DNS-based Authentication of Named Entities (DANE)

Thibault CHÂTIRON
Fangzhou DENG

Sommaire

- Working Group
- DANE
  - Contexte
  - Principe
  - Objectif
- DNSSEC
  - Intégrité + RRSIG (Resorce record signature)
  - Authentification + DNSKEY - DS (Delegation signer)
- TLS
- Fonctionnement
- RR TLSA
- Conclusion

Working Group

- Warren Kumari
  - Ingénieur en sécurité réseau à Google (USA)
- Olafur Gudmundsson
  - Ingénieur Système, spécialiste DNS à Cloudflare (USA)
- Stephen Farrell
  - Chercheur à Connect, institut de recherche de fondation scientifique en Irlande
- Matt Lepinski
  - Chercheur à BBN Technologies à Cambridge

Déroulement

- Début en 2010
- 6 drafts
  - dont 4 soumis à l'IESG pour publication
- 3 RFC :
  - RFC 6394 (2011)
    - Use Cases and Requirements for DANE
  - RFC 6698 (2012)
    - DANE Transport Layer Security (TLS) Protocol: TLSA
  - RFC 7218 (2014)
    - Adding Acronyms to Simplify Conversations about DANE
- Fin prévue en novembre 2015

Contexte

- Pourquoi la communauté IETF a proposé le protocole DANE ?
  - Ces dernières années, des attaques de haut niveau, ciblant l'infrastructure à clés publiques X.509 (PKIX) utilisée pour sécuriser les communications Internet, ont suscité un besoin urgent d'une technologie permettant de corriger la faille de sécurité présente dans l'écosystème PKIX.

Principe

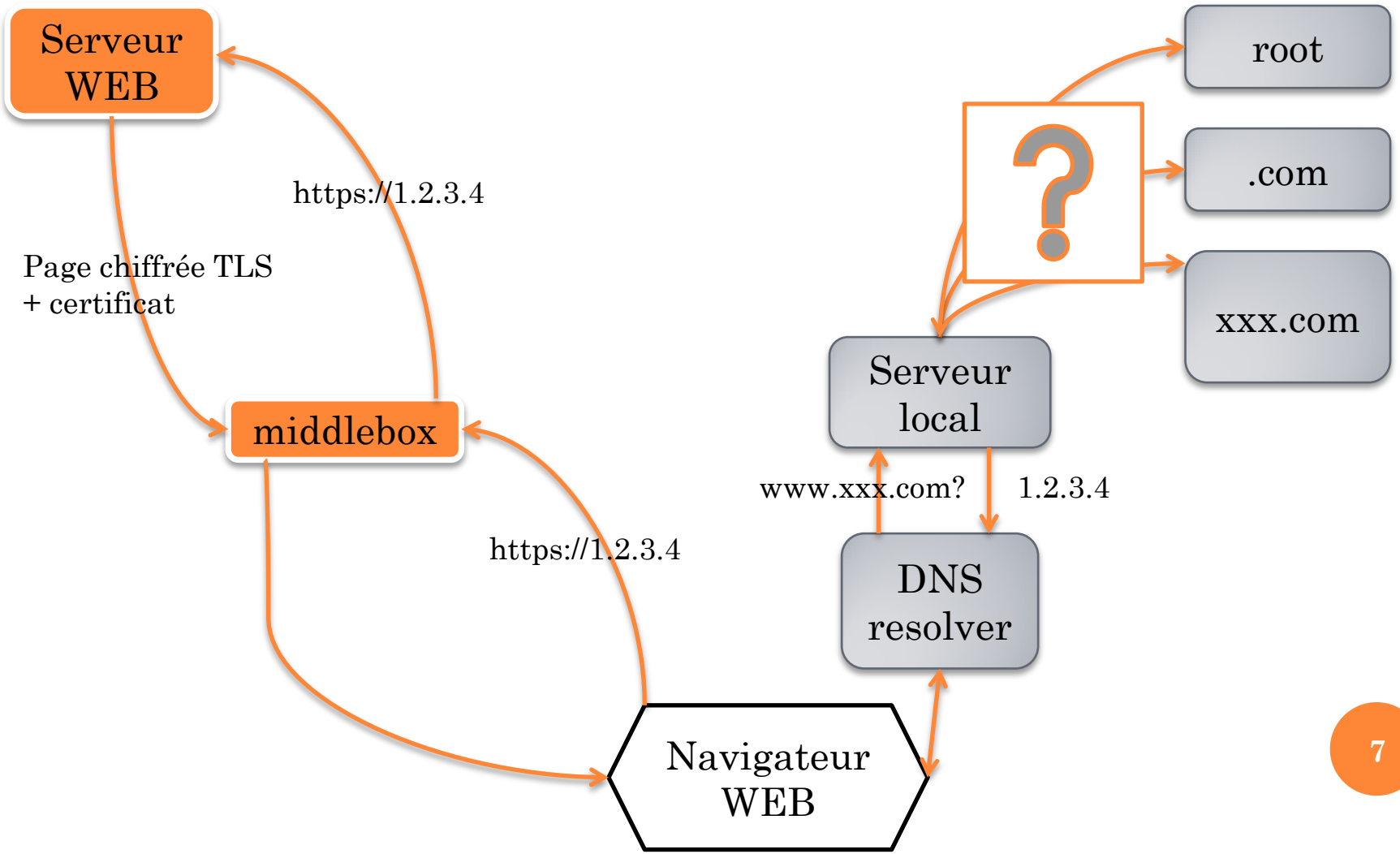
- Ensemble de mécanismes et de techniques qui permettent aux applications Internet d'établir des communications sécurisées par cryptographie en utilisant les informations mises à disposition dans le système DNS.

- Cette démarche s'enregistre dans une logique de sécurisation des accès clients-serveurs en:
  - Sécurisant les requêtes DNS effectuées depuis les postes clients au travers des protocoles/mécanismes DNSSEC et TLS.
  - Mieux sécuriser les accès chiffrés des clients vers le serveurs

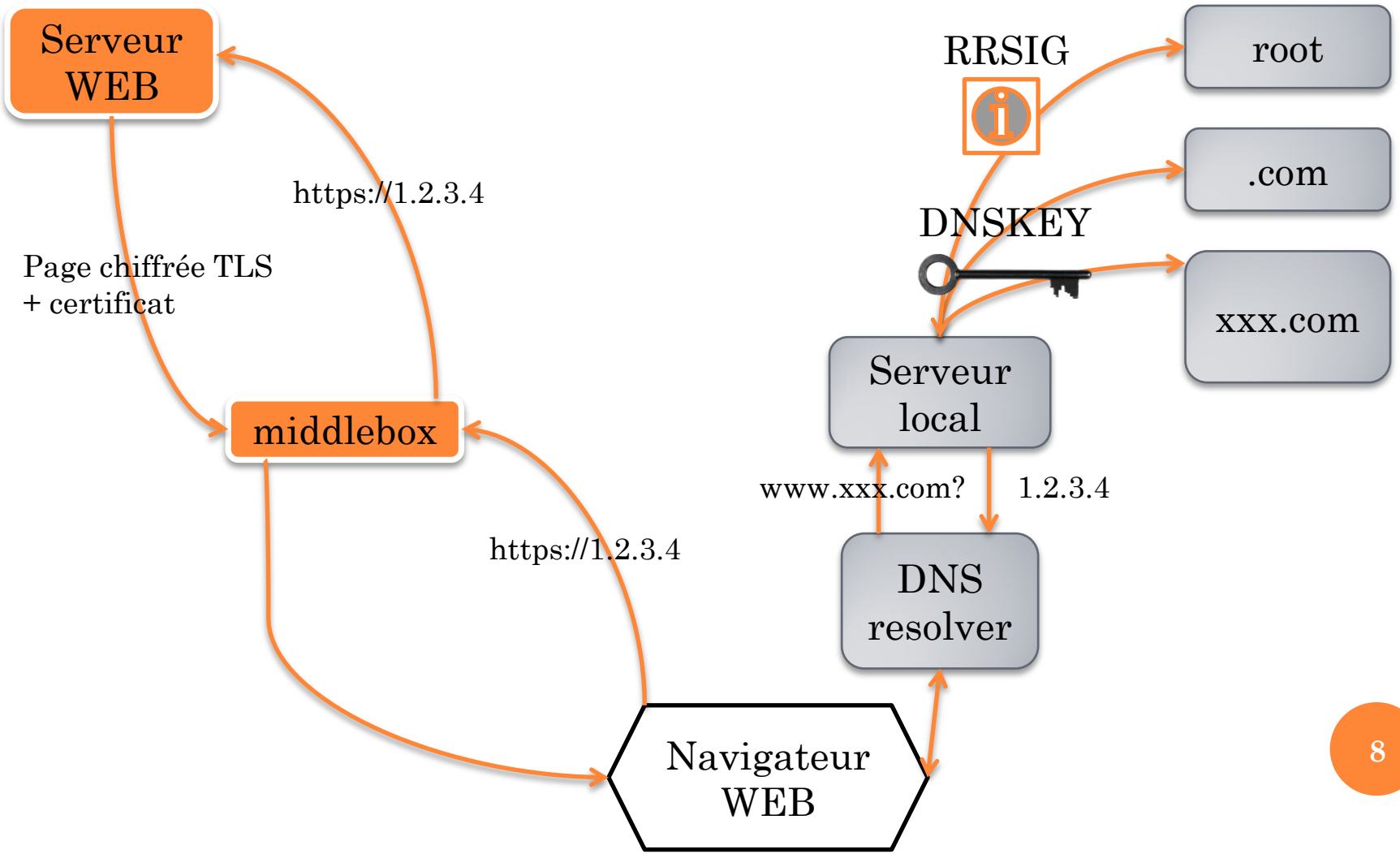
Objectif

- Working Group :
  - comment incorporer DANE et la fonctionnalité dans les protocoles
  - comment utiliser DANE pour SMTP, SMIME, OpenPGP, IPSEC et d'autres protocoles de base électroniques de messagerie tels que (IMAP ou POP)
  - produire un ensemble de directives de mise en œuvre pour les opérateurs et les développeurs d'outils.

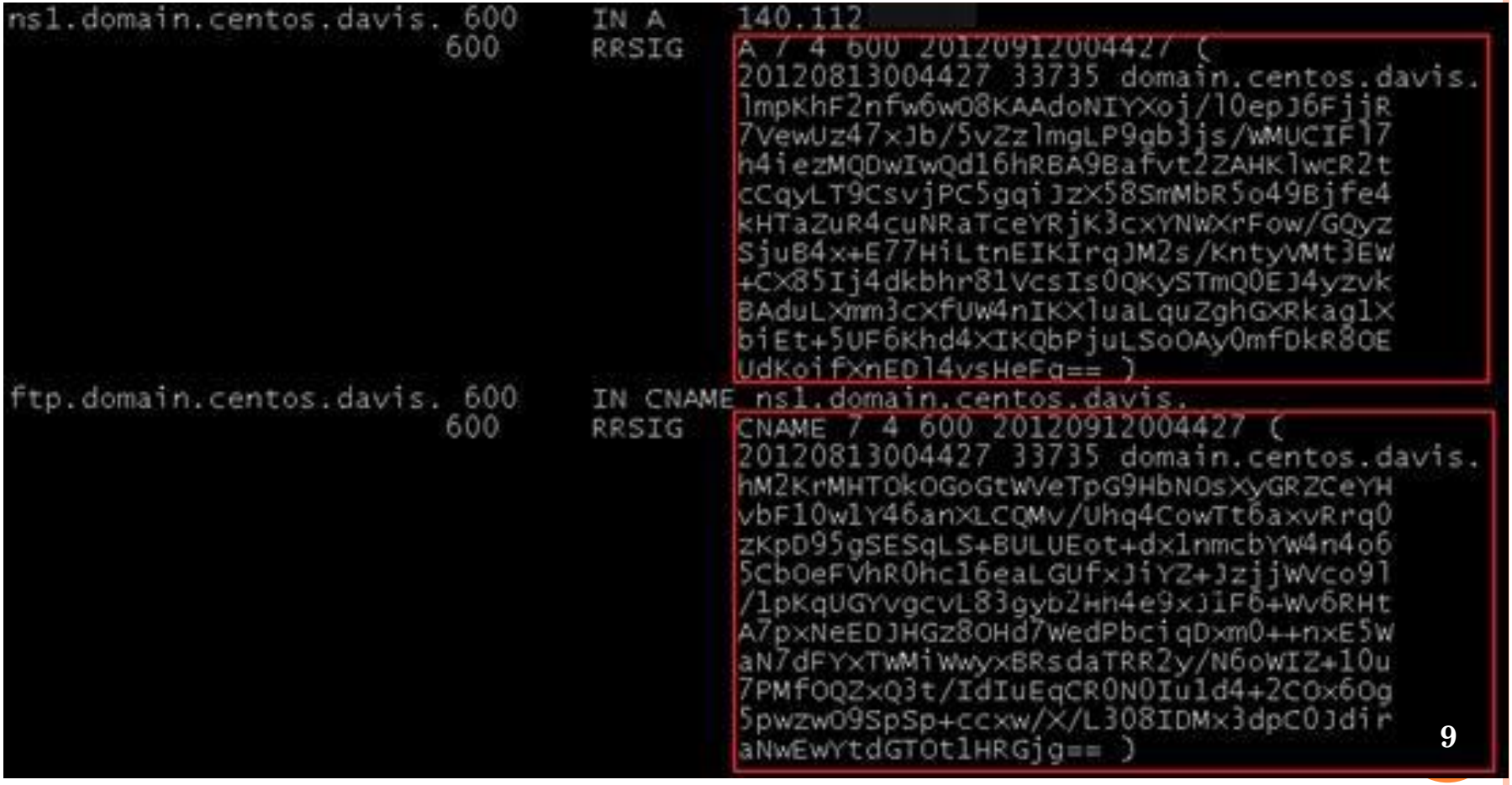
DNSSEC


Serveur WEB
https://1.2.3.4
Page chiffrée TLS
+ certificat
middlebox
https://1.2.3.4
Navigateur WEB
DNS resolver
www.xxx.com?
1.2.3.4
Serveur local
?
root
.com
xxx.com

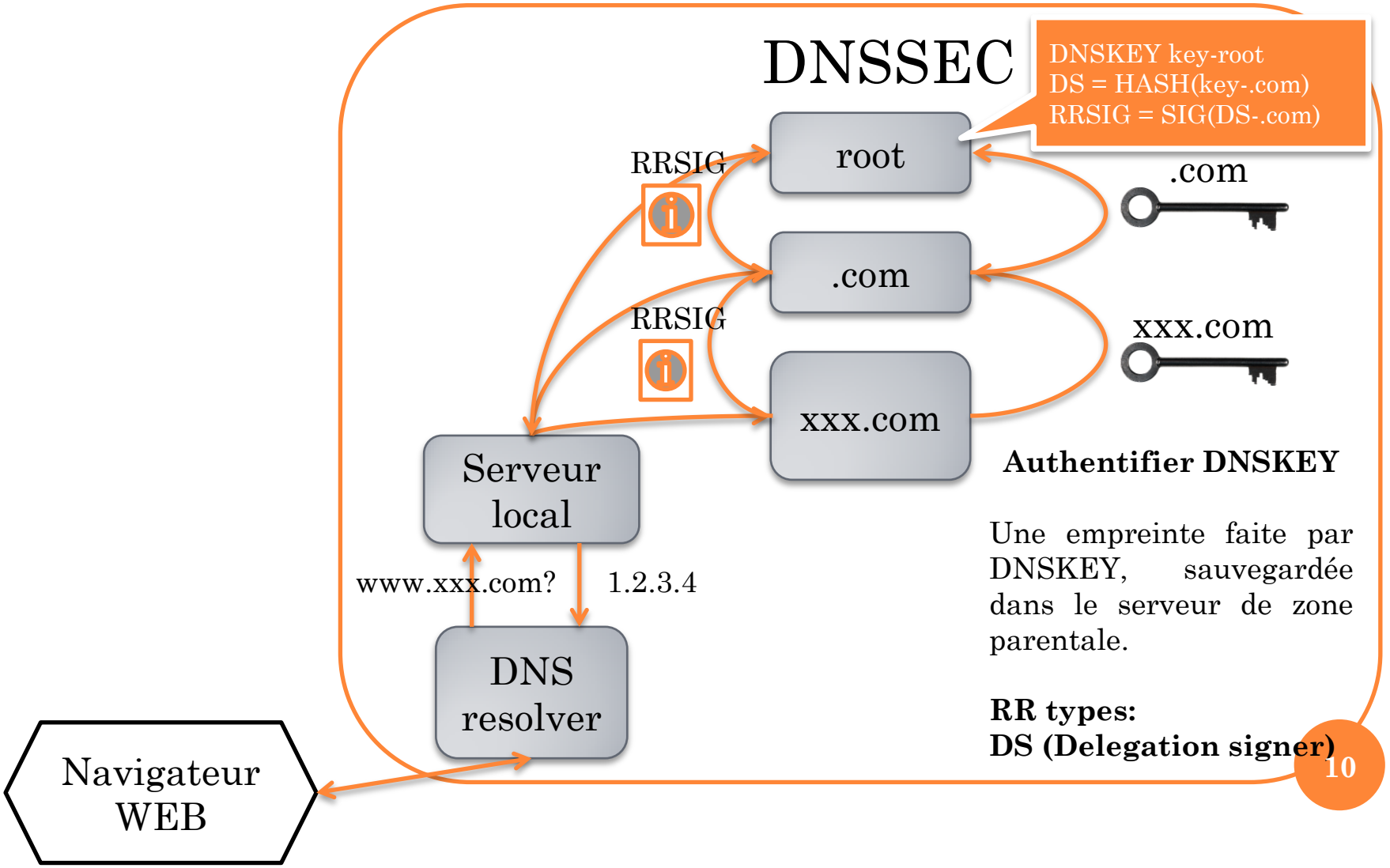
Intégrité


Serveur WEB
https://1.2.3.4
Page chiffrée TLS
+ certificat
middlebox
https://1.2.3.4
Navigateur WEB
RRSIG
root
.com
DNSKEY
xxx.com
Serveur local
www.xxx.com?
1.2.3.4
DNS resolver

Resource record signature



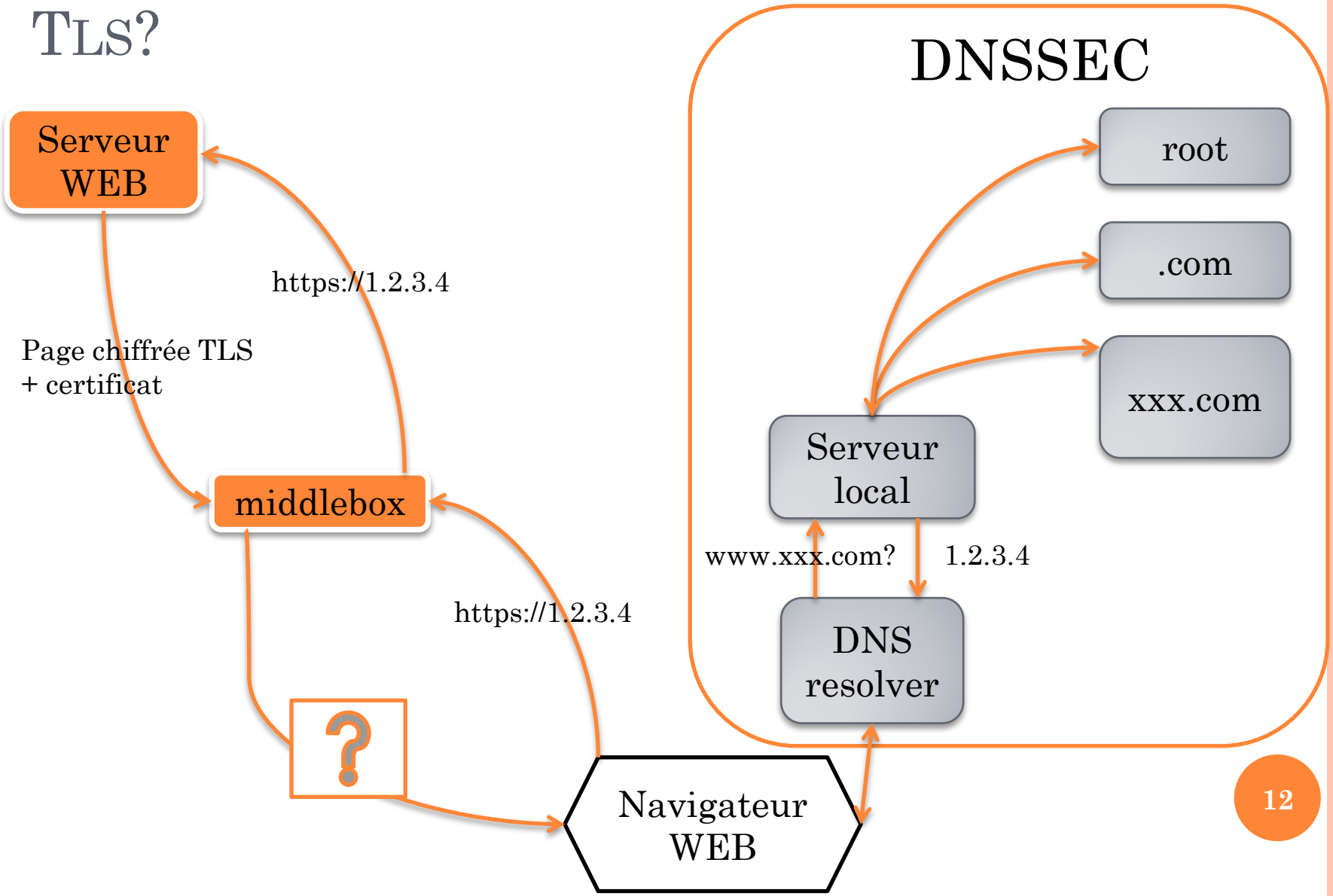
AUTHENTIFICATION



Delegation signer

```
$TTL    600
@       SOA     ns1.centos.davis. root.ns1.centos.davis. ( 811209091 360000 3600 3600000 3600 )
                IN      NS      ns1.centos.davis.
ns1             IN      A       140.112.
www             IN      CNAME   ns1
domain          IN      NS      ns1.domain.centos.davis.
ns1.domain      IN      A       140.112.
domain.centos.davis. IN DS 33735 7 1 A0FBDF45AC0F0AFC6834A8CE2554E3B67B1CC891
domain.centos.davis. IN DS 33735 7 2 A2AFBECEBB42FADEAB69326CE1E9F059626CE843A438EAB720E08C2F 7BE3F209
~
~
~
```

TLS?


DNSSEC
Serveur WEB
https://1.2.3.4
Page chiffrée TLS
+ certificat
middlebox
https://1.2.3.4
?
Navigateur WEB
root
.com
xxx.com
Serveur local
www.xxx.com?
1.2.3.4
DNS resolver

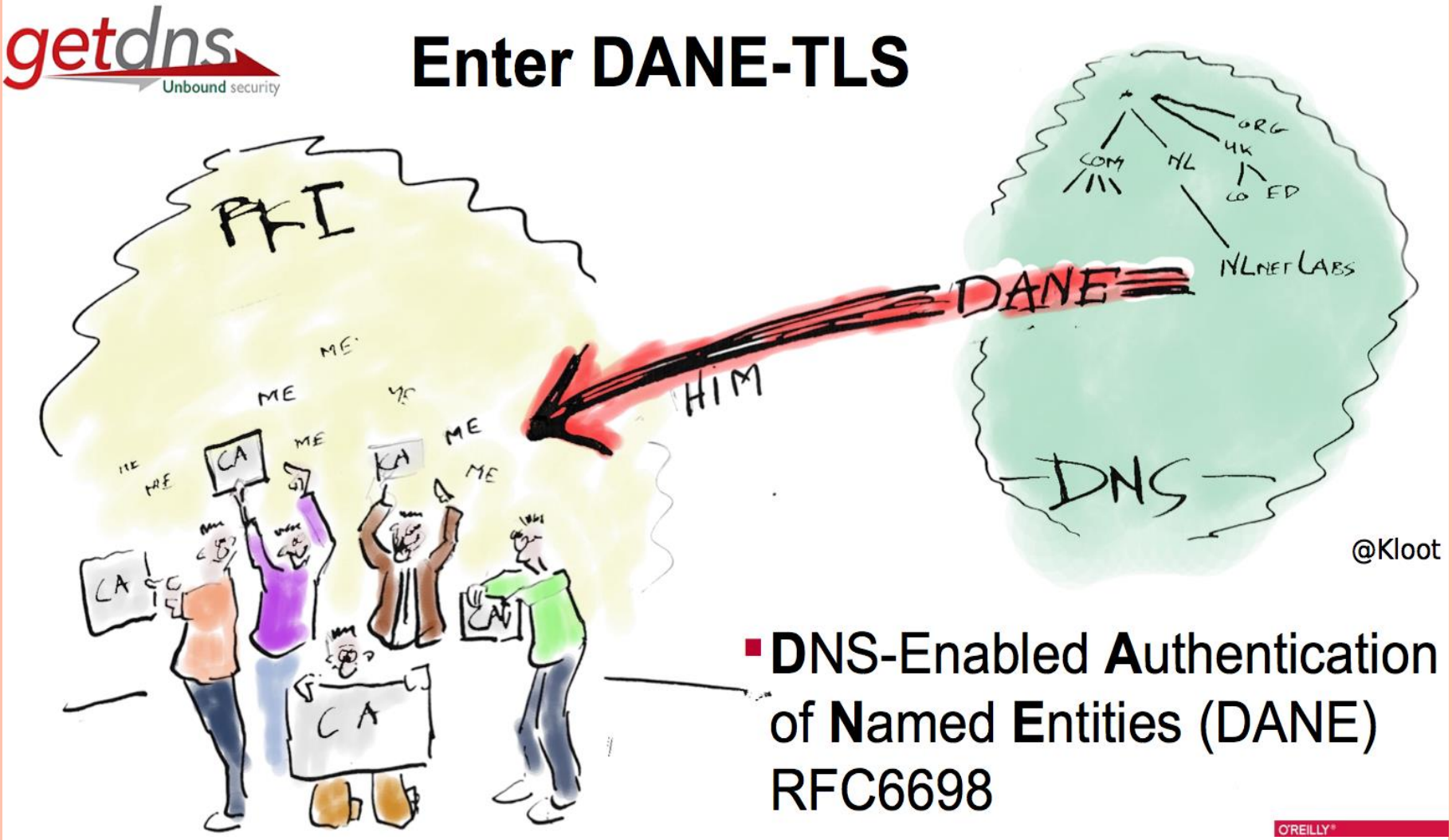
Problématique

- TLS/SSL = fort chiffrement + légère protection d'intégrité
- DNSSEC = forte protection d'intégrité

- Comment pouvons-nous avoir:

  fort chiffrement + forte protection d'intégrité ?

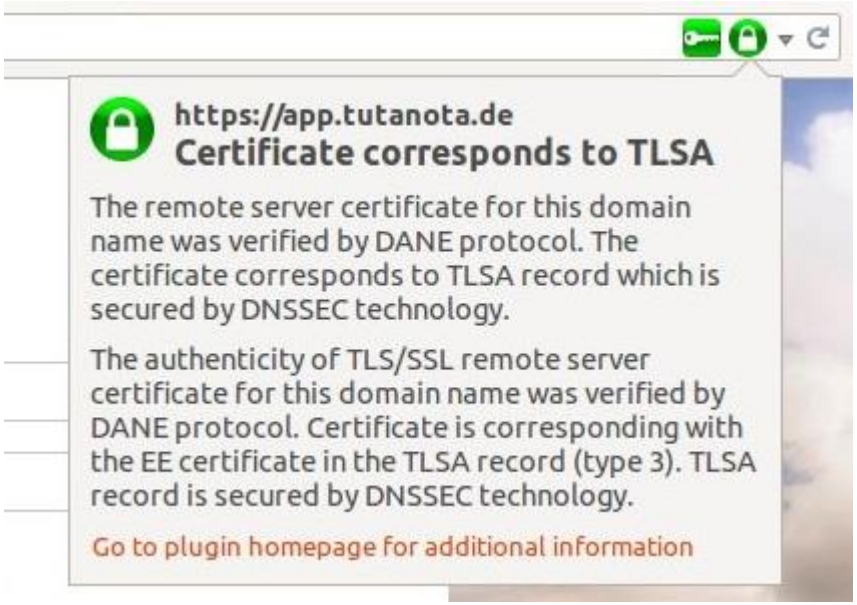
DANE



Source: VERISIGN – ICANN 52

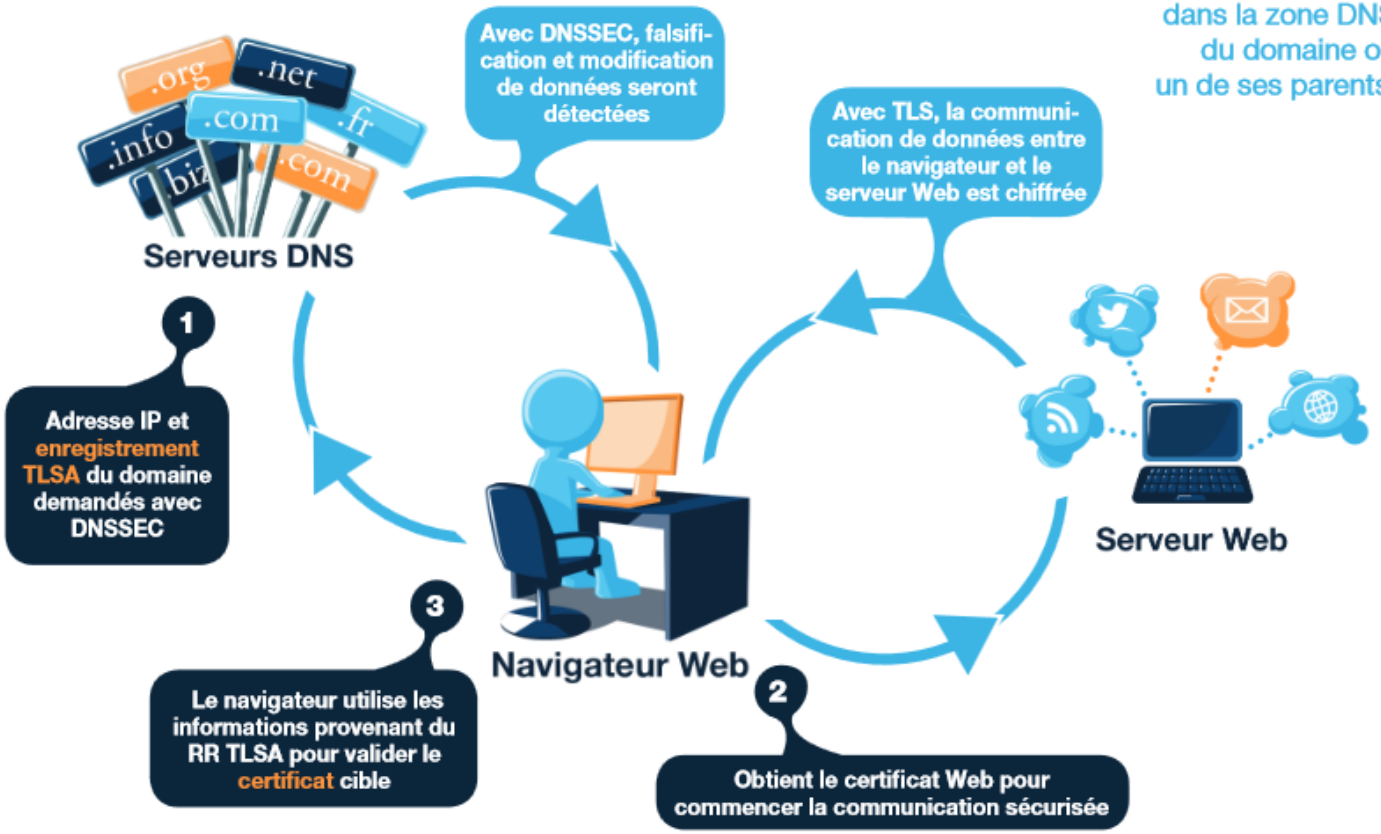
Comment ça marche ?

- Les serveurs de messagerie et les navigateurs peuvent automatiquement vérifier l'authenticité du certificat avant d'établir une connexion SSL de confiance
- DANE fonctionne déjà grâce à des add-ons.



Fonctionnement

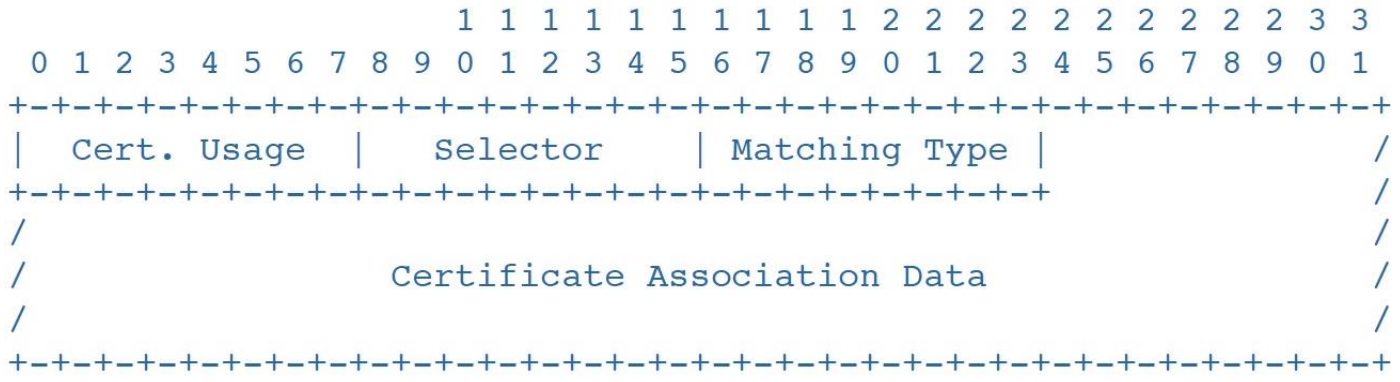
Fig. 4 : Possibilités de compromission d'une communication sécurisée considérablement réduites grâce à DANE & DNSSEC



TLSA RECORD

- Définition d'une nouvelle DNS record type "TLSA", qui sert à authentifier les SSL/TLS certificats.
- CA peut faire garantie pour un certificat en spécifiant les contraintes , ou valider PKIX End-Entity certificat.
- Un CA peut être authentifié directement par un service certificat dans le DNS lui-même.

FORMAT DE DONNÉES



- Certificate Usage – 1 Octet

0 = “CA constraint” (Spécifier un certificat de CA)
1 = “service certificate constraint” (Spécifier un certificat de EE)
2 = “trust anchor assertion” (1 utilisé comme clé public + info)
3 = “domain-issued certificate” (administrateur de nom de domaine)

- Selector – 1 Octet

0 = full certificate
1 = public key only

- Matching Type – 1 Octet

0 = exact match
1 = match SHA-256 hash
2 = match SHA-512 hash

- Certificate Association Data

full certificate, or public key data, or hash value

EXAMPLE TLSA RECORD (FOR WWW)


```
_443._tcp.fedoraproject.org. 263 IN TLSA 0 0 1 (
            19400BE5B7A31FB733917700789D2F0A2471C0C9D506
            C0E504C06C16D7CB17C0 )

_443._tcp.fedoraproject.org. 263 IN RRSIG TLSA 5 4 300 (
            20141114150617 20141015150617 7725
fedoraproject.org.
            hrk0si7I/BWTz0wEtMcFZNUCj/0o5796k5FVuZx6eXrc
            YOe/ChHA/Shu/WHr3iM1yNGi86+8t4wMq9GA+JZthWZC
            ZmENxf9OTNe/t/LBAc2EDW/fMBJq0JO2b4ZkJHXCEyX0
            CDsIYz8shZ20nPGlrsYqwLdQiCeravWcwcJiPuc= )
```

Usage 0 (“CA Constraint”) – this record says:
- For service at fedoraproject.org tcp port 443
- only the CA with the specified SHA-256 certificate fingerprint (19400BE5B…) should be trusted

Conclusion

- Encore peu utilisé
- DANE n'est pas réservé qu'à la navigation sur le Web
  - DANE a été conçu pour résoudre les problèmes relatifs à la navigation sur le Web. Des efforts ont été déployés à l'IETF au sein du groupe de travail DANE pour en étendre l'utilisation à la sécurisation d'autres applications comme la messagerie électronique (s/MIME), la messagerie instantanée (XMPP), etc.
- Application mobile

Références

- **Sécuriser les communications sur Internet de bout-en-bout avec le protocole DANE**https://www.afnic.fr/medias/documents/Dossiers_pour_breves_et_CP/dossier-thematique12_VF1.pdf
- **HTTPS Everywhere? This Email Service Gives You DANE, too**http://blog.tutanota.de/dane-everywhere/2014/10/14/
- **How to Install DANE Add-ons - Tutanota-Blog** http://blog.tutanota.de/dane-how-to-install-browser-addons/2014/10/14/
- **RFC7218** http://tools.ietf.org/html/rfc7218
- **RFC6698** http://tools.ietf.org/html/rfc6698
- **RFC6394** http://tools.ietf.org/html/rfc6394
- **DNSSEC** http://www.internetsociety.org/deploy360/dnssec/
- **DANE: Taking TLS Authentication to the Next Level Using DNSSEC** http://www.internetsociety.org/articles/dane-taking-tls-authentication-next-level-using-dnssec
- Présentation **<DANE demonstration>** - Duane Wessels, Verisign ICANN 49 DNSSEC Workshop
- Présentation **<Introduction to the DANE Protocol>** - ICANN 47 Deploy360 Programme

Merci de votre attention !

QUESTION?