dnssec-keyfromlabel

Outil de génération de clé crypto hardware DNSSEC

dnssec-keyfromlabel génère des fichiers de paire de clé qui référence un objet clé stocké dans un module cryptographique (HSM). Le fichier de clé privée peut être utilisé pour signer une zone de donnée comme si elle était une clé de signature conventionnelle créé par dnssec-keygen, mais la clé est stockée dans le HSM.

Le nom de la clé est spécifié sur la ligne de commande. Il doit correspondre au nom de la zone pour laquelle la clé est générée.

OPTIONS

-a algorithm Sélectionne l'algorithme cryptographique (RSAMD5, RSASHA1, DSA, NSEC3RSASHA1, NSEC3DSA, RSASHA256, RSASHA512, ECCGOST, ECDSAP256SHA256, ou ECDSAP384SHA384). Défaut : RSASHA1.

-3 Utilise un algorithme capable de gérer NSEC3 opur générer une clé DNSSEC. Défaut : NSEC3RSASHA1

engine Spécifie le hardware cryptographique à utiliser

-l label Spécifie le label pour une paire de clé crypto hardware

nametype Spécifie le type propriétaire de la clé. ZONE (pour une clé de zone DNSSEC), HOST, ou ENTITY (pour une clé associée avec un hôte), USER (pour une clé associée avec un utilisateur), ou OTHER (DNSKEY)

-C Mode compatibilité : génère des clé ancien style, dans métadonnée.

-c class Indique que le record DNS contenant la clé devrait avoir la classe spécifiée. Défaut : IN

-f flag Définis le flag spécifié dans le champ flag du record KEY/DNSKEY. Les seuls flags reconnus sont KSK et REVOKE

-G Génère une clé, mais ne la publie pas et ne signe rien avec. Incompatible avec -P et -A

-K directory Définis le répertoire dans lequel les fichiers sont écris

-k Génère des records KEY au lieu de DNSKEY

-L ttl Définis le ttl par défaut à utiliser pour cette clé quand elle est convertie dans un DNSKEY RR. Si la clé est importée dans une zone, c'est le TTL qui sera utilisée pour elle, sauf si un DNSKEY RRset est déjà définis, auquel cas il a précédence.

-p protocol Définis la valeur protocol pour la clé. Le protocol est un nombre entre 0 et 255. Défaut : 3 (DNSSEC). D'autres valeurs possible sont listées dans la rfc2535 et ses successeurs.

-S key Génère une clé comme successeur explicite d'une clé existante. Le nom, l'algorithme, la taille, et le type de clé doivent matcher le prédécesseur. La date d'activation de la nouvelle clé sera mis à la date de désactivation de cette existante. La date de publication sera définis à la date d'activation moins l'interval de pré-publication, qui est 30 jours par défaut.

-t type Indique l'utilisation de la clé. AUTHCONF, NOAUTHCONF, NOAUTH, ou NOCONF. Défaut : AUTHCONF. AUTH réfèrre à la capacité d'authentifier les données, et CONF à la capacité de chiffrer les données.

-v level Définis le niveau de debug

-y Permet de générer des fichiers de clé DNSSEC même si l'ID de clé est en colision avec une clé existante, dans le cas d'une clé à révoquer.

-P date/offset Définis la date à laquelle une clé doit être publiée dans la zone. Après cette date, la clé sera incluse dans la zone mais ne sera pas utilisée pour la signer.

-A date/offset Définis la date à laquelle la clé est activé. Après cette date, la clé sera incluse dans la zone et utilisée pour la signer.

-R date/offset Définis la date à laquelle la clé est révoquée. Après cette date, la clé sera flagé révoquée. Elle sera inclus dans la zone et utilisée pour la signer

-I date/offset Définis la date à laquelle la clé est retiré. Après cette date, la clé sera incluse dans la zone, mais ne sera pas utilisée pour la signer

-D date/offset Définis la date à laquelle la clé est supprimée. Après cette date, la clé ne sera plus incluse dans la zone.

-i interval Définis l'interval de pré-publication pour une clé.

Options de temps

Les dates peuvent être exprimées au format YYYYMMDD ou YYYYMMDDHHMMSS. Si l'argument commence par un '+', ou un '-', il est interprété comme relatif au temps présent. Si un tel temps relatif est suivi pas un des suffixes 'y', 'mo', 'w', 'd', 'h', ou 'mi', alors le temps relatif est calculé en année, mois (de 30 jours), semaines, heure ou minute respectivement. Sans suffix, le temps relatif est exprimé en seconde. Pour empêcher de définir une date, utiliser 'none' ou 'never'

Fichiers générés

Les fichier de clé générés sont nommés sous la forme Knnnn.+aaa+iiiii. Cette chaîne d'identification signifie :

nnnn Est le nom de la clé

aaa La représentation numérique de l'algorithme

iiiii L'identifiant de clé (ou empreinte)

dnssec-keyfromlabel créé 2 fichiers, avec des noms basés sous la forme Knnnn.+aaa+iiiii.key et Knnnn.+aaa+iiiii.private. Le fichier .key contient un record DNS KEY qui peut être inséré dans un fichier de zone, et le fichier .private contient les champs spécifiques à l'algorithme. Ce fichier n'a pas de permission de lecture.