

# Deploying DNSSEC

From a registrar perspective

# Loopia

- The largest registrar of .se-domains
- The world's first registrar to deploy DNSSEC
- One of Sweden's largest DNS-Operators with 500.000 authoritative zones
- Situated in Västerås, about 100km from the capital city of Sweden, Stockholm
- Founded in 1999, named Loopia since 2000
- Organical growth from two to twenty employees
- Part of the Mamut organization since 2007



# Why would a registrar deploy?

- DNSSEC adds (some of) the needed security to the domain names system
- DNSSEC gives you a marketing advantage!
- You will have to, sooner or later?
- You actively work for progress of the Internet
- There is no actual reason not to deploy DNSSEC!



# Are there any reasons to wait?

- Your local ccTLD is not supporting DNSSEC (yet)
  - Still, keep DNSSEC in mind when you...
    - Recruit new employees
    - Look at new software choices
  - Many TLD's is in the process, be ready!
- The resolver operators in your country is not supporting DNSSEC
- Lack of in-house expertise
  - It's out there, go and get it!
  - It's better to be well prepared before starting



# Planning DNSSEC

- Create your own plan for how to deploy DNSSEC
  - Gather information from other parties involved in DNSSEC
    - Registrys
    - Registrars
    - IETF, RIPE, ICANN etc
  - What different ways of doing DNSSEC is there?
    - In-house software development
    - Open source software
    - Buy it in a box



# Planning DNSSEC

- Create your own plan for how to deploy DNSSEC
  - In what manor do you want to supply DNSSEC?
    - What level of customer involvement do you want?
    - What kind of customers do you have?
  - What is the first problem your will run into?
    - Expertise
      - Make sure it's not a single point of failure!
    - Locked to software
      - Separate system for DNSSEC?



# Advice during planning

- The typical end user does not...
  - Need "DNSSEC", they need security!
  - Know what a KSK or ZSK is or does!
  - Need to know what a KSK or ZSK is or does!
- Make sure you create a DNSSEC implementation that is extendable
  - Do not create a system for one specific TLD
  - Make sure your system can handle more than one policy regarding keys
  - Adding new hardware should be easy
- Create a policy statement regarding handling of keys (draft-ljunggren-dps-framework-01)



# Advice during deployment

- Get outside opinions during each phase of deployment
- Tag along in development of the software you are using
- Test each part of the system AND what happens if that part goes down
- Try to avoid as many "single point of failure" as possible
  - How quickly can you get a new signer up and running?
  - What happens if you're provisioning fails during an extended period?
- How many zones can you sign/serve before you need more hardware?
  - You don't want your (lack of) hardware to break your policy's for you

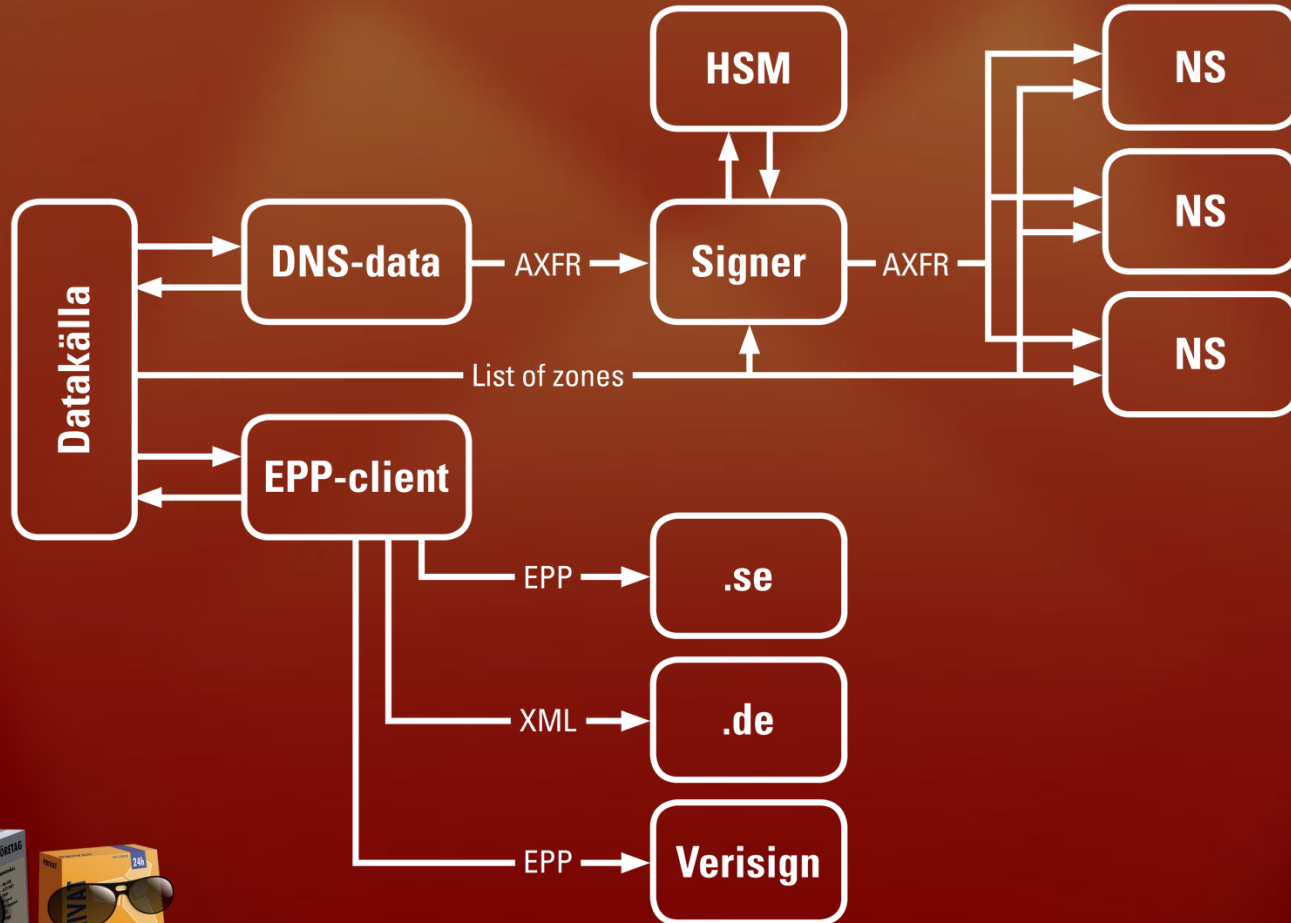


# DNSSEC... Huh?

- Make sure everyone in your organization has at least a clue about DNSSEC!
  - It's an old standard, originated in the 90's
  - Low interest and flaws pushed it into the new millennia
  - It's an "extension" that adds a layer of security to the domain names system
  - The goal was to make it harder to falsify information about a domain name
  - This is done by signing information with keys publicly available
  - The system protects your domain name from several severe risks
  - It is however not a remedy for all evil
  - DDOS-attacks will still shoot you out of the sky



# DNSSEC, the loopia way!



Questions?



Lars-Göran Forsberg  
Registrar Manager

*[lars-goran.forsberg@loopia.se](mailto:lars-goran.forsberg@loopia.se)*  
+46 (0)21 - 470 82 04