DNSSEC Key Ceremonies

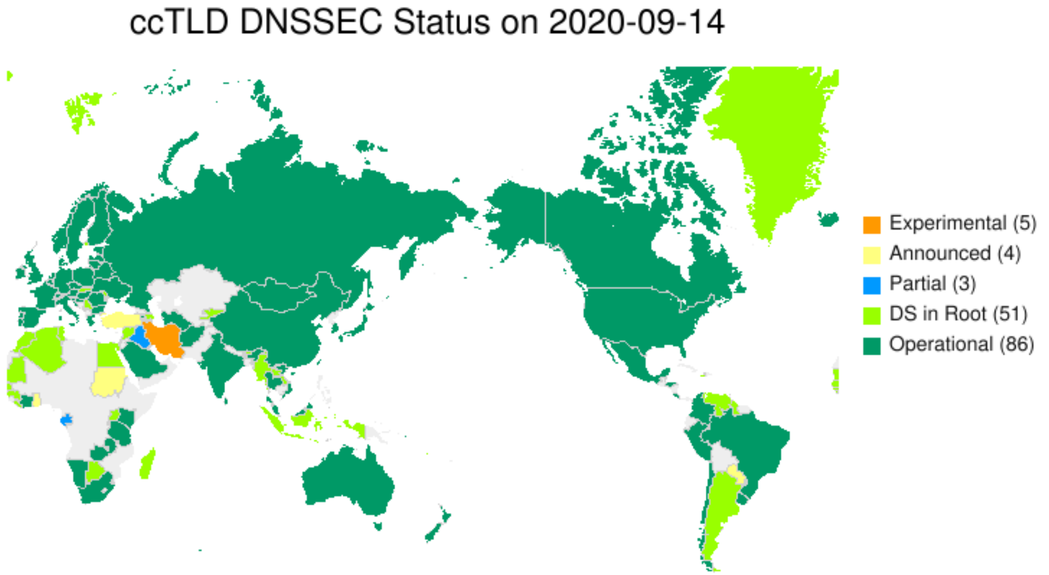
standardising and automating key security

Benno Overeinder

NLNETLABS

Project rationale

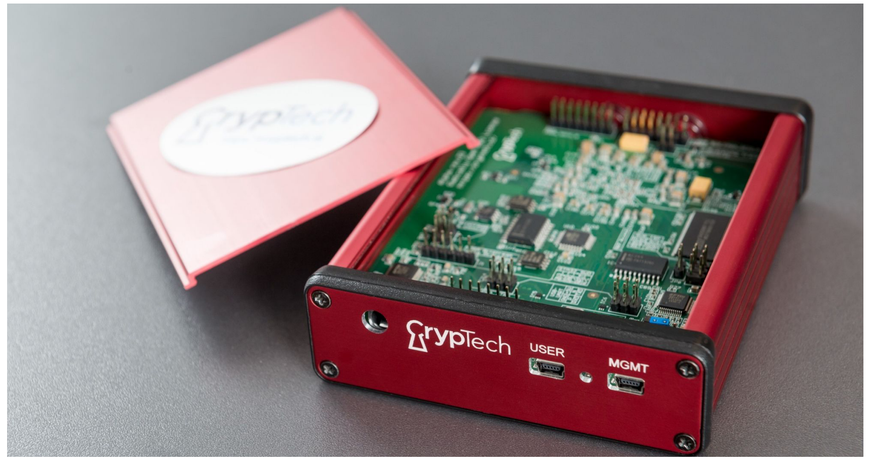
- **DNSSEC** has seen **widespread adoption** over the past decade
- Almost **all top-level domains** are now signed
- High-value domains (such as TLDs) **need strong key protection**
- **Often use HSMs** to protect key material

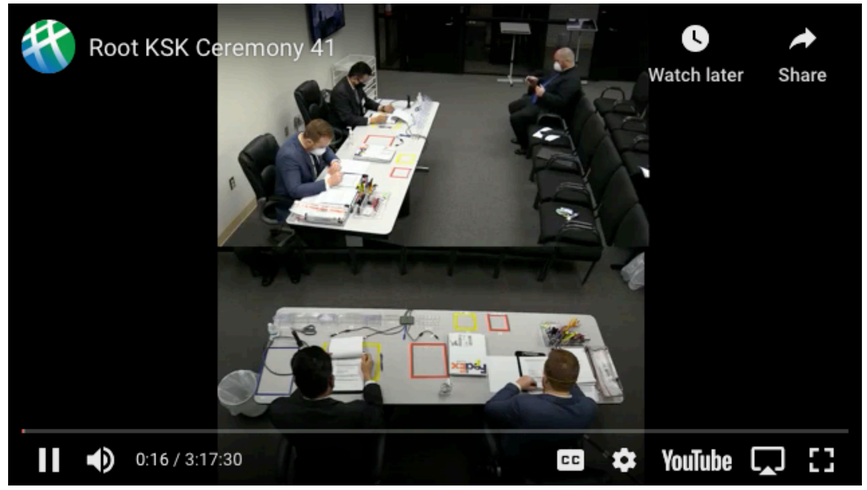


NLNETLABS

Ceremonies

- **HSMs** for high-value domains are often **air-gapped for additional security**
- **Signing with** keys in **air-gapped HSMs requires** a process or **ceremony**
- **E.g.** done **for** the **DNS Root** (organised by IANA)
- **Ceremonies** are **sometimes witnessed** by community representatives or stakeholders



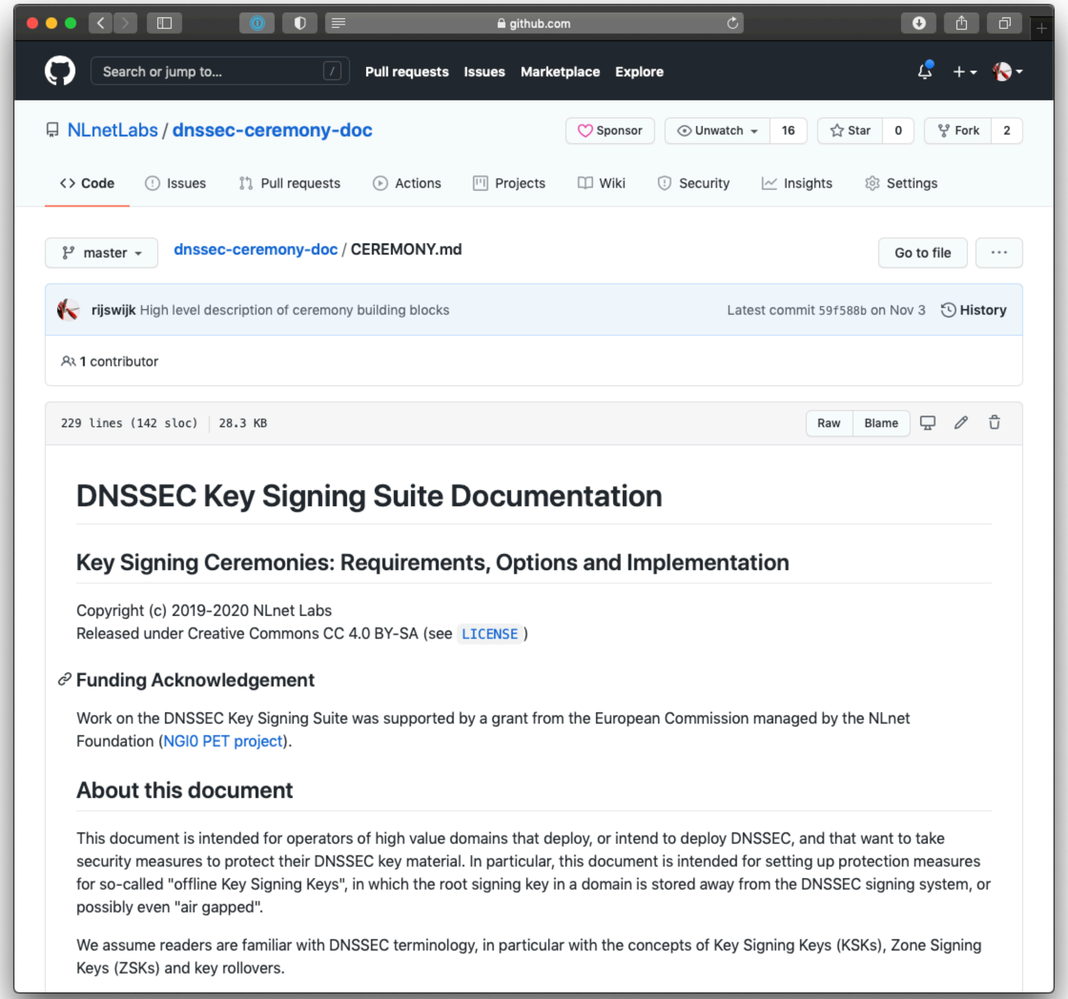


source: https://www.iana.org/dnssec/ceremonies

NLNETLABS

Ceremony requirements & design

- Until now, these **key ceremonies** are **often bespoke in** terms of **process and tooling**
- Making **standardised guidelines** can **help the community**; we documented this
- **Ensure secure ceremonies and** help **automate** the process



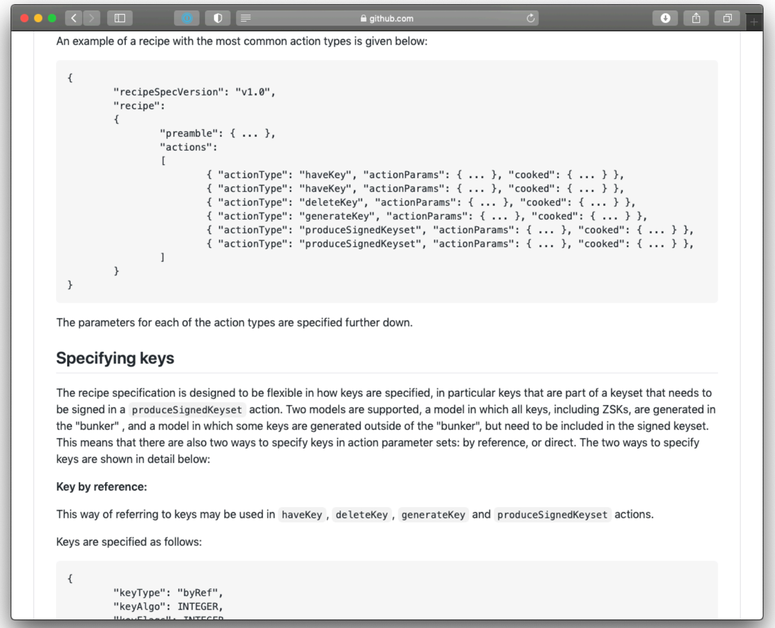
NLNETLABS

Automation with recipes

- **Better standardisation** enables **better automation**

- We introduce the concept of **a "recipe"**; **coherent set of instructions for key ceremony** automation **in** the **secure environment** with the air-gapped HSM

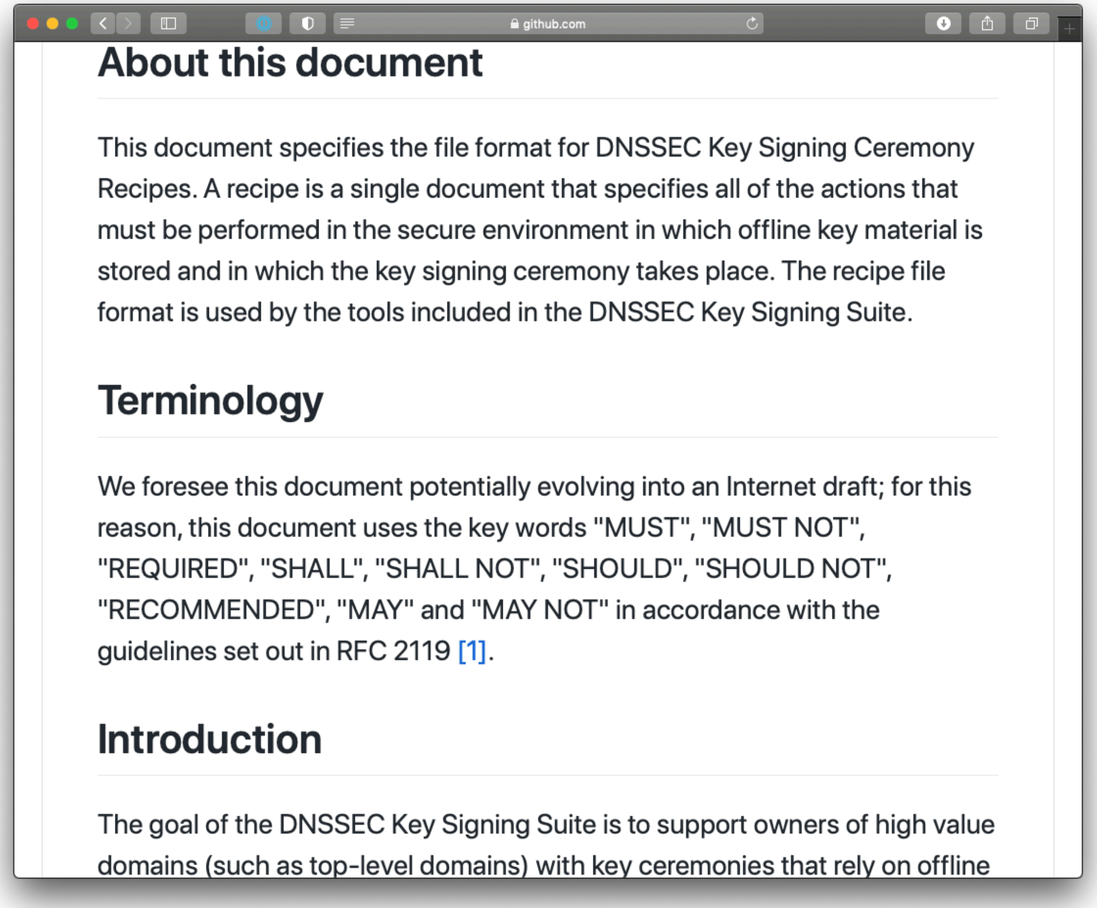
- **Built** the **tools to execute recipes and** prototype **integration with OpenDNSSEC** signer



NLNETLABS

Future work

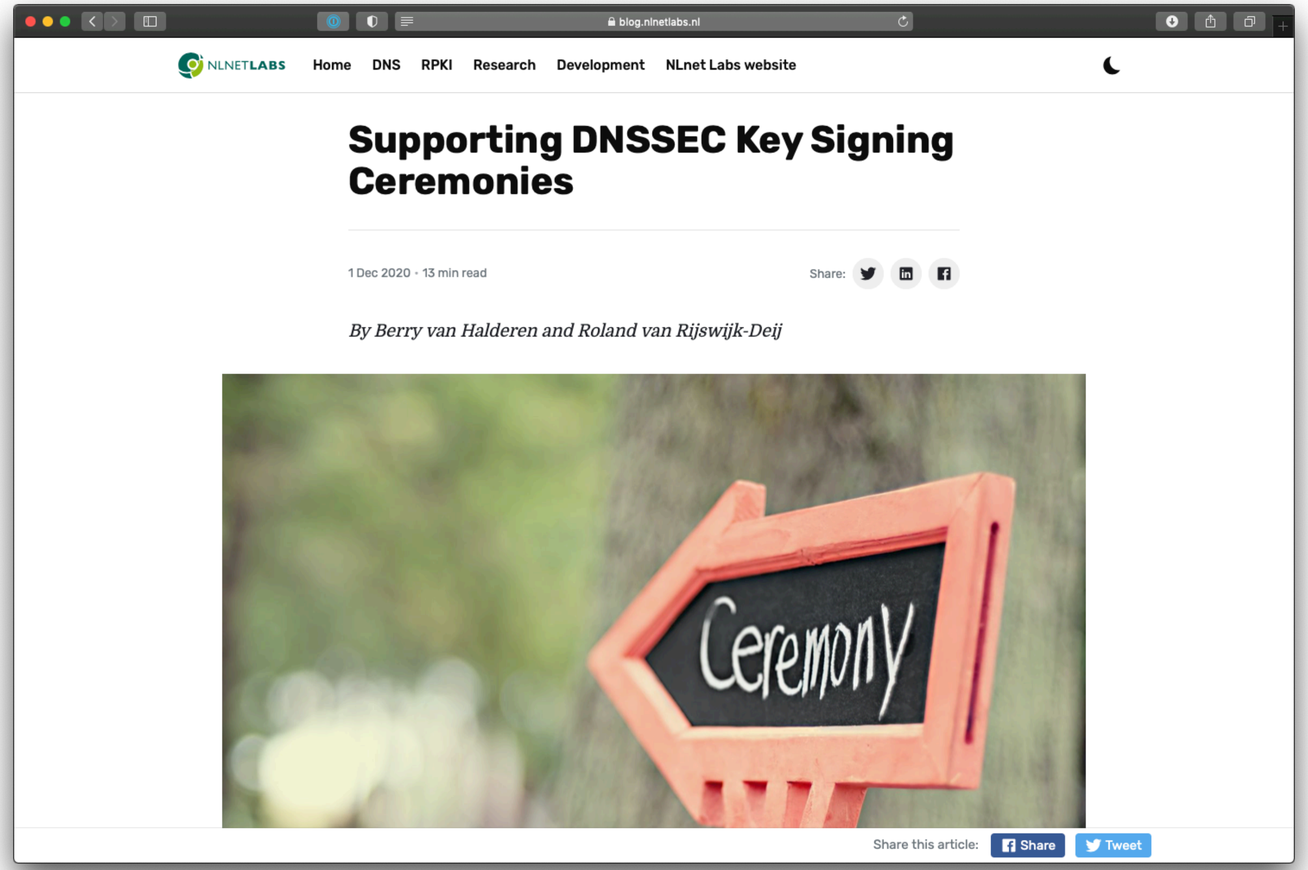
- **Get community feedback!**
- If an interest exists, **take recipe API to IETF** for standardisation
- **Adoption by other** OSS **DNSSEC implementers**



NLNETLABS

Further reading

- We wrote a blog about the project: https://blog.nlnetlabs.nl/supporting-dnssec-key-signing-ceremonies/



Thank you! Questions?

https://nlnetlabs.nl/

@nlnetlabs

labs@nlnetlabs.nl

NLNETLABS