



"la Ciencia sin Moral es Vana"

Universidad Católica de El Salvador
Miembro RAICES

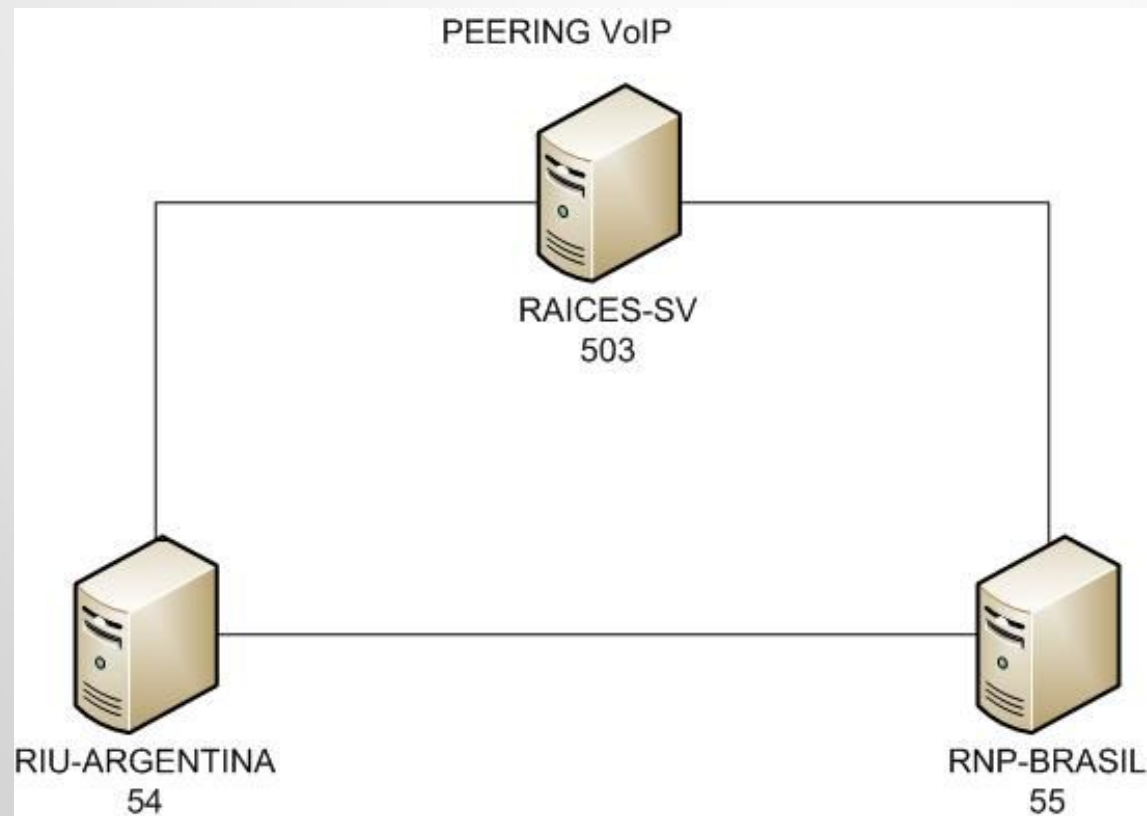


**Incorporación de RAICES a servicio Nrenum.net
y DNSSEC dentro de Proyecto Magic**

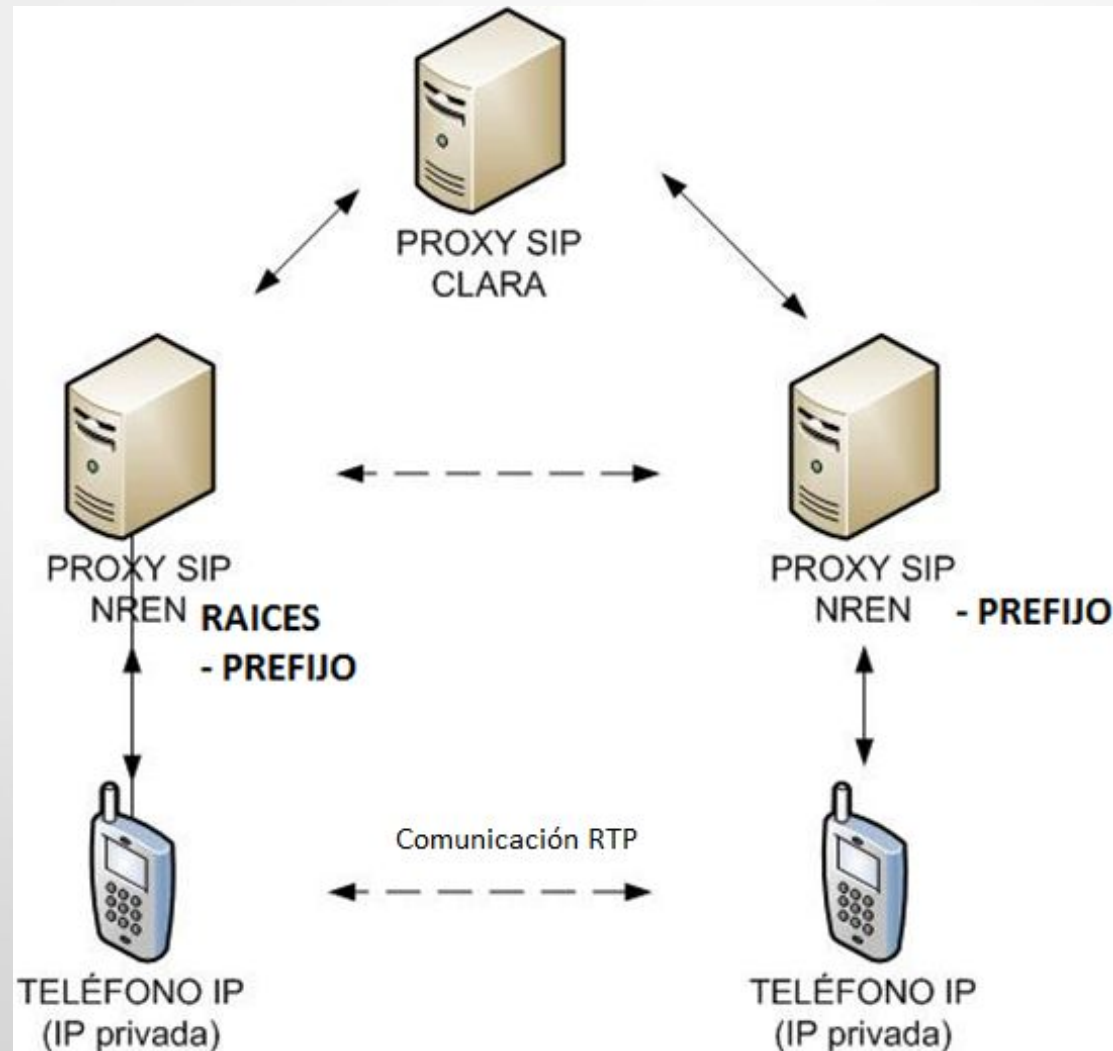
Septiembre de 2016

Escenarios VoIP

- Enlace con red VoIP de Brasil (55)
- Enlace con red VoIP de Argentina (54)



Integración con sistema VoIP de CLARA



Incorporación RAICES a servicio nrenum.net/Proyecto Magic

El Proyecto Magic financiado por la Unión Europea es un proyecto iniciado en mayo de 2015 y que finalizará en abril de 2017. Magic es liderado por varias instituciones a nivel mundial, entre ellas Red Clara.

El servicio NRENUM es liderado en CLARA por
RENATA

Introducción a NRENUM

La norma ITU E.164 define las normas y estructuras de un número telefónico.

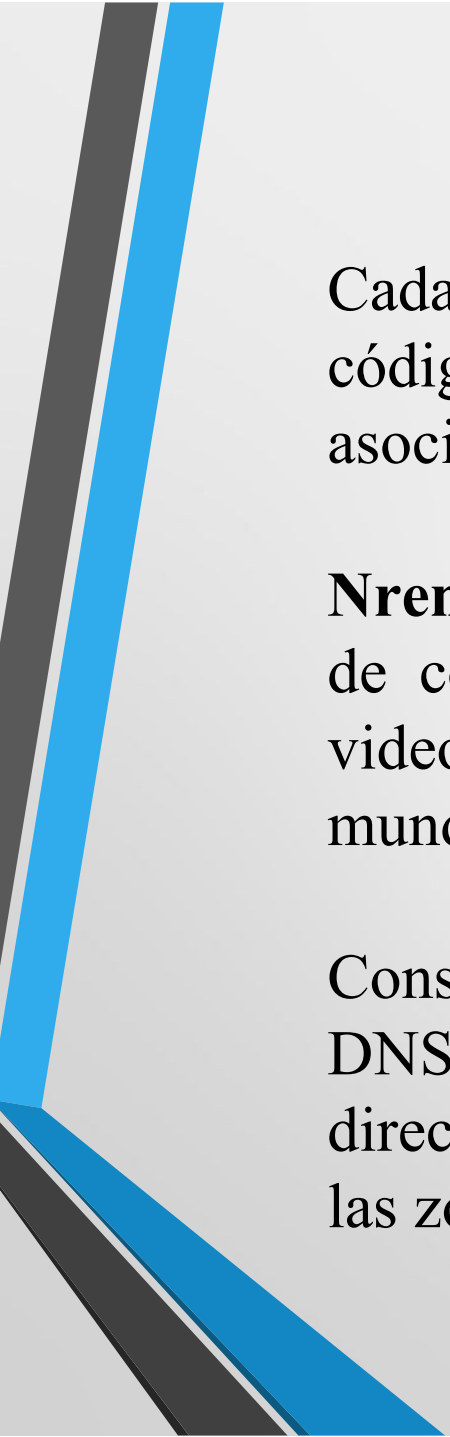
Ej. Cód. de país + prefijo de zona + número de terminal
57 01 5302604 503 24840600

ENUM significa E.164 number mapping y es un protocolo resultado de un grupo de trabajo de Internet (IETF) y que utilizando los sistemas de resolución inversa de nombre de DNS traduce los números telefónicos a direcciones URI.

ENUM es compatible con los protocolos SIP y H.323

NRENUM es la alternativa ENUM para la Academia.

Nrenum.net es un servicio administrado por la organización europea GEANT, el cual ofrece enum a la Academia.



Cada red nacional (NRIE) solicita una zona asociada al código de país, asociando los registros numéricos asociados a los dispositivos de comunicación.

Nrenum.net provee la marcación directa a dispositivos de comunicación (teléfonos, cámaras de videoconferencia, etc) ubicados en cualquier parte del mundo y en tiempo real.

Considerando que ENUM utiliza la resolución inversa DNS para la traducción de números telefónicos a direcciones URI, los números se registran invertidos en las zonas DNS.



Ejemplos:

De zona:

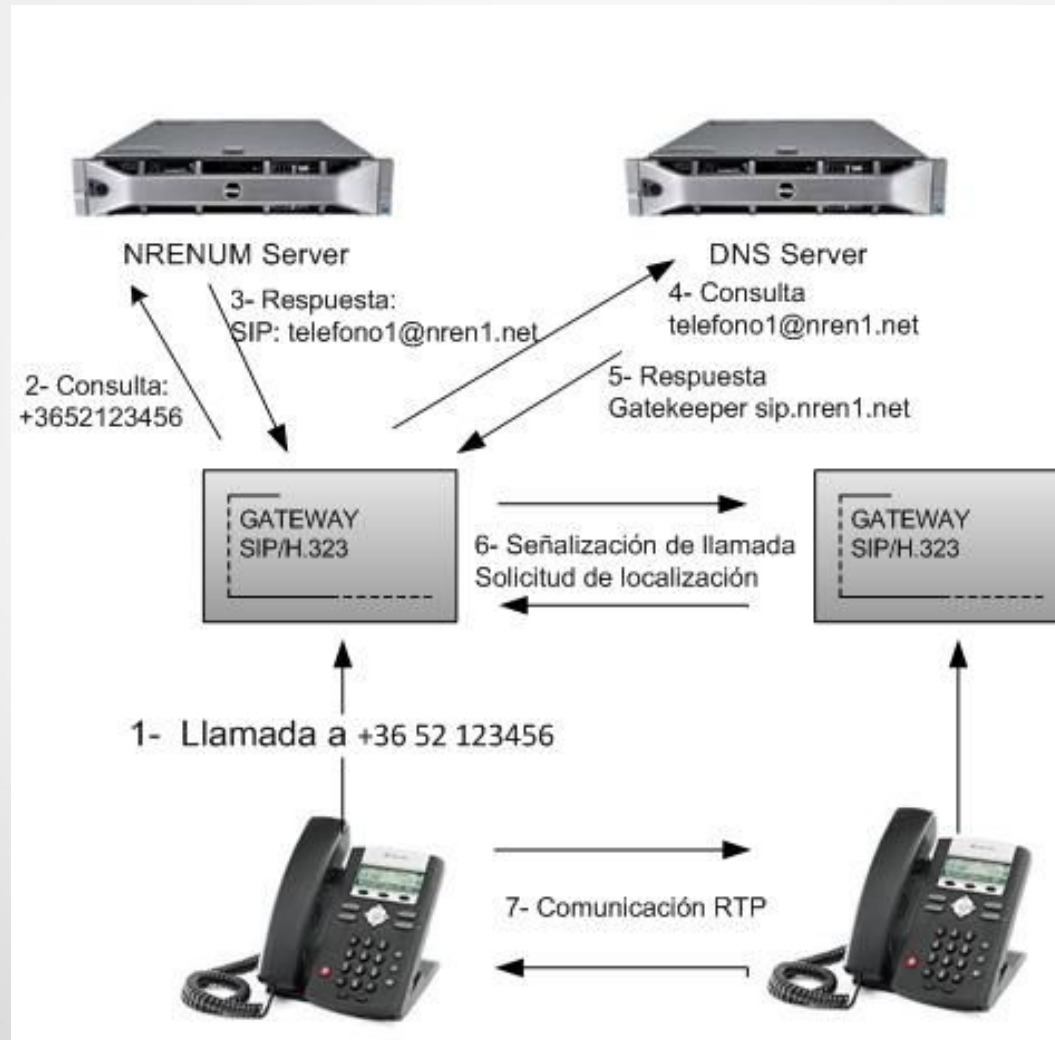
3.0.5.nrenum.net

considerando el código de país para El Salvador + 503

De dispositivo:

0.0.6.4.8.4.2.3.0.5.nrenum.net

LLAMADA VoIP CON NRENUM



Pasos para incorporar/configurar zona 3.0.5.nrenum.net

- Instalar / configurar DNS (bind) primario y secundario (estos servidores deberán tener resolución inversa: registro PTR)
- Registro de números ENUM de dispositivos
(Registros NAPTR –Name Authority Pointer – Número E.164 a URI)
Ej.
0.6.6.0.4.8.4.2.3.0.5.nrenum.net. NAPTR 10 101 "u"
"E2U+sip" "!^.*\$!sip:50324840660@catolica.edu.sv!"
- Solicitud de delegación de zona a nrenum.net a GEANT.
Para el caso de RAICES: 3.0.5.nrenum.net

Continuación de Pasos para incorporar zona

-Configurar nrenum en Gateway de NREN(Asterisk),
agregando la política de enrutamiento.

```
;Política de enrutamiento sistema NRENUM.NET  
exten => _+.,1,Set (Sipuri=${ENUMLOOKUP (${EXTEN}, sip,1,,e164.arpa)})  
exten => _+.,n,GotoIf("${Sipuri}" != "")?dial  
exten => _+.,n,Set (Sipuri=${ENUMLOOKUP (${EXTEN}, sip,1,,nrenum.net)})  
exten => _+.,n,GotoIf("${Sipuri}" = "")?lookupfailed  
exten => _+.,n(dial),Dial (SIP/${Sipuri},60,r)  
exten => _+.,n(lookupfailed),Hangup ()
```

- Pruebas de llamadas utilizando número ENUM, ejemplo a dispositivos SIP y H.323 ubicados en Australia, Hungría, UK, U.S.A.



- Equipo Videoconf. De Australia:
+61 26 2463194
+61 26 2112672
- Equipo SIP/H.323 USA:
+1 703 6916901
- +35 12 104647976

Ingreso de El Salvador (RAICES – 503) a nrenum.net

-30 de septiembre de 2015 se delega el código de país (503) a El Salvador, convirtiéndose en el 38th país en incorporarse a este servicio.

Noticia en red CLARA: www.redclara.net

30 de septiembre 2015: RAICES, la red de El Salvador, se suma a NRENum.net



Tratando de establecer acuerdos de colaboración en tiempo real, el Paquete de Trabajo 4 de **MAGIC** alcanzó un nuevo hito con la incorporación de la red nacional de investigación y educación salvadoreña, **RAICES**, a **NRENum.net**. De este modo, el Código nacional 503, está ahora oficialmente al recaudo de RAICES.

Noticia en sitio de Proyecto Magic: <http://www.magic-project.eu/>

30 September 2015: RAICES, El Salvador, is part of NRENum.net

✍️ Written by María José López Pourailly 📅 Published: 01 October 2015

Seeking for the establishment of agreements for real time collaboration, MAGIC's Work Package 4 achieved a new milestone with the incorporation of the Salvadorian NREN, RAICES to NRENum.net. The country code +503 is now officially delegated to RAICES.

Only two months after NRENum.net announced the incorporation of Ecuador, during the last day of September 2015 the good news was for Central America: "Welcome El Salvador (+503)





Países de Latinoamérica en NRENUM

- Brazil
 - Argentina
 - Colombia
 - Perú
 - Ecuador
 - El Salvador
 - México
 - Uruguay
 - Chile
- Actualmente hay 45 códigos de país delegados a nrenum.net

Crawler.nrenum.net

top country codes

#	country name	E.164	ENUMs
1.)	 Hungary	+36	79605
2.)	 Norway	+47	67859
3.)	 Portugal	+351	52228
4.)	 Brazil	+55	10048
5.)	 Spain	+34	6904
6.)	 North American Numbering Plan	+1	5033
7.)	 Argentina	+54	3462
8.)	 Australia	+61	1956
9.)	 Italy	+39	932
10.)	 Greece	+30	911
11.)	 El Salvador	+503	107
12.)	 United Kingdom	+44	49
13.)	 Netherlands	+31	22
14.)	 India	+91	22
15.)	 Latvia	+371	21
16.)	 Czech Republic	+420	20
17.)	 Hong Kong	+852	20
18.)	 Belgium	+32	11
19.)	 Sri Lanka	+94	10
20.)	 New Zealand	+64	10
21.)	 France	+33	8
22.)	 Chile	+56	1
23.)	 Romania	+40	1
24.)	 Poland	+48	1
25.)	 Ecuador	+593	1

Actualización de zona

3.0.5.nrenum.net a DNSSEC

DNSSEC (DNS Security Extensions) incorpora firmas criptográficas a las consultas y respuestas que permite a tu computadora detectar información falsa

Ventajas:

- integridad de los datos
- registros digitalmente firmados
- previene ataques o problemas de seguridad al DNS (cache poisoning, BIND redirection)

Cont. DNSSEC

Tipos de llaves utilizados:

DNSSEC utiliza

- Key Signing Keys (KSK) y
- Zone Signing Keys (ZSK)

y diferentes algoritmos entre ellos RSA/SHA-256.

Asegurando la zona: 3.0.5.nrenum.net

- Instalar los paquetes y/o dependencias

(considerando que se tiene GNU/Linux y BIND):

```
#apt-get install softhsm opendnssec
```

(softhsm es una implementación de software de un dispositivo criptográfico genérico con una interface PKCS#11)

- Creación de zona segura (/etc/bind/db.3.0.5.nrenum.net)

- Añadir y firmar la zona

(Creación de llaves criptográficas (RSA/SHA-256))

- Verificar que se ha se ha creado el archivo de zona “firmado”, el cual contiene registros RRSIG, DS, DNSKEY (record type 257 y 256).

```
# host -t any 3.0.5.nrenum.net
```

```
# dig 127.0.0.1 -t NAPTR 3.0.5.nrenum.net +dnssec
```

- Reconfiguración de zona named.conf.local apuntando hacia la zona firmada (signed)

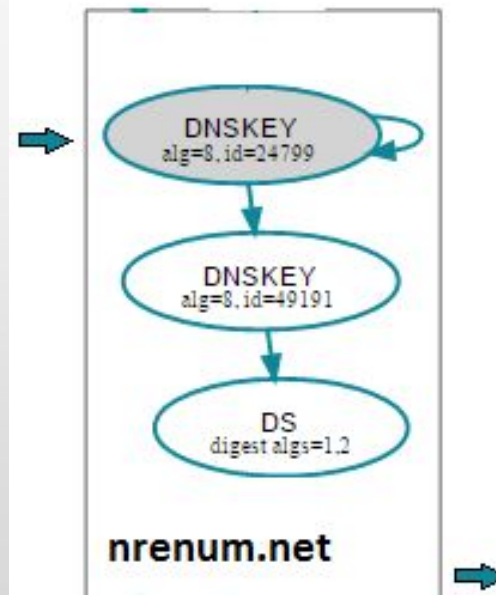
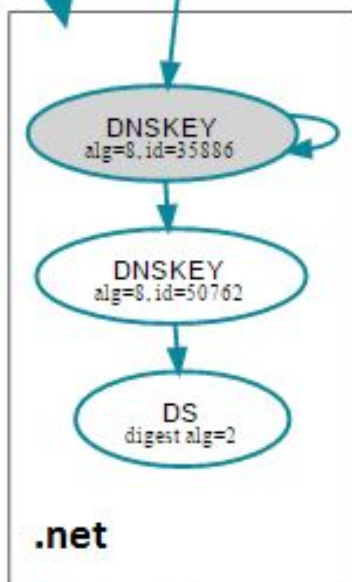
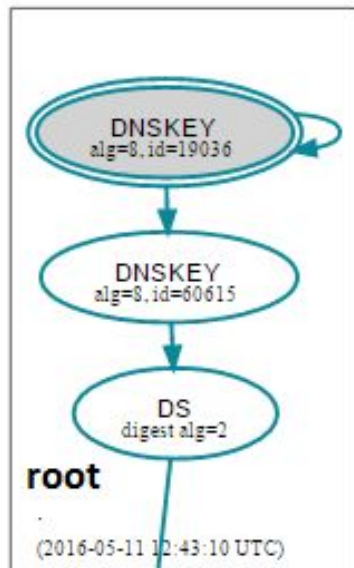
- Reiniciar servicio bind

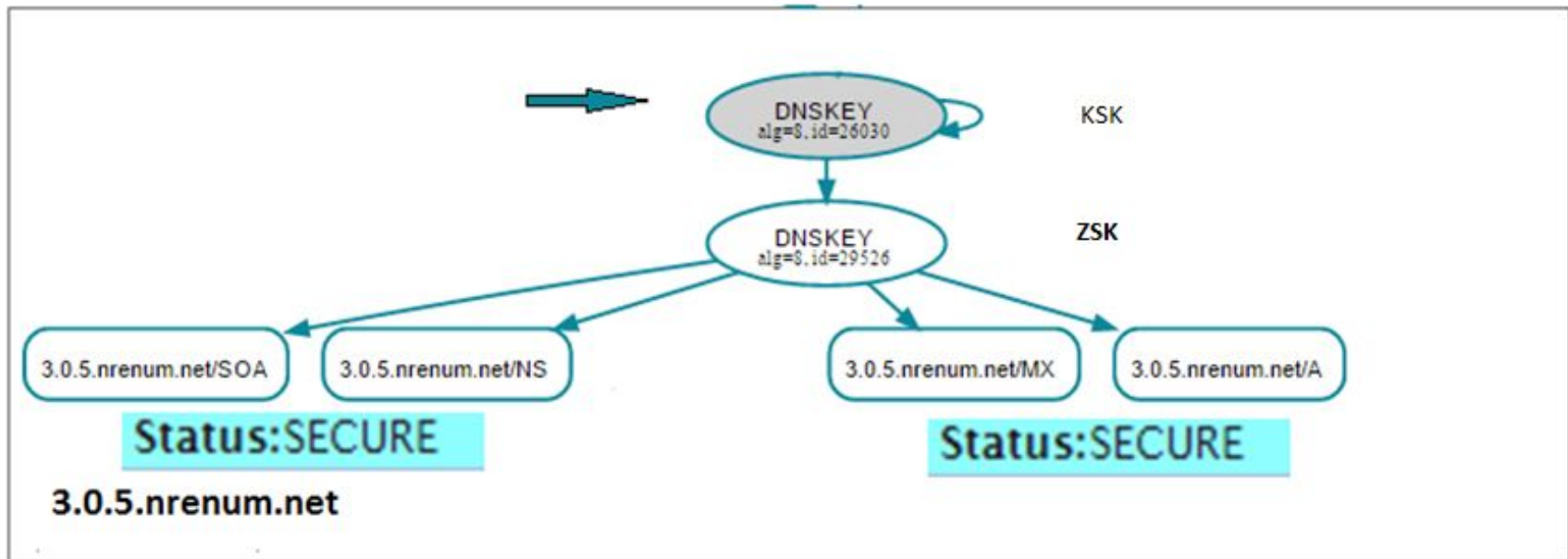
- Exportar llaves hacia zona superior (parent)

```
#ods-ksmutil key export --ds
```

Pruebas y monitoreo DNSSEC

<http://dnsviz.net/d/3.0.5.nrenum.net/dnssec/>





Otro sitio de verificación de DNSSEC:

← → ↻ portfolio.sidnlabs.nl:8080/check/3.0.5.nrenum.net

3.0.5.nrenum.net, "", secure, ""

DNSSEC en servicio NRENUM

Actualmente están utilizando el servicio DNSSEC con NRENUM 10 países:

- Norteamerica: 1 (USA)
- EUROPA: 5 Países (Inglaterra, Rep. Checa, Hungría, Noruega, Polonia,
- LATINOAMERICA: Colombia, Perú, Ecuador y El Salvador
- AUSTRALIA: 1 (Australia)

Fuente: <https://nrenum.net/members/>

CONCLUSIONES/RECOMENDACIONES

- El servicio NRENUM es un importante proyecto de comunicación global en el que investigadores y académicos alrededor del mundo mejoran su trabajo colaborativo
- Muy importante que todas las redes Nacionales (NREI) se incorporen a esta importante iniciativa.
- Las Universidades aprovechen el proyecto MAGIC financiado por Unión Europea, ya que es una buena oportunidad para lograr incorporarse de la mejor manera. (asesoría y apoyo técnico de CLARA por medio de RENATA y de GEANT)
- Asegurar las zonas NRENUM por medio de DNSSEC es una buena práctica que permite a los usuarios del servicio detectar información falsa, verifica la integridad y prevenir diversos ataques o problemas de seguridad relacionados al DNS



"la Ciencia sin Moral es Vana"



Gracias.

Wilfredo Bolaños

wilfredo@catolica.edu.sv

Universidad Católica de El Salvador

Miembro RAICES