DNSSEC
ROULEMENT DES CLES

BENIN DNS FORUM 2018

Cotonou, 11.10.2018

A.A.P Aina – Root KSK Crypto Officer

LES CLÉS DNS

- Clé de signature de zone - ZSK;

- Clé de signature de clés - KSK;

  - Fonctionne comme Point d'Entrée de Sécurité(PES) dans une zone.
    - Configuration d'ancre de confiance (TA)
    - DS au niveau du parent pointe vers elle
    - Interaction avec des tierces parties

- Les CLÉS DNS sont traitées de la même manière dans le protocole;

- Les opérateurs peuvent faire la distinction.

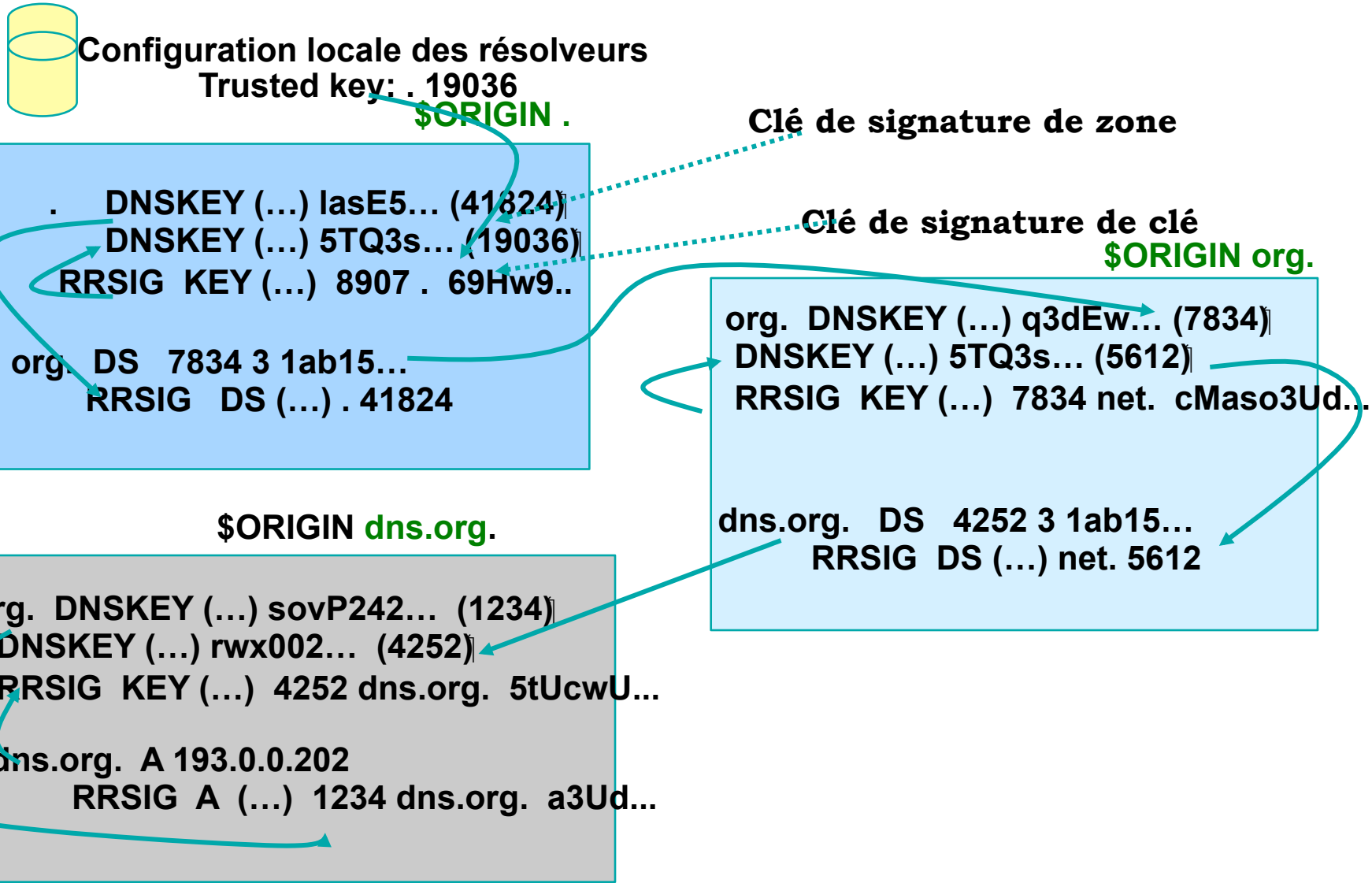
  - Champ « flag » dans le DNSKEY: (257 en pratique) signifie PES.

AVANTAGES DE L'UTILISATION DE CLÉS MULTIPLES

- Roulement KSK a besoin d'interaction

- Roulement du ZSK peut être fait presque instantanément
- Rappelez-vous que le remplacement de KSK peut entraîner
  - Mises à jour d'ancre de confiance (TA)
  - Changement d'enregistrement DS chez le parent
- Permet différentes responsabilités
  - Les juniors peuvent toucher les ZSK au jour le jour
  - Seuls les seniors peuvent toucher les KSK
- Permet d'utiliser différentes tailles de clés

Chaîne de confiance DNSSEC



ROULEMENT DE ZSK « PRE-PUBLISH »

- Introduit le nouveau DNSKEY avant de l'utiliser pour signer les données.
  - Clés «passive » et « active»
  - La clé passive vient d'être publiée, la clé active est utilisée pour la signature

- Vous pouvez également créer deux signatures après avoir introduit la clé, mais cela entraînerait une augmentation de la taille de la zone.

ZSK ROLLOVER (PRE-PUBLISH)

Initial	new DNSKEY	New RRSIGs	DNSKEY removal
SOA0	SOA1	SOA2	SOA3
RRSIG10(SOA1)	RRSIG10(SOA1)	RRSIG11(SOA3)	RRSIG11(SOA3)
DNSKEY 1	DNSKEY 1	DNSKEY 1	DNSKEY 1
DNSKEY 10	DNSKEY 10	DNSKEY 10	DNSKEY 11
	DNSKEY 11	DNSKEY 11	
RRSIG1 (DNSKEY)	RRSIG1 (DNSKEY)	RRSIG1 (DNSKEY)	RRSIG1 (DNSKEY)
RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG11(DNSKEY)	RRSIG11(DNSKEY)

ZSK ROLLOVER (DOUBLE SIGNATURE)

SOA0	SOA1	SOA2
RRSIG10(SOA0)	RRSIG10(SOA1)	RRSIG11(SOA2)
	RRSIG11(SOA1)	
DNSKEY1	DNSKEY1	DNSKEY1
DNSKEY10	DNSKEY10	DNSKEY11
	DNSKEY11	
RRSIG1(DNSKEY)	RRSIG1(DNSKEY)	RRSIG1(DNSKEY)
RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG11(DNSKEY)
	RRSIG11(DNSKEY)	

ROULEMENT KSK

- Vous dépendez de votre parent ou de la communauté toute entière
- Vous ne contrôlez pas les changements des enregistrements DS au niveau du parent
- Utiliser l'ancienne KSK jusqu'à ce que les données expirent du cache
- Roulement Double signature ou « Pre-publish ».

KSK ROLLOVER (Pre-Publish)

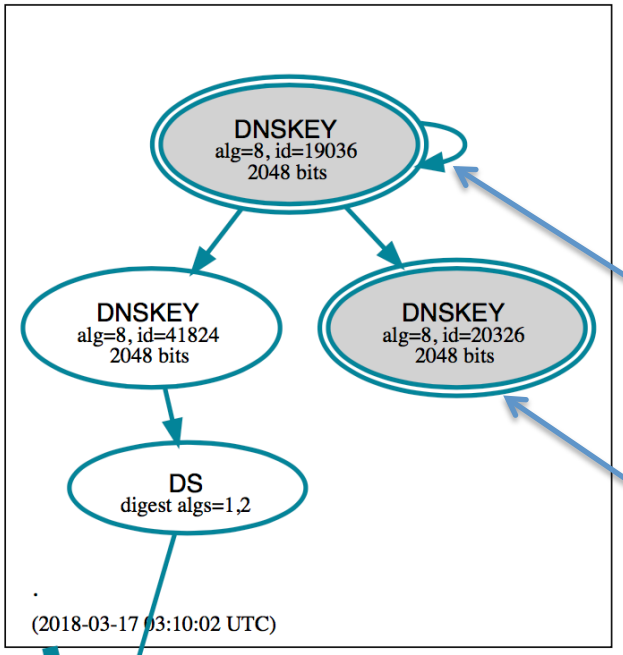
Initial	New DS	New DNSKEY	DS/DNSKEY removal
Parent:			
SOA0	SOA1	SOA1	SOA2
RRSIGpar(SOA0)	RRSIGpar(SOA1)	RRSIGpar(SOA1)	RRSIGpar(SOA2)
DS1	DS1	DS1	DS2
	DS2	DS2	
RRSIGpar(DS)	RRSIGpar(DS)	RRSIGpar(DS)	RRSIGpar(DS)
Child:			
SOA0	SOA0	SOA0	SOA0
RRSIG10(SOA0)	RRSIG10(SOA0)	RRSIG10(SOA1)	RRSIG10(SOA1)
DNSKEY1	DNSKEY1	DNSKEY2	DNSKEY2
DNSKEY10	DNSKEY10	DNSKEY10	DNSKEY10
RRSIG1(DNSKEY)	RRSIG1(DNSKEY)	RRSIG2(DNSKEY)	RRSIG2(DNSKEY)
RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG10(DNSKEY)

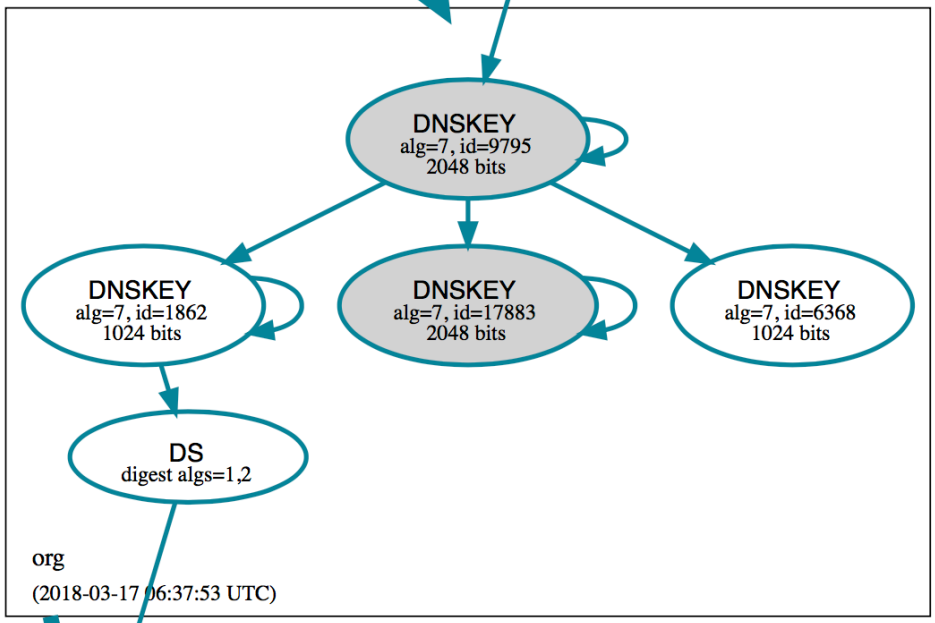
KSK ROLLOVER (double signature)

Initial	New DNSKEY	DS Change	DNSKEY removal
Parent:			
SOA0	SOA0	SOA1	SOA1
RRSIGpar(SOA0)	RRSIGpar(SOA0)	RRSIGpar(SOA1)	RRSIGpar(SOA1)
DS1	DS1	DS2	DS2
RRSIGpar(DS)	RRSIGpar(DS)	RRSIGpar(DS)	RRSIGpar(DS)
Child:			
SOA0	SOA1	SOA1	SOA2
RRSIG10(SOA0)	RRSIG10(SOA1)	RRSIG10(SOA1)	RRSIG10(SOA2)
DNSKEY1	DNSKEY1	DNSKEY1	DNSKEY2
	DNSKEY2	DNSKEY2	
DNSKEY10	DNSKEY10	DNSKEY10	DNSKEY10
RRSIG1(DNSKEY)	RRSIG1(DNSKEY)	RRSIG1(DNSKEY)	RRSIG2(DNSKEY)
	RRSIG2(DNSKEY)	RRSIG2(DNSKEY)	
RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG10(DNSKEY)

Roulement KSK racine en cours

October 11, 2018: KSK-2017 begins to sign the root zone key set (the actual rollover event).
January 11, 2019: Revocation of old KSK.
March 22, 2019: Last day the old KSK appears in the root zone.
August 2019: Old key is deleted from equipment in both ICANN Key Management Facilities.





Questions ???