Sécurité et vie privée : Un nouvel Internet de confiance

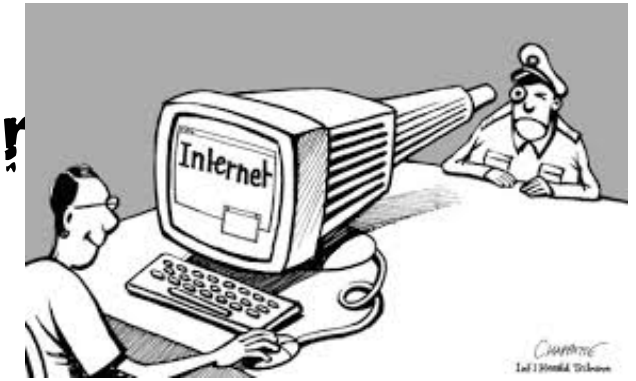
Alain Patrick AINA

AFRINIC-23

Pointe-Noire, 4 décembre 2015

Nouvelles du 6 juin 2013+

C'est officiel: USG et sa NSA font de l'espionnage de masse sur le NET



- Information est critique pour la sécurité
- Appelez ça E-Intelligence
- Illégitime#illégal

LOI n° 2015-912 du 24 juillet 2015 relative au renseignement en France

Etc. . ...

Internet sous attaque selon l'IETF

Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

S. Farrell
Trinity College Dublin
H. Tschofenig
ARM Ltd.

May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Status of This Memo

This memo documents an Internet Best Current Practice.

Définitions: Menaces et problème

Internet Architecture Board (IAB)
Request for Comments: 7624
Category: Informational
ISSN: 2070-1721

R. Barnes
B. Schneier
C. Jennings
T. Hardie
B. Trammell
C. Huitema
D. Borkmann
August 2015

Confidentiality in the Face of Pervasive Surveillance:
A Threat Model and Problem Statement

Abstract

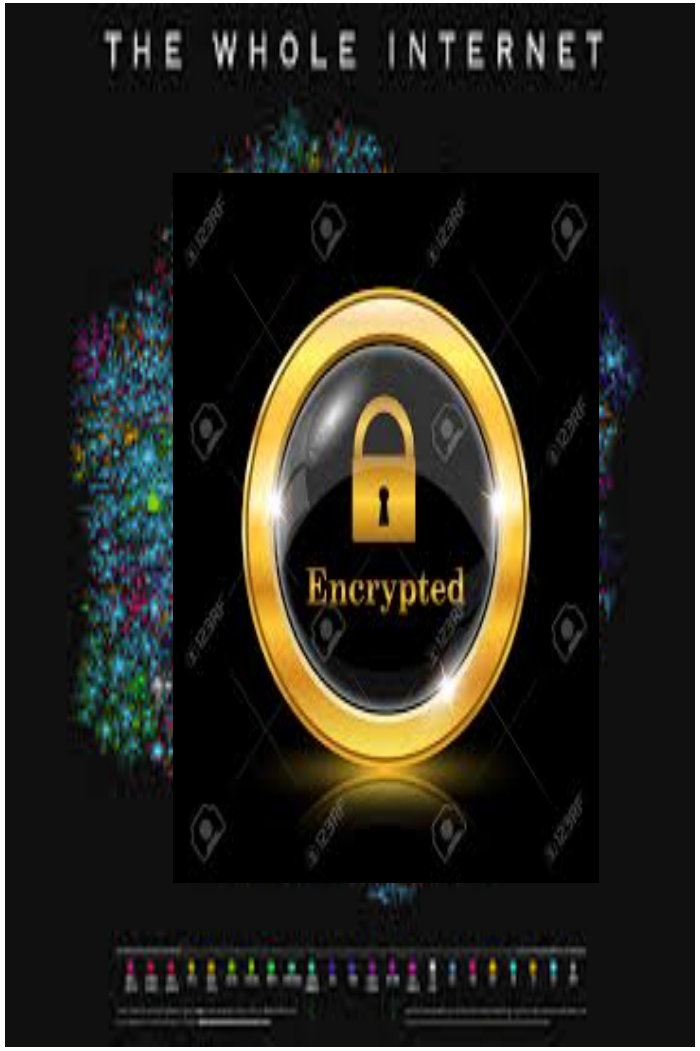
Since the initial revelations of pervasive surveillance in 2013, several classes of attacks on Internet communications have been discovered. In this document, we develop a threat model that describes these attacks on Internet confidentiality. We assume an attacker that is interested in undetected, indiscriminate eavesdropping. The threat model is based on published, verified attacks.

Solutions ?

- ✓ Crypté, crypté, tout crypté
- ✓ Même sans authentification
- ✓ Les protocoles Internet doivent intégrer la protection de la vie privée. . ..

https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

Solutions ?



IPsec, TLS, PGP, SMIME...

DNSSEC a le vent en poupe

ECDSA gagne en puissance

DNSPRIV en discussion

- **RFC7626**
- **https://tools.ietf.org/wg/dprive/**

Cryptographie Post-Quantum déjà envisagée

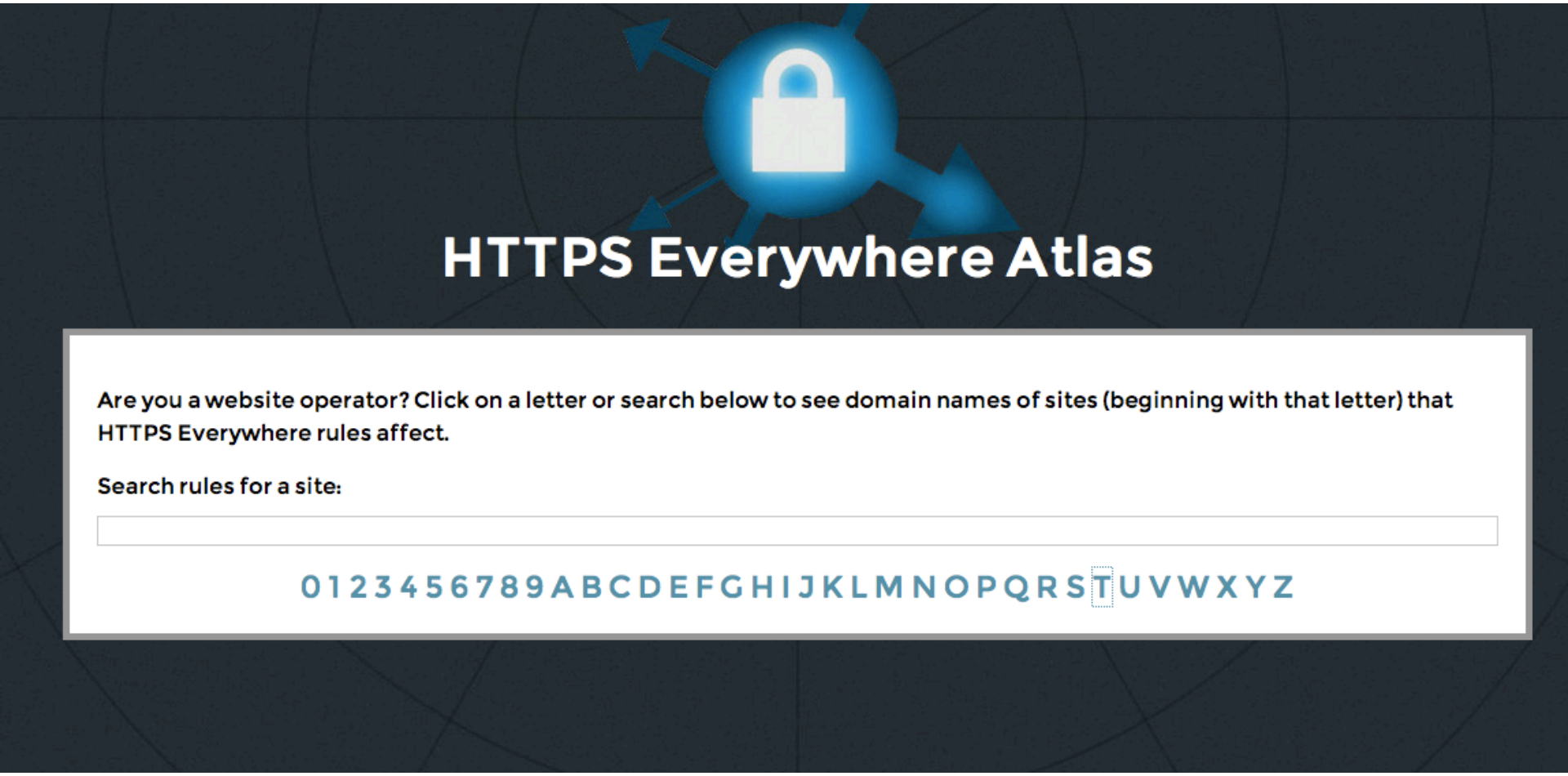
Et alors ?

- ✓ Tout le web over https
- ✓ Anonymat via proxy over VPN
- ✓ Anonymat via VPNs spéciaux
- ✓ Etc...

https partout. . ...

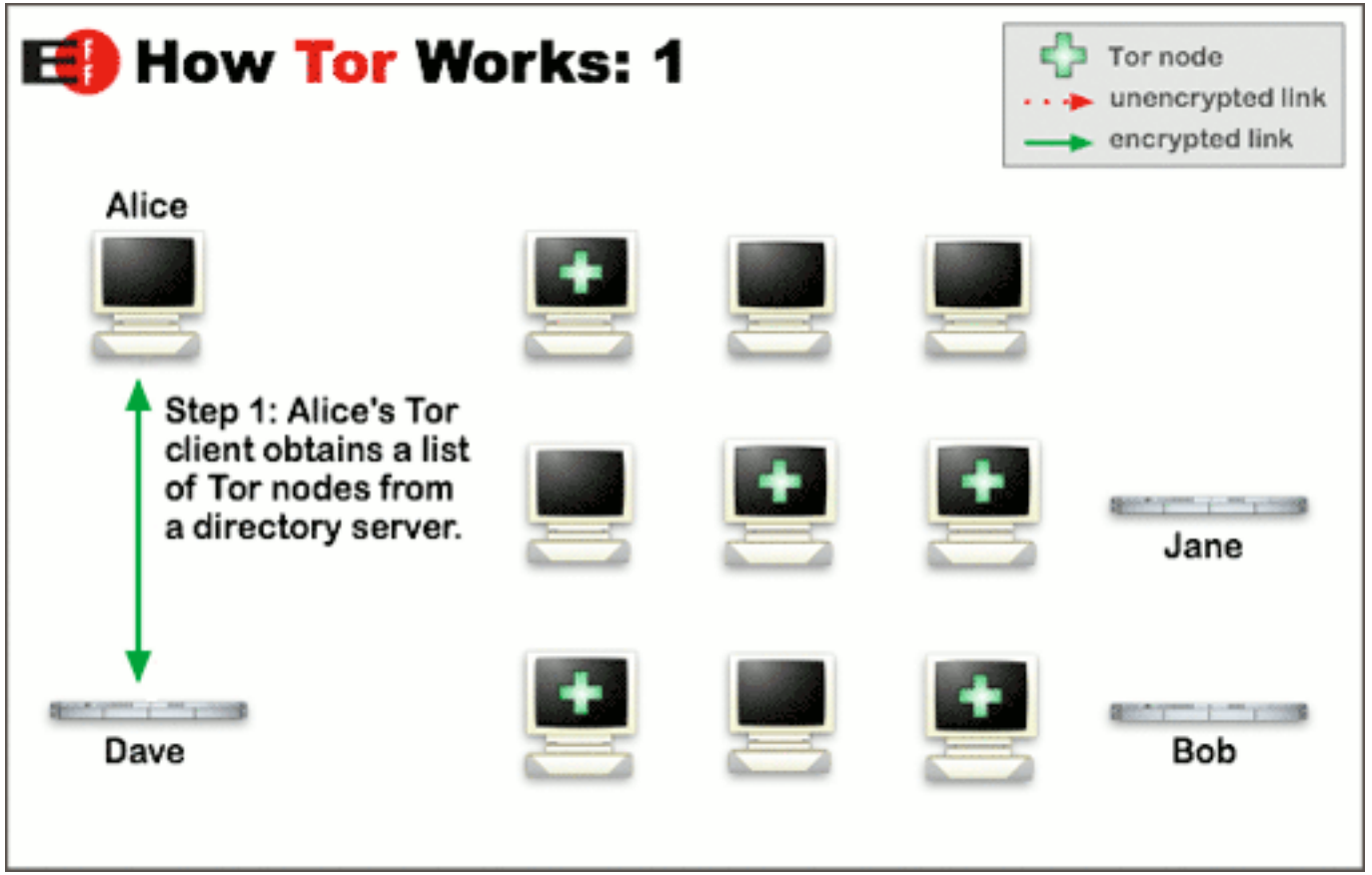
https://www.eff.org/https-everywhere

https partout

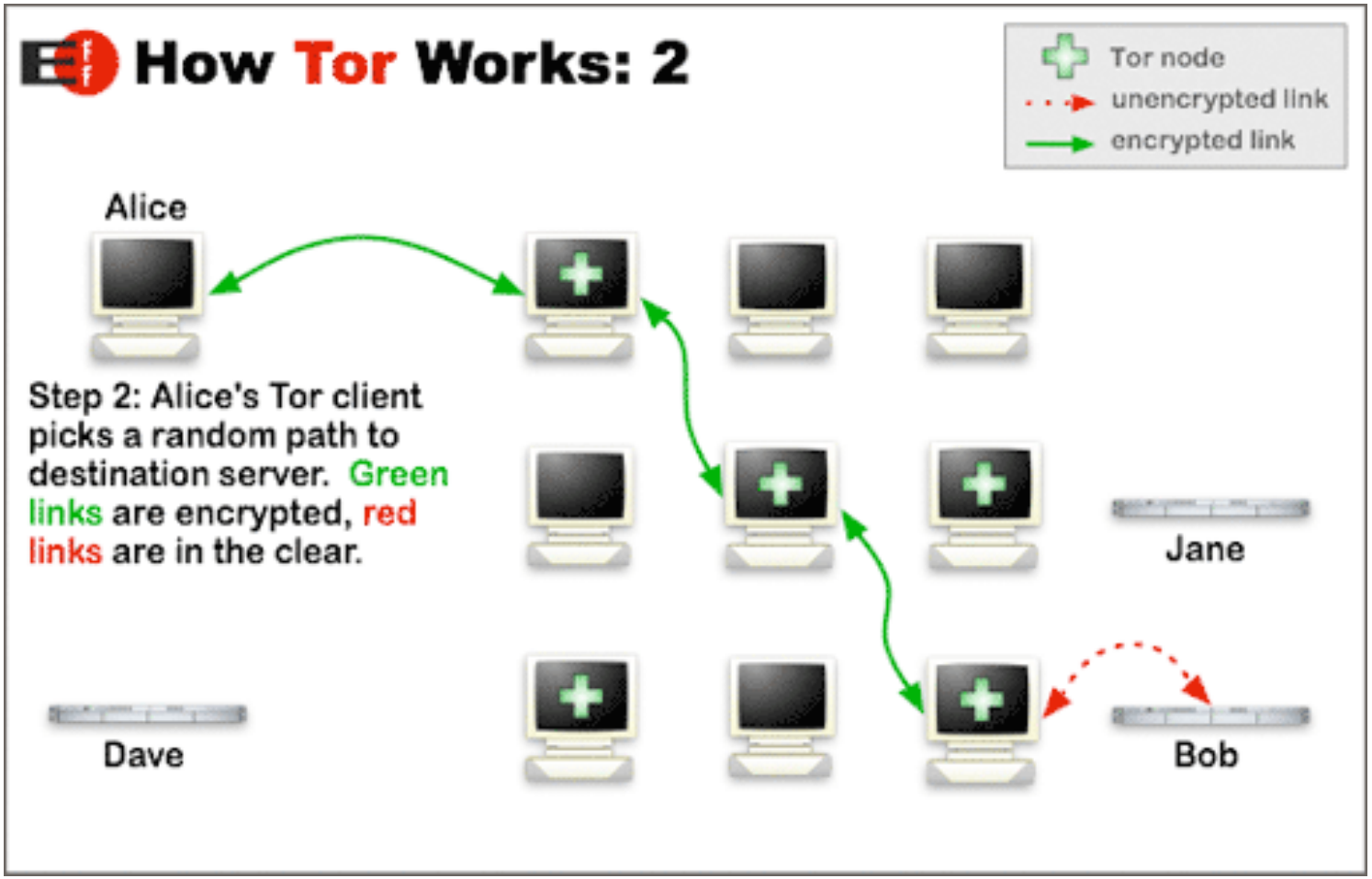


Tor: Un VPN special

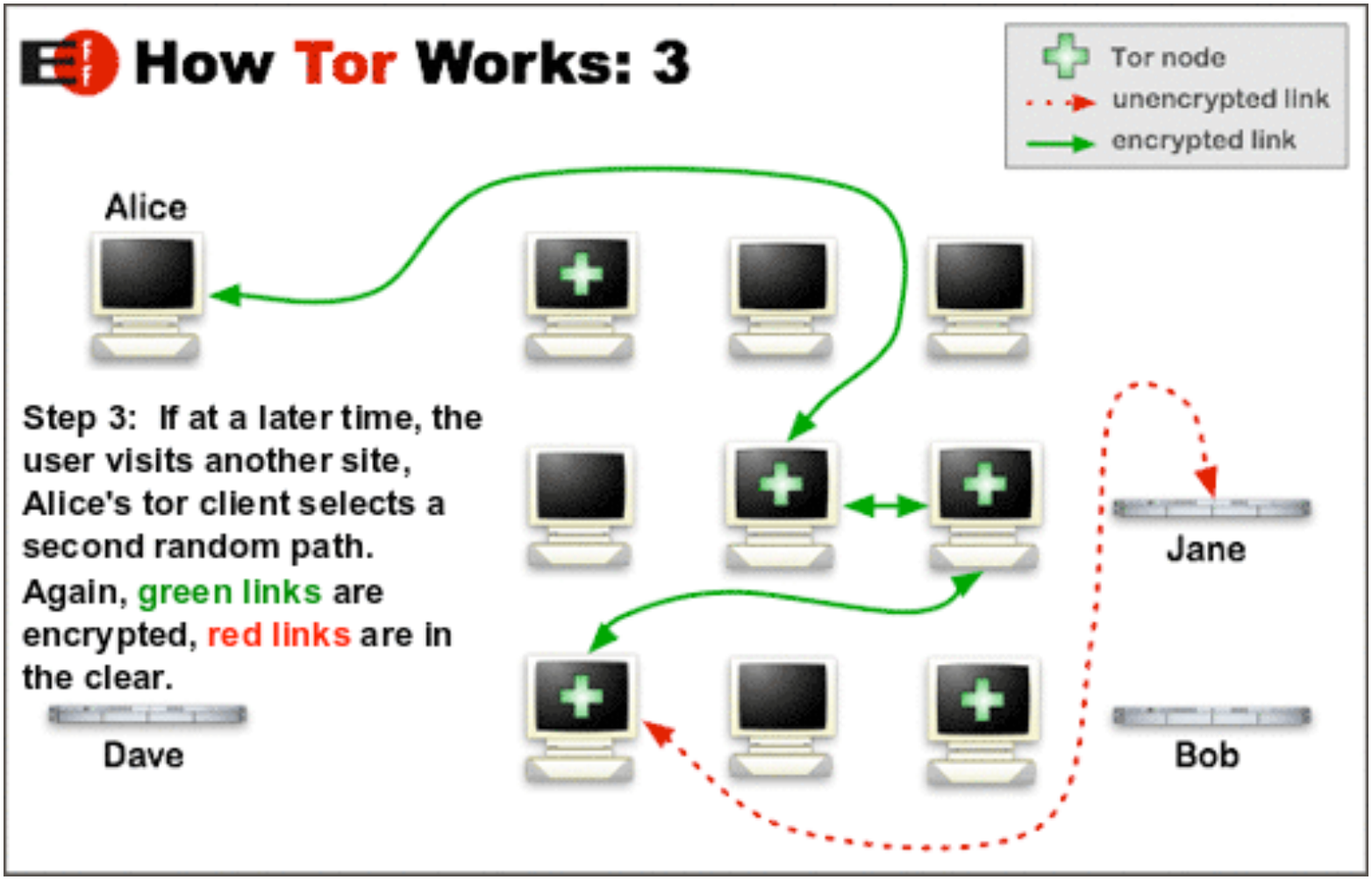
https://www.torproject.org



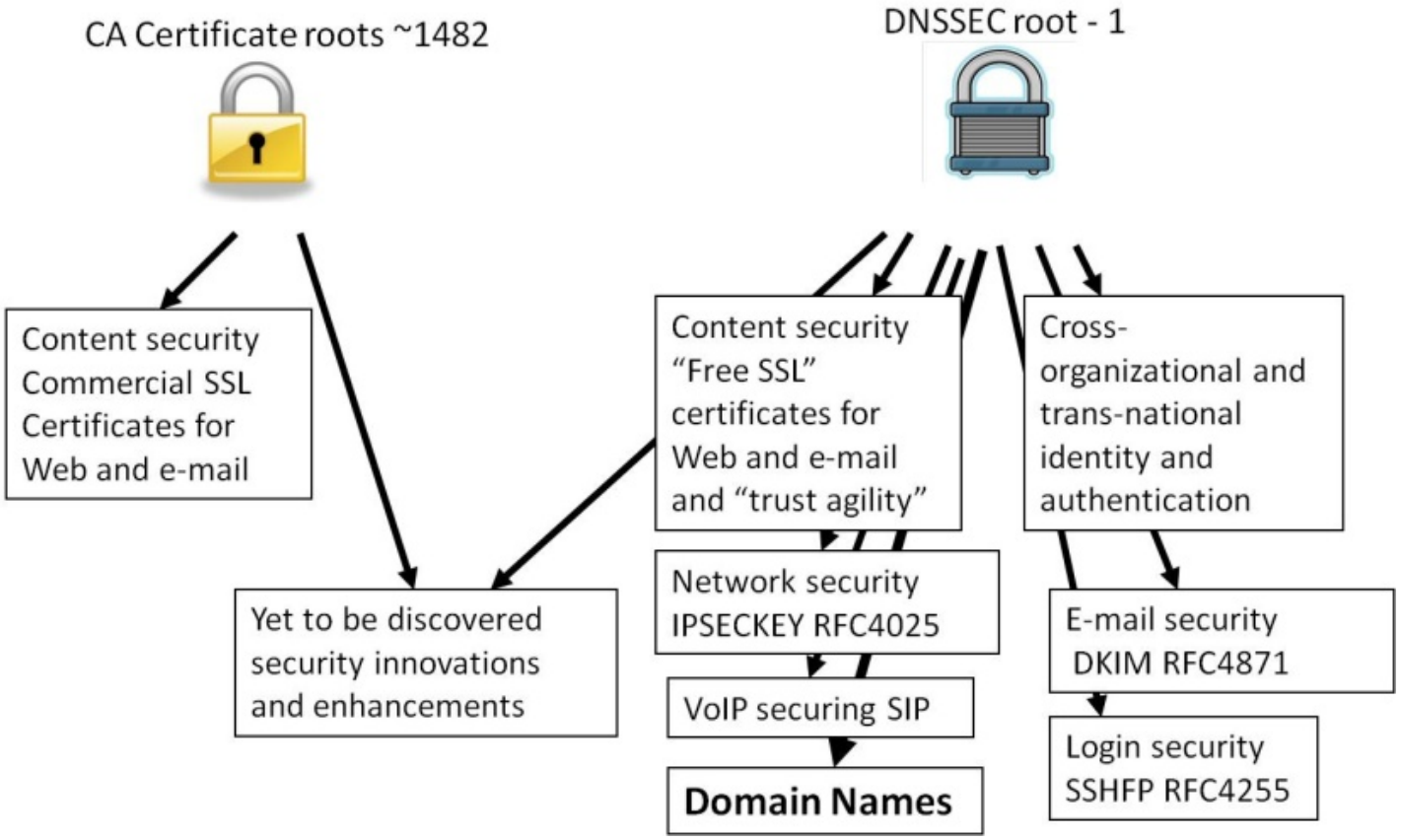
Tor: Un VPN special



Tor: Un VPN special



Authentification et gestion des cles: Plus de ICP ou DNSSEC ?



DNSSEC et DANE ?

DANE (https://tools.ietf.org/wg/dane/)

- ✓ Améliorer le TLS Web pour tous
- ✓ Mail S/MIME pour tous

Autres. . .

- ✓ SSH, IPSEC, VoIP
- ✓ Identité digitale
- ✓ Autres contenus(i.e. configurations)
- ✓ ICP Globale

Plus de CAs!

https://letsencrypt.org/

Le futur nous dira. . .

- ✓ Vie privée contre sécurité nationale ?
  - ✓ Les attentats de Paris ont relancé les débats
- ✓ L'utilisateur saura-t-il faire le bon choix ?
  - ✓ Cryptographie n'a jamais été facile
- ✓ Et les restrictions sur l'export et l'utilisation de la crypto ?

Questions?
Commentaires?
Suggestions ?

Je vous remercie