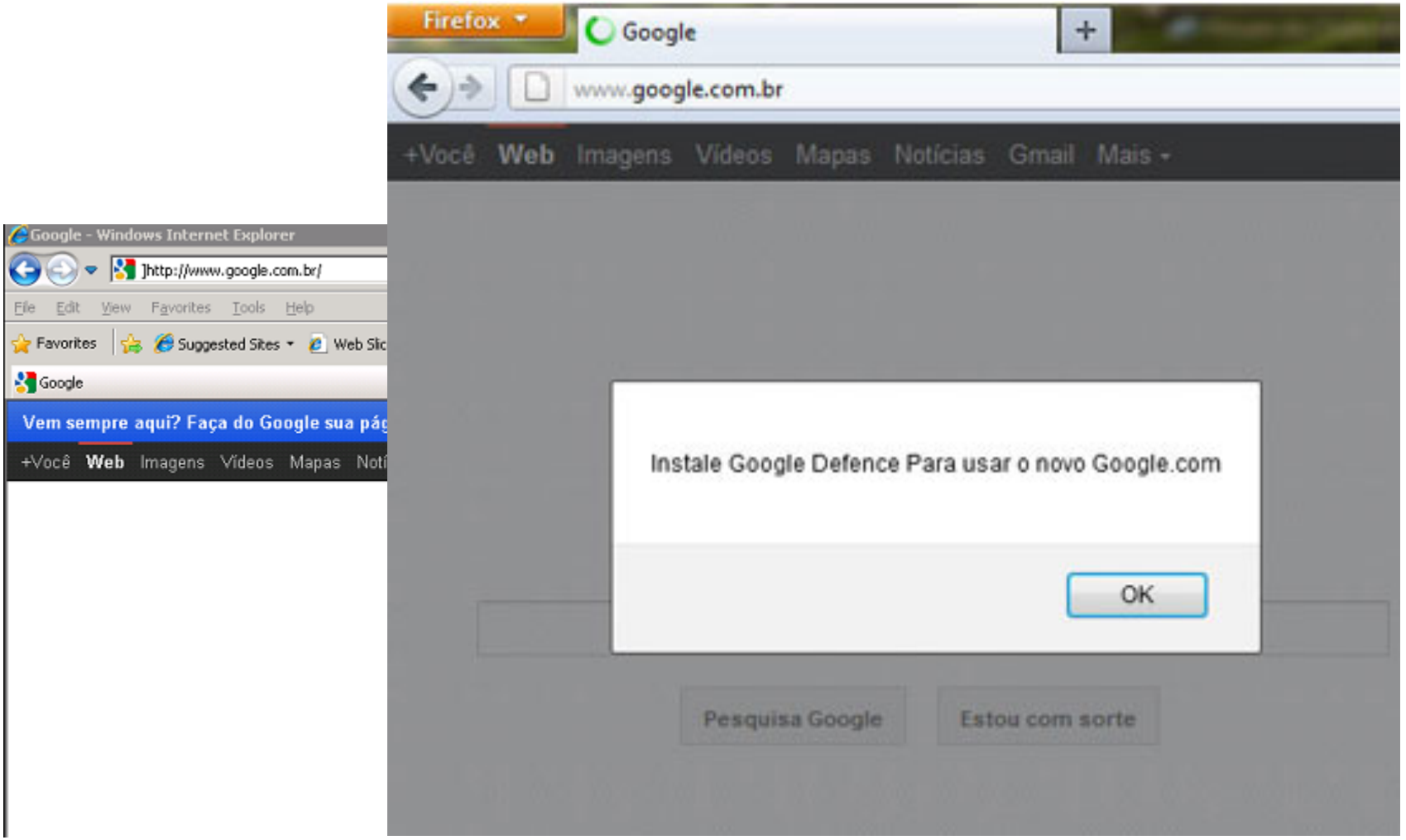
Où est-ce que le DNSSEC rentre en jeu

- ..mais les CPU et les hauts débits disponibles ont rendu le DNS classique vulnérable aux attaques to MITM.
- DNS Security Extensions (DNSSEC) introduit les signatures digitales dans le DNS to cryptographiquement protéger les contenus
- Avec DNSSEC déployé, un fournisseur pourra être sûr que les clients obtiennent des données non modifiées (et visa versa)

Piraterie: DNSChanger - ‘Le plus grand “Takedown” dans l’histoire ’ – 4M machines, 100 pays, $14M

Nov 2011 http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/
End-2-end DNSSEC validation would have avoided the problems

Piraterie: ISPs victimes de série d'attaque DNS



7 Nov 2011 http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil

End-2-end DNSSEC validation would have avoided the problems

Piraterie: Autre DNS détournements DNS*

- 25 Dec 2010 - E-Payement russe «Giant ChronoPay »
- 18 Dec 2009 – Twitter – “cyber armée iranienne”
- 13 Aug 2010 – attaque de phishing gmail par la chine
- 25 Dec 2010 - détournement DNS en Tunisie
- 2009-2012 google.*
  - April 28 2009 Google Puerto Rico redirige dans des attaques DNS
  - May 9 2009 Maroc a temporairement saisi le domaine google
- 9 Sep 2011 – Certificats Diginotar compromis pour les utilisateurs iraniens
- 7 Jan 2013 – Turktrust / EGO
- SSL / TLS ne vous dit si vous avez été envoyé au bon site, il vous indique simplement si le nom DNS correspond au nom dans le certificat. Malheureusement la majorité des site web dépendent du DNS pour valider les identités Le DNS est sollicité pour des choses inattendues a travers des canaux non sécurisés.

*A Brief History of DNS Hijacking - Google
http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

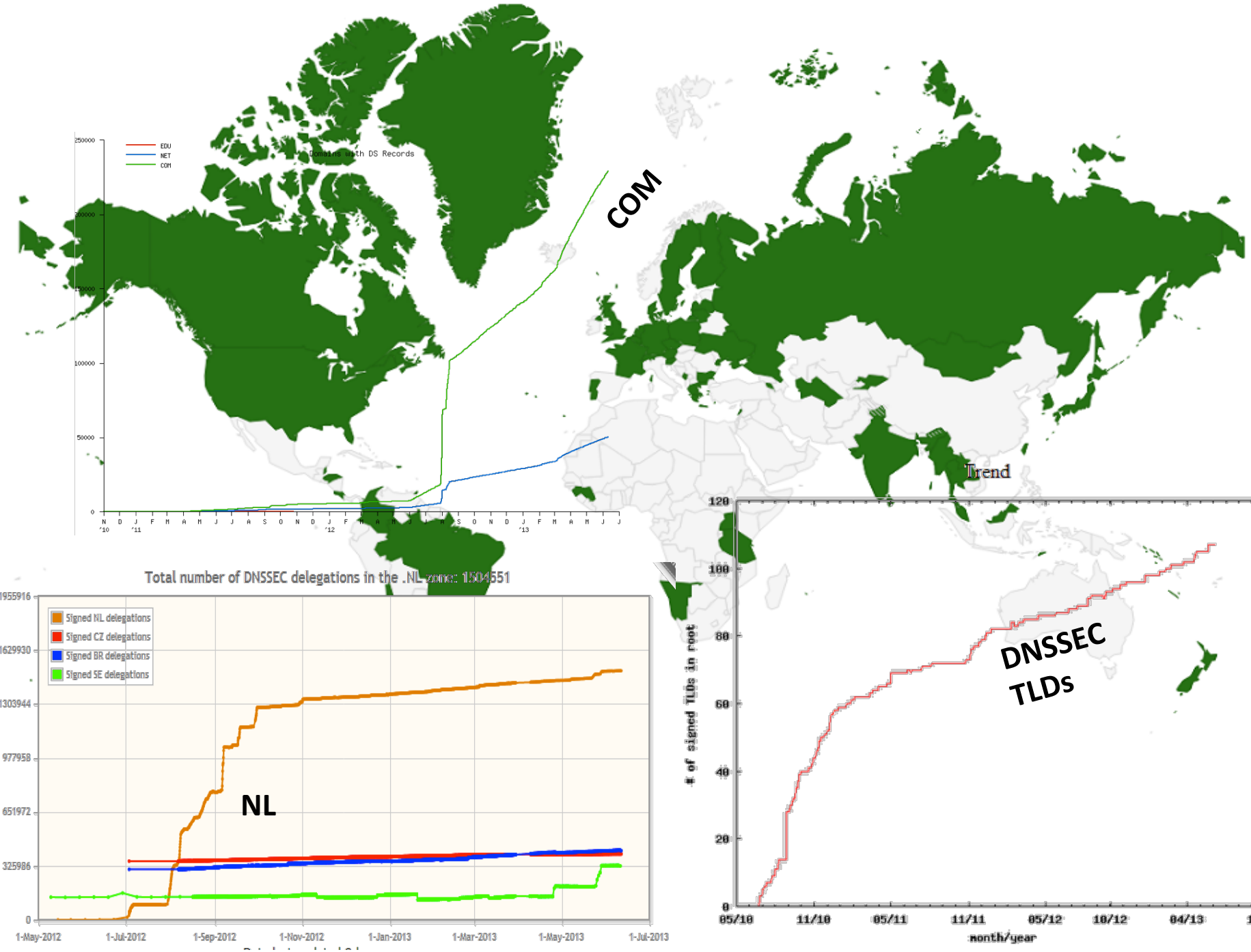
Opportunités d'affaires pour DNSSEC

- La Cyber sécurité devient de plus en plus une préoccupation importante pour les entreprises, gouvernements, et utilisateurs finaux. DNSSEC est un outil important qui fait de la différence.
- Le DNSSEC est le plus important upgrade sécurité à l'infrastructure Internet de ces 20 dernières années . C'est une plateforme pour de nouvelles applications de sécurité (pour ceux qui voient les opportunités).
- Le déploiement de l'infrastructure DNSSEC a été rapide mais nécessite une expertise. Être à l'avant de la courbe est un avantage concurrentiel.

Intérêts DNSSEC des gouvernements

- Gouvernements de SE, BR, NL, CZ et autres encouragent le déploiement de l'infrastructure DNSSEC à diffèrent niveau
- Mars 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, et Verizon ont promis de se conformer aux recommandations US FCC [1] qui inclut DNSSEC.. "A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,"[2].
- 2008 US .gov mandate. 85% operational. [3]

[1] FCC=Federal Communications Commission=US communications Ministry
[2] http://securitywatch.pcmag.com/security/295722-isps-agree-to-fcc-rules-on-anti-botnet-dnssec-internet-routing
[3] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf
http://fedv6-deployment.antd.nist.gov/snap-all.html


EDU
NET
COM
Domains with DS Records
COM
Trend
Total number of DNSSEC delegations in the .NL zone: 1504551
Signed NL delegations
Signed CZ delegations
Signed BR delegations
Signed SE delegations
NL
DNSSEC
TLDs
# of signed TLDs in root
month/year

DNSSEC – Où en sommes-nous

- Déployé sur 289/480 TLDs (.tz .nl .tt .sb .sx .cr .ag .hn .lc .bz .pr .br .gn .nz .ca .cl .de .uk .co .in .ru .pф .de .my ملیسیا .asia .tw 台灣, .kr 한국 .com .net, .post .cn .etc)
- La racine est signée** et auditée
- >86% des noms de domaines pourraient avoir DNSSEC
- Obligatoire pour les nouveaux GTLDs. Support de base par les registrars ICANN
- Adoption des ISPs en croissance*
- Des solutions de signatures***
- Adoption S/W H/W croisante : NLNetLabs, ISC, Microsoft, PowerDNS, Secure64…? openssl, mozilla: Support DANE de 1ere heure
- Standard IETF sur les certificats SSL DNSSEC (RFC6698)
- Adoption par les acteurs majeurs …(Apple iPhone/iPad, Google 8.8.8.8, …)

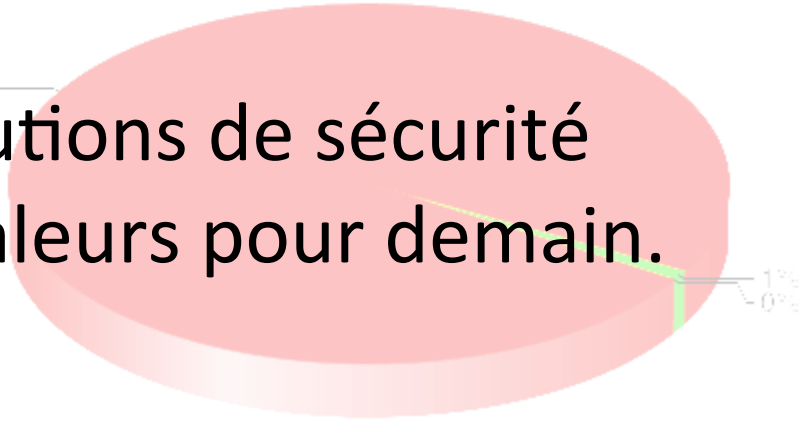
***COMCAST Internet (18M), TeliaSonera SE, Sprint,Vodafone CZ,Telefonica CZ, T-mobile NL, SurfNet NL, SANYO Information Technology Solutions JP, others..**

****Int'l bottom-up trust model /w 21 TCRs from: TT, BF, RU, CN, US, SE, NL, UG, BR, Benin, PT, NP, Mauritius, CZ, CA, JP, UK, NZ…**

***** Partial list of registrars: https://www.icann.org/en/news/in-focus/dnssec/deployment**

Mais…

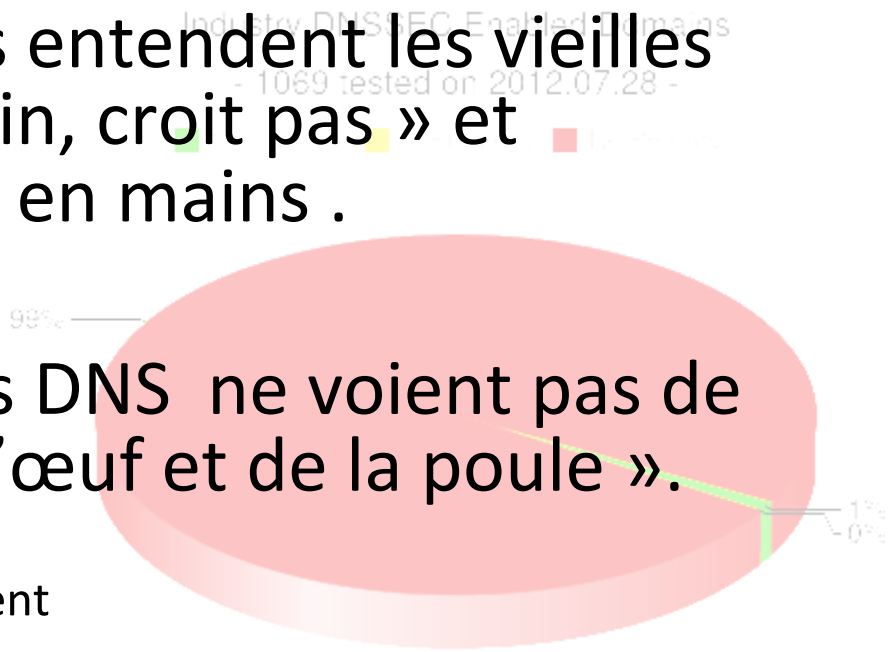
- Le déploiement est encore < 1% (~2M) au niveau des SLDs et suivants.
- DNSChanger et autres ont montré les besoins actuels. (i.e La validation DNSSEC end-2-end aurait évité ces problèmes)
- L'innovation dans les solutions de sécurité (e.g., DANE) montre les valeurs pour demain.



*** http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-com http://www.thesecuritypractice.com/the_security_practice/2011/12/all-paypal-domains-are-now-using-dnssec.html http://www.nacion.com/2012-03-15/Tecnologia/Sitios-web-de-bancos-ticos-podran-ser-mas-seguros.aspx**

DNSSEC: Quel est le problème?

- Beaucoup de départements IT ne connaissent pas DNSSEC ou sont très occupés à éteindre d'autres feux
- Quand ils s'y intéressent, ils entendent les vieilles histoires de « Peur, incertain, croit pas » et manquent de solutions clés en mains .



- Les registrars*/ hébergeurs DNS ne voient pas de demandes. Problème de " l'œuf et de la poule ».

*but required by new ICANN registrar agreement

Que pouvez-vous faire

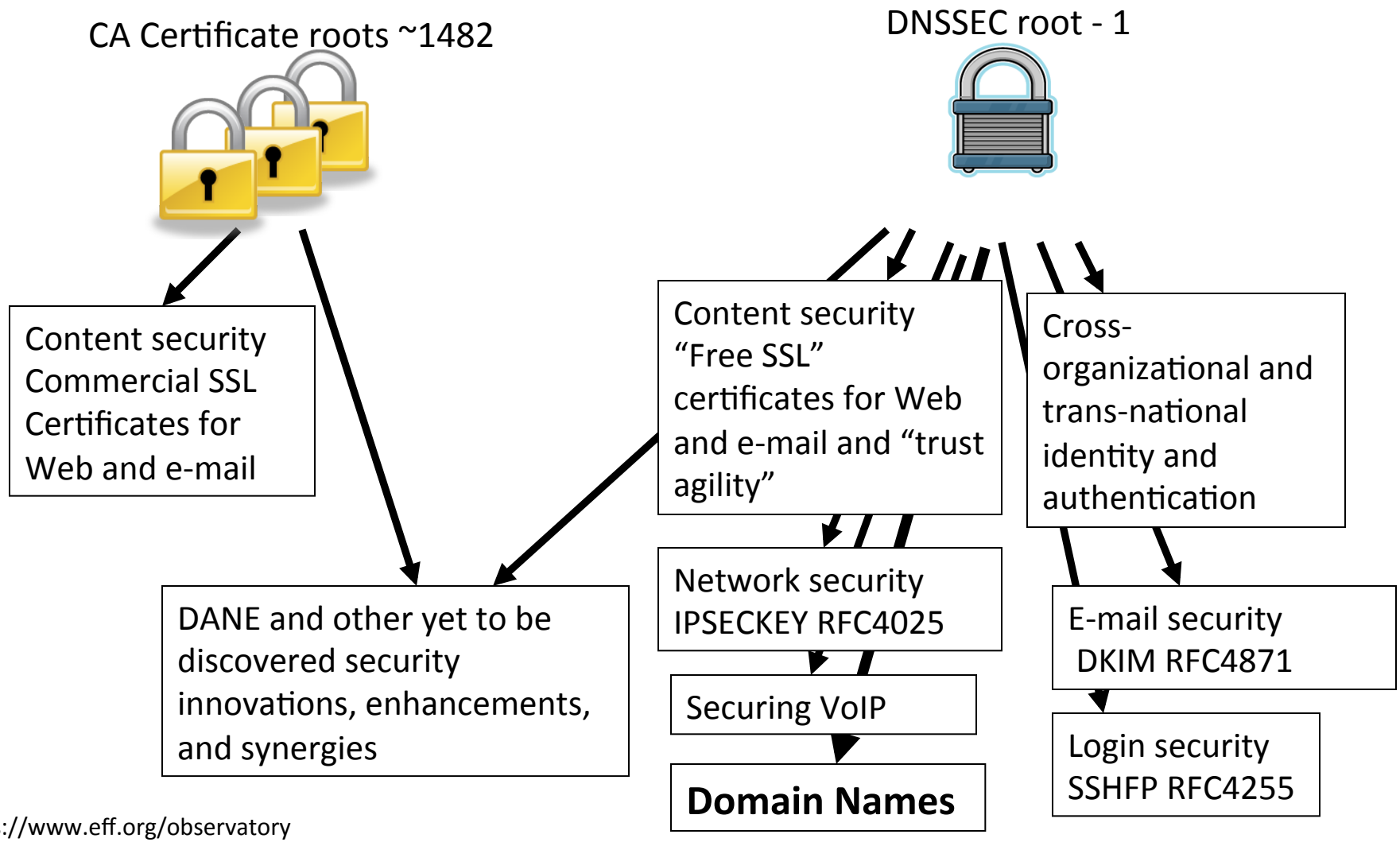
- ***Entreprises:***
  - Signer vos noms de domaine
  - Activer la validation sur vos résolveurs DNS
- ***Utilisateurs:***
  - Demander à votre ISP d'activer la validation DNS sur le résolveur
- ***Tous:***
  - Profiter de ICANN, ISOC et autres organisations qui offrent de l'éducation et formation DNSSEC

Je sens des opportunités !

Le jeu change par le upgrade de l'infrastructure du coeur de l'internet

- "More has happened here today than meets the eye. An infrastructure has been created for a hierarchical security system, which can be purposed and re-purposed in a number of different ways. .." – Vint Cerf (June 2010)

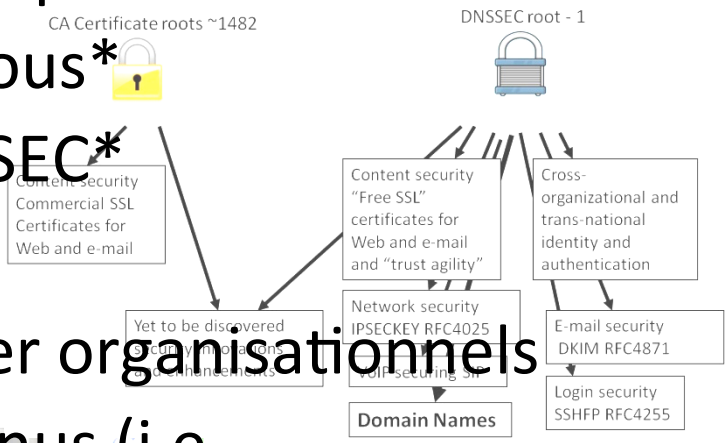
Le mauvais: Dilution de la confiance SSL
Le bon : DNSSEC = « ICP Globale “free” »



https://www.eff.org/observatory
http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

Opportunités: Nouveaux produits de sécurité

- Améliorer le SSL web et certificats pour tous*
- Sécuriser e-mail (S/MIME) pour tous*
- Valider les accès distants SSH, IPSEC*
- Sécuriser VoIP
- Systèmes d'identités digitales inter organisationnels
- Sécuriser la délivrance des contenus (i.e. configurations, updates, clés)
- Sécuriser les efforts « Smart Grid »
- Un ICP global
- Augmenter la confiance dans le e-commerce



A good ref http://www.internetsociety.org/deploy360/dnssec/

***IETF standards complete or currently being developed**

Hmm…Comment je fais confiance à ceci?

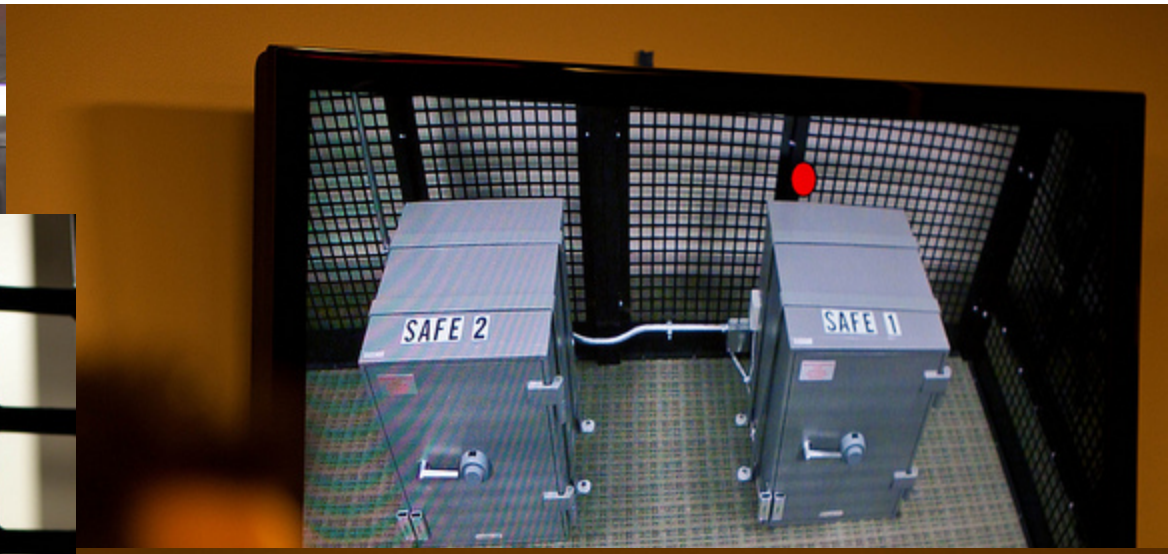
DNSSEC à la racine par ICANN (et ailleurs)

FIPS 140-2 level 4

SysTrust

DCID 6/9

http://www.flickr.com/photos/kjd/sets/72157624302045698/



Photos: Kim Davies


ICA

Photos: Kim Davies

DNSSEC: Upgrade de l'infrastructure Internet pour aider à la résolution des problèmes d'aujourd'hui et créer les opportunités de demain.

Questions ?