# DNSSEC Operations

Domain Transfers

# What’s in a domain?

- “Domain name” is a technical term in the DNS relating to a namespace
- Uniqueness of names is maintained by a system of registries
- There’s a common structure registry -> registrar -> registrant
- The provider that does DNSSEC signing (and holds the private keys) can be different
- The provider that serves the resulting zone in the DNS can be different
- The people that manage content or services associated with a domain can all be different

# Transferring a signed domain

- “Transfer” is a registry operation
  - We can transfer an existing domain from registrar A to registrar B
  - Before the transfer, registrar A is responsible for making changes in the registry with respect to the domain
  - After the transfer, registrar B is responsible
- The kind of data that we might want to update include DNS servers and DS record sets
- In principle, changing the registrar (transferring a domain) is straightforward and doesn’t matter whether the domain is signed or not. The DNS is not affected

# None of this matters in the real world

- Domain names are things people buy from web designers
- Credentials for interacting with registrars can be held anywhere
- Registrars are a competitive business, and often provide DNS hosting, web pages from templates, e-mail forwarding, other services
- Many registrars have resellers
- No actual registrant has ever heard of the word registrant
- Nobody knows who is involved in any of this
  - “Ask Tony in Marketing, he generally sets up our web sites”

# What can go wrong?

- If the losing registrar supports DNSSEC but the winning registrar does not, your DS RRSets might become marooned
  - Unable to change DS RRSets (no KSK rolls)
  - Unable to remove DS RRSets (no going unsigned)
- If the registrars provide DNS hosting, including signing, the ability to create signatures with the old key might be lost
  - Losing registrar and winning registrar need to cooperate to effect a KSK roll between providers, unless they can share all their key material with each other
  - There are timing issues
  - There is no agreed automation
  - There is no real expectation or requirement that they will cooperate

# Isn’t this a problem?

- Lots of people think it is
  - The people who don’t think it is also don’t really know anything about DNSSEC
- The trouble is that the problem really results from a rich and varied ecosystem of businesses and functions that tie a domain name at a registry to the people who are using it
  - The registry-registrar-registrant model sounds elegant and simple, but it isn’t
  - Even if it was elegant and simple, it’s a tiny piece of the picture
- So as someone who depends on domain names and who has decided to use DNSSEC, what should I do?

# Pragmatic Advice

- Keep track of who your suppliers are
  - Understand the particular collection of vendors that corresponds to your web page, or e-mail service, or whatever: registrars, resellers, web designers, service consultants, ISPs
  - Understand who is responsible for signing your zone
    - Who keeps the private keys
- If you sign your zone yourself (your private keys) you are in control
  - Chances are that domain transfers and changes in DNS hosting are easy
- For everybody else
  - Make sure you know how to go insecure (remove DS RRs from parent zone)
  - Go insecure before you make changes to your (e.g.) registrar
  - Re-implement DNSSEC afterwards

# Effect on your Users

- People use resources published insecurely in the DNS all the time
  - Most zones on the Internet are not signed
  - Few zones that people use the most are signed, because offering services at Internet-scale often relies upon unusual, custom DNS software that doesn't support DNS
- Remember that DNSSEC allows relying parties to know whether they should expect something to be signed
  - Without a DS record set in the parent, there is no expectation of signatures in the child
- Being prepared to go insecure is operationally necessary anyway
  - It's a reliable defence against unexpected disasters
  - Build it in to your disaster recovery plan