Automatización de DNSSEC con el registro CDS

Hugo Salgado - .CL
LACNOG 2022 - Santa Cruz, Bolivia

DNSSEC (en 3 diapositivas)

- ¿Qué es DNSSEC?
  - Criptografía asimétrica en DNS
  - Autenticidad, Integridad y Negación auténtica

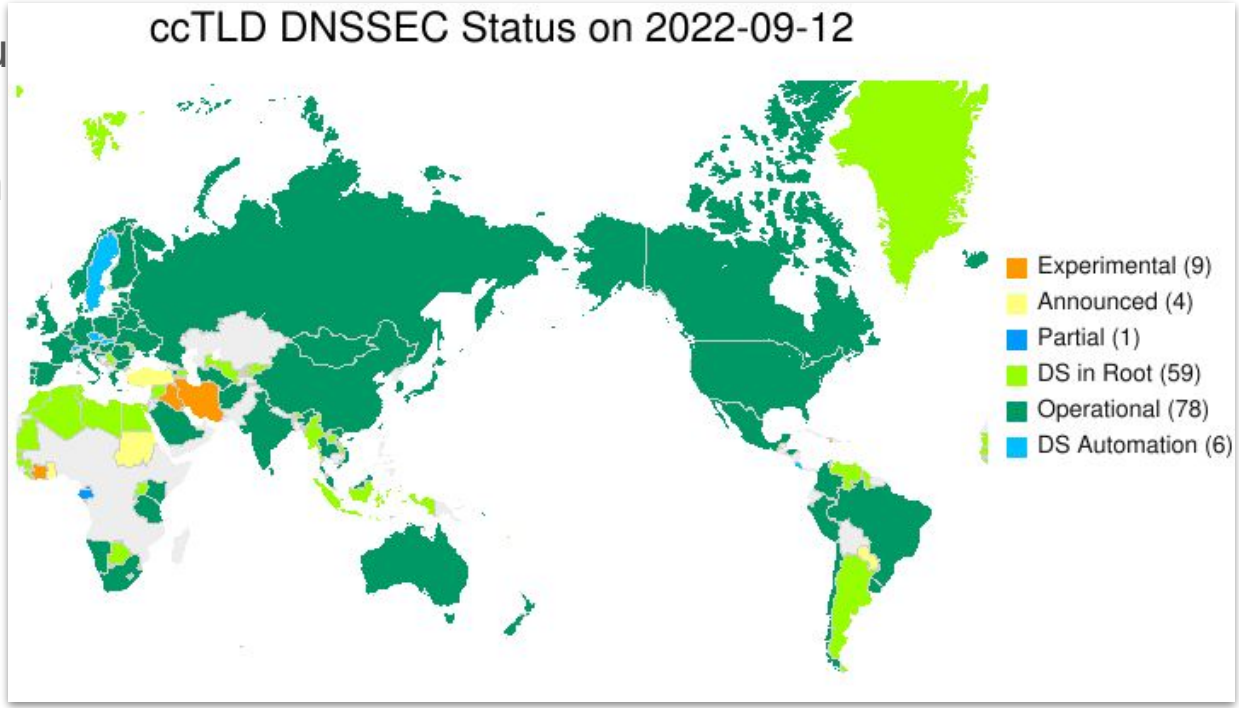
    DNS normal +
    - Firmas
    - Llaves
    - Negación segura
    - Delegación segura

DNSSEC (en 3 diapositivas)

- ¿Qué es DNSSEC?
- ¿En qué estamos?

DNSSEC (en 3 diapositivas)

- ¿Qu
- ¿En



Mapa de Internet Society, Deploy360
https://www.internetsociety.org/deploy360/dnssec/maps/

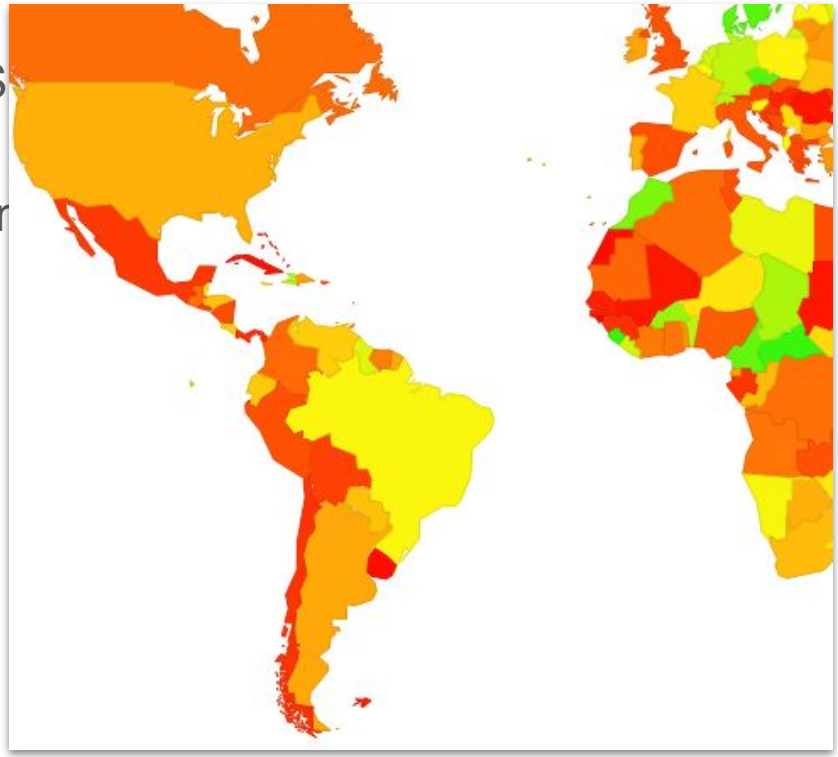
DNSSEC (en 3 diapositivas)

- ¿Qu
- ¿En

Mapa de Internet Society, Deploy360
https://www.internetsociety.org/deploy360/dnssec/maps/

DNSSEC (en 3 diapositivas)

- ¿Qué es DNS
- ¿En qué estar

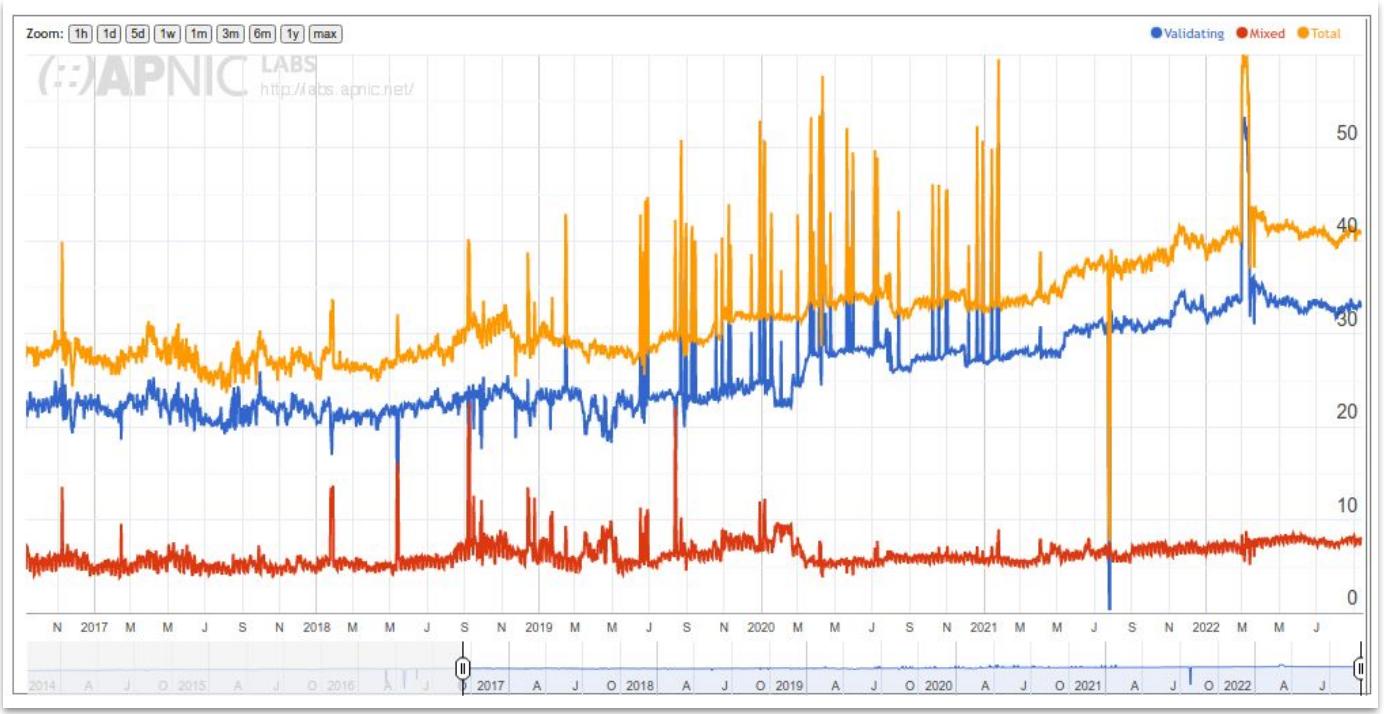


Validación	
BR	51
VE	42
EC	41
PY	39
AR	34
CO	22
BO	13
PE	16
CL	10

APNIC Labs, DNSSEC Validation by country
https://stats.labs.apnic.net/dnssec

DNSSEC (en 3 diapositivas)

- ¿Qu
- ¿En



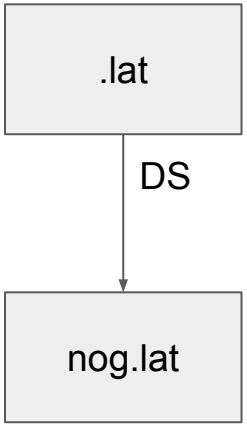
APNIC Labs, Use of DNSSEC Validation for Americas
https://stats.labs.apnic.net/dnssec

DNSSEC (en 3 diapositivas)

- Qué es DNSSEC
- En qué estamos (números de penetración y despliegue)
- Automático y simple, soporte en software open source y hosting externo
  - creación de llaves
  - firma de zonas
  - rotaciones
  - cambio de algoritmos

DS: El último paso manual

- Todo bien… **SALVO** el envío de DS al padre
  - fue así por diseño!
- Paso necesario para activar la cadena de validación
- Cada registrar y registry lo hace distinto!
  - muy pocos dan API
- No hay posibilidad de delegar la acción al DNS hosting
- Entonces el gran problema: no se puede automatizar



La solución: CDS, “el DS del hijo”

- Registro nuevo, estándar IETF (RFC8078, marzo 2017)
  “Managing DS Records from the Parent via CDS/CDNSKEY”

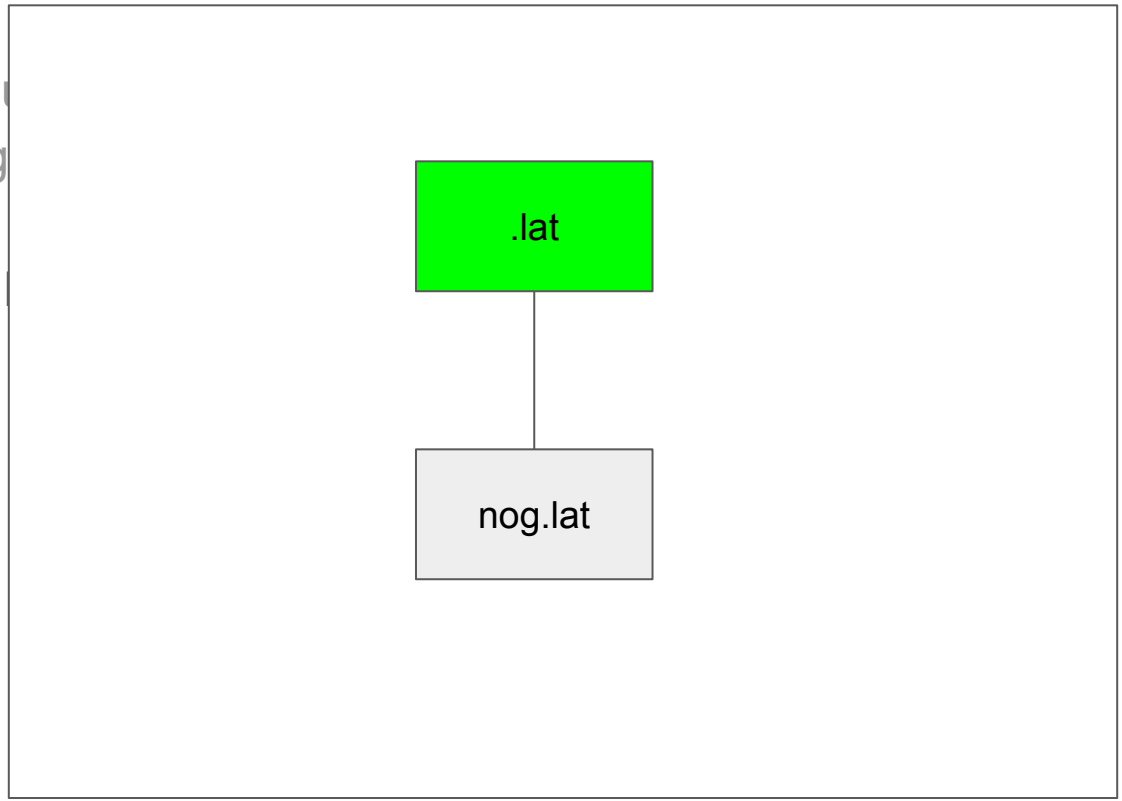
La solución: CDS, “el DS del hijo”

- Registro nuevo, estándar IETF (RFC8078, marzo 2017)
  “Managing DS Records from the Parent via CDS/CDNSKEY”

- Publica el hijo y escanea el padre

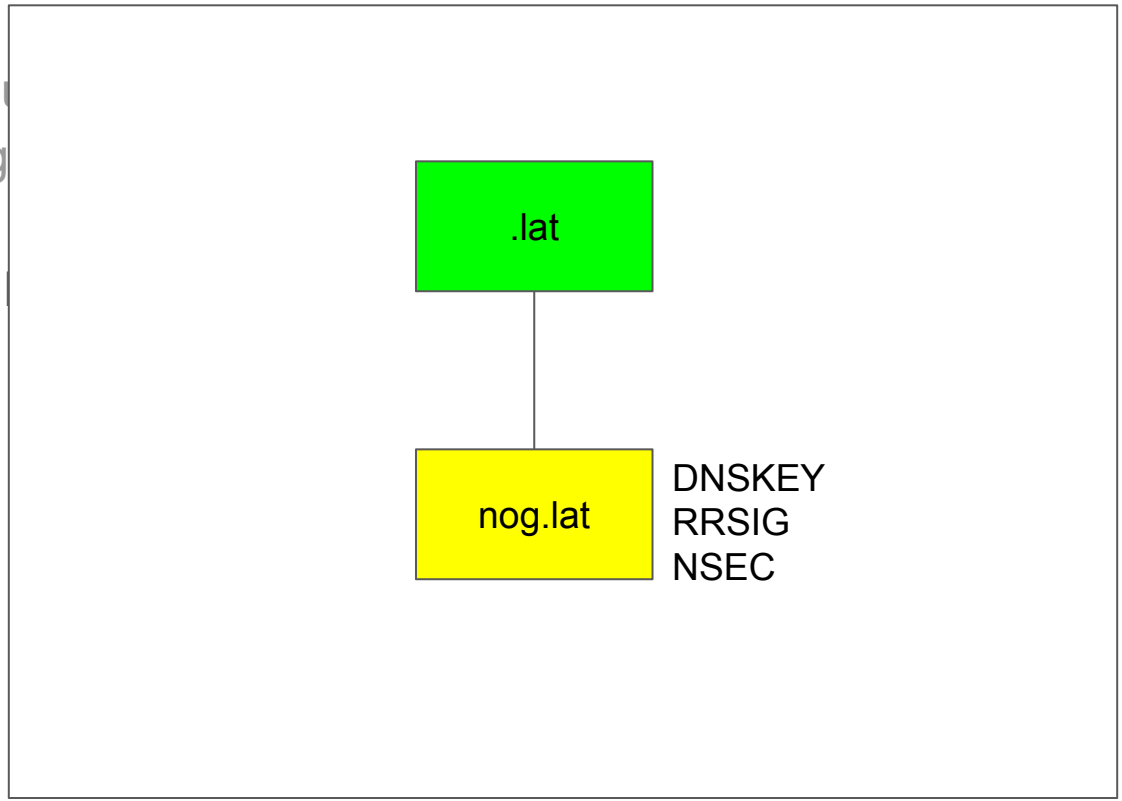
La solución: CDS, “el DS del hijo”

- Registro nu
  “Managing
- Publica el



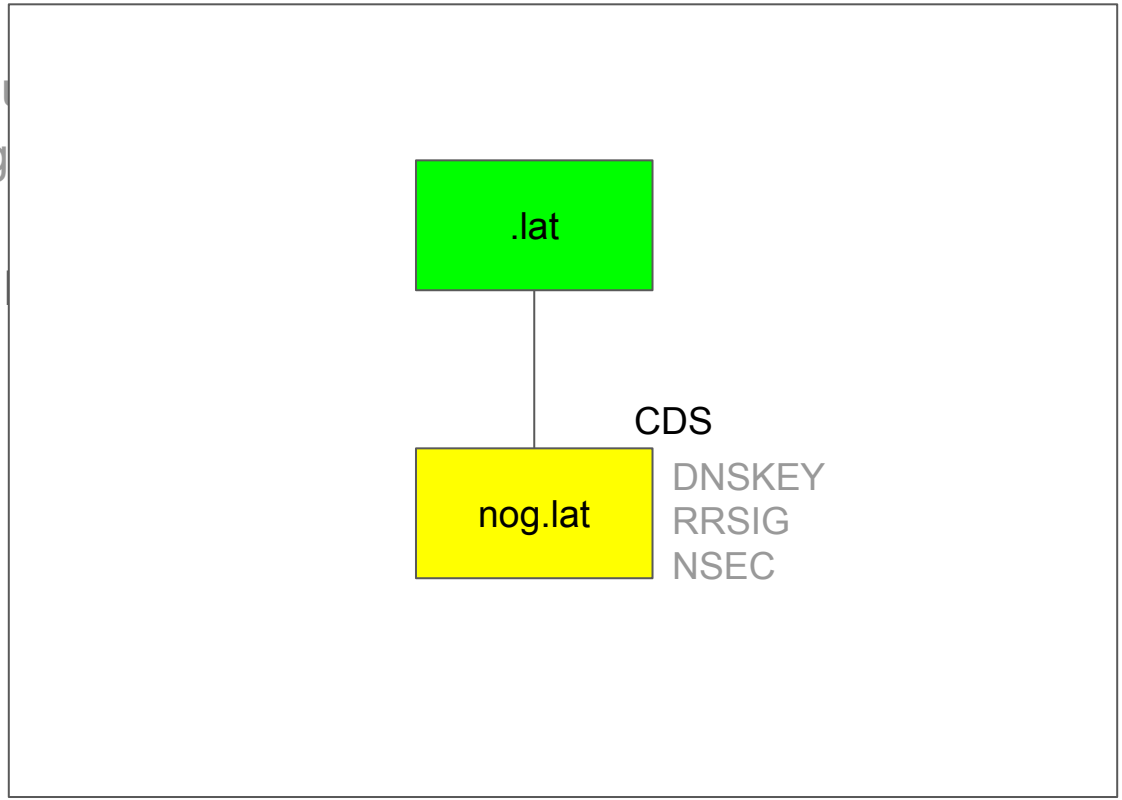
La solución: CDS, “el DS del hijo”

- Registro nu
  “Managing
- Publica el



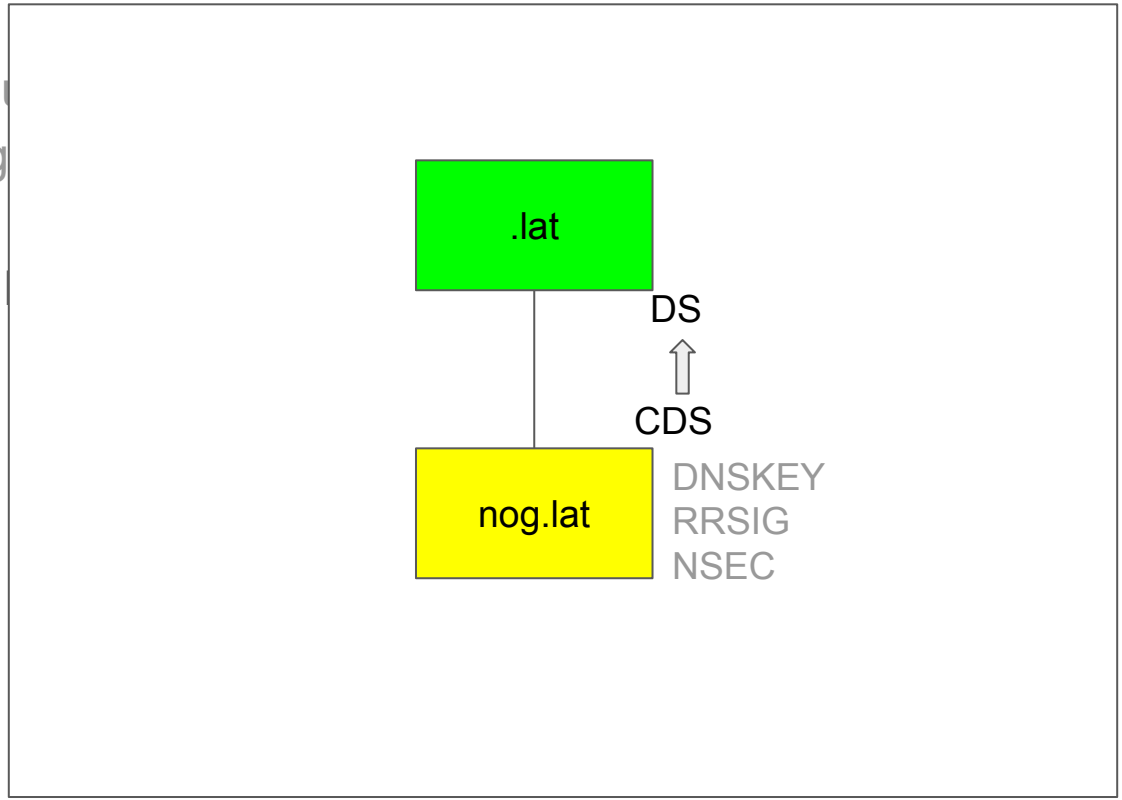
La solución: CDS, “el DS del hijo”

- Registro nu
  “Managing
- Publica el



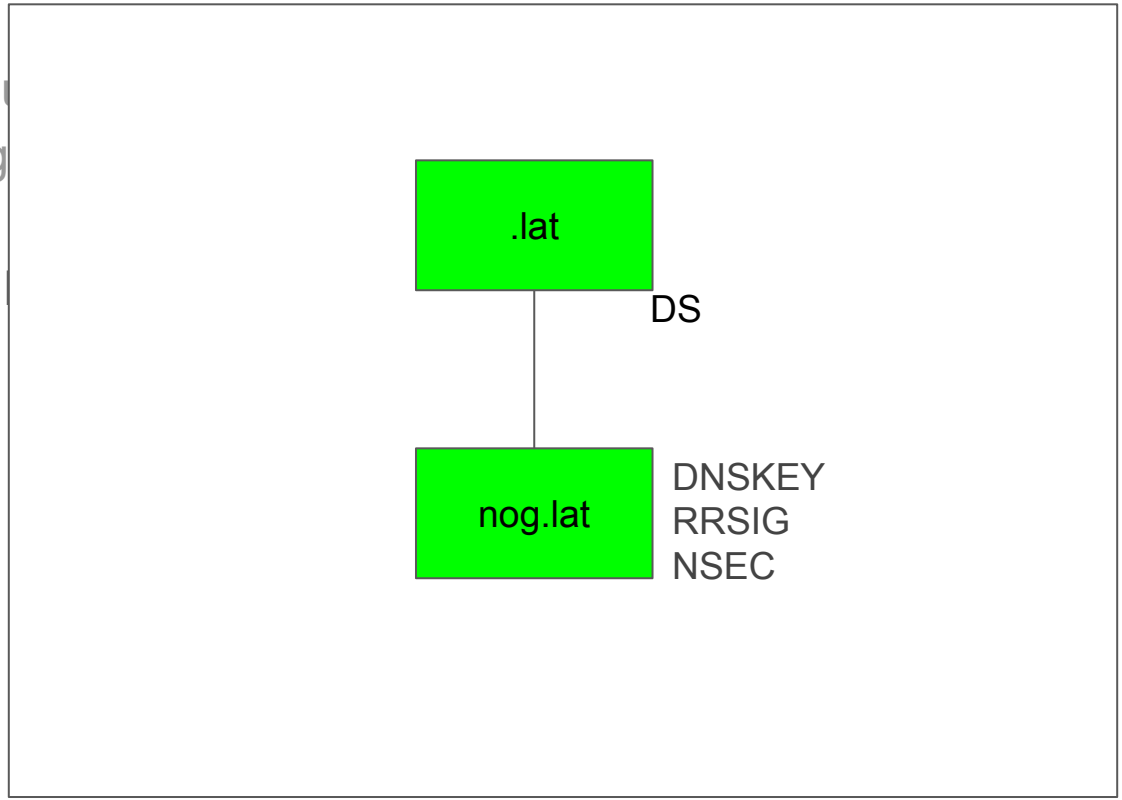
La solución: CDS, “el DS del hijo”

- Registro nu
  “Managing
- Publica el



La solución: CDS, “el DS del hijo”

- Registro nu
  “Managing
- Publica el



La solución: CDS, “el DS del hijo”

- Registro nuevo, estándar IETF (RFC8078, marzo 2017)
  “Managing DS Records from the Parent via CDS/CDNSKEY”
- Publica el hijo y escanea el padre
- Pensado en rollovers
- Pero: también se puede hacer bootstrap
  - condiciones de cada registry (básicamente esperar X días)
  - se viene una técnica sin delay

Estado de técnica CDS

- Soportado automáticamente en DNS autoritativo Bind y Knot.
- Soportado en hosting de DNS (Cloudflare, Google Domains, etc)
- Uso en TLDs
  - .se
  - RIPE (reverso)
  - En nuestra región .CR, y .CL en marcha blanca

¿Cómo se utiliza en la práctica?

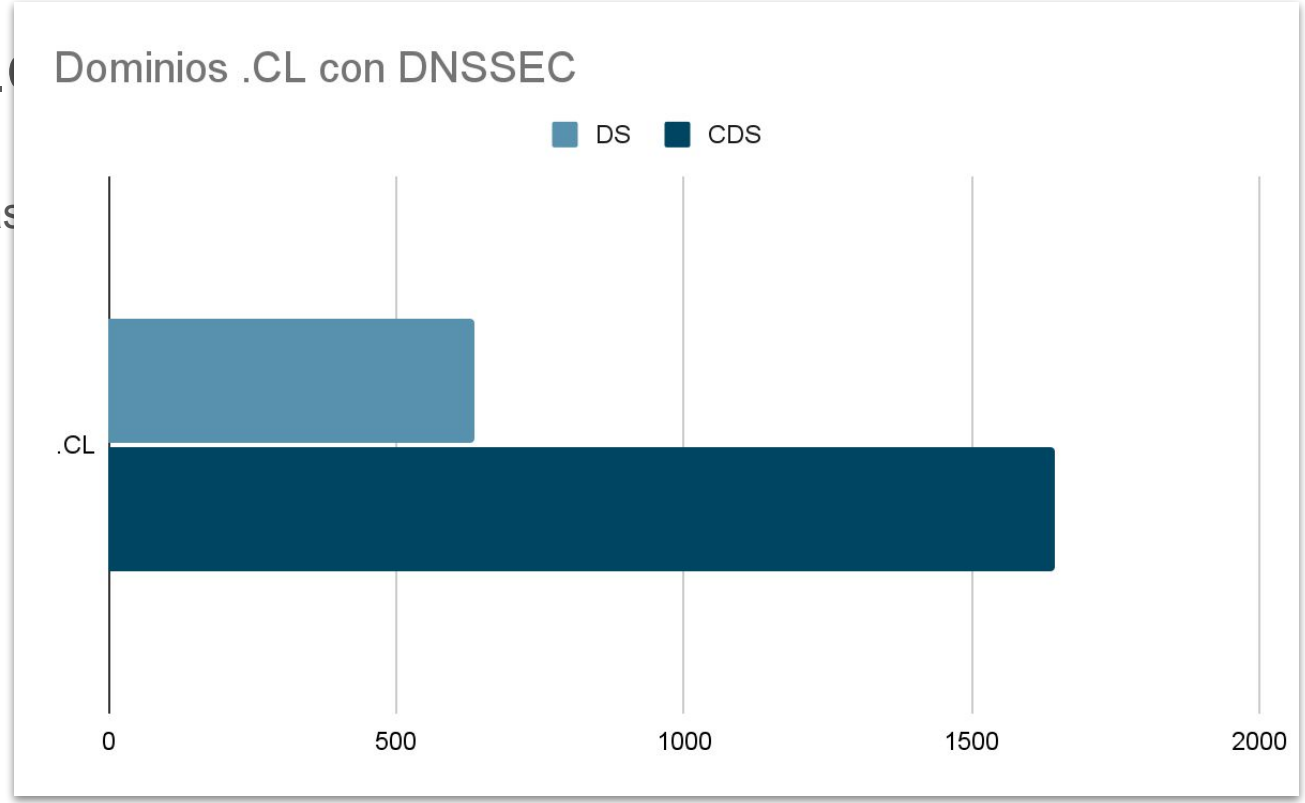
- Ejemplo de algunas configuraciones
    - Bind
        - automático al usar “dnssec-policy”, esperando el timing correspondiente
    - Knot
        - cds-cdnskey-publish: none | delete-dnssec | rollover | always | double-ds

Algunos números

- Caso .CL
    - Casi el triple de los dominios que firma, no envía DS!

Algunos números

- Caso .
  - Cas



Conclusión

- ¡Al fin DNSSEC full automatizado! (fire & forget)
- Esperemos una pronta adopción en TLDs y Registries

Gracias

Hugo Salgado
hsalgado@nic.cl

NIC Chile - .CL