Introduction à DNSSEC

AROC Bamako, Mali, 2010

Qu'est ce que DNSSEC?

Problèmes DNS

- Empoisonnement du cache
- Attaque ”homme au milieu”
- Confidentialité
- Fiabilité
- Attaque d'amplification

Lesquels de ces problèmes DNSSEC adresse-t-il ?

Attaque d'amplification

- Les serveurs DNS peuvent être utilisés comme des amplificateurs de paquet
  - UDP, petites requêtes, grosses réponses
- DNSSEC fait de vos serveurs DNS d'encore plus *gros* amplificateurs de paquet
  - Toujours UDP, réponses encore plus grandes

Fiabilité

- Dans un contexte général, DNSSEC n'aide pas à rendre votre DNS plus fiable
- En fait, il rend votre DNS plus fragile, en rendant plus difficile l'effort de maintenir un service stable

Confidentialité

- DNSSEC ne protège pas la confidentialité des questions & réponses
- N'importe qui interceptant une requête/réponse peut voir les détails
- Il n'y a pas de *chiffrement* ici

Intégrité, Authentification

- DNSSEC fournit un mécanisme pour que les *données* publiées dans le DNS puissent comporter des signatures cryptographiques.
  - Réponses sécurisées incluant des signatures
  - Les clients recevant les réponses peuvent vérifier l'authenticité de celles-ci

3 pages sur le chiffrement

Chiffrement

- Chiffrement à clé publique (PKC)
  - X.509, PGP, ssh, DNSSEC
- Paires de clé (publique, privée)
  - Utiliser la privée pour signer les données
  - Utiliser la publique pour vérifier les signatures

Clé privée

- La clé privée doit rester privée et en securité
  - Le degré de sécurité dépend de l'usage de la clé
  - Une clé compromise signifie que l'on ne peut plus faire confiance aux signatures
  - Une signature par une clé compromise est plus dangereuse qu'aucune signature

Clé publique

- La clé publique doit être largement distribuée
  - Elle doit aussi être correcte

Protocole DNSSEC

Réflexions sur le DNS

- Quand nous utilisons le DNS pour distribuer des clés, il faut bien se rappeler:
  - Le DNS est très largement distribué
  - Les informations ne sont pas mises à jour instantanément
  - Il faut bien réfléchir à l'interaction des TTL et des caches

Les clés publiques dans le DNS

- Dans DNSSEC, les clés sont distribués avec les données DNS elles-même
- Utiliser le RRset DNSKEY
- Offre différentes tailles de clé, et d'algorithmes de chiffrement

Une clé DNSSEC

[octopus:~]% dig isoc.org **DNSKEY** +noall +answer

; **<<>>** DiG 9.6.0-APPLE-P2 **<<>>** isoc.org DNSKEY +noall +answer

;; global options: +cmd

isoc.org. 14387 IN DNSKEY 257 3 7
AwEAAcE/XrxyyTSkw3ly60jsF4gz5kvn4QM6E0plIjnnjENmeWNPZxNf
BYIKZnJxf3GaoI+qFeqbSc085jOXZiBMSRMQFkfsJNZgCsyVhas3lMoM
HXEcEewNCPWv2D6TCYGHiVJaTJ0+6we19hIZZlrgJxfPxOXx9CUAzltQ
CCvGD055P+yexHdMNWNvcxqt+1qtVt03heIWhf6QH5lhWaIHQWMXJlky
KrgVwXHZHcvUebXqhhJfGZhGGU64x7HpNP3llCRqsut7iWsMLo8yBl3m
R7eo/pUc6HF3M9E7hl53fg722xMxVA60kkDZqTp1FUzOCK5AagY+ISNz mKtOLgPcxCs=

isoc.org. 14387 IN DNSKEY 256 3 7
AwEAAZj8B7CEDfD4C1iJRJkZCxi6dz+dbVhqUUenXLRBDDtgm1BoF3jq
v1Yj+DW+UT29Mzcg1aTR3lXMV1DZcmvHytvtl1N+y02CFSgYVQ+GOxv0
HSRRJhpWTD9sv5/Pr42bJ8eyNZ8cauyIwsHnd+kpVY60Q36VhdK8ZnhZ x69wpwzF

[octopus:~]%

Signature de RR avec DNSSEC

- Chaque groupe d'enregistrements (RRset) peut avoir 0 ou plusieurs signatures
  - Les signatures apparaissent dans un RRset RRSIG avec le même nom de ”propriétaire”
  - Les signatures ont une date d'inception et d'expiration
    - On doit donc re-signer régulièrement

Une signature RRSIG

```
[octopus:~]% dig www.isoc.org A +dnssec +noall +answer

; <<>> DiG 9.6.0-APPLE-P2 <<>> www.isoc.org A +dnssec +noall +answer

;; global options: +cmd

www.isoc.org.           16040   IN      A       212.110.167.157

www.isoc.org.           16040   IN      RRSIG   A 7 3 86400 20101014085009
20100930085009 33644 isoc.org.
YhsanPDyYO9tilrwZEHituzhzG8OwF1Peq1MMmY3/q6bE82mSiDxxi/Q
hH4GeoYO5EKrcfpuRWLcPNJ3f/3HEc/SCYvF4gPyezJ6XFcbFvUAG4y5
ZR+dt9KawvrDYlOxtk31xgLeWRm3ryOqJgH+8OGLAg2W77xapEdofkfd ENo=

[octopus:~]%
```

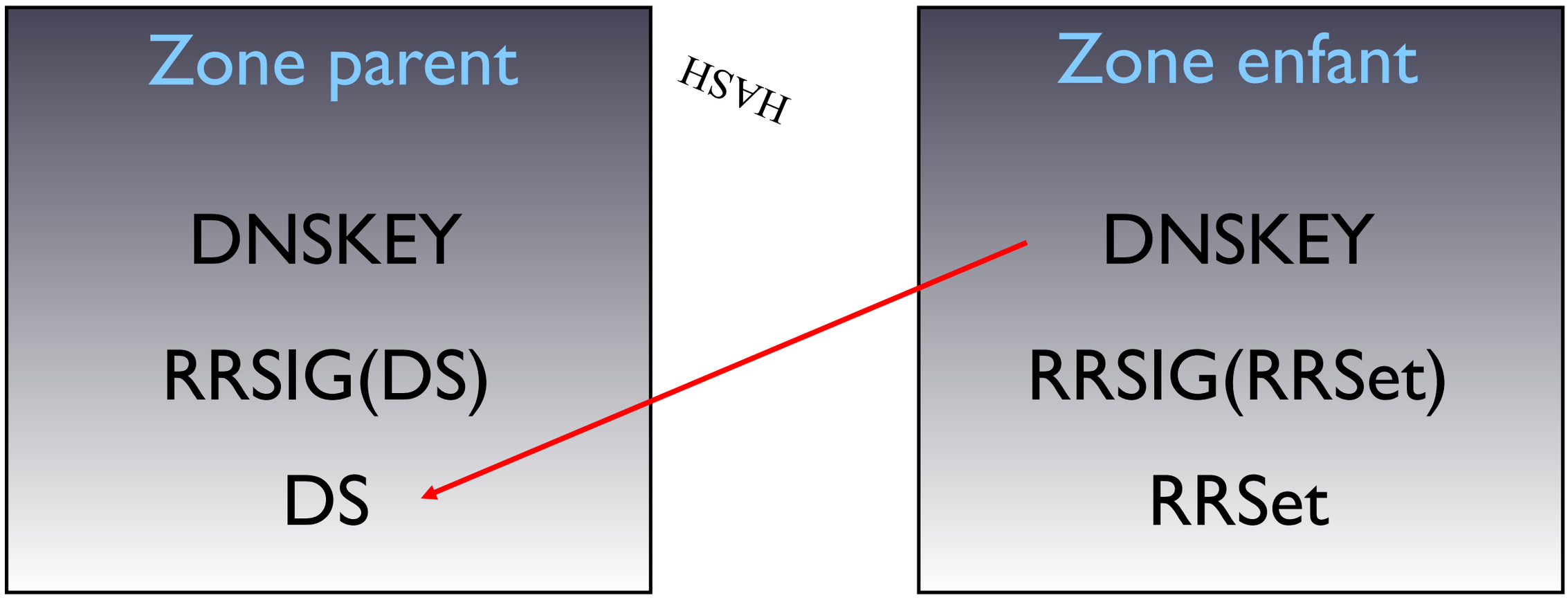
Chaîne de confiance

- Si on peut faire confiance à la clé publique qui correspond à la clé privée qui a produit une signature, on peut faire confiance à cette signature
- Si on peut faire confiance à la signature, on peut confiance aux données signées par cette signature
- Comment fait-on on confiance à la clé publique ?

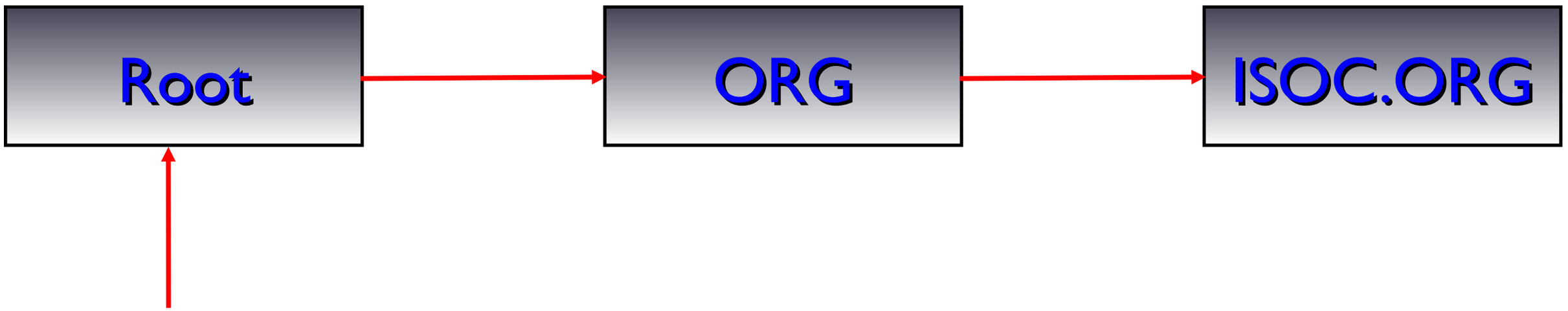
Signataire de Délégation

- DS = Delegation Signer RR
  - Un hash de la clé publique
  - Il est lui-même signé
  - C'est ainsi qu'on étend la confiance aux délégations

Chaîne de confiance



Chaîne de confiance



Ancre de racine (Root Anchor)

- À un moment ou un autre, un validateur DNSSEC aura besoin d'include une Ancre de racine dans le logiciel
- L'ancre de confiance de la racine
- http://www.iana.org/dnssec/

Deux RRset DNSKEY

- En 2010 on utilise deux jeux de clés DNSKEY par zone
  - ZSK – Zone Signing Key – Clé de Signature de Zone
    - Signer les données dans la zone
  - KSK – Key Signing Key – Clé de Signature de Clé
    - Signer les jeux RRset DNSKEY

ZSK – clé de signature de zone

- Puisqu'on a besoin de re-signer régulièrement, la ZSK doit être ”en ligne”
- Elle est utilisée souvent, donc elle peut-être courte et utilise ainsi moins de CPU
- On peut ainsi remplacer la ZSK sans impliquer d'autres acteurs

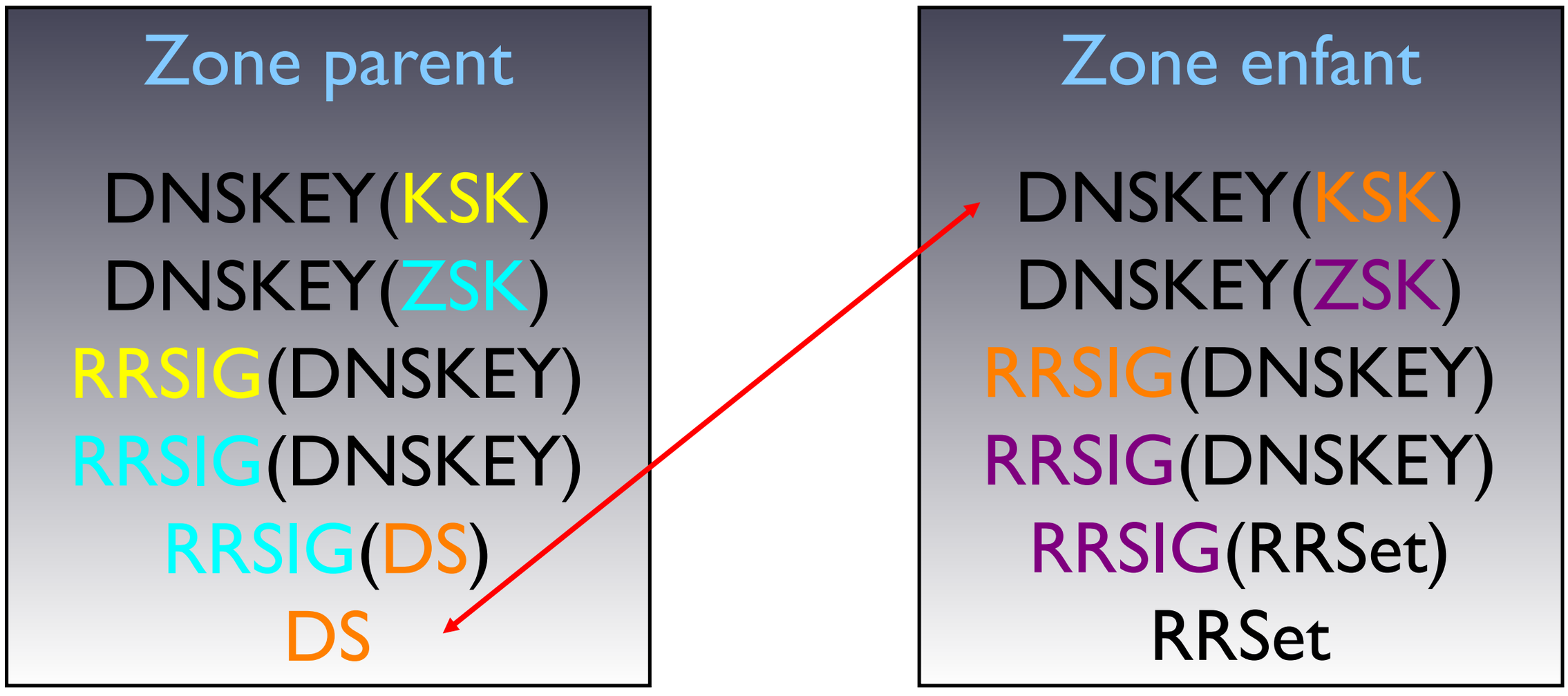
KSK

- La KSK est la clé qui correspond au DS dans la zone parent
- On a besoin de la KSK pour signer la ZSK.

On doit conserver la KSK dans un endroit sûr

- Pas besoin de garder la KSK en ligne
- Changer la KSK nécessite de parler avec votre parent (mise à jour du DS)

KSK and ZSK


Zone parent
DNSKEY(KSK)
DNSKEY(ZSK)
RRSIG(DNSKEY)
RRSIG(DNSKEY)
RRSIG(DS)
DS
Zone enfant
DNSKEY(KSK)
DNSKEY(ZSK)
RRSIG(DNSKEY)
RRSIG(DNSKEY)
RRSIG(RRSet)
RRSet

[KZ]SK dans la nature

[octopus:~]% dig isoc.org **DNSKEY** +noall +answer

; **<<>>** DiG 9.6.0-APPLE-P2 **<<>>** isoc.org DNSKEY +noall +answer

;; global options: +cmd

```
isoc.org.               14387   IN      DNSKEY 257 3 7
AwEAAcE/XrxyyTSkw3ly60jsF4gz5kvn4QM6E0plIjnnjENmeWNPZxNf
BYIKZnJxf3GaoI+qFeqbSc085jOXZiBMSRMQFkfsJNZgCsyVhas3lMoM
HXEcEewNCPWv2D6TCYGHiVJaTJ0+6we19hIZZlrgJxfPxOXx9CUAzltQ
CCvGD055P+yexHdMNWNvcxqt+1qtVt03heIWhf6QH5lhWaIHQWMXJlky
KrgVwXHZHcvUebXqhhJfGZhGGU64x7HpNP3llCRqsut7iWsMLo8yBl3m
R7eo/pUc6HF3M9E7hl53fg722xMxVA60kkDZqTp1FUzOCK5AagY+ISNz mKtOLgPcxCs=

isoc.org.               14387   IN      DNSKEY 256 3 7
AwEAAZj8B7CEDfD4C1iJRJkZCxi6dz+dbVhqUUenXLRBDDtgm1BoF3jq
v1Yj+DW+UT29Mzcg1aTR3lXMV1DZcmvHytvtl1N+y02CFSgYVQ+GOxv0
HSRRJhpWTD9sv5/Pr42bJ8eyNZ8cauyIwsHnd+kpVY60Q36VhdK8ZnhZ x69wpwzF
```

[octopus:~]%

DS dans la nature

```
[octopus:~]% dig @a0.org.afilias-nst.org ISOC.ORG SOA +dnssec +noall +auth

; <<>> DiG 9.6.0-APPLE-P2 <<>> @a0.org.afilias-nst.org ISOC.ORG SOA +dnssec +noall +auth

; (1 server found)

;; global options: +cmd

ISOC.ORG.               86400   IN      NS      [...]

ISOC.ORG.               86400   IN      DS      3330 7 2
7AD5E47FFFFA05AE70D5166E01B7836E34AD3032541D95DB9D1E9D7D 3AFB33D4

ISOC.ORG.               86400   IN      DS      3330 7 1 268B71BF480AE2C1484BB1DBA7E0A42089D90298

ISOC.ORG.               86400   IN      RRSIG   DS 7 2 86400 20101009155117 20100925145117 37812 org.
IMqcyadyAGU+DynuTCz7JgJga+jjEii7PAxQha+q0k8AoGLzhwaI1kWQ
bDgt7fLKi8HiJPX5eOouGVvS2RIx82+wNabM9/1cGHO41xYk3t/ttP/L
GkqjewoAsw+6X/2k92FnEUqkIotlWuXJSVvqzv4FDh0LRF+wjxc2IYMa CQI=

[octopus:~]%
```

Transport DNS

- Le bon vieux DNS a été conçu pour marcher en UDP, ≤ 512 octets
  - Retombe en TCP sinon
- Les DNS modernes savent gérer des gros paquets DNS UDP (EDNS0, RFC 2671)
- DNSSEC → messages DNS plus gros
  - Attention aux coupes-feu mal configurés!

Le reste...

- Est-ce que DNSSEC est vraiment bénéfique pour les utilisateurs finaux ?
- Validation dans le résolveur (bit AD)
- Validation dans les applications (i.e.: plugins applicatifs, comme Firefox)
- C'est le tout début!

Le reste

- Vérifiabilité de la non-existence
  - On ne peut pas signer les enregistrements qui n'existent pas
  - Les enregistrements NSEC ou NSEC3 ”bouchent les trous” entre les enregistrements
  - Et on signe les enregistrements NSEC/NSEC3

DNSSEC pour les Registres

Et alors ?

- Que cela signifie-t-il pour un registre ?
  - Besoin d'implémenter des processus compliqués et du stockage sécurisé
  - Besoin de signer les zones
  - Accepter et intégrer les DS des zones déléguées – quel mécanisme ?
  - Besoin vous-même de communiquer votre DS à la zone parent – quel mécanisme ?

NSEC et NSEC3

- Lequel utiliser ?
- Simple règle:
  - Si cela ne vous gêne pas que tout le monde puisse récupérer une copie de la zone → NSEC
  - Si vous n'autorisez normalement pas les transferts de zones anonymes → NSEC3

Gestion de clé

- Comment sécuriser la ZSK ?
- Comment sécuriser la KSK ?
  - Question importante
  - Pas de réponse simple là
  - Analyse de risque, consultation, audit

Communication

- Communiquer avec vos clients
  - Expliquer bénéfices et risques de DNSSEC
- Communiquer avec les utilisateurs
  - Montrer comment valider une réponse
  - Expliquer les changement opérationnels (coupes-feu, TCP, taille de la réponse, ...)

Et aussi!

- Rappelez-vous: DNSSEC rend vos zones plus fragiles et ”cassantes” qu'auparavant
  - Il faut avoir une *très* bonne stabilité dans ses opérations existantes
  - Définition de procédures d'urgence pour mettre à jour les DS RRSets de vos zones

Logiciels libres

- BIND9
  - http://www.isc.org/
- OpenDNSSEC
  - http://www.opendnssec.org/

Resources

- Liste de diffusion dnssec-deployment
  - http://www.dnssec-deployment.org/
- Liste de diffusion dns-operations
  - http://www.dns-oarc.net/
- Travail de standardisation
  - IETF dnsop, dnsext working groups

État du déploiment du DNS, Septembre 2010

Déploiement

- La racine a été signée en Juillet 2010
- Beaucoup de TLDs déjà signés
  - 48 sur 294
    - ARPA, BE, BG, BIZ, BR, CAT, CH, CL, CZ, DK, EDU, EU, FI, FR, GOV, INFO, KG, LI, LK, MUSEUM, NA, NL, NU, ORG, PM, PR, PT, RE, SE, TF, TH, TM, UK, US, ...
    - http://stats.research.icann.org/dnssec/

Introduction à DNSSEC

AROC Bamako, Mali, 2010