Latin American and Caribbean Internet Addresses Registry

LACNIC DNSSEC

Implementación y operación

Document date: 01/02/2013

Document version: -06 (2014-12-08)

LACNIC http://www.lacnic.net

Latin American and Caribbean Internet Addresses Registry

Table of Contents

Zonas DNS gestionadas por LACNIC

Zonas Reversas

Las zonas reversas operadas por LACNIC son:

177.in-addr.arpa
179.in-addr.arpa
181.in-addr.arpa
186.in-addr.arpa
187.in-addr.arpa
189.in-addr.arpa
190.in-addr.arpa
191.in-addr.arpa
200.in-addr.arpa
201.in-addr.arpa
2.1.1.0.0.2.ip6.arpa
3.1.1.0.0.2.ip6.arpa
0.8.2.ip6.arpa

Zonas Directas

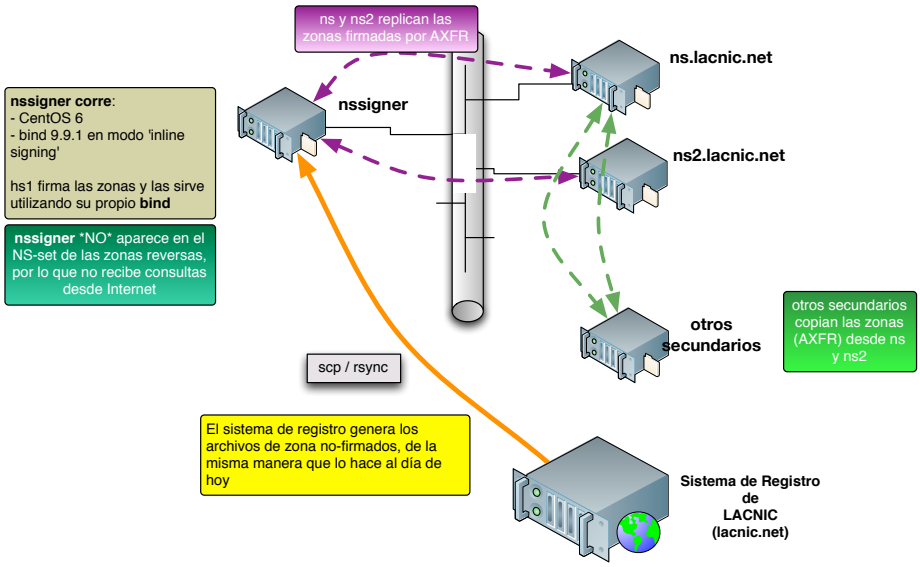
Las zonas directas operadas por LACNIC son:

programafrida.com
programafrida.net
programafrida.org
lacnog.net
lacnog.com
lacnog.org
fridaprogram.com
fridaprogram.org
fridaprogram.net
lacnic.org
lacnic.net
flip-6.net
flip-6.org
flip-6.com
portalipv6.net

proyectoamparo.net
lacnic.net.uy
lacnic.org.uy
lacnic.uy

Arquitectura

Diagrama general



Generación de las zonas reversas

Las zonas reversas (sin firmar) son generadas por dos scripts (dnsrevpublisher y dnsrevpublisher_v6) en el servidor 'lacnic.net'.

Estos scripts son ejecutados por un script 'front end' llamado revpub.sh (~/bin/revpub.sh) en el crontab del usuario 'lacnic' cada 4 horas (6 publicaciones diarias), comenzando a las 3.30 AM. Luego del fin de cada proceso de publicación los archivos de zona son copiados por scp al servidor ns.lacnic.net.

Antes de comenzar la copia de las zonas el script 'revpub.sh' crea un archivo de lock en ns.lacnic.net (`/usr/local/named/var/named/lock`) que permite realizar la exclusión mutua de los procesos de recarga de las zonas.

En ns.lacnic.net las zonas quedan almacenadas en el directorio `/usr/local/named/var/named`.

El "Hidden Signer"

El "*hidden signer*" (HS) es un servidor que reside en una red no expuesta directamente a Internet y es el que cumple las funciones de generación y almacenamiento de claves criptográficas así como también realiza la re-firma periódica de las zonas de DNS.

El software que se utiliza es BIND 9.9.2 (última versión a la fecha, diciembre 20, 2012) en modo "*inline-signing"* con algunos scripts en shell que automatizan algunas tareas.

Configuración y operación del "Hidden Signer"

Configuración general

Todo el software relevante (bind99 y scripts creados por LACNIC) están instalados bajo el usuario bind99 y deben ejecutarse personalizando ese usuario, de lo contrario pueden presentarse efectos no deseados como alteración de permisos y otras fallas.

La única excepción es el arranque y parada del demonio named, lo cual debe ejecutarse como root.

Creación del usuario bind99

El usuario 'bind99' se crea con el siguiente comando:

```
# useradd -m bind99
```

Compilación del bind 9.9.x

Los pasos para compilar el bind 9.9.x son los siguientes, a ejecutar siempre bajo el usuario bind99:

1. Obtener la última versión del código fuente
    a. Visitar http://www.isc.org
2. Instalar dependencias

```
apt-get install libssl-dev
```

3. Configurar el código
    a. Ejecutar:

```
./configure --prefix=/home/bind99
```

    b. Ejecutar:

```
make
make install
```

4. Compilar
5. Instalar

Layout de la configuración, archivos de zona

El layout general de archivos bajo `/home/bind99` está diseñado de acuerdo a la siguiente estructura:

```
.
├─── bin
├─── etc
├─── lib
├─── sbin
├─── share
│    └─── man
│         ├─── man1
│         ├─── man3
│         ├─── man5
│         └─── man8
└─── var
     ├─── keys
     ├─── log
     ├─── run
     │    └─── named
     └─── zones
```

```
        ├─── lacnic_external
        └─── lacnic_internal
```

Script de arranque automático

El script de arranque automático del bind99 es el siguiente (compatible con sistemas Fedora/CenOS). En lo posible este script debe llamarse /etc/init.d/bind99.

```
#!/bin/sh
# Startup script for program
#
# chkconfig: 345 85 15
# description: BIND/named 9.7.2-P2
# processname: named
# pidfile: /var/run/named.pid


# Source function library.
. /etc/rc.d/init.d/functions


B9HOME="/home/bind99"
B9USR="bind99"
B9ARGS="-4"

case "$1" in
  start)
        echo -n "Starting bind9-lacnic: "
        daemon  $B9HOME/sbin/named $B9ARGS -u $B9USR -c
$B9HOME/etc/named.conf
        echo
        touch /var/lock/subsys/named
        ;;
  stop)
        echo -n "Shutting down bind9-lacnic: "
        killproc named
        echo
        rm -f /var/lock/subsys/named
        rm -f /var/run/named.pid
        ;;
  status)
        status named
        ;;
  restart)
```

```
        $0 stop
        $0 start
        ;;
  reload)
        echo -n "Reloading process-name: "
        killproc process-name -HUP
        echo
        ;;
  *)
        echo "Usage: $0 {start|stop|restart|reload|status}"
        exit 1
esac


exit 0
```

Configuración del 'rndc'

La utilidad "rndc" es una herramienta de línea de comando que facilita la administración del servicio "*named*" en forma local. Puede utilizarse también en forma remota pero este capítulo no trata esta segunda funcionalidad.

Archivos relevantes

Los archivos necesarios para utilizar el comando "*rndc*" son:

```
/home/bind99/etc/named.conf   - Configuracion del servicio "named"
/home/bind99/etc/rndc.key     - Archivo de clave para "rndc"
```

Veamos la generación de los 2 archivos necesarios.

1. Generación del archivo de clave "rndc.key"

Generar la clave con el comando *rndc-confgen*, los parámetros mínimos pueden ser:

-a Genera el archivo de clave en el directorio /home/bind99/etc/
-b Largo de clave
-k El nombre que le daremos a la clave
-r Fuente de datos aleatorios

```
rndc-confgen -a -b 256 -k clave-rndc -r /dev/urandom
```

este comando crea en */home/bind99/etc/* un archivo llamado "*rndc.key*" con el contenido de la clave de 256 bits, el nombre "*clave-rndc*" y el algoritmo por defecto "*hmac-md5*"

```
key "clave-rndc" {
      algorithm hmac-md5;
      secret "irwfZwBUJjkh+j47h6WN9fp3PbVFbzWnzFLMJEch0S4=";
};
```

2. Generación del archivo de configuración de bind "*named.conf*"

Este archivo debe incluir la clave generada en el punto anterior de esta forma:

```
include "/home/bind99/etc/rndc.key";
```

y además permitir la administración del *bind* instalado, desde el host local y con la clave generada

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { "clave-rndc"; };
};
```

el archivo *named.conf* quedará entonces asi:

```
include "/home/bind99/etc/rndc.key";
controls {
      inet 127.0.0.1 allow { localhost; } keys { "clave-rndc"; };
};
```

Parámetros para rndc

El comando "rndc" tiene la forma siguiente:

```
rndc <options> <command> <command-options>
```

y algunas de las opciones son:

refresh - Refresca la base de datos del servidor de nombres.

stats - Descarga las estadísticas actuales de named al archivo /home/bind99/etc/named.stats.

reload - Recarga los archivos de zona pero mantiene todas las respuestas precedentes situadas en caché. Esto permite realizar cambios en los archivos de zona sin perder todas las resoluciones de nombres almacenadas. Si se desea afectar solamente una zona específica con el parámetro "reload" se debe pasar el nombre de zona a la opción "*reload*", por Ej:

```
rndc reload example.com
```

Gestión de zonas

Introducción

Los pasos para agregar una nueva zona para ser firmada son los siguientes:

1. Creación de par de claves
2. Configuración del 'hidden master'
3. Configuración de los servidores públicos
4. Publicación del registro DS en la zona padre

Agregar una nueva zona firmada

Para agregar una nueva zona a ser firmada se deben seguir los siguientes pasos:

- En los servidores públicos (ns.lacnic.net y ns2.lacnic.net) se modifica la configuración de la zona para que pase a ser una zona esclava del 'hidden master':

```
zone  "example.net" {
        type slave;
        masters { 200.3.15.13; };
        allow-notify { 200.3.15.13; };
        also-notify { 200.192.232.53; 200.160.0.217; };
};
```

- En el 'hidden master' se agrega la zona en el archivo "named.conf.<tipo>.local":

```
zone example.net {
      type master;
      file "var/zones/direct/example.net";
      key-directory "var/keys/";
      inline-signing yes;
      auto-dnssec maintain;
      allow-transfer {200.3.13.11; 200.3.13.10;};
      notify explicit;
      also-notify {200.3.13.11; 200.3.13.10;};
      ixfr-from-differences yes;
```

```
        max-journal-size 40M;
};
```

- Crear dos pares de claves (ZSK / KSK):
    - La ZSK:

```
dnssec-keygen -a RSASHA1 -b 2048 -n ZONE -r /dev/urandom \
      -I now+12mo -D now+13mo example.net
```

        - Los parámetros son:
            - -a: Suite de algoritmos criptográficos a utilizar (RSASHA1 en este caso)
            - -b: Largo de clave en bits
            - -n: Tipo de clave (siempre será ZONE en nuestro caso)
            - -r: Dispositivo para generar entropía (usar /dev/urandom, en caso contrario es muy, pero muy lento)
            - -I: fecha de inactivación (dentro de 12 meses)
            - -D: fecha de borrado (dentro de 13 meses)
            - example.net: Nombre de la zona para la que utilizaremos la clave
    - La KSK:

```
dnssec-keygen -a RSASHA1 -b 2048 -n ZONE –f KSK -r /dev/urandom \
      -I now+24mo -D now+25mo example.net
```

        - Los parámetros:
            - -f: Flags de la clave, en este caso la marcamos como KSK
            - (los demás son idénticos a los usados para crear la ZSK)

Uso de NSEC3 para zonas que lo requieran

El procedimiento es similar salvo las siguientes observaciones:

- Las claves se deben generar con RSASHA256 como algoritmo de cifrado y el switch '-3' para que las mismas queden listas para ser usadas con NSEC3
- Luego de cargada la zona se debe insertar un registro NSEC3PARAM lo cual puede ser realizado de manera dinámica (rndc) o agregarse estáticamente en el archivo de zona mismo

Comment [CM1]: Confirmar !!

Refirmado cuando la zona cambia

A la hora de hacer cambios en una zona es fundamental incrementar el "serial" del registro SOA. Si esto no se hace, la lógica de refirmado de las zonas seguramente va a funcionar mal.

Previamente a incrementar el número de serie de la zona debemos verificar el número de serie actual. Este no necesariamente coincide con el que vemos en el archivo de zona no firmado debido a que el proceso automático de firma incrementa el número de serie automáticamente cada vez que la zona es re-firmada.

El número de serie a utilizar debe ser mayor que el que esta siendo utilizado en la zona firmada.

Para chequear el serial actual:

```
[bind99@signer ~]$ dig @localhost soa example.net +short
NS.example.net. hm.example.net. 2013010853 7200 3600 604800 172800
```

El comando es '`rndc reload example.net`':

```
[bind99@signer direct]$ rndc reload example.net
zone reload queued | up-to-date
```

Configurar parámetros de timing en las claves

El comando es '**`dnssec-settime`**', ejemplo:

```
dnssec-settime -f -P now -A now -I now+3d -D now+1w \
Kexample.net.+008+52180
```

- Los parámetros son:

- –f: forzar configuración de metadata de timing en archivos de clave creados conversiones anteriores que no tenían esta información. Opcional.
- –P: fecha de publicación de la clave (publish)
- –A: fecha de activación de la clave (activation)
- –I: fecha de inactivación de la clave (inactivation)
- –D: fecha de borrado de la clave (deletion)

Publicación del registro DS en la zona padre

Extracción del registro DS a partir de la KSK de la zona

En el directorio ~/var/keys se debe ejecutar el siguiente comando siempre sobre el archivo de clave de la KSK:

```
# dnssec-dsfromkey -T 3600 -1 K3.1.1.0.0.2.ip6.arpa.+008+24956.key
```

Resultado:

```
3.1.1.0.0.2.ip6.arpa. 3600 IN DS 24956 8 1
67BD5687E6C5479B019211AEB7F0C9096FA45584
```

Los parámetros son:

- -T: TTL
- -1: Algoritmo de hash (SHA1 en este caso, se puede usar -2 para generar DS con SHA2)
- (Posicional final): Nombre del archivo ".key" que contiene el registro DNSKEY de la KSK

Es posible automatizarlo para crear los registros DS de manera masiva:

```
for x in $(grep -iH "key-sign" *arpa* | cut -d: -f1); do dnssec-dsfromkey
-T3600 -1 $x ; dnssec-dsfromkey -T3600 -2 $x ; done
```

Zonas directas bajo un gTLD

En el caso de los .net/.com/.org y demás gTLDs el mecanismo de publicación del registro DS varía de acuerdo al registrar utilizado. En el caso de LACNIC las zonas están registradas en GoDaddy (http://www.godaddy.com) y la publicación de los registros DS se realiza a través de la interfaz de gestión de dominios dentro de la opción 'Nameservers'.

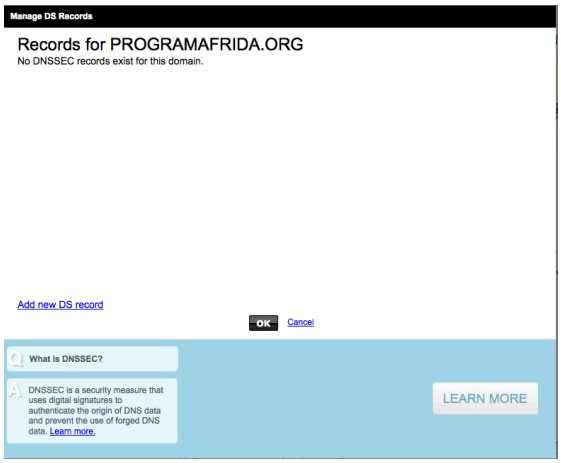


Figure 1: Paso #1 para publicar un DS en GoDaddy

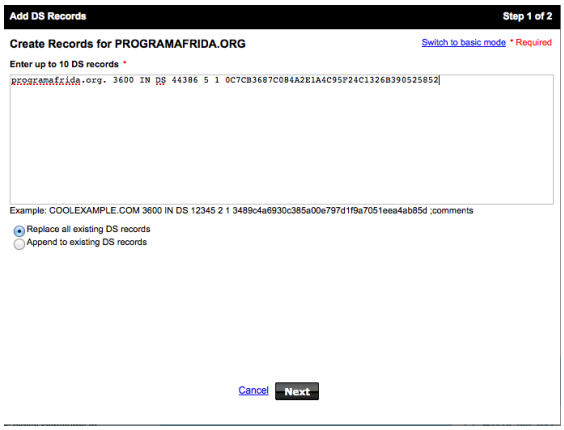


Figure 2: Paso #2

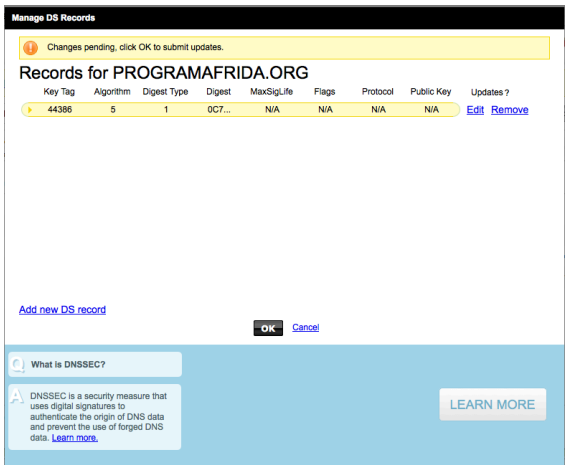


Figure 3: Paso final

Zonas reversas bajo IANA

La publicación de registros DS bajo IANA se realiza utilizando la interfaz rDNS. Para mas información sobre este sistema ver el documento [DRAFT-rDNS].

Backups y Restauración

Archivos de zona y de claves

Los archivos de zona (particularmente los de las zonas directas) y los archivos de clave (K*.key y K*.private) son los activos de información mas importantes de la instalación.

Un respaldo mínimo puede hacerse mediante el comando 'tar':

```
sudo –i –u bind99
cd $HOME
tar czvf backup-dnssec-<fecha>.tar.gz ~/var/zones ~/var/keys
```

Restauración

El proceso de restauración en otro servidor involucra reinstalar el software (bind 9.9.2) recreando todo el ambiente descripto en las secciones anteriores.

Es de notar que en caso de tener que restaurar el sistema de firmado en un servidor que tenga otra dirección IP se hace necesario modificar la configuración de NS y NS2 para que copien las zonas del servidor restaurado.

Verificación y monitoreo de las zonas

Verificación de funcionamiento

La verificación básica de funcionamiento y de consistencia se hace localmente en el ***hidden signer*** con el comando 'dig':

```
[bind99@signer ~]$ dig @localhost 201.in-addr.arpa soa +multi +dnssec
+noall +answer

; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2 <<>> @localhost 201.in-
addr.arpa soa +multi +dnssec +noall +answer
; (2 servers found)
;; global options: +cmd
201.in-addr.arpa. 86400 IN SOA NS.LACNIC.NET. hostmaster.LACNIC.NET. (
                        2013012511 ; serial
                        1800       ; refresh (30 minutes)
                        900        ; retry (15 minutes)
```

```
                        691200     ; expire (1 week 1 day)
                        10800      ; minimum (3 hours)
                        )
201.in-addr.arpa. 86400 IN RRSIG SOA 5 3 86400 20130224135503 (
                        20130125125503 29508 201.in-addr.arpa.
                        0wmD6ZeqSQDpBuziIxYt8R4NNanZVVbKl8Uf/vunXG8s
                        kMi+owCxV6xIXhonslJ7ScdxyvdjM1UCvFnXpzs7WFTL
                        6jjkXzbOYXJbRH77YO1fZSP6qnyQfxl36+3ldiqOkPV1
                        O69GkJ37TAGZ692lkiihvdrcTZwmor9kjyRwYyHvEv6L
                        NdcSpwMzN7A2kmfQpn74Rci3HAB59nigkTqj68z9Khlb
                        QzTJnvDxLjSaqy6V4GiExkmJjrN+7g87K/qbbXBpl0Bi
                        jEiStueCPQmf9dL4n8yHdAsrtSahQz4qEgWg240Toj8S
                        X5RF/3btBcjndFLMMm69LbzaZMelyRW+UA== )
```

A verificar:

- Número serial del SOA, debe ser igual o mayor que el que está listado en el archivo de zona no firmado correspondiente.
- Presencia de uno o mas registros RRSIG en la respuesta. Estos registros son los que contienen las firmas DNSSEC. En caso de no estar presentes la zona no está firmada y habría que verificar el porqué.
- En el registro RRSIG se identifican el comienzo y final de la validez de las firmas. Las mismas deben estar válidas.

Monitoreo proactivo

Bajo la aplicación de recolección de estadísticas OpenData (http://opendata.labs.lacnic.net/) hay scripts monitoreando las zonas firmadas con DNSSEC. El principal valor que se mide es el tiempo restante para la expiración de las firmas.

En la URL http://opendata.labs.lacnic.net/dnsstats/pages/zone_detailed.html se pueden acceder a estas estadísticas.

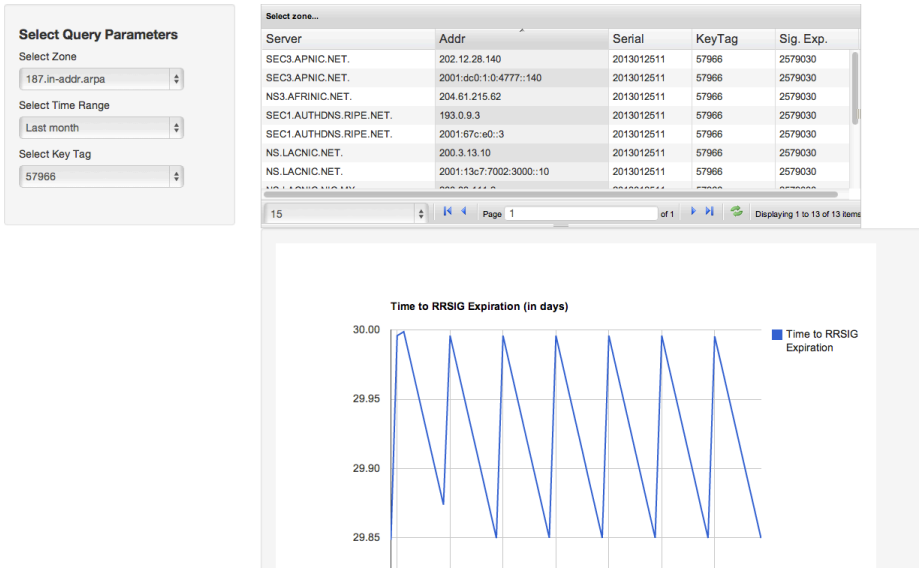


Figure 4 - Tiempo de expiración restante para las firmas de 187.in-addr.arpa

Integración con plataformas de monitoreo

<<falta>>

Rotación del número de serie de una zona

Debido a como bind99 hace el manejo de los seriales de las zonas puede ser necesario resetear el número de serie. Esto se debe a que el serial que genera inicialmente puede ser bastante mayor que el actual y eso no ser compatible con la generación automática de zonas (por ejemplo en el caso de las zonas reversas).

El procedimiento está descripto en [SERIAL-ROT] y consiste en adicionar saltos de 2^31 al serial actual, recargar la zona, esperar que todos los secundarios la repliquen y repetir hasta llegar al serial deseado.

Rotación de claves (Key Rollovers)

Rotación de la KSK

Para rotar la KSK se deben seguir los siguientes pasos:

1. Crear el nuevo par de claves
2. Firmar la zona con el nuevo par de claves
3. Publicar la zona firmada con el nuevo par
4. Publicar el nuevo DS en la zona padre
5. Esperar al menos 1 TTLs de la zona
6. Retirar el DS de la clave anterior de la zona padre
7. Revocar la KSK vieja con el siguiente comando:

```
dnssec-settime -R now -I now+1h -D now+4h K191.in-addr.arpa.+005+11911
```

<<falta>>

Rotación de la ZSK

1. Crear el nuevo par de claves ZSK
2. Firmar la zona con la nueva y vieja ZSK
3. Esperar al menos 1 TTL de la zona
4. Setear los tiempos de inactivación y borrado del par de claves anterior con este comando

```
dnssec-settime -I now+1h -D now+4h K191.in-addr.arpa.+005+11911
```

5. Esperar al menos 1.5 TTL de la zona
6. Retirar la KSK vieja

<<falta>>

Migración desde OpenDNSSEC

Convertir claves de ods a bind

Comando softhsm y softhsm-keyconv, ejemplo:

```
softhsm --export 44890.pem --slot 0 --id 6417001997c8c2bf612e297c35b2c0a6
--pin 12345
softhsm-keyconv --tobind --in e7c72e14faa23df9514be1f7f77a646d.pem --pin
12345 --name proyectoamparo.net. --algorithm RSASHA256
```

En caso de tener que convertir claves de manera masiva es posible automatizar el proceso de la siguiente manera:

```
ods-ksmutil key list --verbose | grep ".arpa" | grep active | awk '{if
($2=="KSK") fksk="--ksk"; else fksk=""; print "softhsm-keyconv --tobind -
-in "$6".pem --pin 12345 --algorithm RSASHA256 --name "$1". "fksk}' | sh
-x
```

Referencias

[SERIAL-ROT] “How to Reset the Serial Number of a Zone”:
http://www.microhowto.info/howto/reset_the_serial_number_of_a_dns_zone.html#idp14640