Universidad Nacional de Asunción
CNC
Centro Nacional de Computación
NIC.py
32 AÑOS 1991 - 2023 .PY te conecta al mundo
Universidad Católica "Nuestra Señora de la Asunción"
LABORATORIO de Electrónica Digital

# PARAGUAY 2023 INTERNET GOVERNANCE FORUM

FORO DE GOBERNANZA DE INTERNET PARAGUAY


# DNSSEC

## para .py

Conceptos y práctica experimental

Universidad Nacional de Asunción
CNC
Centro Nacional de Computación

NIC.py

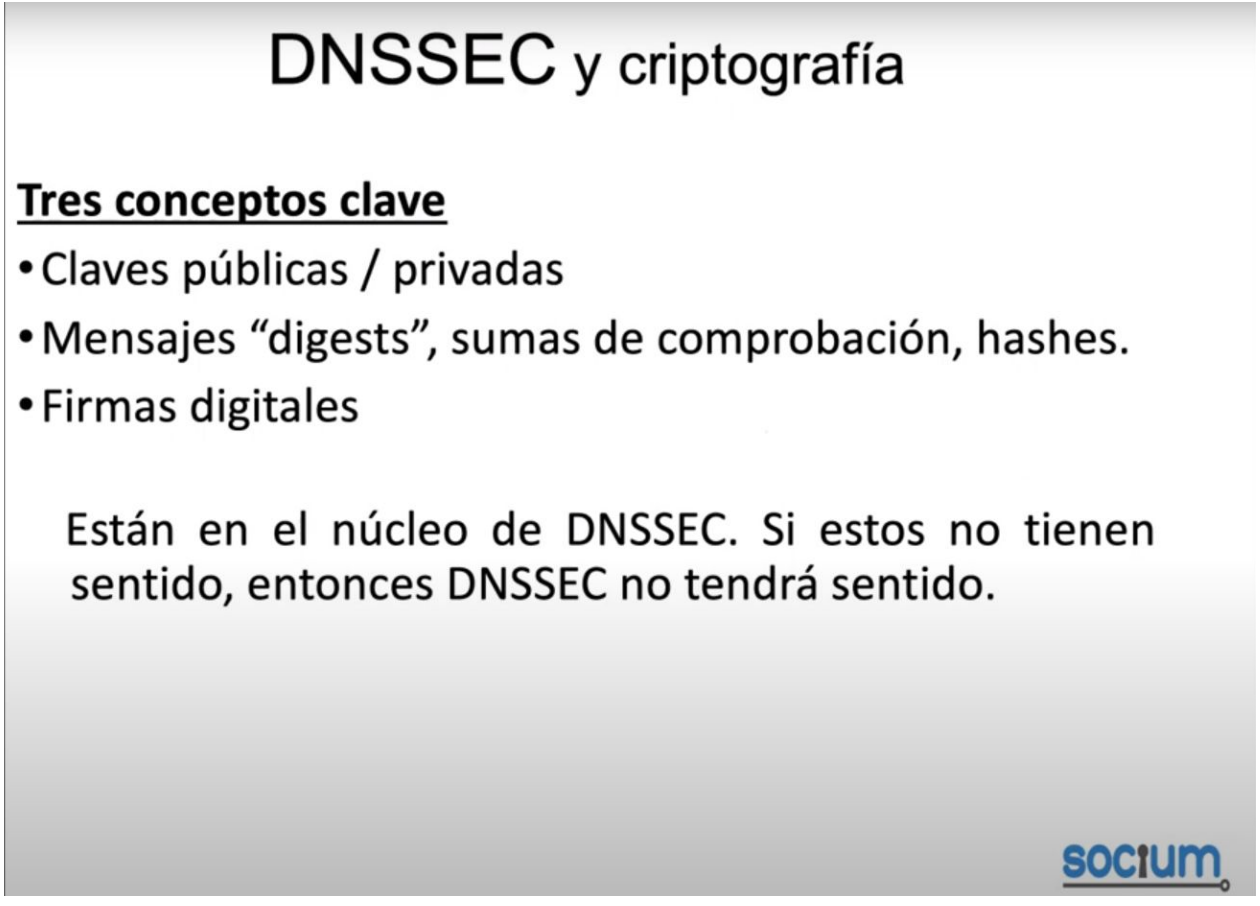
32 AÑOS 1991 - 2023
.PY te conecta al mundo

Universidad Católica
"Nuestra Señora de la Asunción"

# AGENDA

- Repaso de conceptos generales: DNS y DNSSEC
- Propuesta para implementación
- Procedimiento de encadenamiento

# REPASO


DNSSEC y criptografía
Tres conceptos clave
• Claves públicas / privadas
• Mensajes “digests”, sumas de comprobación, hashes.
• Firmas digitales
Están en el núcleo de DNSSEC. Si estos no tienen sentido, entonces DNSSEC no tendrá sentido.
socium

# REPASO

## Texto cifrado

- Comenzamos con ***texto plano***. Algo que puedas leer.
- Aplicamos un algoritmo matemático al ***texto plano***.
- El algoritmo es el ***cifrado***.
- El texto plano se convierte en ***texto cifrado***.
- Crear un cifrado seguro es un proceso difícil.
- El proceso de estandarización para AES, el reemplazo para el envejecimiento del protocolo DES, tomó 5 años.

socium

# REPASO


Llaves
• En la criptografía simétrica, un texto simple se transforma en un texto cifrado, y nuevamente en texto plano utilizando una clave para el cifrado (el algoritmo utilizado) en ambos extremos.
• Suponiendo que se conoce el método de cifrado, la seguridad del texto cifrado se basa en la llave. Éste es un punto crítico. Si alguien obtiene su llave, se compromete su texto plano.
socium

# REPASO

Cifrado simétrico


La misma clave se utiliza para cifrar el documento antes de enviarlo y para descifrarlo una vez que se recibe

socium

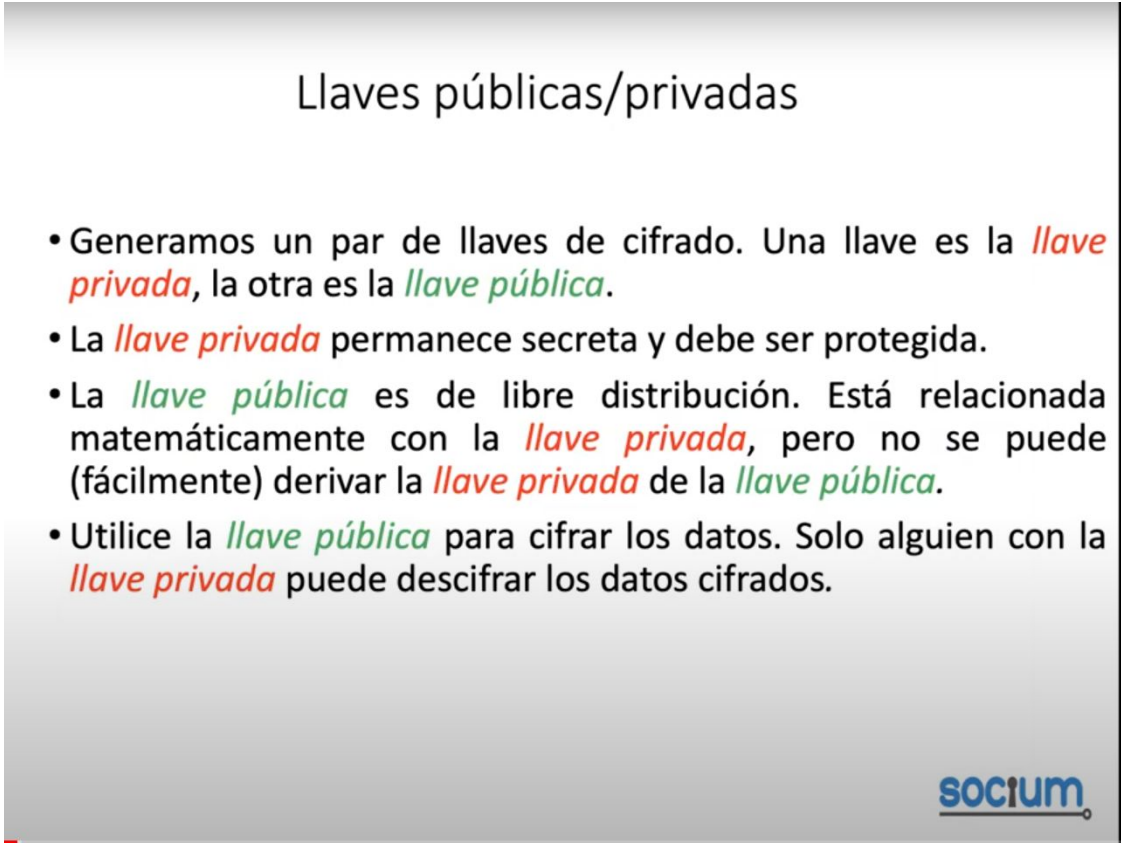
# REPASO

Cifrado simétrico

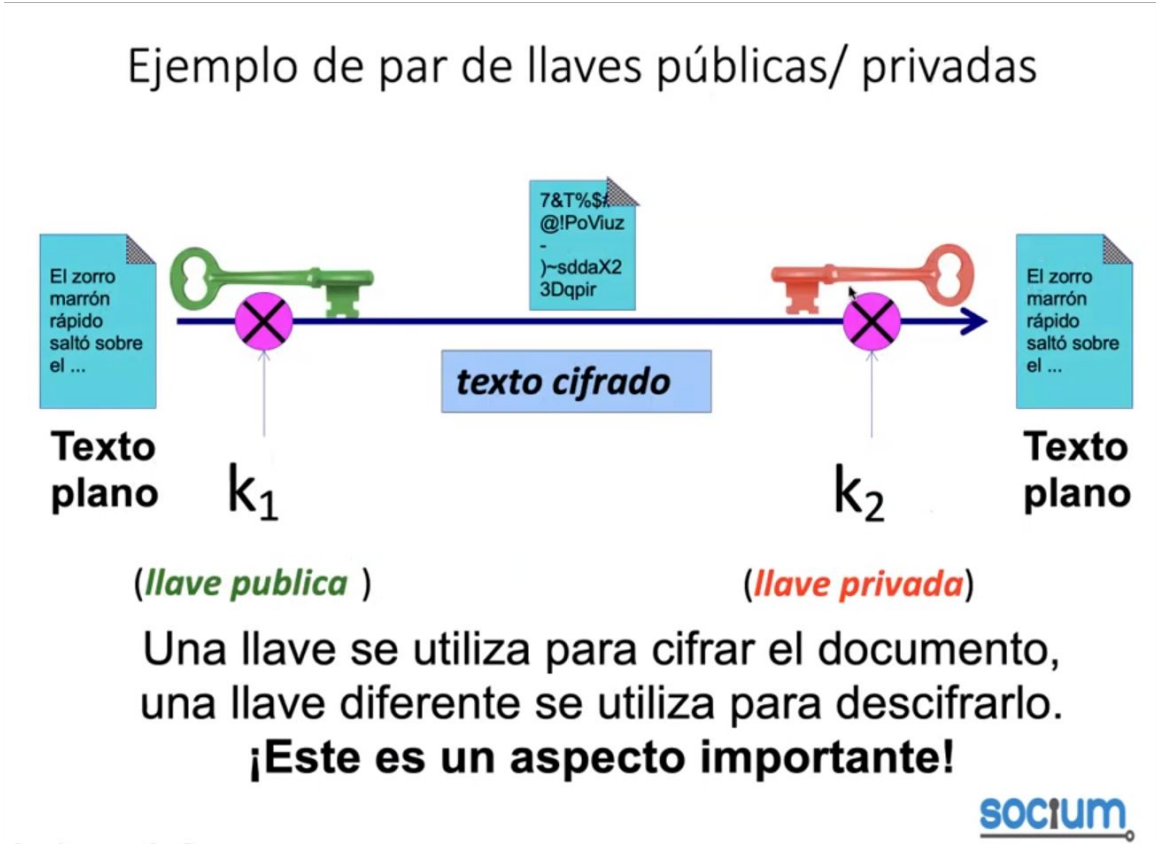
**Llave única/Cifrados simétricos**

Problema: ¿Cómo hacer para distribuir de manera segura la clave a todas las partes destinadas?

# REPASO


Llaves públicas/privadas
• Generamos un par de llaves de cifrado. Una llave es la llave privada, la otra es la llave pública.
• La llave privada permanece secreta y debe ser protegida.
• La llave pública es de libre distribución. Está relacionada matemáticamente con la llave privada, pero no se puede (fácilmente) derivar la llave privada de la llave pública.
• Utilice la llave pública para cifrar los datos. Solo alguien con la llave privada puede descifrar los datos cifrados.
socium

# REPASO


Ejemplo de par de llaves públicas/ privadas
El zorro marrón rápido saltó sobre el ...
7&T%$
@!PoViuz
-
)~sddaX2
3Dqpir
texto cifrado
El zorro marrón rápido saltó sobre el ...
Texto plano
k1
k2
Texto plano
(llave publica )
(llave privada)
Una llave se utiliza para cifrar el documento,
una llave diferente se utiliza para descifrarlo.
¡Este es un aspecto importante!
socium

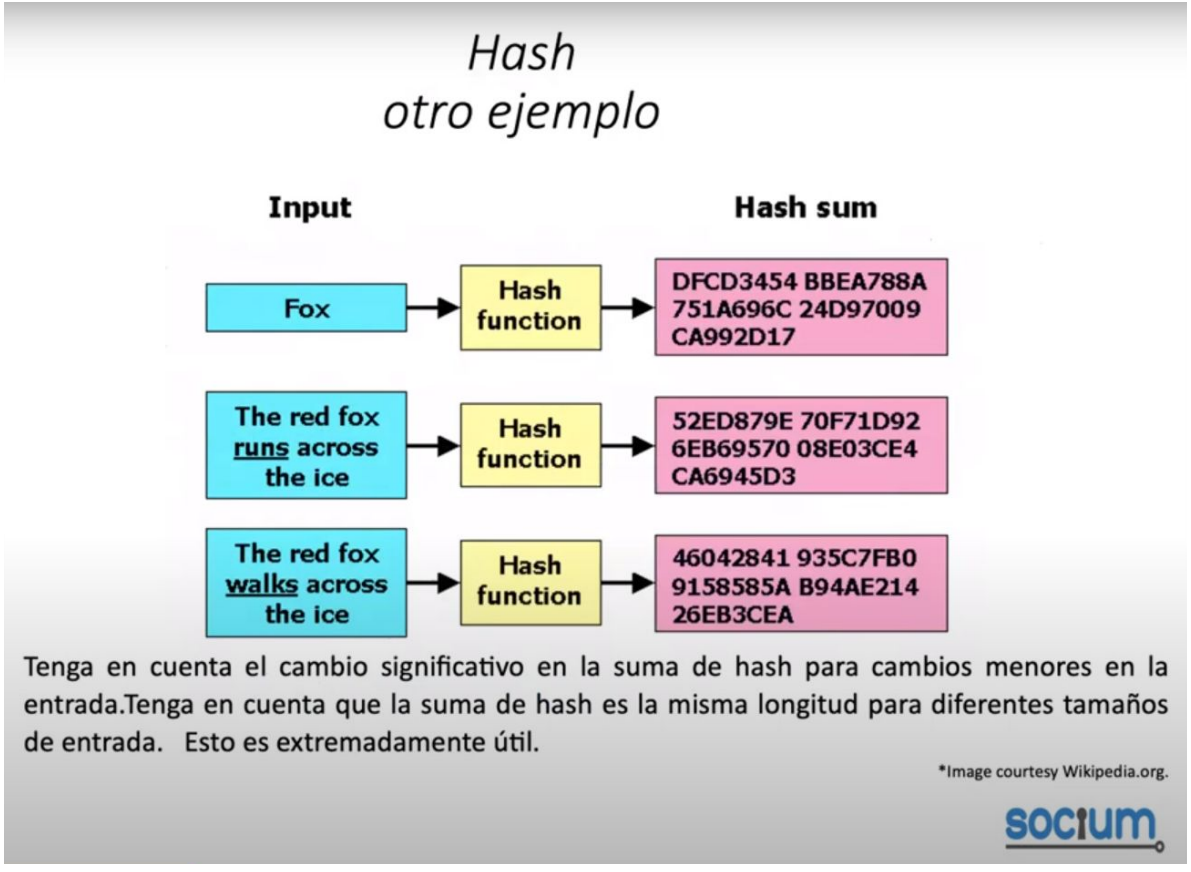
# REPASO

## Funciones de hash unidireccionales

- Una función matemática que genera un resultado de longitud fija independientemente de la cantidad de datos que pase a través de él. Generalmente muy rápido.
- No puede generar los datos originales a partir del resultado de longitud fija, por lo tanto, el término "unidireccional".
- Es de esperar que no pueda encontrar dos conjuntos de datos que produzcan el mismo resultado de longitud fija. Si lo haces, esto se llama una colisión. (Ejemplo, md5).
- El resultado de longitud fija se conoce como **un resumen de mensaje o una suma de comprobación o un hash.**

socium

# REPASO


Hash
otro ejemplo
Input
Hash sum
Fox
Hash function
DFCD3454 BBEA788A 751A696C 24D97009 CA992D17
The red fox runs across the ice
Hash function
52ED879E 70F71D92 6EB69570 08E03CE4 CA6945D3
The red fox walks across the ice
Hash function
46042841 935C7FB0 9158585A B94AE214 26EB3CEA
Tenga en cuenta el cambio significativo en la suma de hash para cambios menores en la entrada.Tenga en cuenta que la suma de hash es la misma longitud para diferentes tamaños de entrada. Esto es extremadamente útil.
*Image courtesy Wikipedia.org.
socium

# REPASO

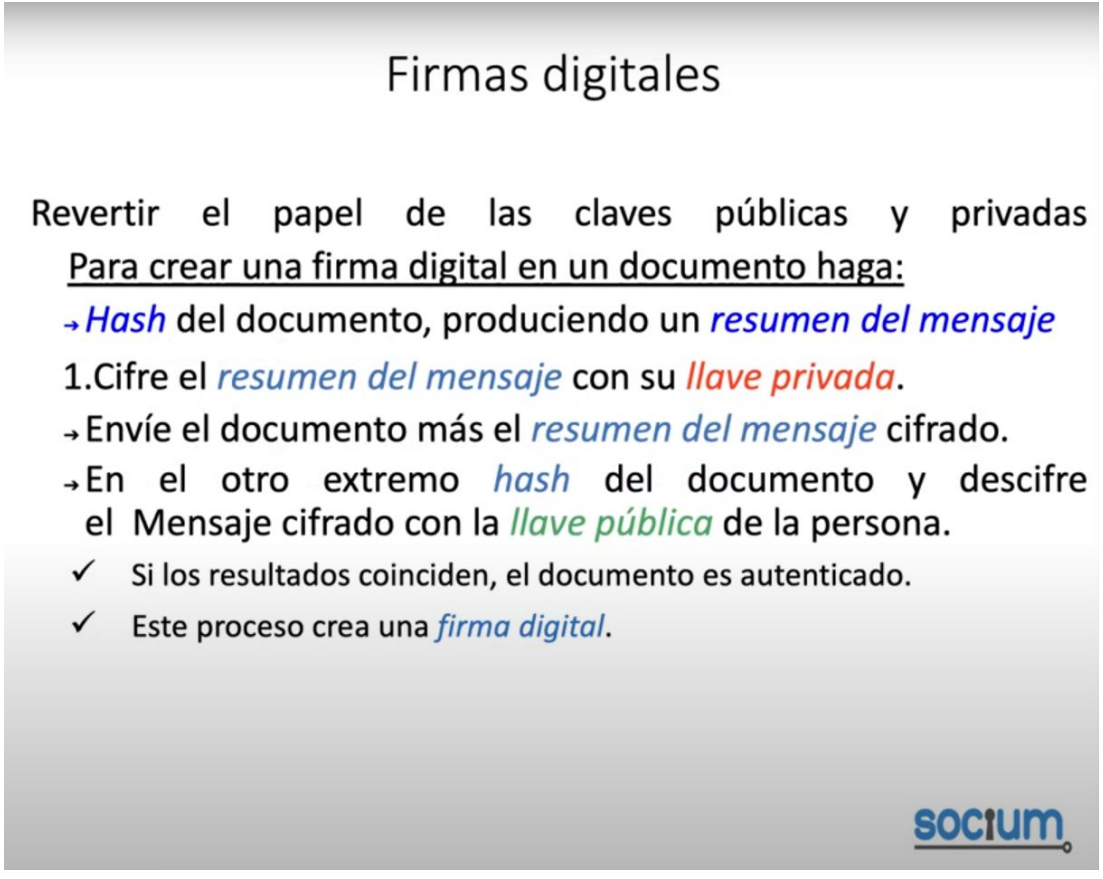
## ¿Para qué sirve esto?

**Hay varios:**

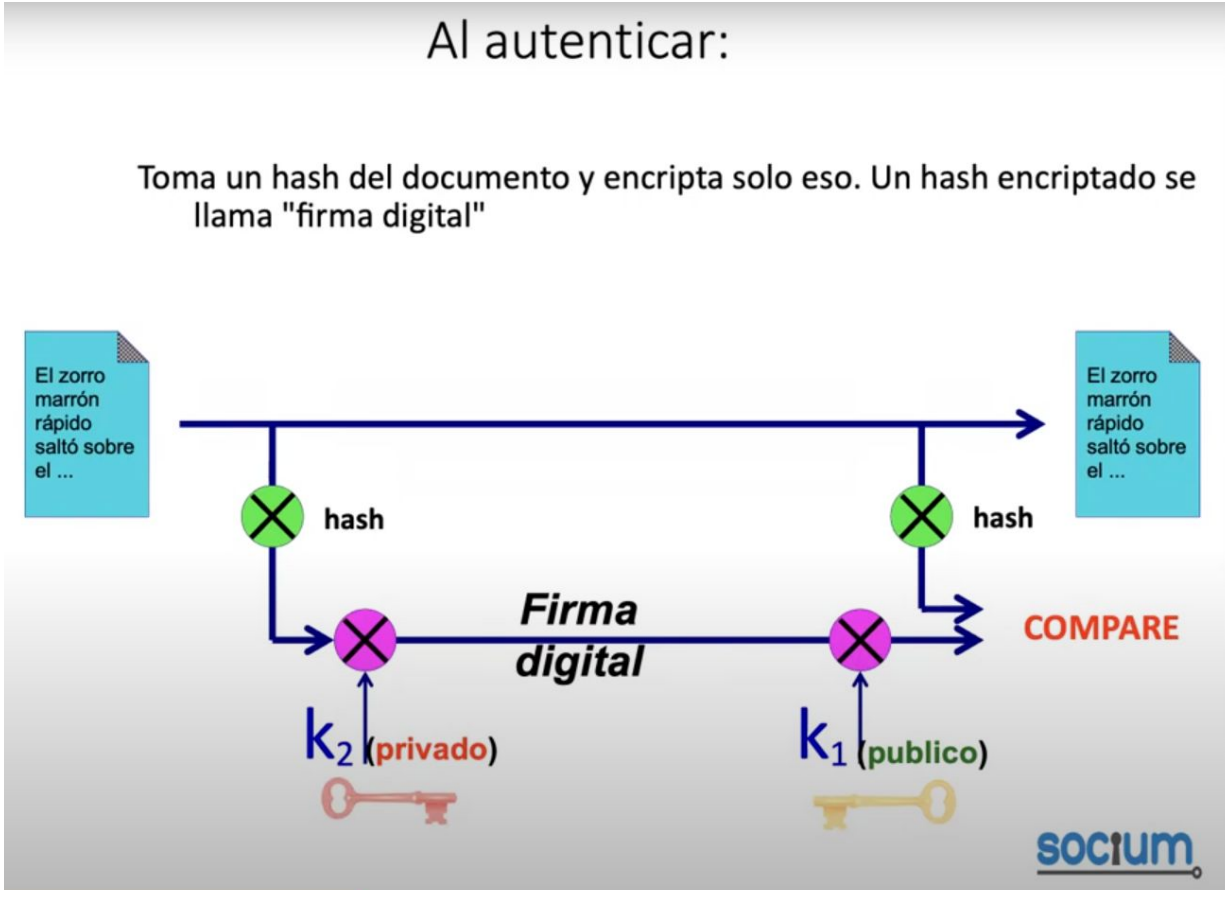
- Cifrado de contraseñas (en Linux, Unix y Windows), utilizando múltiples rondas de hashing (MD5 u otro).
- Puede ejecutar muchos megabytes de datos a través de una función de hash, pero solo tiene que verificar un número fijo de bits de información (160-512 bits). Esto se utiliza para crear una *firma digital*.

socium

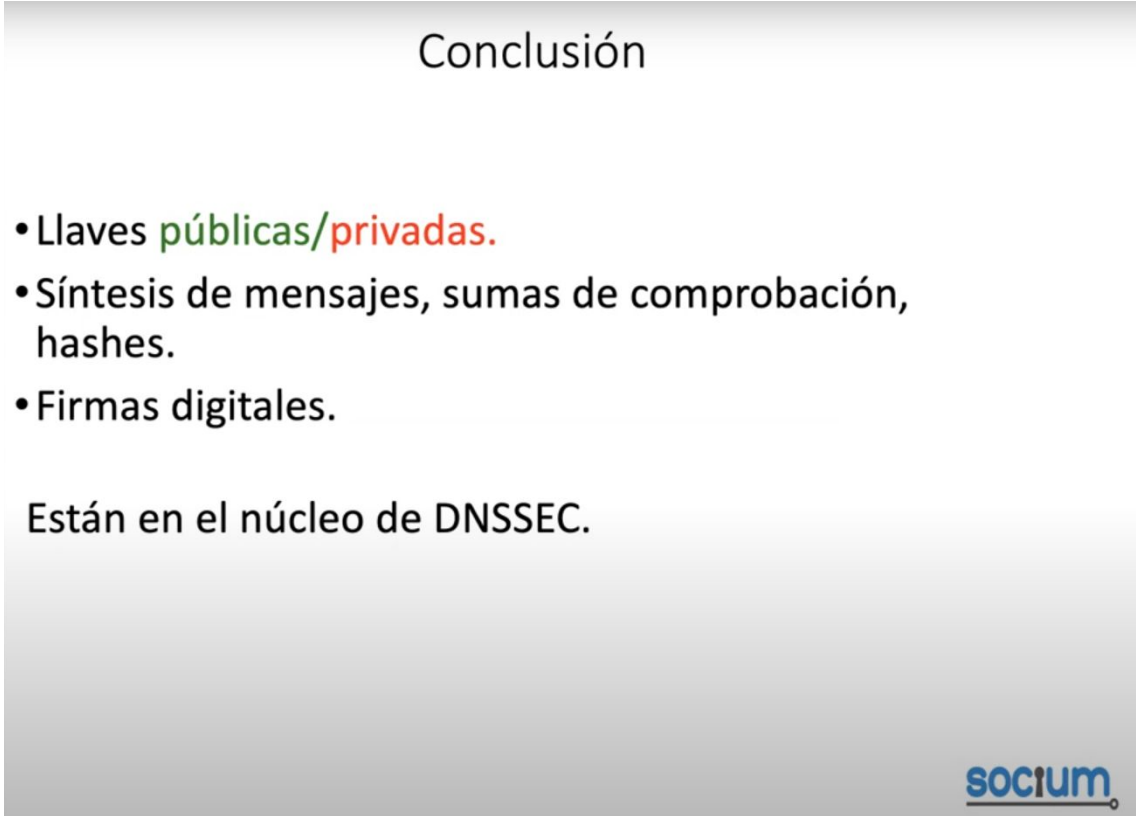
# REPASO


Firmas digitales
Revertir el papel de las claves públicas y privadas
Para crear una firma digital en un documento haga:
→ Hash del documento, produciendo un resumen del mensaje
1.Cifre el resumen del mensaje con su llave privada.
→ Envíe el documento más el resumen del mensaje cifrado.
→ En el otro extremo hash del documento y descifre el Mensaje cifrado con la llave pública de la persona.
✓ Si los resultados coinciden, el documento es autenticado.
✓ Este proceso crea una firma digital.
socium

# REPASO


Al autenticar:
Toma un hash del documento y encripta solo eso. Un hash encriptado se llama "firma digital"
El zorro marrón rápido saltó sobre el ...
hash
hash
El zorro marrón rápido saltó sobre el ...
Firma digital
COMPARE
k2 (privado)
k1 (publico)
socium

# REPASO


Conclusión
• Llaves públicas/privadas.
• Síntesis de mensajes, sumas de comprobación, hashes.
• Firmas digitales.
Están en el núcleo de DNSSEC.
socium

# REPASO

- El formato de zona de BIND es muy común, así que lo usaremos aquí:

```
zone. SOA nsX.zone. hostmaster.zone.
                ( 2009022401  ; serial
                  1d          ; refresh
                  12h         ; retry
                  1w          ; expire
                  1h )        ; neg. TTL

zone.       NS  ns.zone.
            NS  ns.otherzone.

zone.       MX  5 server.otherzone.
www.zone.    A  1.2.3.4
```

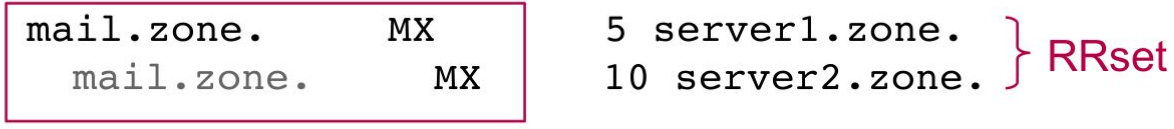

# REPASO

- Estructura de los récords:

```
NAME        [TTL]   TYPE   DATA (type specific)
-------------------------------------------------
host.zone.   3600   A      10.20.30.40
sub.zone.   86400   MX     5 server.otherzone.
```

# REPASO

- Múltiples records con *el mismo nombre y tipo* se agrupan en Resource Record Sets (RRsets):




UNIVERSITY OF OREGON

NSRC Network Startup Resource Center

# REPASO

## DNSSEC – breve resumen

- Autenticidad de datos e integridad al firmar los RRSets con una clave privada
- Claves públicas (DNSKEYS), para verificar las firmas (RRSIGs)
- Los sub-dominios firman sus zonas con su llave privada
  - La autenticidad de la llave se establece gracias a la firma/checksum del record delegation signer (DS) por la zona superior
- Repetir en la zona superior...
- No es tan difícil en papel
  - Operativamente, es un poco más complicado

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

## DNSSEC – breve resumen

- Autenticidad de datos e integridad al firmar los RRSets con una clave privada
- Claves públicas (DNSKEYS), para verificar las firmas (RRSIGs)
- Los sub-dominios firman sus zonas con su llave privada
  - La autenticidad de la llave se establece gracias a la firma/checksum del record delegation signer (DS) por la zona superior
- Repetir en la zona superior...
- No es tan difícil en papel
  - Operativamente, es un poco más complicado

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

## DNSSEC - Conceptos

- Cambia el modelo de confianza de DNS de “abierto” y ”de confianza” a uno de ”verificable”
- Uso extensivo de criptografía asimétrica para lograr:
  - Autenticación del origen
  - Integridad de los datos
  - Autenticidad de la negación de existencia
- No se trata de proveer confidencialidad
- DNSSEC no implica una carga computacional en los servidores autorizados ( != los *firmantes* )
- No se cambia esencialmente el protocolo
  - Puede coexistir con la infraestructura actual
    - ... Bueno, más o menos (EDNS0)

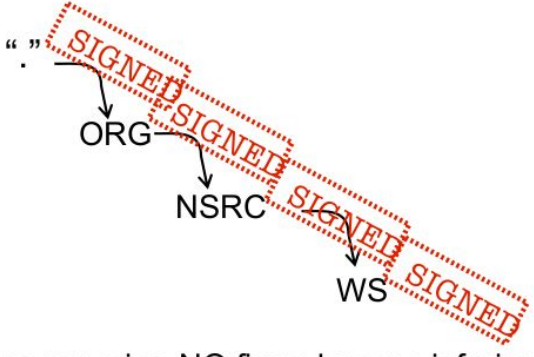
UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

## DNSSEC - conceptos

- Crear una cadena de confianza usando el modelo existente basado en delegaciones para la distribución que es el DNS
- No se firma la zona completa, se firma un RRset




- Nota: la zona superior NO firma la zona inferior.
  - La superior firma un *apuntador* (hash) a la *clave* usada para firmar los datos en la zona inferior (importante!)

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

## DNSSEC: nuevos RRs

Se añaden cuatro nuevos Resource Records*:

1. **DNSKEY**: Llave pública utilizada en el proceso de firmado.
2. **RRSIG**: Firma de un RRset
3. **NSEC/NSEC3**: Provisto como evidencia de que el nombre y/o el tipo de RR no existe
4. **DS**: Delegation Signer. Contiene el *hash* de la clave pública usada para firmar la llave que a su vez servirá para firmar los datos de la zona. Se siguen los RRs DS hasta encontrar una zona "de confianza" (idealmente la raíz).

***Vea la excelente discusión de Geoff Huston en**
http://ispcolumn.isoc.org/2006-08/dnssec.html

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

## DNSSEC: KSK y ZSK

- Para permitir la renovación de claves (“rollovers”), se generan dos pares de claves:
  - **Key Signing Key (KSK)**
    - Referenciada por la zona superior (Secure Entry Point), en forma de DS (Delegation Signer)
    - Usada para firmar la Zone Signing Key (ZSK)
  - **Zone Signing Key (ZSK)**
    - Firmada por la Key Signing Key
    - Usada para firmar los RRsets
- Esta disociación permite la renovación del ZSK sin tener que renovar la KSK (y el DS en la superior) – menos interacción administrativa

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

## DNSSEC: DS

- Dos hashes generados por defecto:
  - 1 SHA-1 MANDATORY
  - 2 SHA-256 MANDATORY
- Hay nuevos algoritmos que están en proceso de estandarización
- Esto ocurrirá continuamente a medida que los algoritmos se determinen inseguros

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

## Firmar la zona (utilizando las herramientas BIND)

1. Generar los pares de claves
2. Incluir los récords DNSKEYs públicos en el contenido de la zona
3. Firmar la zona con la llave secreta ZSK
4. Publicar la zona
5. Enviar los récords DS a la zona superior
6. Esperar...

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

# 1. Generar las claves

```
# Generar la ZSK
dnssec-keygen [-a rsasha1 -b 1024] -n ZONE  myzone

# Generar la KSK
dnssec-keygen -a [rsasha1 -b 2048] -n ZONE -f KSK
 myzone
```

Esto generó 4 ficheros:

- Kmyzone.+005+*id_of_zsk*.key
- Kmyzone.+005+*id_of_zsk*.private
- Kmyzone.+005+*id_of_ksk*.key
- Kmyzone.+005+*id_of_ksk*.private

UNIVERSITY OF OREGON

NSRC

```
root@vm-taller:/var/lib/bind# dnssec-keygen -a ECDSAP256SHA256 -b 1024  udnssec30-taller.com.py.hosts
Generating key pair.
Kudnssec30-taller.com.py.hosts.+013+13536
root@vm-taller:/var/lib/bind# dnssec-keygen -a ECDSAP256SHA256 -b 1024  -f KSK udnssec30-taller.com.py.hosts
Generating key pair.
Kudnssec30-taller.com.py.hosts.+013+41145
```

# REPASO

## 2. Incluir las claves en la zona

Incluya los records DNSKEY para la ZSK y KSK en la zona, para que sean firmados con el resto de los datos:

```
cat Kmyzone*key >>myzone
```

O utilice la instrucción $INCLUDE para que sean cargados al leer la zona:

```
$INCLUDE "Kmyzone.+005+id_of_zsk.key"
$INCLUDE "Kmyzone.+005+id_of_ksk.key"
```

UNIVERSITY OF OREGON

NSRC Network Startup Resource Center

# REPASO

## 3. Firmar la zona

Firme su zona

```
# dnssec-signzone myzone
```

- *dnssec-signzone* usará todos los valores por defecto para la duración de la firma, el número de serie no será incrementado, y las claves privadas para firmar serán determinadas automáticamente.
- Firmar hará lo siguiente:
  - Ordenar los datos (lexicográficamente)
  - Insertar:
- Récords NSEC
- Récords RRSIG (firma de cada RRset)
- Récords DS de ficheros *key-set* de sub-zonas (para la zona superior)
  - Generar ficheros key-set y DS-set, para enviar a la zona superior

UNIVERSITY OF OREGON

NSRC Network Startup Resource Center

# REPASO

## 3. Firmar la zona (2)

- ISC BIND
- Desde la versión 9.7.0, BIND puede firmar y re-firmar sus zonas automáticamente
  - Facilita las cosas significativamente
  - Pero la generación de las claves, la gestión y la renovación aún tienen que hacerse por separado.

- La versión 9.8.0 introduce la firma en línea

  → Integración más sencilla en la cadena de producción existente.

UNIVERSITY OF OREGON

NSRC Network Startup Resource Center

# REPASO

## 4. Publicar las zonas firmadas

- Para publicar la zona firmada es necesario configurar el servidor para que cargue el fichero de la zona firmada.
- ... pero usted aún tiene que enviar sus récords DS de manera segura a la zona superior, de lo contrario, nadie sabrá que usted está firmando su zona con DNSSEC

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

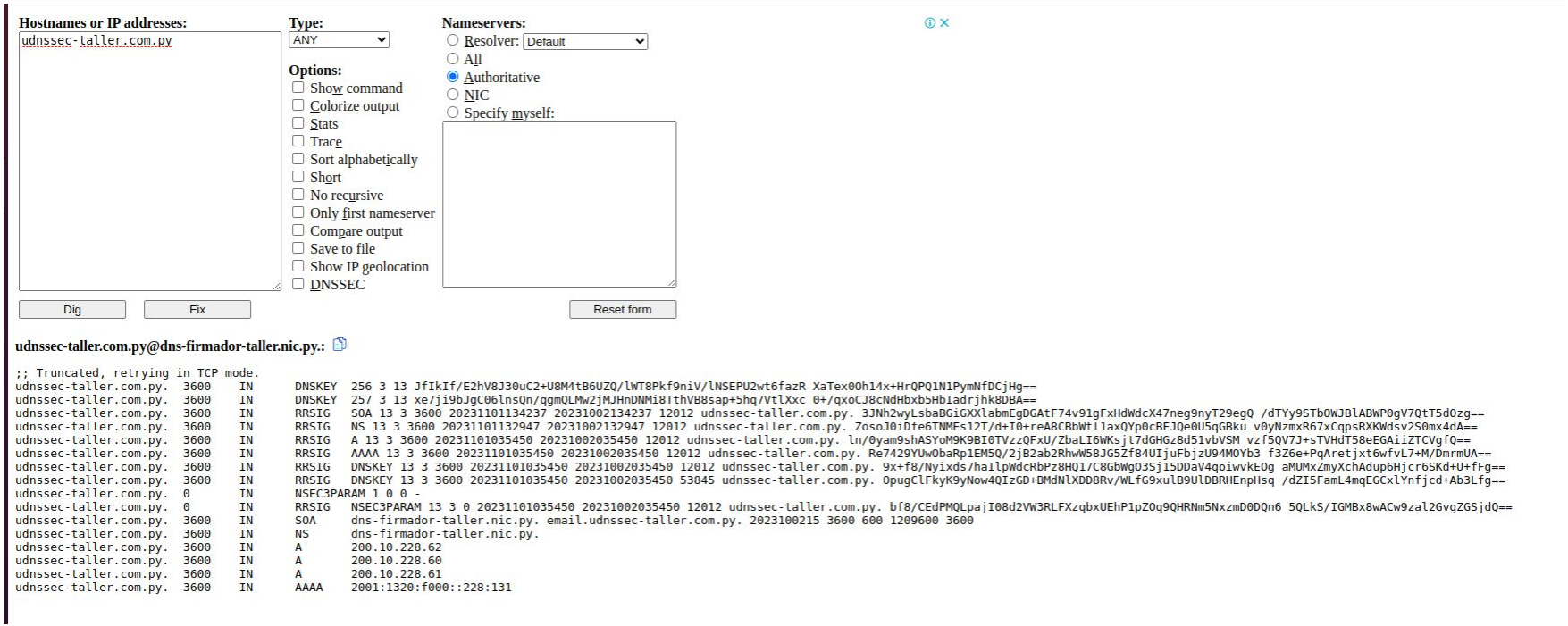
## 4. Publicar las zonas firmadas

```
mfretes@mfretes:~$ dig @8.8.8.8 udnssec-taller.com.py ANY

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 udnssec-taller.com.py ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49906
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 16, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;udnssec-taller.com.py.         IN      ANY

;; ANSWER SECTION:
udnssec-taller.com.py.  3600    IN      DNSKEY  256 3 13 JfIkIf/E2hV8J30uC2+U8M4tB6UZQ/lWT8Pkf9niV/lNSEPU2wt6fazR XaTex0Oh14x+HrQPQ1N1PymNfDCjHg==
udnssec-taller.com.py.  3600    IN      DNSKEY  257 3 13 xe7ji9bJgC06lnsQn/qgmQLMw2jMJHnDNMi8TthVB8sap+5hq7VtlXxc 0+/qxoCJ8cNdHbxb5HbIadrjhk8DBA==
udnssec-taller.com.py.  3600    IN      RRSIG   SOA 13 3 3600 20231101134237 20231002134237 12012 udnssec-taller.com.py. 3JNh2wyLsbaBGiGXXlabmEgDGAtF74v91gFxHdWdcX47neg9nyT29egQ /dTYy9STbOWJBlABWP0gV7QtT5dOzg==
udnssec-taller.com.py.  3600    IN      RRSIG   NS 13 3 3600 20231101132947 20231002132947 12012 udnssec-taller.com.py. ZosoJ0iDfe6TNMEs12T/d+I0+reA8CBbWtl1axQYp0cBFJQe0U5qGBku v0yNzmxR67xCqpsRXKWdsv2S0mx4dA==
udnssec-taller.com.py.  3600    IN      RRSIG   A 13 3 3600 20231101035450 20231002035450 12012 udnssec-taller.com.py. ln/0yam9shASYoM9K9BI0TVzzQFxU/ZbaLI6WKsjt7dGHGz8d51vbVSM vzf5QV7J+sTVHdT58eEGAiiZTCVgfQ==
udnssec-taller.com.py.  3600    IN      RRSIG   AAAA 13 3 3600 20231101035450 20231002035450 12012 udnssec-taller.com.py. Re7429YUwObaRp1EM5Q/2jB2ab2RhwW58JG5Zf84UIjuFbjzU94MOYb3 f3Z6e+PqAretjxt6wfvL7+M/DmrmUA==
udnssec-taller.com.py.  3600    IN      RRSIG   DNSKEY 13 3 3600 20231101035450 20231002035450 12012 udnssec-taller.com.py. 9x+f8/Nyixds7haIlpWdcRbPz8HQ17C8GbWgO3Sj15DDaV4qoiwvkEOg aMUMxZmyXchAdup6Hjcr6SKd+U+fFg==
udnssec-taller.com.py.  3600    IN      RRSIG   DNSKEY 13 3 3600 20231101035450 20231002035450 53845 udnssec-taller.com.py. OpugClFkyK9yNow4QIzGD+BMdNlXDD8Rv/WLfG9xulB9UlDBRHEnpHsq /dZI5FamL4mqEGCxlYnfjcd+Ab3Lfg==
udnssec-taller.com.py.  0       IN      NSEC3PARAM 1 0 0 -
udnssec-taller.com.py.  0       IN      RRSIG   NSEC3PARAM 13 3 0 20231101035450 20231002035450 12012 udnssec-taller.com.py. bf8/CEdPMQLpajI08d2VW3RLFXzqbxUEhP1pZOq9QHRNm5NxzmD0DQn6 5QLkS/IGMBx8wACw9zal2GvgZGSjdQ==
udnssec-taller.com.py.  3600    IN      SOA     dns-firmador-taller.nic.py. email.udnssec-taller.com.py. 2023100215 3600 600 1209600 3600
udnssec-taller.com.py.  3600    IN      NS      dns-firmador-taller.nic.py.
udnssec-taller.com.py.  3600    IN      A       200.10.228.61
udnssec-taller.com.py.  3600    IN      A       200.10.228.60
udnssec-taller.com.py.  3600    IN      A       200.10.228.62
udnssec-taller.com.py.  3600    IN      AAAA    2001:1320:f000::228:131

;; Query time: 152 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: lun oct 02 13:20:53 -03 2023
;; MSG SIZE  rcvd: 1202
```

# REPASO

## 4. Publicar las zonas firmadas

https://digwebinterface.com/?hostnames=udnssec-taller.com.py&type=ANY&useresolver=8.8.4.4&ns=auth&nameservers=



**Hostnames or IP addresses:** udnssec-taller.com.py

**Type:** ANY

**Options:**
- Show command
- Colorize output
- Stats
- Trace
- Sort alphabetically
- Short
- No recursive
- Only first nameserver
- Compare output
- Save to file
- Show IP geolocation
- DNSSEC

**Nameservers:**
- Resolver: Default
- All
- Authoritative
- NIC
- Specify myself:

Dig | Fix | Reset form

**udnssec-taller.com.py@dns-firmador-taller.nic.py.:**

```
;; Truncated, retrying in TCP mode.
udnssec-taller.com.py.  3600    IN      DNSKEY  256 3 13 JfIkIf/E2hV8J30uC2+U8M4tB6UZQ/lWT8Pkf9niV/lNSEPU2wt6fazR XaTex0Oh14x+HrQPQ1N1PymNfDCjHg==
udnssec-taller.com.py.  3600    IN      DNSKEY  257 3 13 xe7ji9bJgC06lnsQn/qgmQLMw2jMJHnDNMi8TthVB8sap+5hq7VtlXxc 0+/qxoCJ8cNdHbxb5HbIadrjhk8DBA==
udnssec-taller.com.py.  3600    IN      RRSIG   SOA 13 3 3600 20231101134237 20231002134237 12012 udnssec-taller.com.py. 3JNh2wyLsbaBGiGXXlabmEgDGAtF74v91gFxHdWdcX47neg9nyT29egQ /dTYy9STbOWJBlABWP0gV7QtT5dOzg==
udnssec-taller.com.py.  3600    IN      RRSIG   NS 13 3 3600 20231101132947 20231002132947 12012 udnssec-taller.com.py. ZosoJ0iDfe6TNMEs12T/d+I0+reA8CBbWtl1axQYp0cBFJQe0U5qGBku v0yNzmxR67xCqpsRXKWdsv2S0mx4dA==
udnssec-taller.com.py.  3600    IN      RRSIG   A 13 3 3600 20231101035450 20231002035450 12012 udnssec-taller.com.py. ln/0yam9shASYoM9K9BI0TVzzQFxU/ZbaLI6WKsjt7dGHGz8d51vbVSM vzf5QV7J+sTVHdT58eEGAiiZTCVgfQ==
udnssec-taller.com.py.  3600    IN      RRSIG   AAAA 13 3 3600 20231101035450 20231002035450 12012 udnssec-taller.com.py. Re7429YUwObaRp1EM5Q/2jB2ab2RhwW58JG5Zf84UIjuFbjzU94MOYb3 f3Z6e+PqAretjxt6wfvL7+M/DmrmUA==
udnssec-taller.com.py.  3600    IN      RRSIG   DNSKEY 13 3 3600 20231101035450 20231002035450 12012 udnssec-taller.com.py. 9x+f8/Nyixds7haIlpWdcRbPz8HQ17C8GbWgO3Sj15DDaV4qoiwvkEOg aMUMxZmyXchAdup6Hjcr6SKd+U+fFg==
udnssec-taller.com.py.  3600    IN      RRSIG   DNSKEY 13 3 3600 20231101035450 20231002035450 53845 udnssec-taller.com.py. OpugClFkyK9yNow4QIzGD+BMdNlXDD8Rv/WLfG9xulB9UlDBRHEnpHsq /dZI5FamL4mqEGCxlYnfjcd+Ab3Lfg==
udnssec-taller.com.py.  0       IN      NSEC3PARAM 1 0 0 -
udnssec-taller.com.py.  0       IN      RRSIG   NSEC3PARAM 13 3 0 20231101035450 20231002035450 12012 udnssec-taller.com.py. bf8/CEdPMQLpajI08d2VW3RLFXzqbxUEhP1pZOq9QHRNm5NxzmD0DQn6 5QLkS/IGMBx8wACw9zal2GvgZGSjdQ==
udnssec-taller.com.py.  3600    IN      SOA     dns-firmador-taller.nic.py. email.udnssec-taller.com.py. 2023100215 3600 600 1209600 3600
udnssec-taller.com.py.  3600    IN      NS      dns-firmador-taller.nic.py.
udnssec-taller.com.py.  3600    IN      A       200.10.228.62
udnssec-taller.com.py.  3600    IN      A       200.10.228.60
udnssec-taller.com.py.  3600    IN      A       200.10.228.61
udnssec-taller.com.py.  3600    IN      AAAA    2001:1320:f000::228:131
```

# REPASO

## Caducidad de las firmas

- Las firmas caducan en 30 días por defecto (BIND)
- Es necesario firmar regularmente:
  - Para mantener una ventana constante de validez para las firmas de un RRset *existente*
- Para firmar *RRsets nuevos* y *actualizados*

- Quién hace esto ?

- Las claves en sí NO caducan...
  - Pero sí necesitan ser renovadas...

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# REPASO

## Caducidad de las firmas

- Las firmas caducan en 30 días por defecto (BIND)
- Es necesario firmar regularmente:
  - Para mantener una ventana constante de validez para las firmas de un RRset *existente*
- Para firmar *RRsets nuevos* y *actualizados*

- Quién hace esto ?

- Las claves en sí NO caducan...
  - Pero sí necesitan ser renovadas...

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# PROPUESTA

## Implementación con: BIND 9.18, Ubuntu 22.04, WEBMIN

**BIND**

#sudo apt-get upgrade
#sudo apt install -y bind9 bind9utils bind9-doc dnsutils

**WEBMIN**

# curl -o setup-repos.sh https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
# sh setup-repos.sh
# apt-get install webmin --install-recommends

**Recursos para descarga**

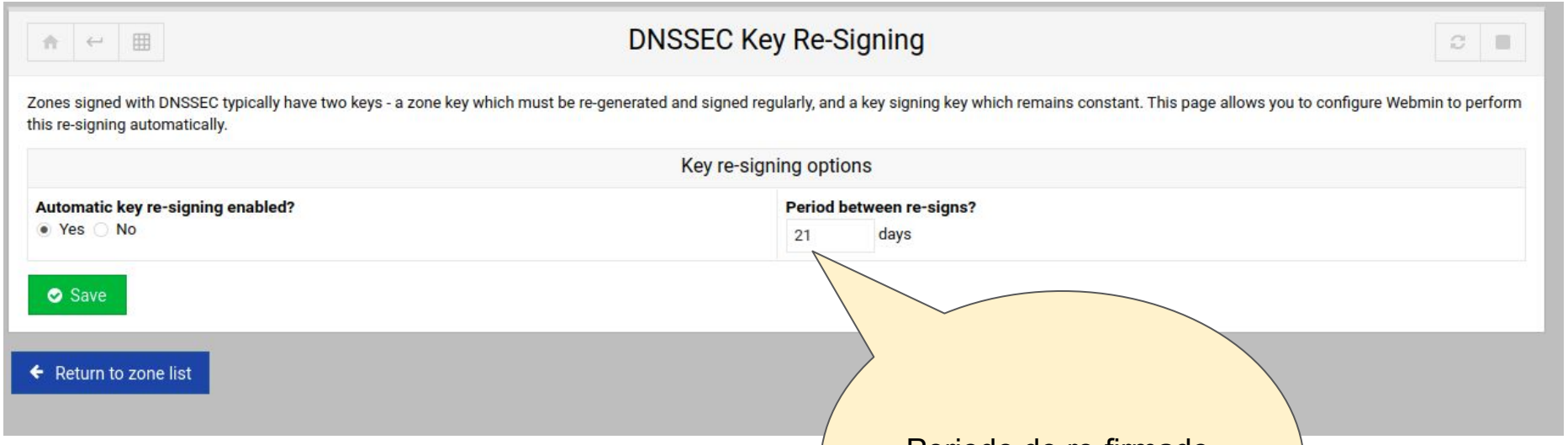
https://www.nic.py/dnssec

**Ref.**

https://webmin.com/

# PROPUESTA

## Implementación con: BIND 9.18, Ubuntu 22.04, WEBMIN



# PROPUESTA

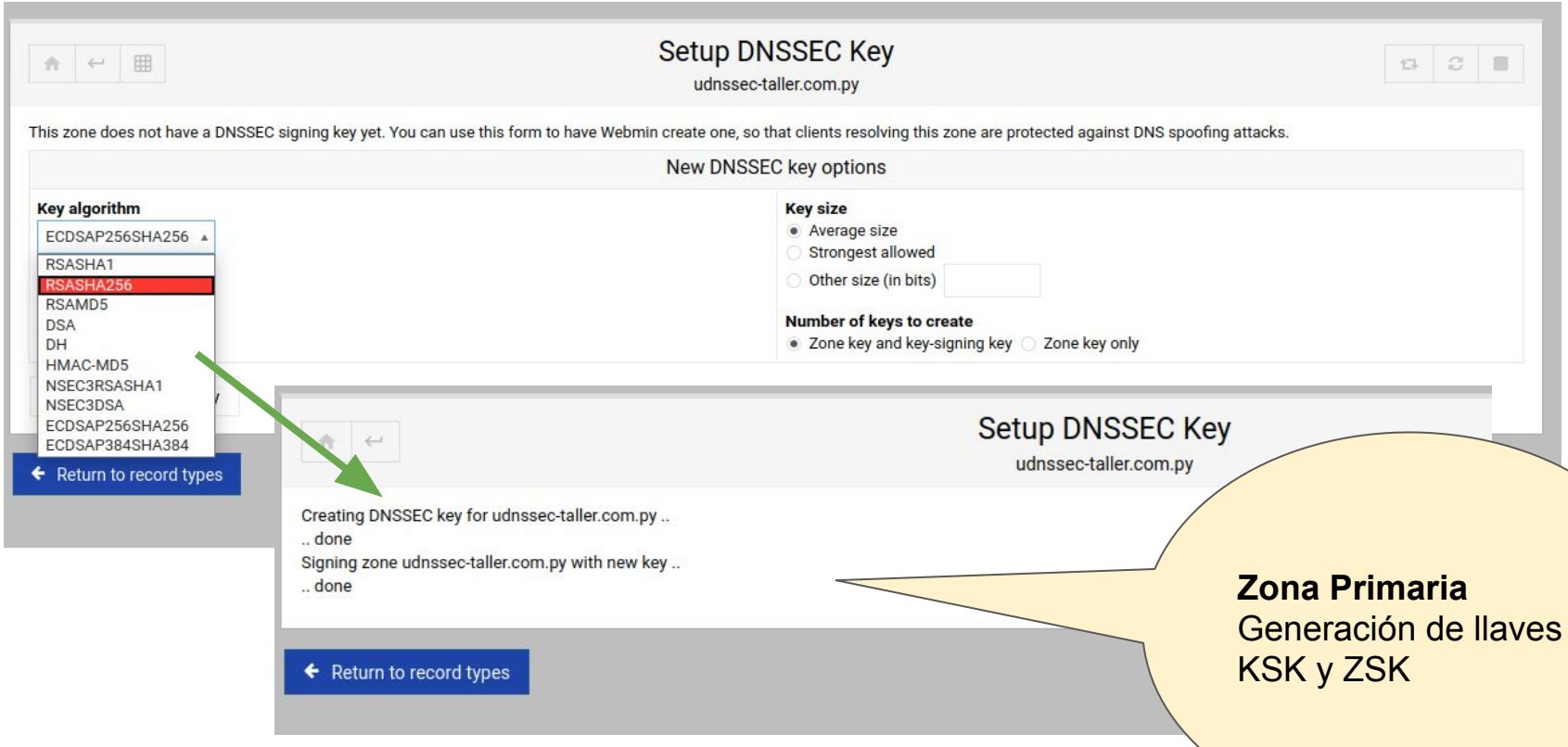
## Implementación con: BIND 9.18, Ubuntu 22.04, WEBMIN

**PRÁCTICA**

- Generar las llaves
- Firmar y publicar la zona
- Realizar análisis preliminar
- Realizar el encadenamiento con la Zona Superior “.PY”

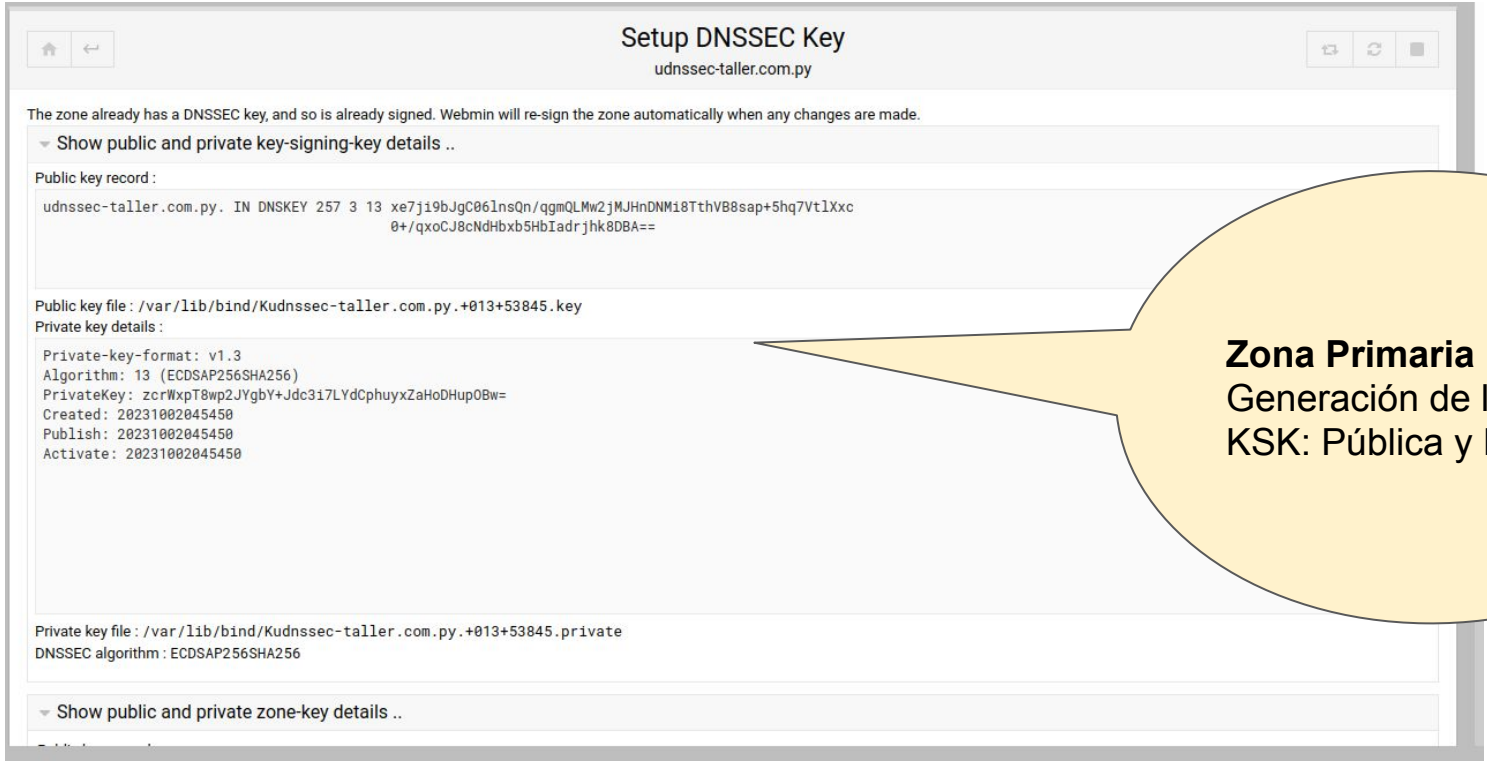
# PROPUESTA

## Implementación con: BIND 9.18, Ubuntu 22.04, WEBMIN



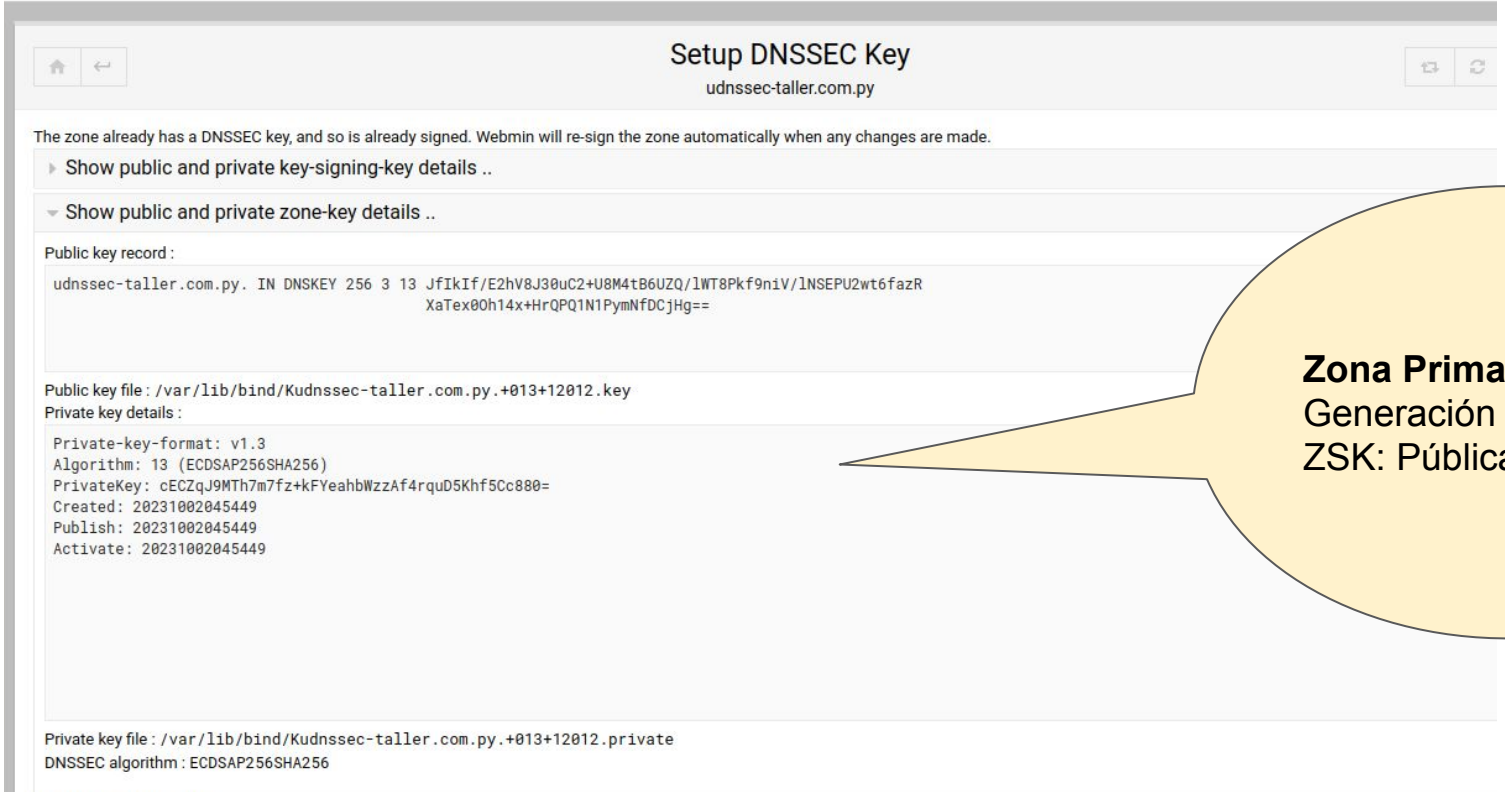
# PROPUESTA

## Implementación con: BIND 9.18, Ubuntu 22.04, WEBMIN



# PROPUESTA

## Implementación con: BIND 9.18, Ubuntu 22.04, WEBMIN




**Zona Primaria**
Generación de llaves
ZSK: Pública y Privada

# PROPUESTA

## Implementación con: BIND 9.18, Ubuntu 22.04, WEBMIN


**Zona Primaria**
DS: Delegation Signer
(Hash del KSK)

# PROPUESTA

## Implementación con: BIND 9.18, Ubuntu 22.04, WEBMIN

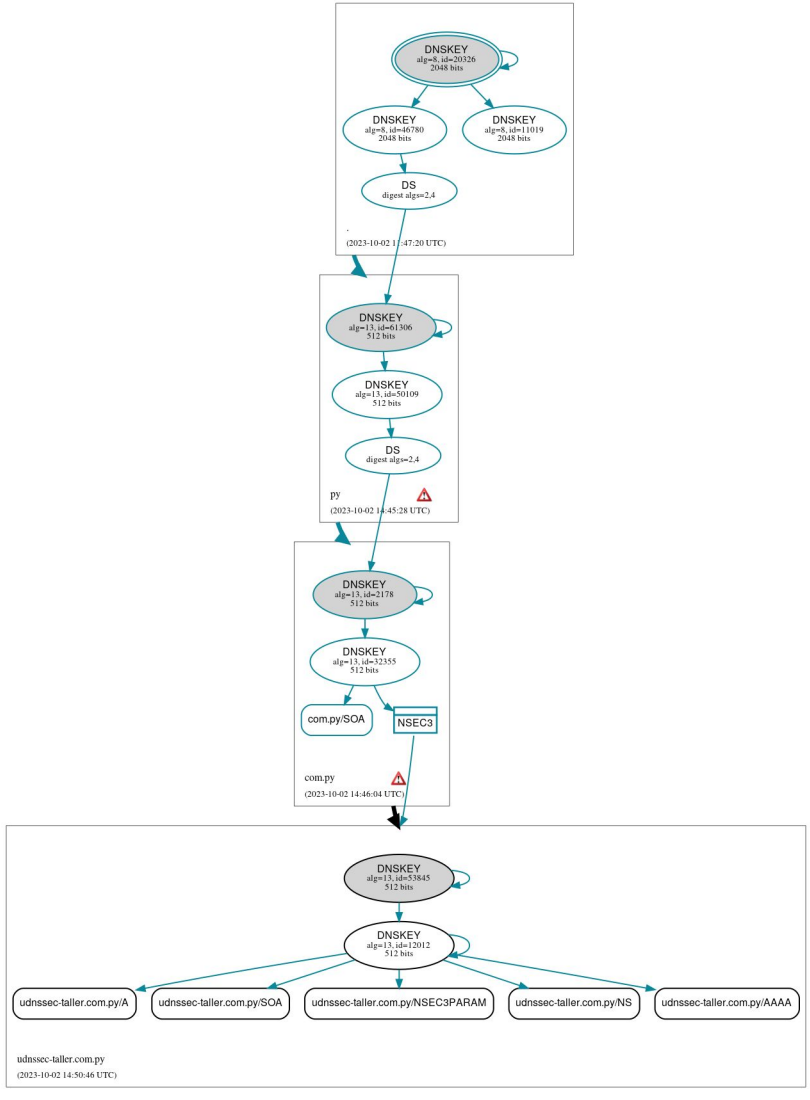
```
root@vm-taller:/var/lib/bind# pwd
/var/lib/bind
root@vm-taller:/var/lib/bind# ls -l *udnssec-taller.com.py*
-rw-r--r-- 1 root root  106 oct  2 05:02 dsset-udnssec-taller.com.py.
-rwxrwxr-x 1 root bind  362 oct  2 04:54 Kudnssec-taller.com.py.+013+12012.key
-rwxrwxr-x 1 root bind  187 oct  2 04:54 Kudnssec-taller.com.py.+013+12012.private
-rwxrwxr-x 1 root bind  361 oct  2 04:54 Kudnssec-taller.com.py.+013+53845.key
-rwxrwxr-x 1 root bind  187 oct  2 04:54 Kudnssec-taller.com.py.+013+53845.private
-rwxr-xr-x 1 root bind 3105 oct  2 05:02 udnssec-taller.com.py.hosts
root@vm-taller:/var/lib/bind#
```

# ENCADENAMIENTO

## Análisis preliminar

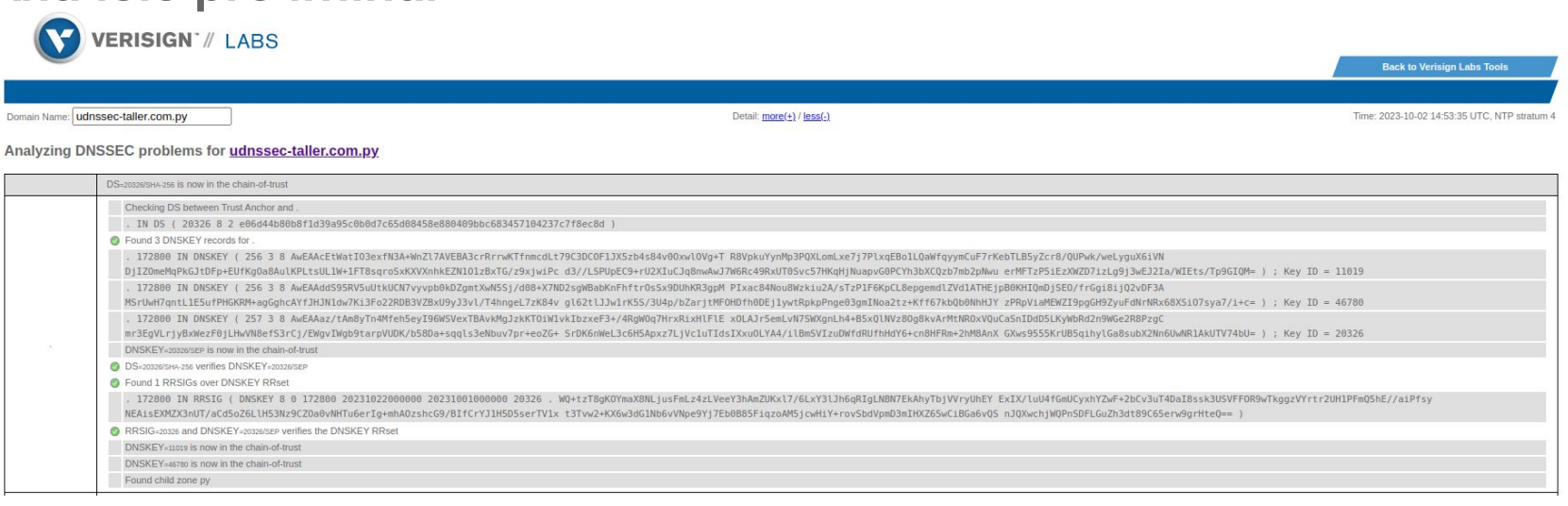
**DNSVIZ**

https://dnsviz.net/



# ENCADENAMIENTO

## Análisis preliminar




**DNSSEC Analyzer**
https://dnssec-analyzer.verisignlabs.com/

# ENCADENAMIENTO

## Declaración de Registro DS - NIC.PY


**NIC.PY**
https://www.nic.py/modificaciones/

udnssec-taller.com.py. IN DS 53845 13 2
9D046796D9C4B604AE573354275A76FA6CDA851AD2DE34D61F8C51181176DAF1

# ¿Iniciamos el proceso con tu dominio?

✔ Escríbenos, y preparamos un plan de trabajo…

dnssec@nic.py


dnssec@nic.py