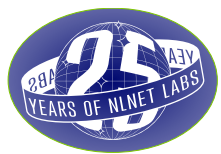


# Flexible Key Management in Nameshed

Philip Homburg [philip@nlnetlabs.nl](mailto:philip@nlnetlabs.nl)



# Nameshed

**name•shed** | 'neɪm ʃɛd | *noun*

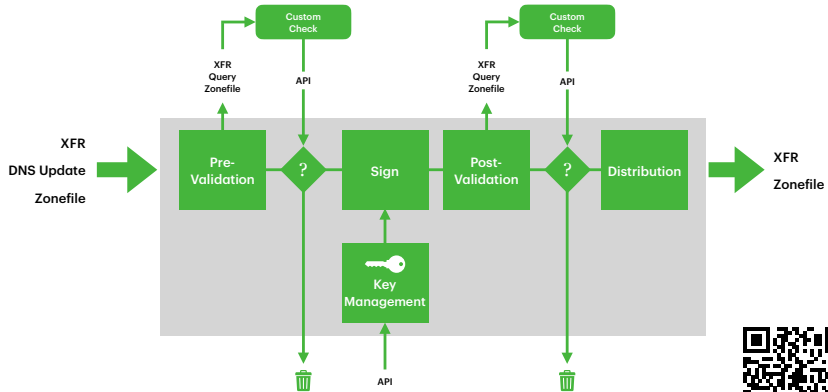
the result of bikeshedding a working title for your DNS software and likely using it as the name you release with. See also, *Unbound*.

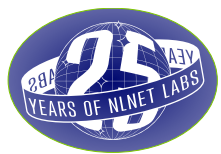
A new DNSSEC-signing solution in Rust

- ▶ OpenDNSSEC has fulfilled its lifetime goals
- ▶ Served the DNS community well for many years
- ▶ Keep the strengths, improve on the weaknesses
- ▶ We intend to announce End-of-Life for OpenDNSSEC this year

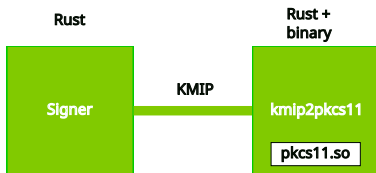


# Nameshed architecture

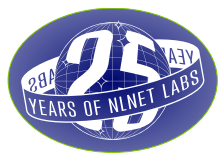




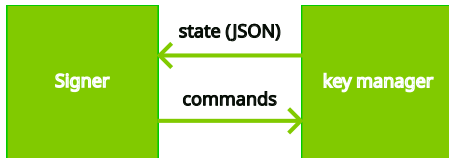
# Isolating PKCS #11



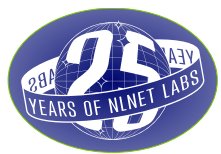
- ▶ Avoid loading an unknown shared library into the signer process.
- ▶ Could provide debugging benefits.
- ▶ Network transparency without tricks.



# Separate key management

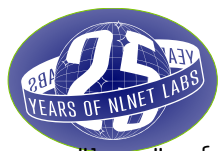


- ▶ Signer signs zone with ZSK.
- ▶ Signer receives signed DNSKEY, CDS, and CDNSKEY RRsets from key manager.



# Empty state file

```
{  
  "keyset": {  
    "name": "example.org",  
    "keys": {},  
    "rollstates": {}  
  },  
  "dnskey_rrset": [],  
  "ds_rrset": [],  
  "cds_rrset": [],  
  "ns_rrset": []  
}
```



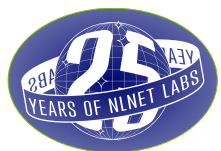
## key in state file

```
"keys": {  
  [...]  
    "Kexample.org.+008+15744.key": {  
      "privref": "Kexample.org.+008+15744.private",  
      "keytype": { "Zsk": {  
        "old": false, "signer": true, "present": true,  
        "at_parent": false } },  
      "algorithm": 8, "key_tag": 15744,  
      "timestamps": {  
        "creation": { "secs": 1749124161, "nanos": 128341254 },  
        "published": { "secs": 1749124161, "nanos": 128355921 },  
        "visible": null, "ds_visible": null, "rrsig_visible": null,  
        "withdrawn": null  
      } } },  
    "rollstates": { "AlgorithmRoll": "Propagation1" }
```



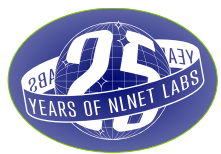
# CSK is slightly different

```
"keys": {  
  [...]  
    "keytype": {  
      "Csk": [  
        { "old": false, "signer": true, "present": true, "at_parent": true },  
        { "old": false, "signer": true, "present": true, "at_parent": false }  
      ]  
    },  
    "algorithm": 8, "key_tag": 9311,  
    "timestamps": {  
      "creation": { "secs": 1749124640, "nanos": 195327403 },  
      "published": { "secs": 1749124640, "nanos": 195357229 },  
      "visible": { "secs": 1749124770, "nanos": 945611300 },  
      "ds_visible": null,  
      "rrsig_visible": { "secs": 1749124770, "nanos": 945611300 },  
      "withdrawn": null } } },
```



# DNSKEY/CDS/CDNSKEY

```
"dnskey_rrset": [  
  "example.org. 3600 IN DNSKEY 257 3 8 [...]"  
  "example.org. 3600 IN RRSIG DNSKEY 8 2 3600 1751543840 1749038240 [...]"  
],  
"ds_rrset": [  
  "example.org. 3600 IN DS 9311 8 2 [...]"  
],  
"cds_rrset": [  
  "example.org. 3600 IN CDNSKEY 257 3 8 [...]"  
  "example.org. 3600 IN RRSIG CDNSKEY 8 2 3600 1751543987 1749038387 [...]"  
  "example.org. 3600 IN CDS 9311 8 2 [...]",  
  "example.org. 3600 IN RRSIG CDS 8 2 3600 1751543987 1749038387 [...]"  
],  
"ns_rrset": []
```



# Questions?

labs@nlnetlabs.nl

<https://blog.nlnetlabs.nl/>

<https://github.com/NLnetLabs/nameshed>

<https://github.com/NLnetLabs/kmip2pkcs11>

