DNS/DNSSEC/DPRIVE

- IETF 96 Hackathon

- Problem Solved – DNS security and privacy enhancements and interoperabilty

- Method of Solution – multiple user stories, multiple open source prototypes

Highlight 1: DNSSEC Transparency

- Like Certificate Transparency, but with DS posts instead of X.509

  - draft-zhang-trans-ct-dnssec

- Server running as of 5AM (see Linus' tweet)

- Client is talking to the server (Go and Miek's DNS library)

- Server is Erlang with getdns

- Linus, Daniel & MC

Highlight 2: DNS64

- A v6-only endpoint now has support for DNS64

- Addressing issues identified by Jen Linkova (Google) presentation at RIPE 72

- Coming soon: test this from getdnsapi.net/query.html

- Identified several high-profile DNSSEC-signed sites from Alexa 1M that do not support IPv6 (including mail.com)
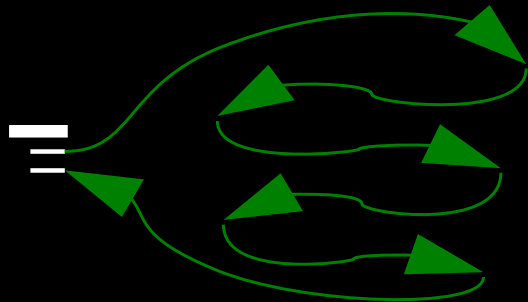
Highlight 3: Universal Access reviews

- **getdns**: Good support but not 100% compliant yet (solution identified for next release)

- **systemd-resolved** service

  - hmm.. first experiments with D-Bus interface show it doesn't work, even though is documented that it

```
▼ Domain Name System (query)
    [Response In: 4]
    Transaction ID: 0x0437
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▼ \346\231\256\351\201\215\346\216\245\345\217\227-\346\265\213\350\257\225.\344\270\226\347\225\214: type A, class IN
        Name: \346\231\256\351\201\215\346\216\245\345\217\227-\346\265\213\350\257\225.\344\270\226\347\225\214
        [Name Length: 26]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Team Participants

- John Dickinson, SINODUN

- Sara Dickinson, SINODUN

- Daniel Kahn Gillmore, ACLU

- Jim Hague, SINODUN

- Shumon Huque, Verisign

- Shane Kerr, BII

- Rick Lamb, ICANN

- Ed Lewis, ICANN

- David Lawrence, Akamai

- Jerry Lundström, OARC

- Allison Mankin, Salesforce

- Linus Nordberg, NORDUnet

- Joel Purra, Consultant

- Benno Overeinder, NLnet Labs

- Melinda Shore, No Mountain

- Andrew Sullivan, DYN

- Ondřej Surý, CZ.NIC

- Willem Toorop, NLNet Labs

- Paul Wouters, Red Hat

- Mohammad Hassan Zahraee, University of Paderborn

- Daniel & MC, Netno

- GREEN – first Hackathon, new to IETF

Project List

- Continued work on dnssec-chain-query in BIND
- Full implementation (Javascript) of Shane's dns-http draft
- Implementation of draft-pauly-ipsecme-split-dns, will interop with Apple implementation this week
- Python module for query triggering the IPSEC tunnel
- Implementation of DNS64 in getdns
- Multiple getdns bindings (Perl, Python updates, node.js, Go)
- Universal Access reviews
- RFC 7858 (DNS-over-TLS) engineering and interop (getdns, Unbound, Knot)
- Review and re-design of getdns Universal Access functions
- Soft HSM

More Highlights
(not presented)

getdns Bindings

- More work on node.js and Python

- Perl bindings started here and almost finished!

- Go binding started…basics are working!

- Also, start of native Go implementation of the getdns API functions

Perl Bindings for getdns

- Net::GetDNS 0.01 released

- Contains Net::GetDNS::XS with >70% implemented getdns interfaces

- Async lookups to anonymous Perl sub's works

https://github.com/DNS-OARC/p5-Net-GetDNS

Go Bindings for getdns

- Go wrapper in the style of Python

- Why? Way quicker solution to produce than native implementation (with a performance hit?)

- Basic queries working, output from getdns response dict in Go Lists and Maps will be available here:

    - https://portal.sinodun.com/stash

- Relative Go newbie managed this during Hackathon!

DNS-over-TLS

- Security work on better socket privilege management in debian for DNS-over-TLS servers

- Knot resolver DNS-over-TLS support almost ready for merge into main code

- kdig tool is getting DNS-over-TLS added as we speak