

# DNSSEC Validation Monitor

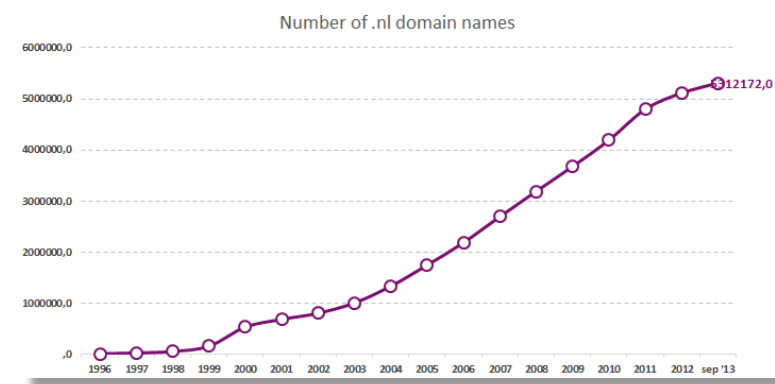
March 26, 2014

DNSSEC Workshop @ ICANN49

Marco Davids and Cristian Hesselman

# SIDN Labs

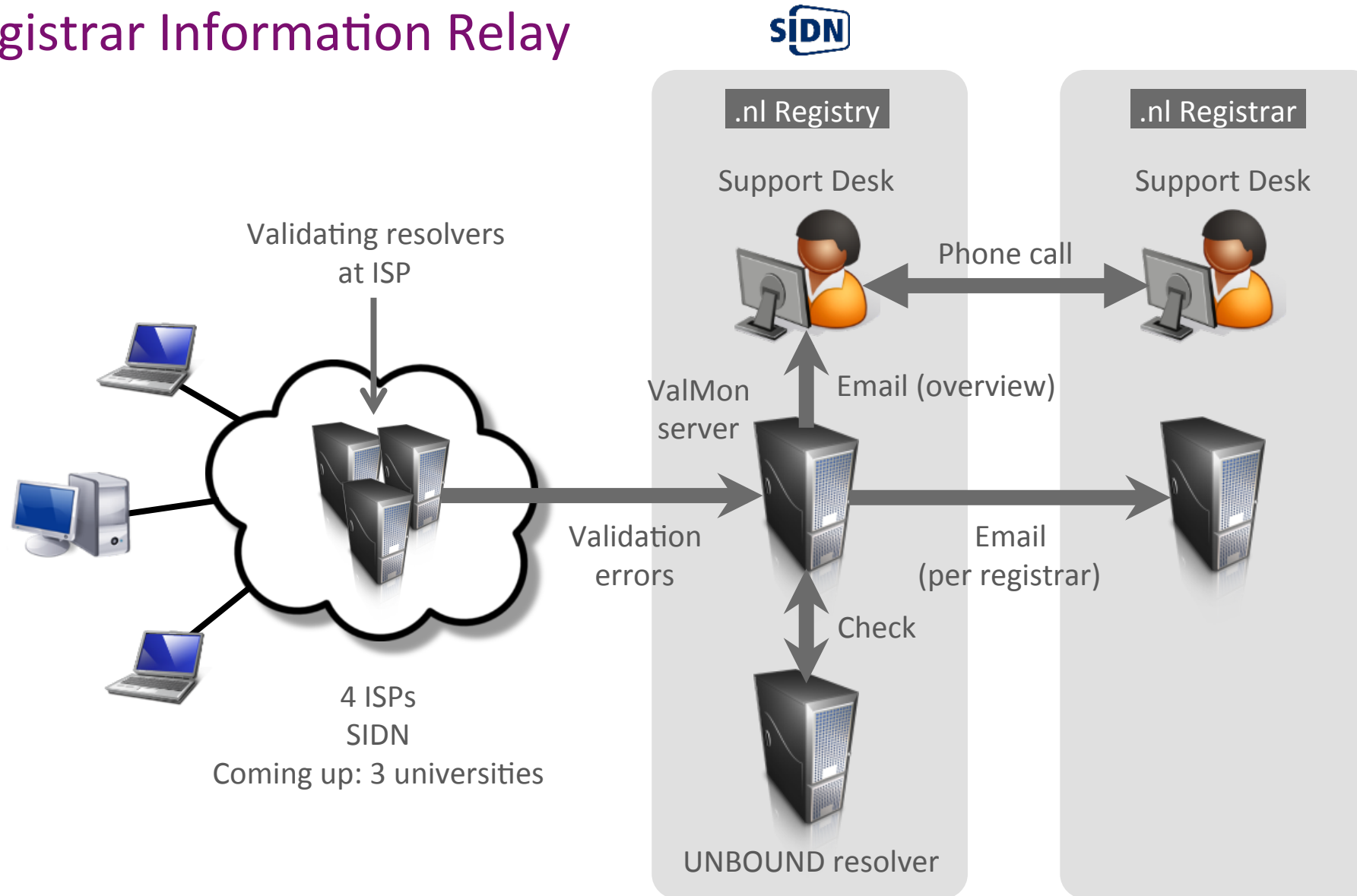
- R&D team SIDN
- SIDN = registry for the Netherlands (.nl)
- 5.4M domain names, 1.500 registrars
- Largest DNSSEC zone in the world (1.7M signed)
- RSP for .amsterdam (capital) and .aw (Aruba)



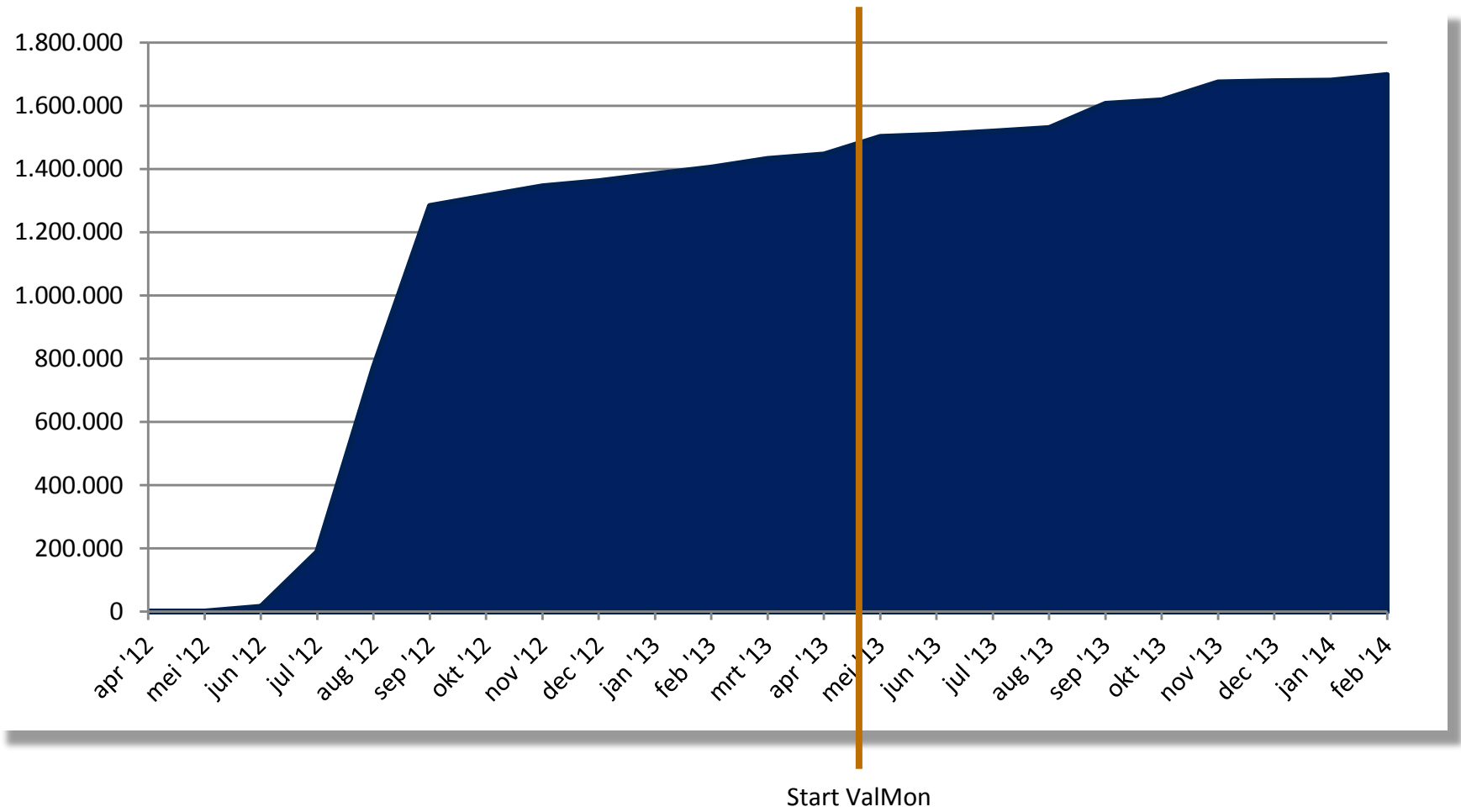
# DNSSEC Validation Monitor (ValMon)

- Experimental service that informs registrars of validation errors occurring at Dutch ISPs for their signed domain names (reduce information asymmetry)
- Goal: reduce validation error rates at Dutch ISPs, thus stimulate adoption of DNSSEC validation
- Motivation: relatively high numbers of validation errors
  - Mostly due to transfers to registrars that do not support DNSSEC (9,6% of transfers, Oct 2012)
  - Other sources: ISPs and DNSSEC Portfolio Checker (<http://portfolio.sidnlabs.nl:8080/form>)
- Low error rates important to ISPs because
  - Validation errors generate support calls (50 EUR/65 USD/76 SGD per call)
  - ISP customers don't understand why a site goes black while it still works via their neighbor's ISP
  - ISPs take the hit for errors (unintentionally) caused by others

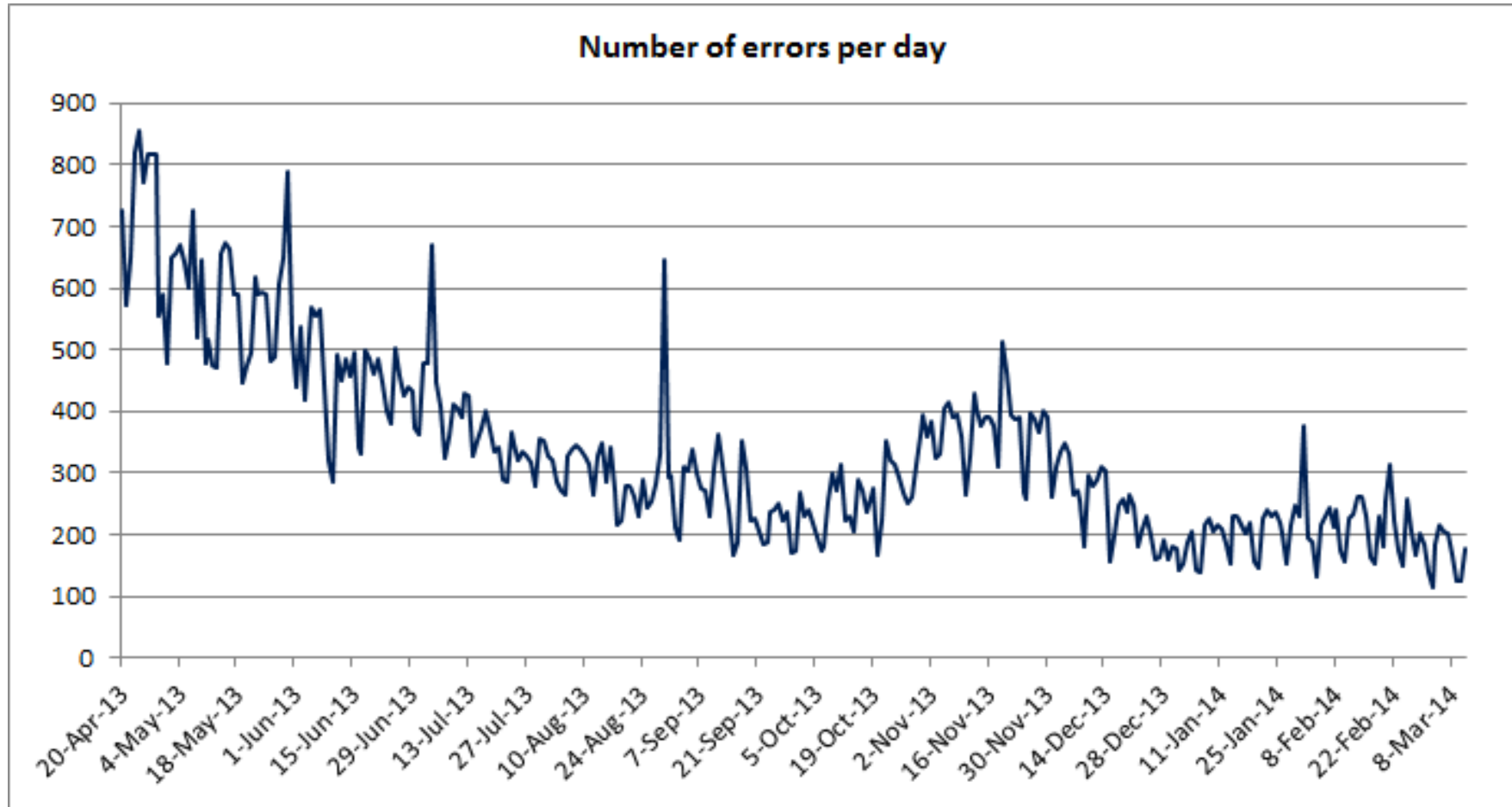
# ISP-registrar Information Relay



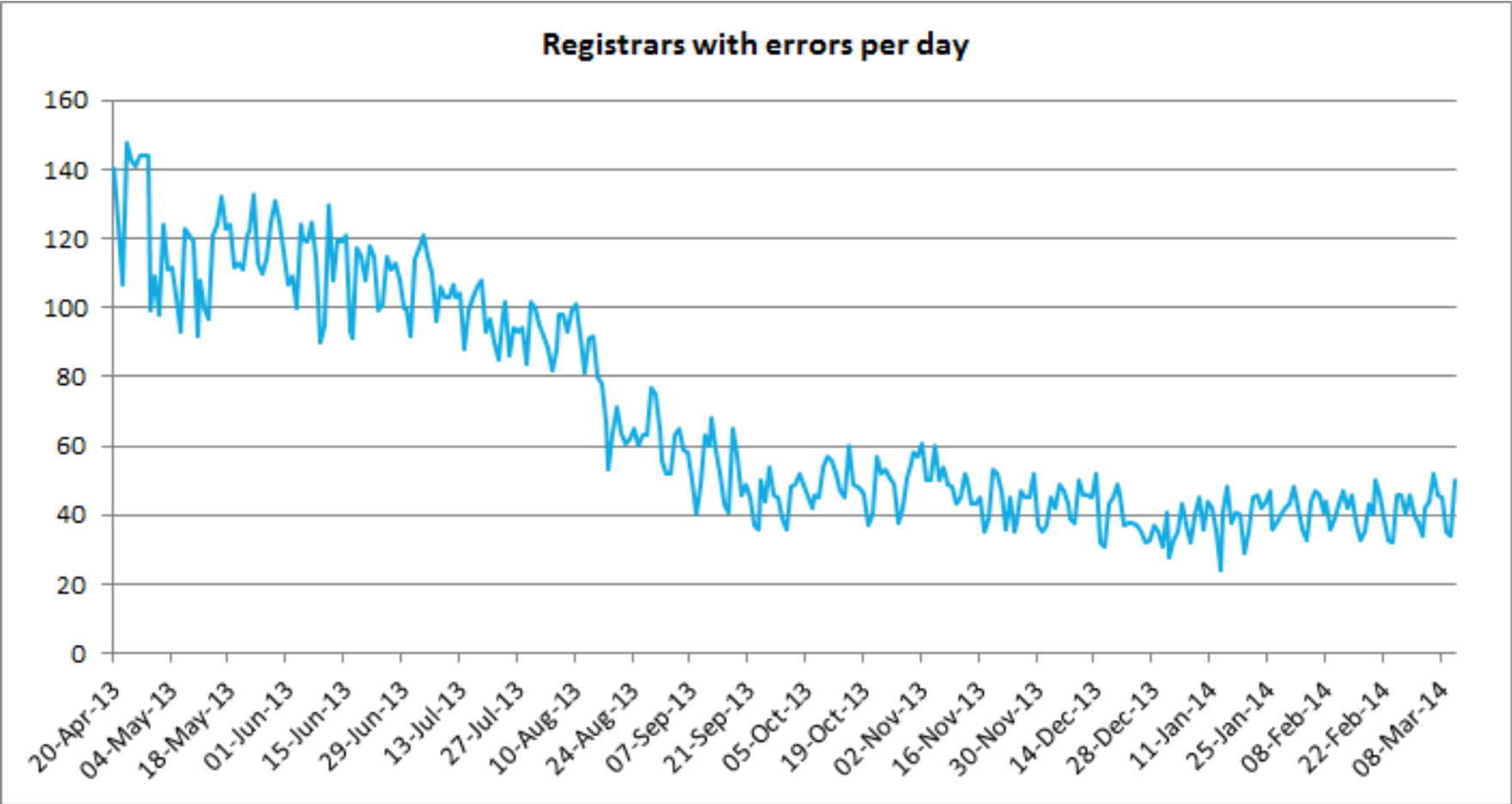
# DNSSEC Signing .nl



# Validation Errors



# Registrars



# Types of Validation Errors

## UNBOUND Error Reports (24 hours)

1 DS got unsigned  
185 No DNSKEY record  
11 SERVFAIL no DS  
57 cname proof failed  
1 covering NSEC3 was  
132 nameerror proof failed  
1 no DNSSEC records  
6 no NSEC3 records  
11 no keys have  
4 no signatures from  
1 no signatures over  
3 nodata proof failed  
7 signature crypto failed  
6 signature expired from  
858 wildcard proof failed

← As a result of domain name transfers

← NXDOMAIN-related errors

← NSEC/NSEC3-related errors

## 3<sup>rd</sup> Level Validation Errors

www.example.nl. [OK]  
\_tsdns.\_tcp.example.nl. [ERROR]



# Lessons Learned

- ValMon appears to work!
- Also seeing validation errors at 3<sup>rd</sup> level, which we would not have seen at the registry-level
- Sites sometimes broken for weeks because registrars don't have a validating resolver themselves
- Errors also caused by resellers, need to stimulate registrars to exercise more control over their resellers

# Questions?

Marco Davids

[marco.davids@sidn.nl](mailto:marco.davids@sidn.nl)

Cristian Hesselman

[cristian.hesselman@sidn.nl](mailto:cristian.hesselman@sidn.nl)

[www.sidn.nl](http://www.sidn.nl) | [www.sidnlabs.nl](http://www.sidnlabs.nl)

