

RENOUVELLEMENT DE CLES DNSSEC

Alain Aina

aalain@afinic.net



DNSKEY en résumé

- Zone Signing Key (ZSK)
- Key Signing Key (KSK)
 - Fonctionne comme un point d'entrée de sécurité de la zone
 - Configuration du Trust-anchor
 - Le DS parental pointe sur cela
 - Interaction avec une tierce partie
- Les DNSKEYs sont tous traités de la même façon dans le protocole
- Les opérateurs peuvent faire une distinction
 - Regardez les champs du flag: impaire (257 dans la pratique) signifie SEP

Les Avantages de l'utilisation de deux clés distinctes

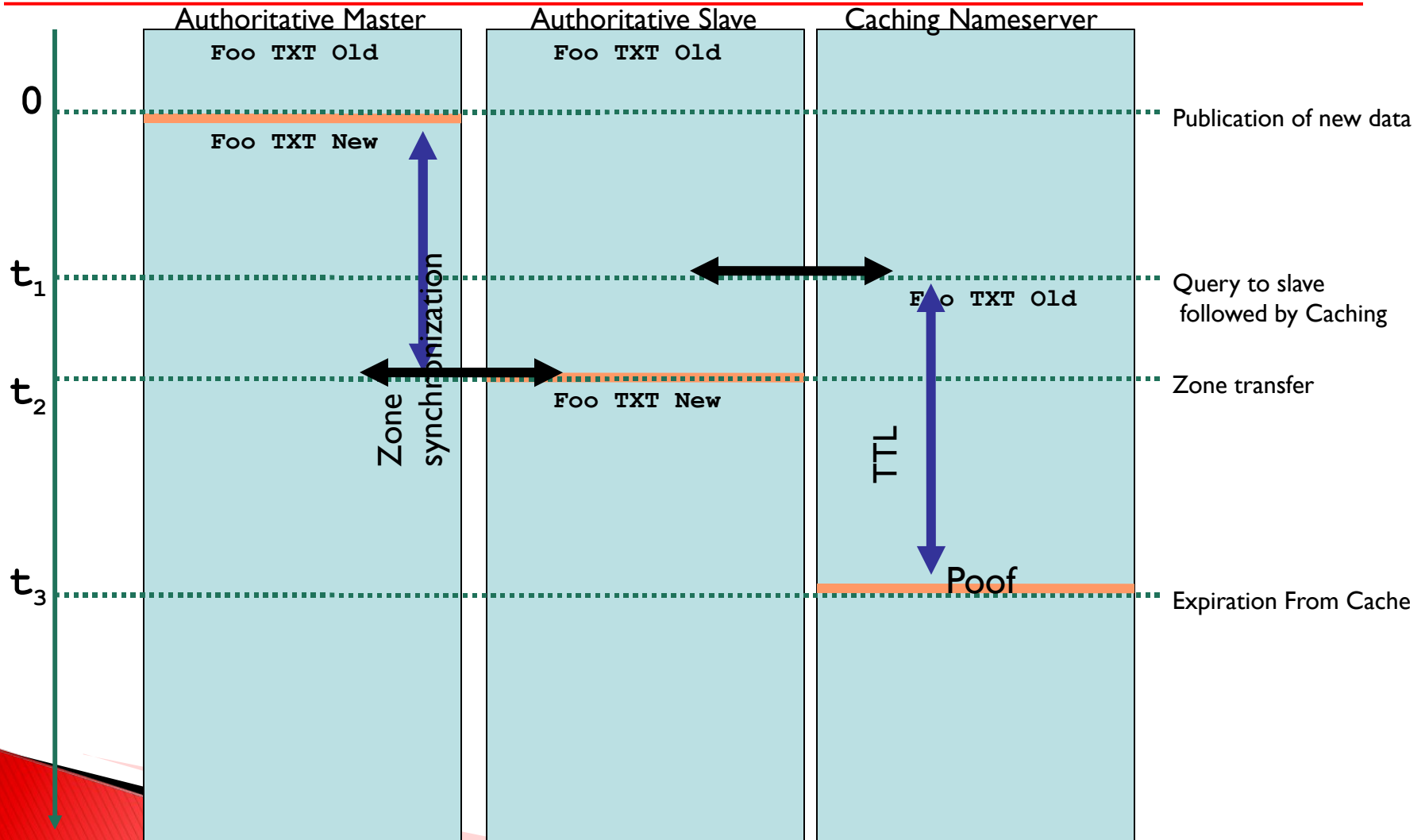
- Le renouvellement du KSK a besoin d'interaction, le renouvellement des ZSKs peut se faire de manière quasiment instantanée
- Rappelez-vous que le remplacement du KSK peut conduire :
 - à des mises à jour du Trust-anchor
 - au changement de l'enregistrement DS au niveau du parent
- Autorise différentes responsabilités
 - Les ZSKs peuvent être touchés au jour le jour par le staff junior
 - Les KSKs ne peuvent seulement être touchés que par le staff senior

Renouvellement instantané de clés?

- N'oubliez pas que le DNS utilise des caches.
 - Il prend un peu de temps pour avoir la propagation de nouvelles informations
- Lorsque vous avez de nouvelles données, il devrait être possible d'utiliser des DNSSIGs valides à partir du cache
- Lorsque vous avez d'anciennes données du cache, il devrait être possible d'utiliser de nouveaux DNSSIGs.
- Assurez vous que les anciennes et les nouvelles clés sont disponibles
- Ou assurez vous que les anciennes et les nouvelles signatures sont disponibles

Propriétés de synchronisation

time

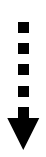


Renouvellement du ZSK par pré-publication

- Introduire le nouveau DNSKEY avant de commencer à l'utiliser pour signer les données.
 - Clés 'passive et active'
 - La clé passive est juste publiée, la clé active est utilisée pour la signature
- Vous pouvez aussi créer deux signatures après l'introduction de la clé, mais cela ferait croître votre fichier de zone

Renouvellement du ZSK

```
dnssec-signzone -k ksk example.com zsk1
```



Create passive zsk2



```
dnssec-signzone -k ksk example.com zsk2
```



ksk	ksk	ksk
zsk1	zsk1	zsk2
	zsk2	
Sig ksk	Sig ksk	Sig ksk
Sig zsk1	Sig zsk1	Sig zsk2
Zone data	Zone data	Zone data
Sig zsk1	Sig zsk1	Sig zsk2

time

At least TTL DNSKEY

RRS

Renouvellement du KSK

- Vous dépendez de votre parent.
 - Vous ne pouvez pas contrôler quand le parent change ou publie l'enregistrement DS.
- Utilisez l'ancien KSK jusqu'à ce que l'ancien DS ait eu le temps d'expirer des caches.

DS1

DS2

dnssec-signzone -k ksk1 example.com zsk

dnssec-signzone -k ksk2 example.com zsk

dnssec-signzone -k ksk1 -k ksk2 example.com zsk

Create ksk2 and
send to parent

remove ksk1

ksk1	ksk1	ksk1	ksk2
	ksk2	ksk2	
zsk	zsk	zsk	zsk
Sig ksk	Sig ksk1	Sig ksk1	
	Sig ksk2	Sig ksk2	Sig ksk2
Sig zsk	Sig zsk	Sig zsk	Sig zsk
Zone data	Zone data	Zone data	Zone data
Sig zsk	Sig zsk	Sig zsk	Sig zsk

time

At least TTL DS RRs

Erratum

- o RFC4641 contient des erreurs dans les tableaux
 - Certains espaces manquent dans les tableaux

initial	nouveau DNSKEY	nouveau RRSIGs	DNSKEY supprimé
SOA0	SOA1	SOA2	SOA3
RRSIG10 (SOA0)	RRSIG10 (SOA1)	RRSIG11 (SOA2)	RRSIG11 (SOA3)
DNSKEY1	DNSKEY1	DNSKEY1	DNSKEY1
DNSKEY10	DNSKEY10	DNSKEY10	DNSKEY11
	DNSKEY11	DNSKEY11	
RRSIG1 (DNSKEY)	RRSIG1 (DNSKEY)	RRSIG1 (DNSKEY)	RRSIG1 (DNSKEY)
RRSIG10 (DNSKEY)	RRSIG10 (DNSKEY)	RRSIG11 (DNSKEY)	RRSIG11 (DNSKEY)

