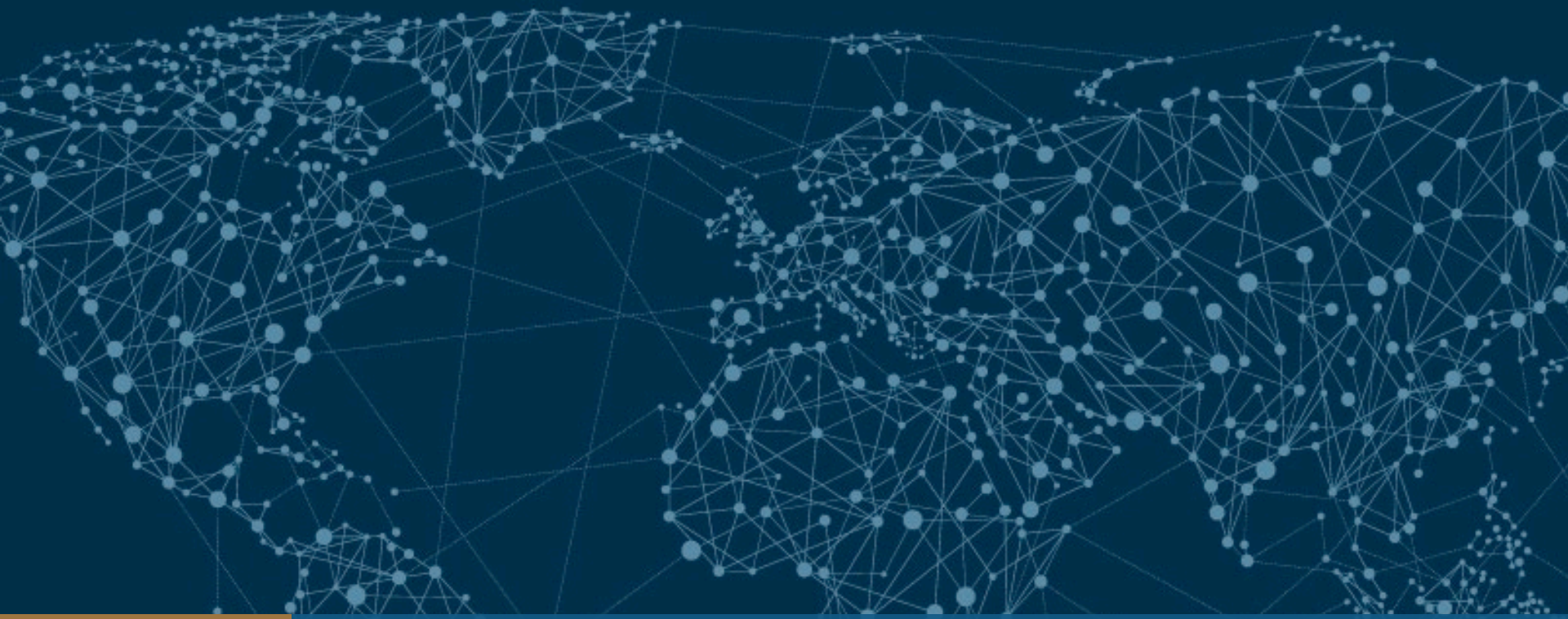


Gestión de la KSK en la Raíz

Andrés Pavez | LACNIC 26 LACNOG 2016 | Septiembre de 2016
andres.pavez@icann.org

Esta presentación fue previamente preparada por Ed Lewis (edward.lewis@icann.org) y levemente modificada para este público

Agenda

1. Antecedentes sobre DNS, DNSSEC
2. Gestión de la Zona Raíz
3. Rol de ICANN como la entidad encargada del mantenimiento de la KSK

¿Por qué se debe dar esta charla?

- Una de las funciones de IANA que ICANN desempeña es la gestión de la llave para la firma de llave (KSK) de las Extensiones de Seguridad (DNSSEC) de la zona raíz del DNS

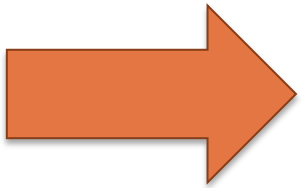
- Saber qué es la KSK y cómo se maneja, ayuda a juzgar si debe tener confianza en la seguridad en función de ella y en DNSSEC en general

Seguridad a pequeña escala

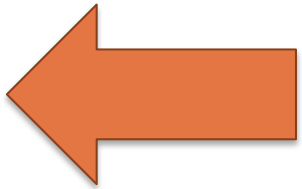
- El primer paso es entender cómo funciona DNSSEC de manera abstracta
- ¿Cómo protege los datos en el sistema?

Para ingenieros a los que no les gustan los protocolos

¿Cuál es la dirección IPv6 para www.lacnic.net?

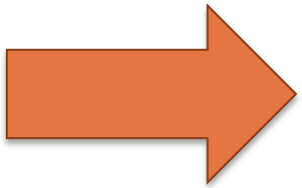


www.lacnic.net. es W::Z



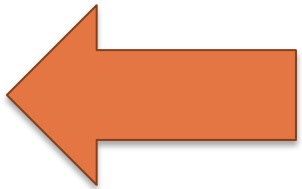
DNSSEC para aquellos a los que no les gustan los protocolos

¿Cuál es la dirección IPv6 para www.lacnic.net?



www.lacnic.net. es W::Z

Firma digital de lacnic.net que abarca la respuesta

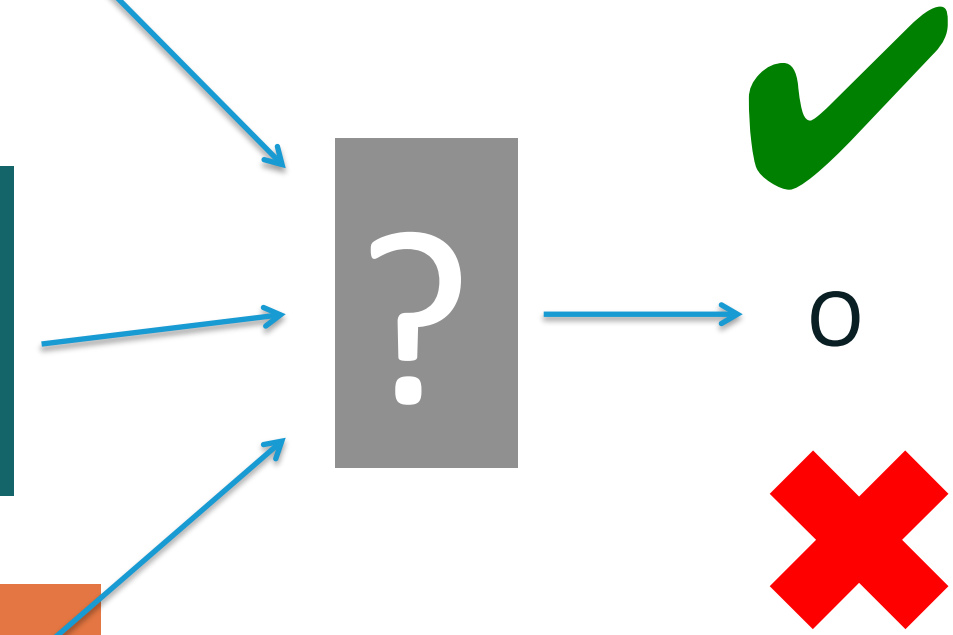


Verificación criptográfica de una firma

La dirección IPv6 para www.lacnic.net es W::Z

Firma digital por lacnic.net que abarca la respuesta

Alguna Cosa

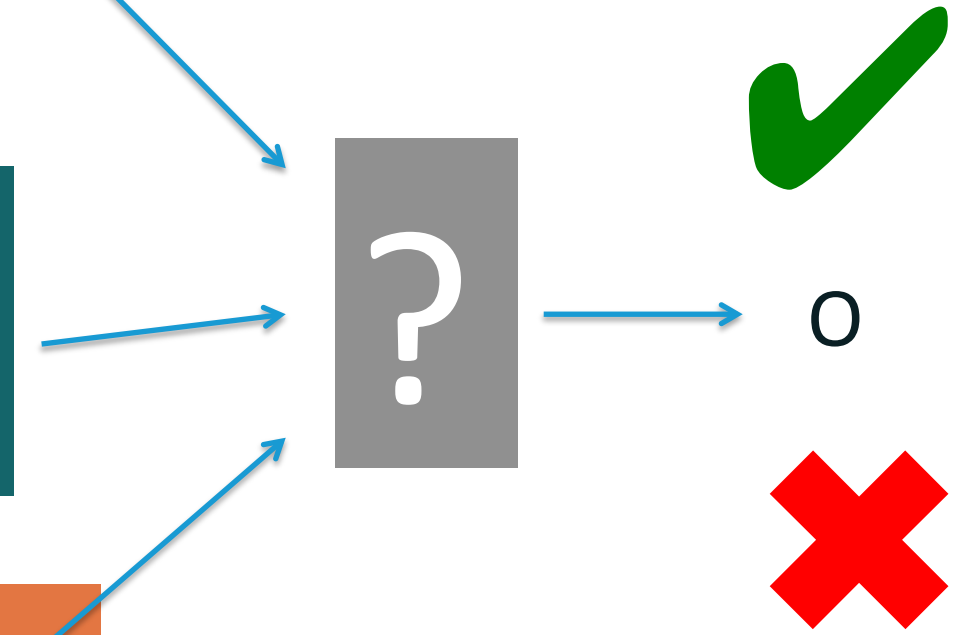


Verificación criptográfica de una firma

La dirección IPv6 para www.lacnic.net es W::Z

Firma digital por lacnic.net que abarca la respuesta

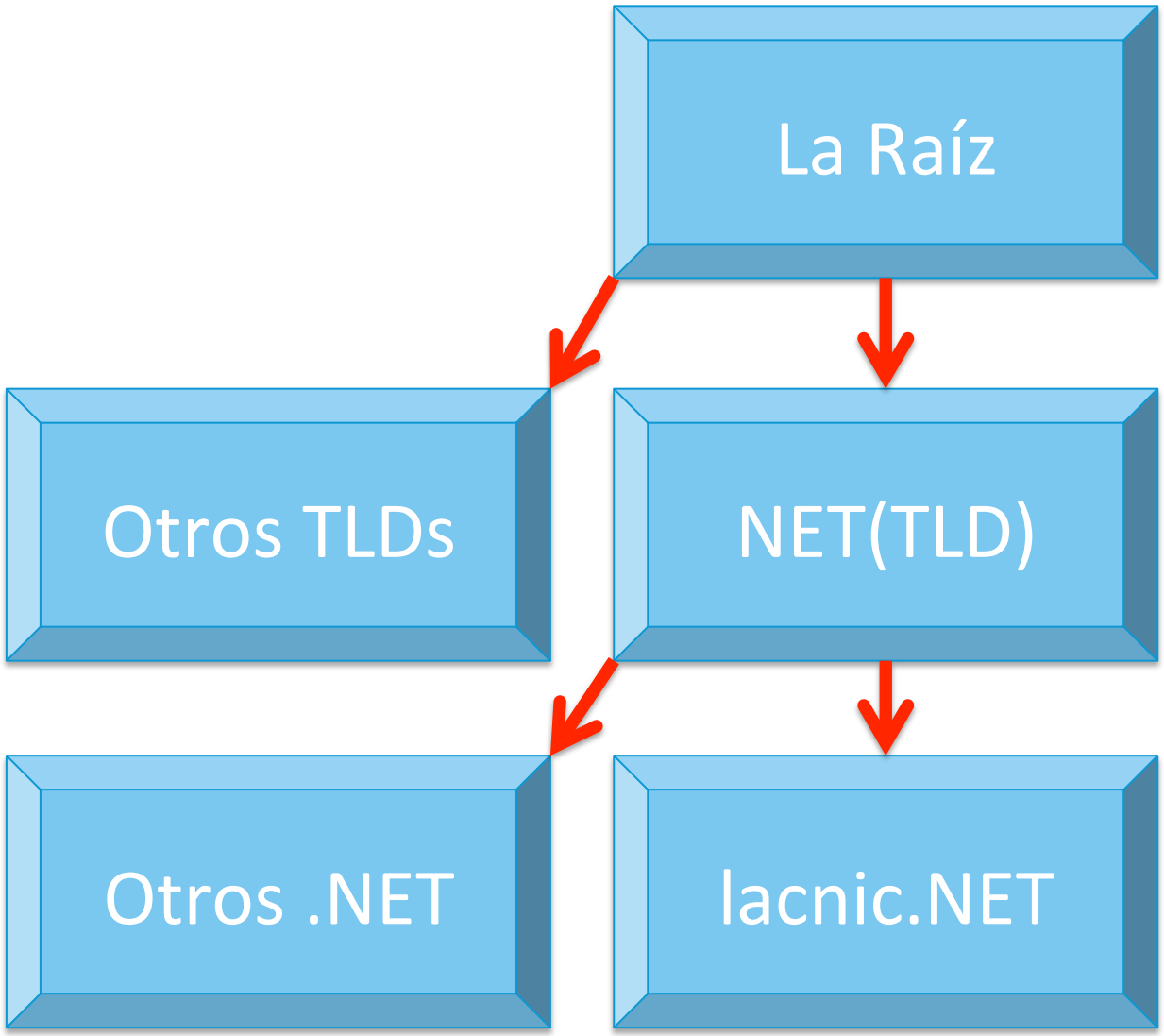
lacnic.net. llave ZSK



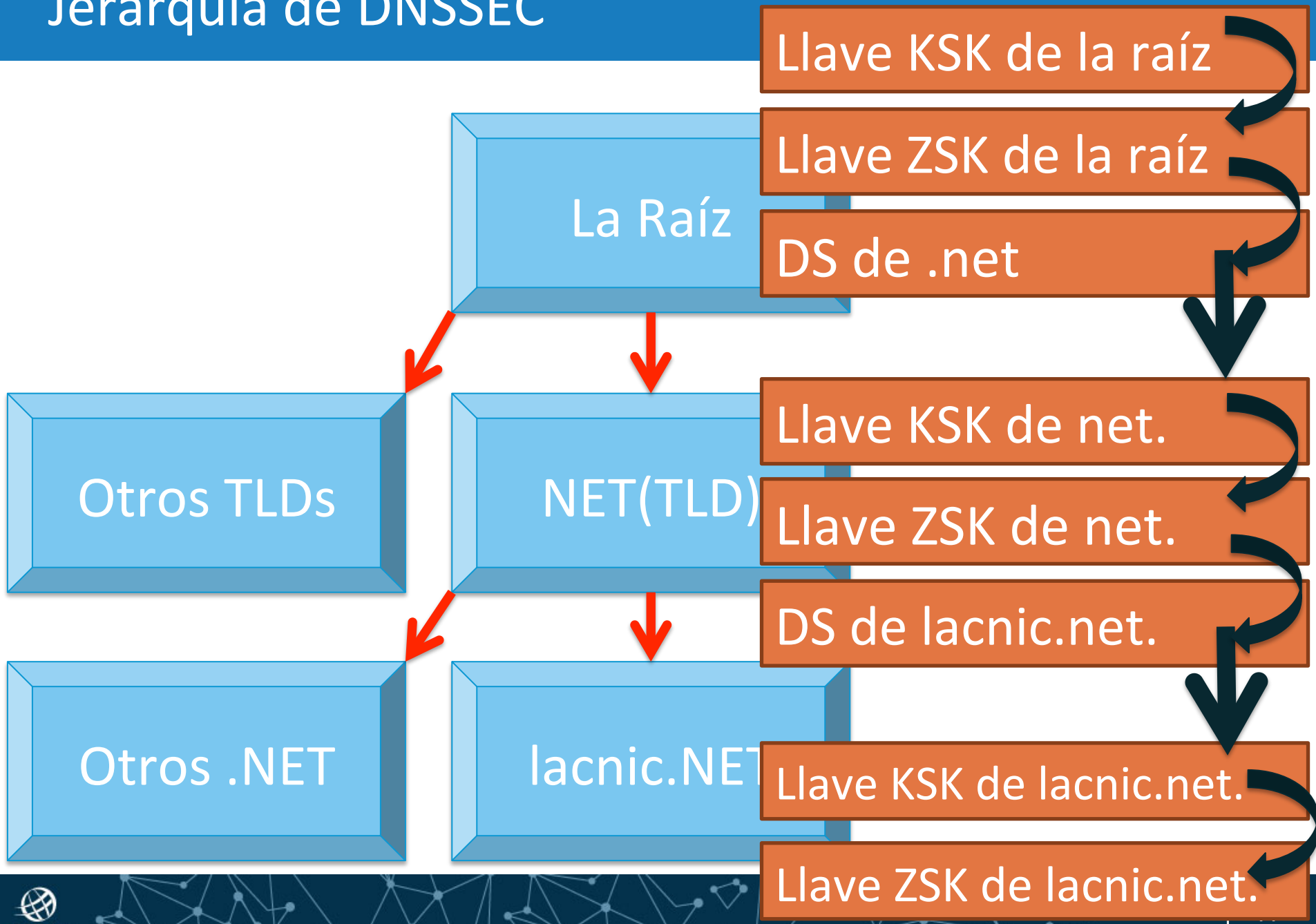
Seguridad a gran escala

- DNSSEC se basa en la jerarquía del DNS
- En DNSSEC se inventaron dos roles para las llaves:
  - Llave para la firma de datos de la zona raíz (ZSK)
  - Llave para la firma de la llave (KSK)
- Y en el punto de delegación (padre)
  - Firmante de delegación (DS)

El DNS es jerárquico



Jerarquía de DNSSEC



Cadena de confianza

- Los cuadros naranjas muestran una “cadena de confianza”
- Si uno confía en la KSK de la zona raíz, se pueden realizar vínculos a la ZSK, firmando los datos
- Por esto es que confiar en la KSK de la zona raíz es muy importante

Confiando en la KSK de la raíz

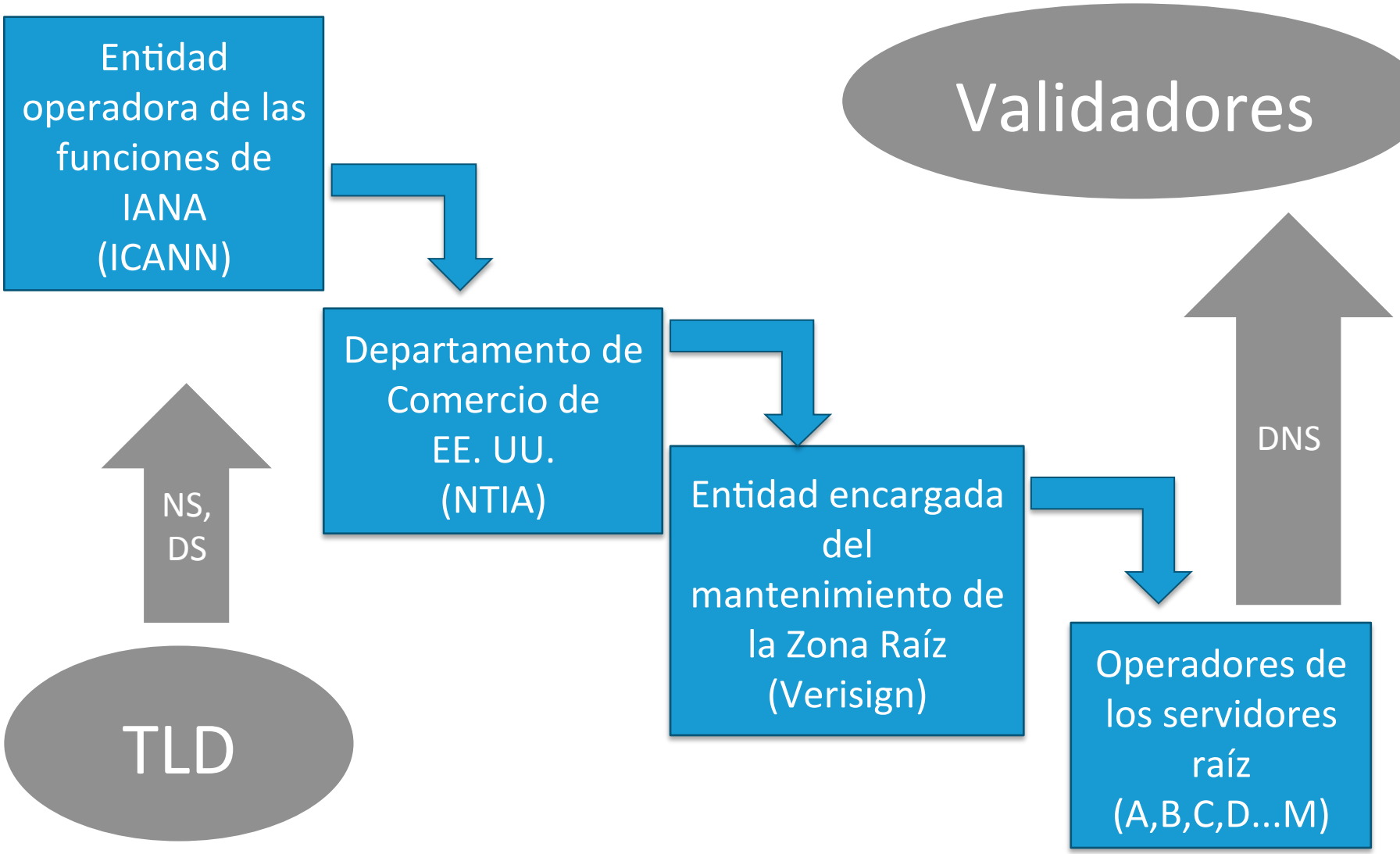
- El ciclo de vida de la KSK de la raíz
  - Desde la creación hasta la destrucción
  - Uso
  - Riesgos
- Distribución de la KSK de la raíz
  - Vía DNS
  - Vía sitio web
  - Incrustada en código
  - Verificación fuera de banda

Roles en la gestión de Llaves

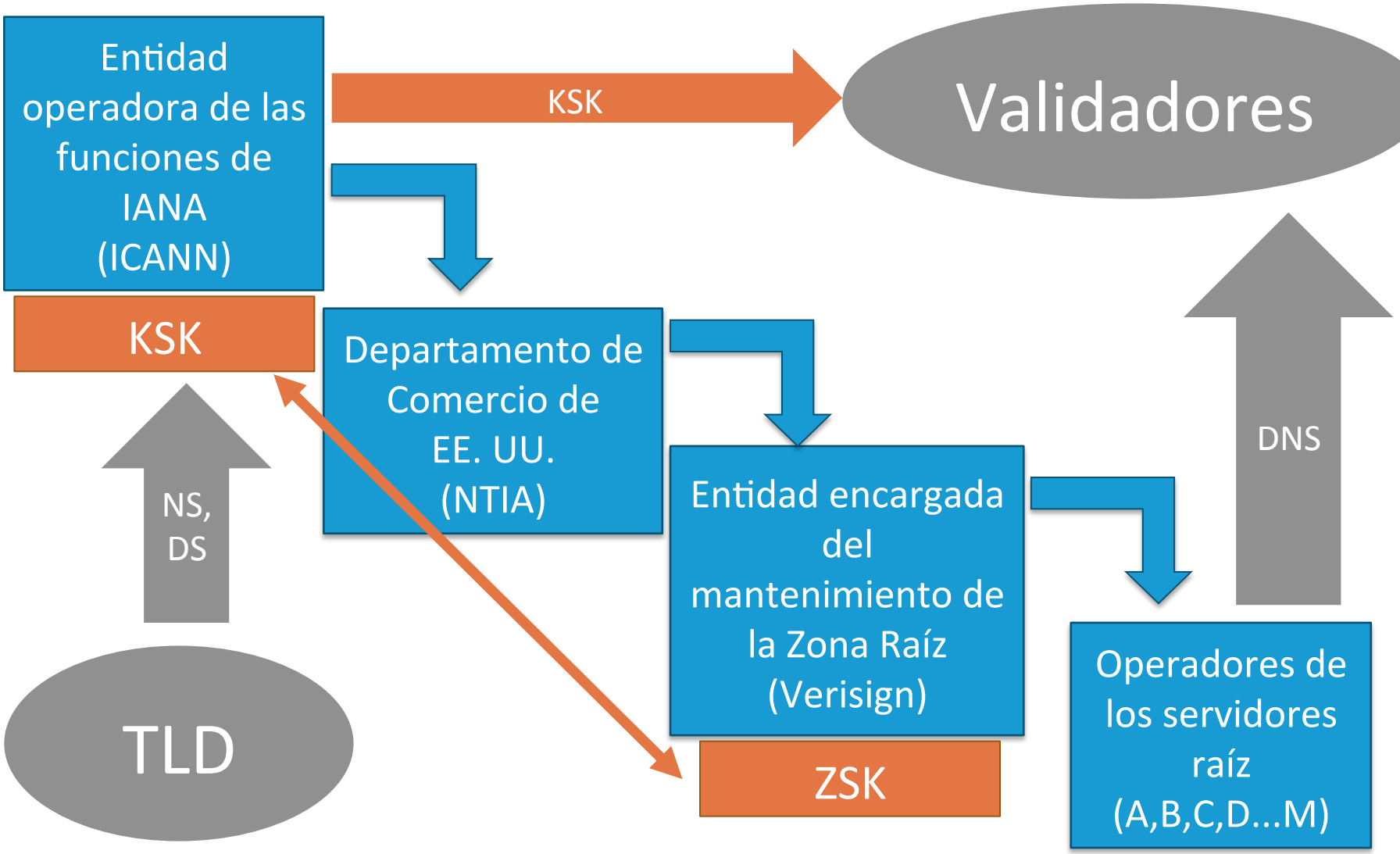
- ICANN administra la KSK de la zona raíz como parte del cumplimiento del Contrato de Funciones de IANA
  - El Contrato de Funciones de IANA es gestionado por la Administración Nacional de Telecomunicaciones e Información de los Estados Unidos (NTIA) del Departamento de Comercio de los EE.UU.

- Verisign gestiona la ZSK de la zona raíz como entidad encargada del mantenimiento de la Zona Raíz, en virtud de un Acuerdo de Cooperación con NTIA

Gestión de la Zona Raíz



Gestión de la Zona Raíz



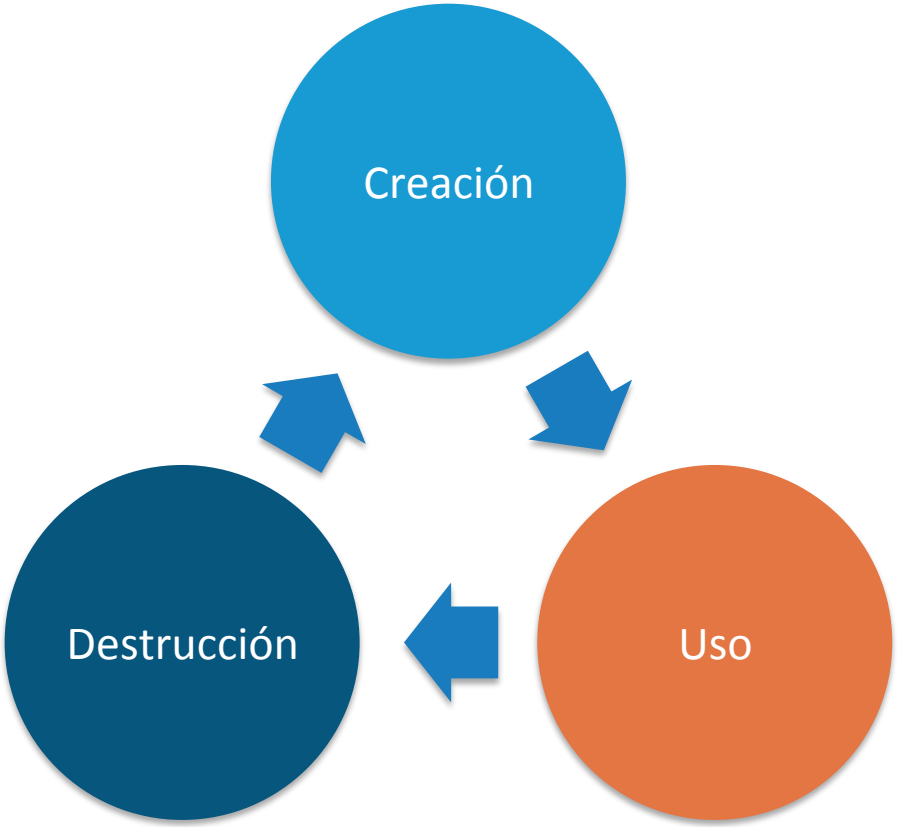
Reglas de operación

- La KSK es operada en conformidad con las reglas estipuladas en la Declaración de Prácticas de DNSSEC (DPS):
  - https://www.iana.org/dnssec/icann-dps.txt

- La ZSK es operada en conformidad con la siguiente DPS:
  - https://www.verisign.com/assets/dps-zsk-operator-1532.pdf

Operación de la KSK

- La gestión de la KSK incluye:
  - El ciclo de vida: Creación, uso, destrucción
  - Manteniendo su seguridad
  - Habilitando la validación de DNSSEC



Otro detalle sobre las Llaves

- KSK y ZSK son, en realidad, un par de llaves
  - Llaves Privada y Pública
  - Las llaves privada y pública están especialmente vinculadas: lo que una cifra, la otra lo descifra y viceversa

Llave KSK Pública

Llave KSK Privada

Llave ZSK Pública

Llave ZSK Privada

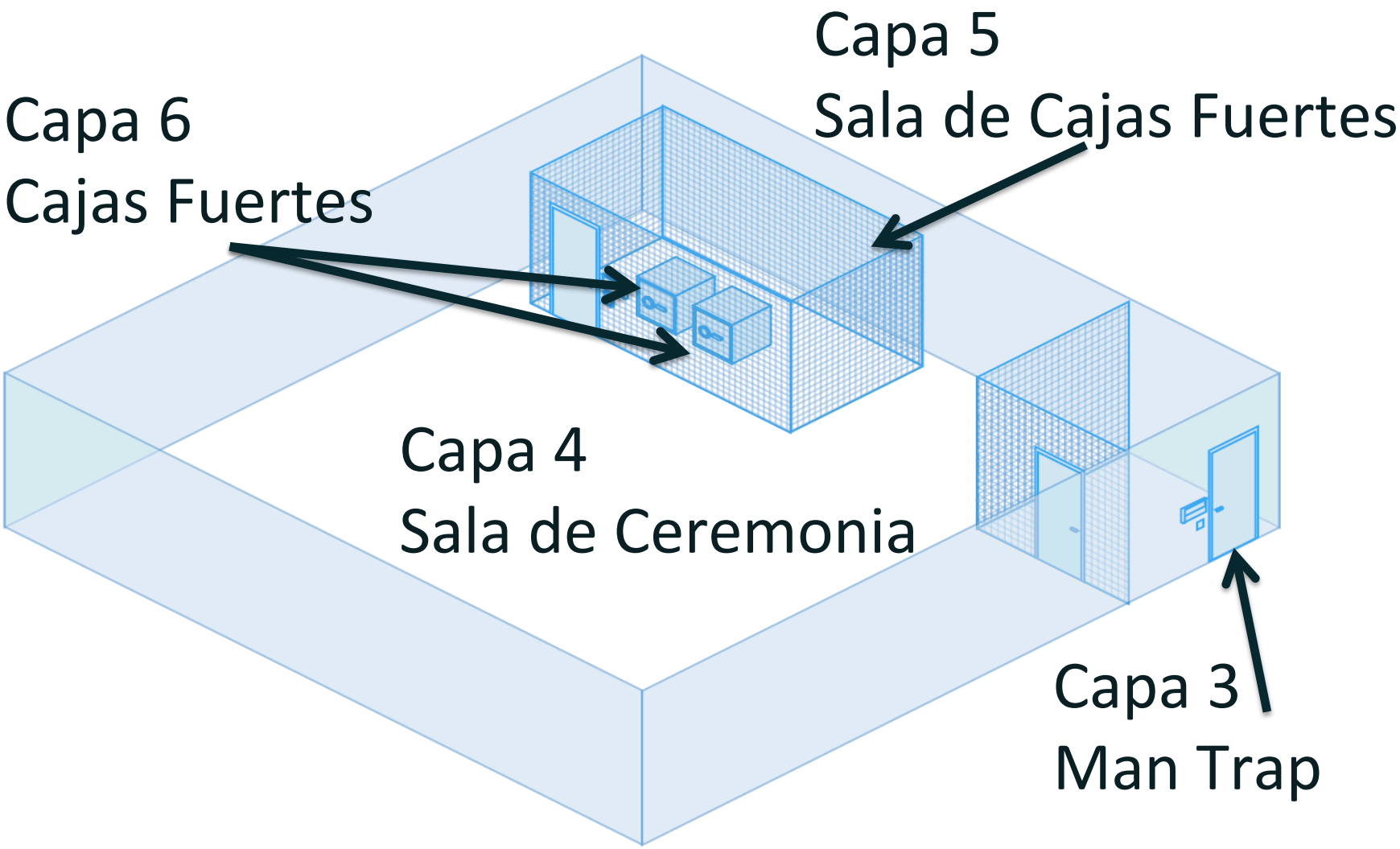
Principios de diseño

- Generar confianza de la comunidad en la KSK
  - Participación externa activa
    - 21 voluntarios para cubrir roles (descritos más adelante)
  - Revisión de terceros
    - Auditoria SysTrust/SOC-3
  - Enfatizar detección de incidentes
  - Participación de personal de diferentes áreas
  - Recuperación ante desastres

Una base segura

- La maquinaria para las operaciones de la KSK en la Zona Raíz incluye:
  - Centro de datos, capas de acceso (jaulas, cajas fuertes, cajas de seguridad)
  - Hardware configurado para funcionar aislado y sólo con funciones necesarias, todo el software está disponible para revisión
  - Todas las operaciones que implican el uso de la llave privada son grabadas y se utilizan bolsas que permiten evidenciar si han sido alteradas
  - Publicación de Declaración de Prácticas de DNSSEC

“Vista” física en capas 3 - 4 – 5 - 6



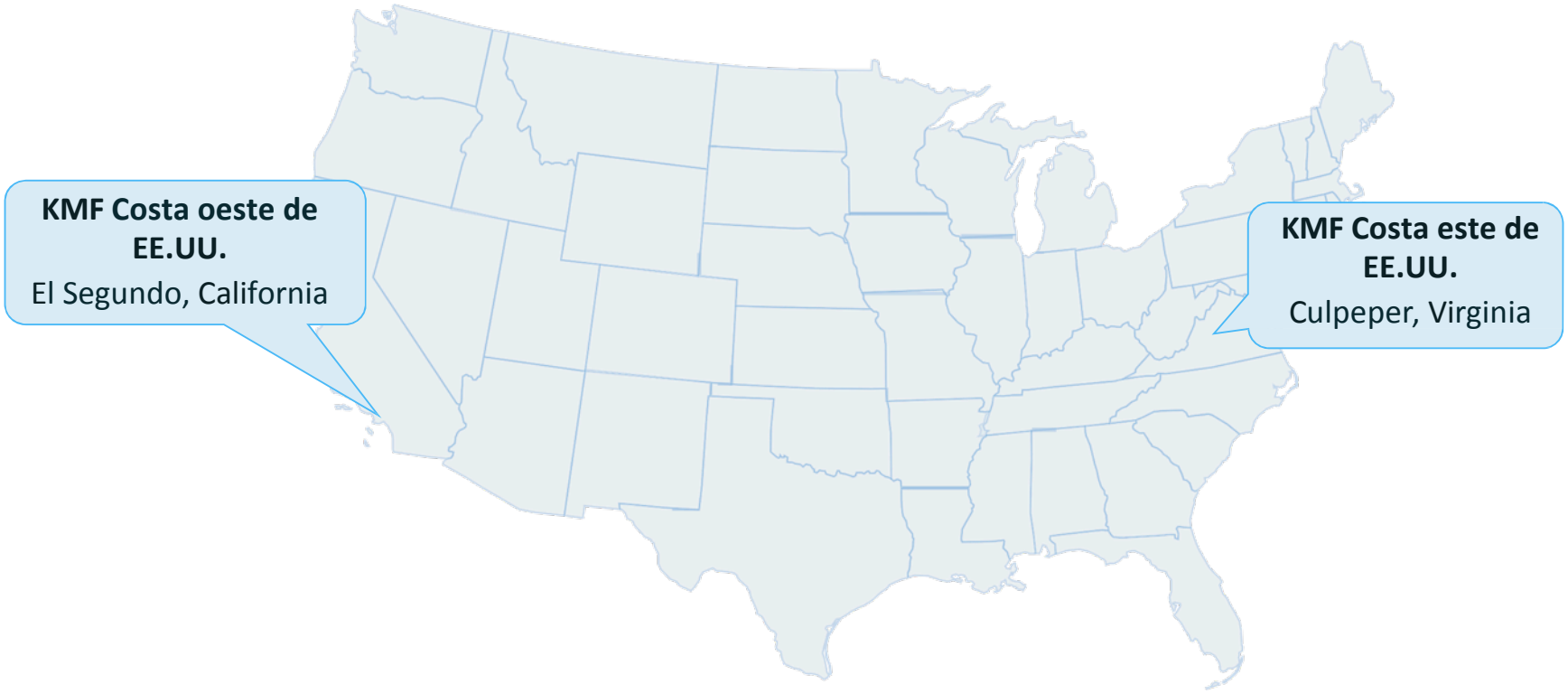
Ceremonias

- Para utilizar la KSK (llave privada)
- Cada vez que la KSK se activa es durante una ceremonia
  - Testigos presenciales, auditores, transmisión en vivo
  - https://www.iana.org/dnssec/ceremonies
- Entre ceremonias, todos los activos de la KSK se mantienen en bolsas que permiten evidenciar si hubo alteración o manipulación
- En la ceremonia se “explica” cuándo y por qué se rompen sellos

Creación de la KSK de la Zona Raíz

- Creada en junio de 2010
- Instalada en dos HSM en Culpeper, Virginia, EE. UU. (16 de junio de 2010)
  - Se firman las primeras ZSK de la zona raíz
- Copiada por redundancia en otros dos HSM en El Segundo, California, EE. UU. (12 de julio de 2010)
  - Se firmó el segundo conjunto de ZSK de la zona raíz
- Video y materiales disponibles en línea:
  - https://www.iana.org/dnssec/ceremonies

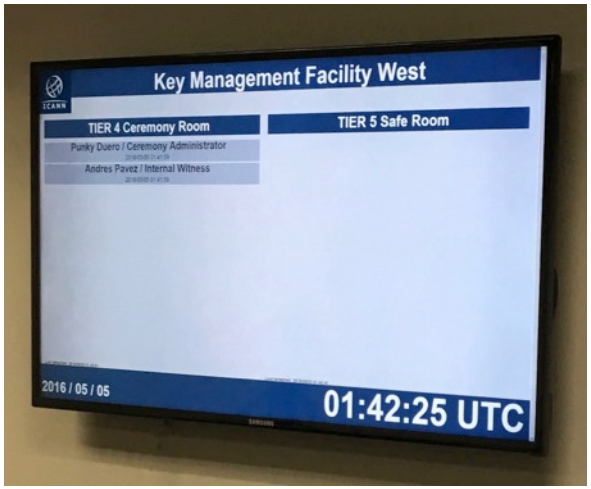
Uso de la KSK desde entonces



- Las salas de ceremonias, conocidas como **instalaciones en las cuales se administra la llave (KMF)**, están ubicadas dentro de dos instalaciones vigiladas, una en la costa oeste y otra en la costa este de EE. UU.

Fotomontaje de las primeras ceremonias

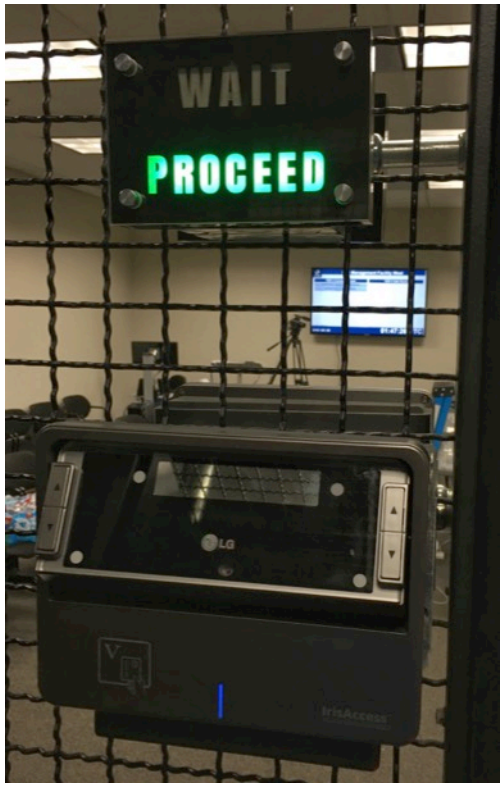
Algunas fotos de las KMF



Pantalla de ocupación de capas y relog de Ceremonia

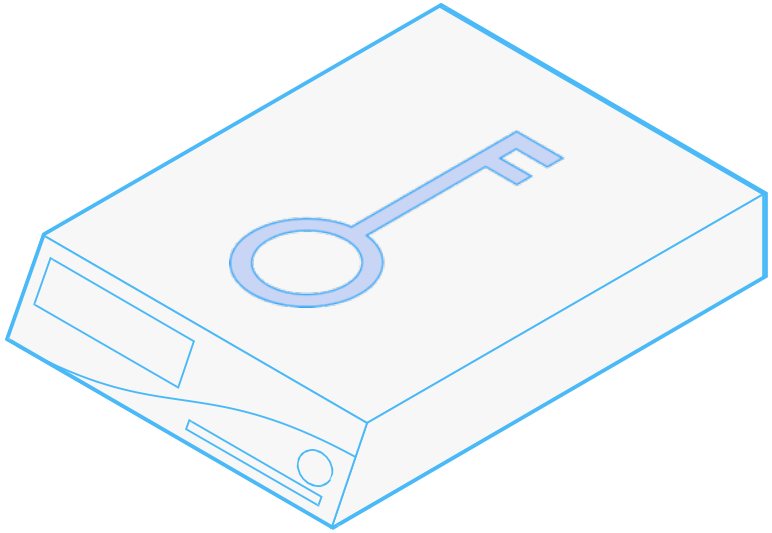
Capa 3
Temporizador

Vista de Jaula de capa 3 a capa4



Vista de jaula de capa 5 a capa 4

Módulo de Seguridad de Hardware (HSM)



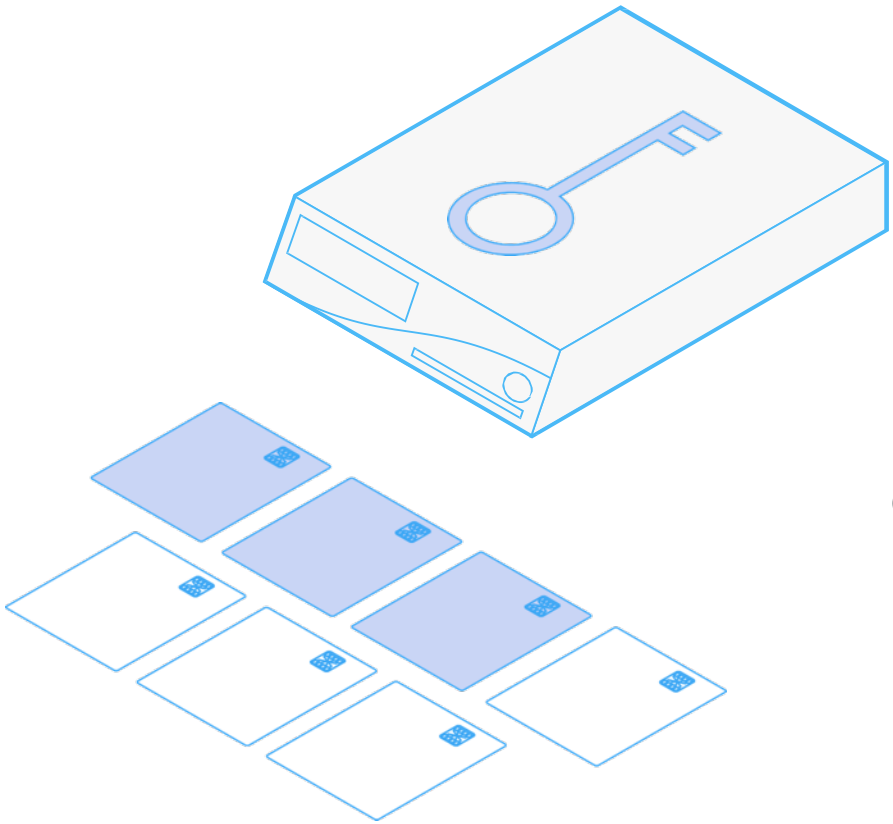
- La llave para la firma de la llave (KSK) se almacena en un dispositivo conocido como **Módulo de Seguridad de Hardware** (HSM) cuyo único fin es almacenar llaves criptográficas de manera segura. El dispositivo está diseñado para que sea a prueba de alteraciones. Si se produce un intento de abrirlo, el contenido se destruye automáticamente.

No es la llave, es el HSM

- El HSM hace que el robo de la llave sea impráctico
  - Pero se puede robar el HSM

- ¿De qué manera está protegido?
  - Seguridad física
  - Seguridad “para utilizar el HSM”

Credenciales

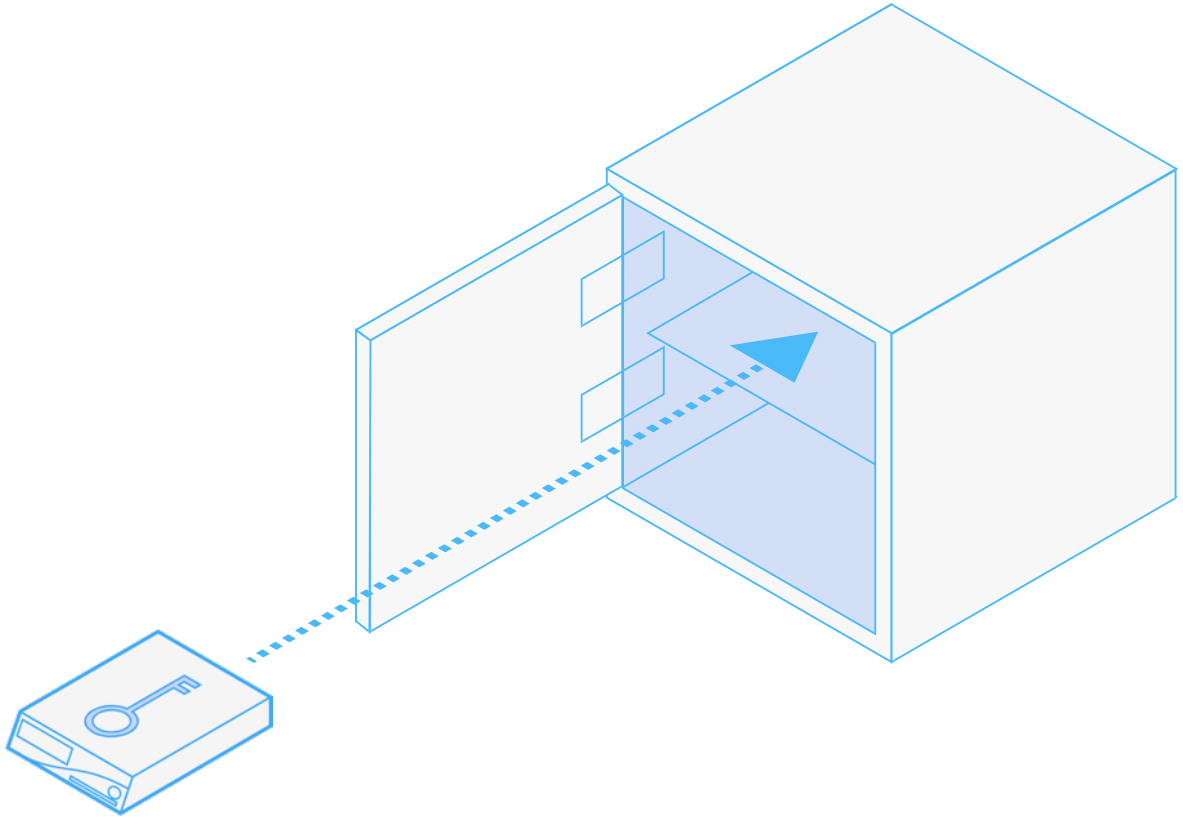


- Existen siete tarjetas inteligentes que pueden activarse en cada dispositivo. El dispositivo está configurado de manera tal que **3 de las 7** tarjetas inteligentes deban estar presentes para que el mismo pueda utilizarse.

Representantes confiables de la comunidad (TCR)

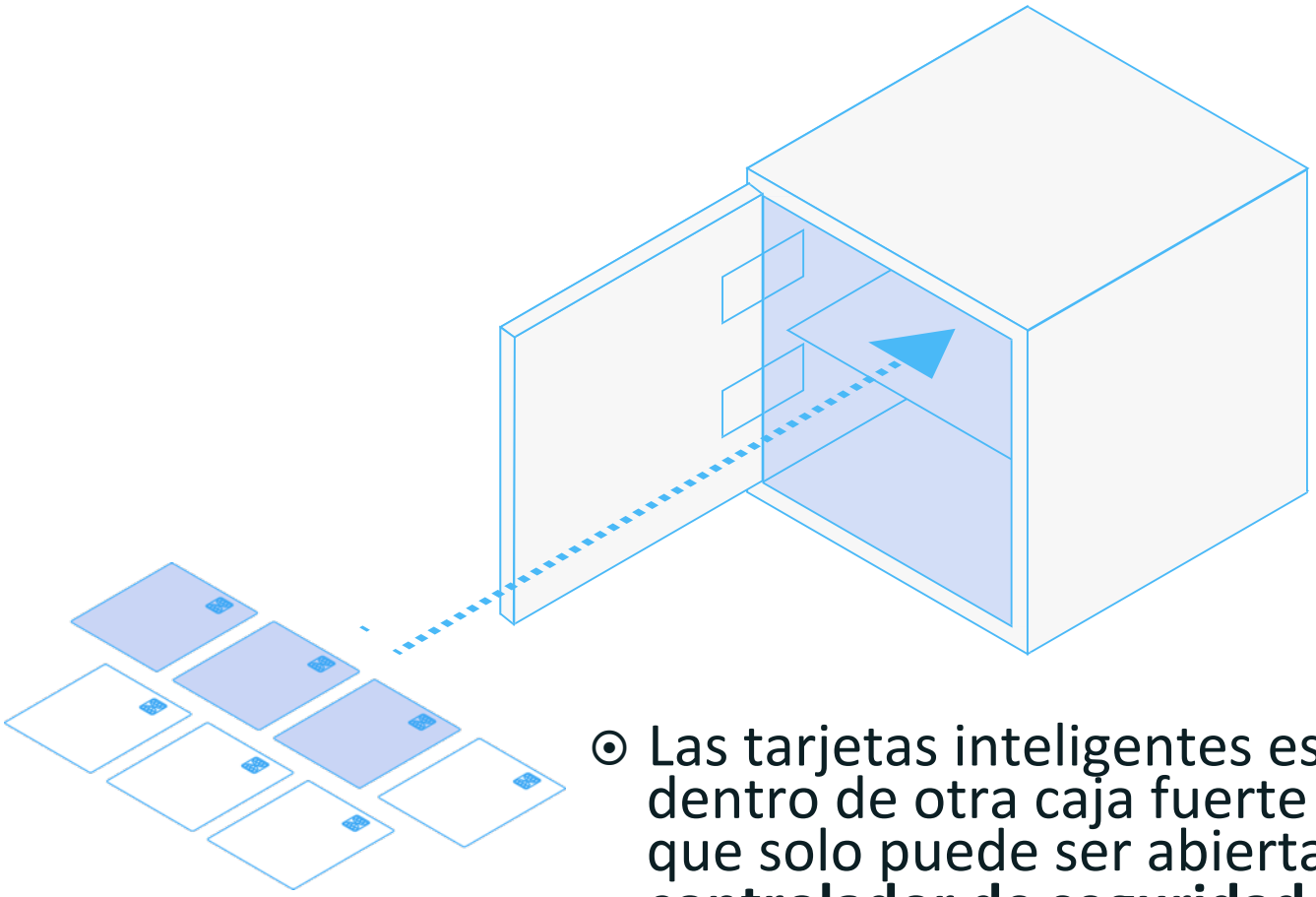
- Cada tarjeta inteligente es entregada a un miembro de la comunidad de ICANN, conocido como **representante confiable de la comunidad**. Para tener acceso a la llave para la firma de la llave, al menos tres de estos TCR deben estar presentes.

Caja Fuerte 1 – Caja fuerte de hardware



- El HSM está almacenado en una caja fuerte de alta seguridad, que solo puede ser abierta por una persona designada, el **controlador de seguridad de cajas fuertes**. La caja fuerte está monitoreada con sensores sísmicos y otros sensores.

Caja Fuerte 2 – Caja fuerte de credenciales



- Las tarjetas inteligentes están almacenadas dentro de otra caja fuerte de alta seguridad, que solo puede ser abierta por un **controlador de seguridad de cajas fuertes** diferente. Las cajas de seguridad que protegen a cada una de las tarjetas inteligentes solo pueden ser abiertas por los TCR

Protección de la KSK de la Zona Raíz

- Dos grupos de siete funcionarios criptográficos
  - Personas que no pertenecen al personal de ICANN seleccionadas a través de un proceso en 2010, ubicados en todo el mundo
  - Un grupo para Culpeper, otro para El Segundo
  - Se necesitan tres de siete para iniciar un HSM

- Siete titulares de credenciales de recuperación de llave
  - No pertenecientes al personal de la ICANN, como arriba
  - Verificación anual de posesión de tarjeta inteligente
  - Cinco de siete titulares deben ser congregados para reensamblar la llave

Recuperación

- Al momento en que la llave KSK (privada) es utilizada
  - Las firmas se generan para el próximo trimestre calendario
  - Esto permite 3 meses (aproximadamente) de tiempo de recuperación ante una falla

- Es importante señalar esto – para evitar pánico

Historial de cambios

- HSM
  - Existe una suposición dada de que una batería interna crítica dura 5 años
  - A la marca de 5 años se realiza una “actualización técnica”

- KSK
  - La KSK nunca se ha cambiado desde su creación en 2010

¿Por qué cambiar la KSK?

- A la larga, los secretos
  - se olvidan (todos los HSM pueden fallar)
  - se exponen (la llave privada se copia fuera del HSM)
  - se descubren (alguien hace una ingeniería inversa)
- ¿Eso sucederá pronto? Probablemente no.
- Pero ¿qué sucede si esto pasa?
  - Preparación/Práctica

Publicación de la KSK

- Mantener en secreto la parte secreta es fundamental para que la KSK tenga valor

- Para que tenga valor, la parte pública de la KSK debe ser utilizada
  - La exactitud importa (¡evite errores por cortar y pegar!)
  - La legitimidad importa (asegúrese de que sea la “real”)

Obtención de la llave KSK pública

- Vía DNS
  - Tan confiable como los datos en el DNS no protegido
  - Exactitud, seguro, pero puede cuestionarse su legitimidad
- Vía Web
  - https://www.iana.org/dnssec/files
  - Protegida por firma y certificado X.509
- Vía otros medios
  - Presentaciones, amigos, código
  - ¡Recuerde siempre verificar la legitimidad!

Identificación de la KSK

- A septiembre de 2016, ésta es una forma de identificar la llave:

<KeyDigest id="Kjqmt7v"
validFrom="2010-07-15T00:00:00+00:00">
<KeyTag>19036</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>
49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1C
DDE32F24E8FB5
</Digest>
</KeyDigest>

Otra Vista de la llave KSK pública

- A septiembre de 2016, ésta es otra forma de identificar la llave:

```
.                       172800  IN      DNSKEY  257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=
```

Nota de advertencia

- No se base sólo en el contenido de estas diapositivas
- Utilícelas para verificar lo que ve a través de otros medios
- Y recuerde, usted decide en qué confiar

Para más información

- Únase a la lista de correo electrónico:
  - https://mm.icann.org/mailman/listinfo/root-dnssec-announce

- Síganos en Twitter
  - @ICANNtech
  - Hashtag: #KeyRoll

- Visite la página web:
  - https://www.icann.org/resources/pages/ksk-rollover

Participe en ICANN

Gracias y preguntas

Contácteme
Email: andres.pavez@icann.org
Sitio web: icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations