DNSSEC Example by .BG

nothing fancy, but it works

For DNS Registries

Daniel Kalchev

Why implement DNSSEC?

- DNSSEC is an logical extension to the DNS protocol. Call it DNSsec(ond) generation?
- Provides assurance that DNS data is authentic.
- Protection against common DNS attacks.
- Improves registration quality. Important component of the DNS Registry practice.
- Introduces more discipline in the process of DNS service provision. No more half-baked DNS.
- Not so much about 'security' but more of 'quality' improvement for the DNS.

DNSSEC: ingredients
(or what you need to deploy DNSSEC)

- DNSSEC support in nameserver infrastructure.
- Key creation/management platform.
- Signing keys security.
- Key management policy.
- Appropriate zone signing platform.
- Automated zone signing.
- Automated key rollover process.
- Signature delegation policy.

DNSSEC support in nameserver infrastructure

- Major authoritative nameserver vendors already provide DNSSEC support:
  - BIND9
  - NSD
  - Nominium
  - Secure64
  - If you use non DNSSEC aware server, complain to your vendor! DNSSEC is not something new.
- Verify your nameservers are compliant
- Plan for possible server / bandwidth upgrades.

Key Creation/Management

- Need to securely create quality KSK and ZSK pairs.
  - Good entropy source
  - Crypto accelerators
  - Key pools
- Chose adequate key sizes
- Support key rollovers by keeping status and history.

Signing keys security

- Need to protect the private KSK.
  - smartcards, tokens, tamper proof devices; split keys; encrypted files; ZSK keysets; network segmentation
  - better to destroy/lose the key than disclose it!
- Hiding the private KSK in a safe does not protect you from data corruption (registry database compromise).
- Significant issue while the DNS root is not signed.
- ZSK can be rotated frequently / at will.

Zone signing platform

- Adequate/sufficient signature performance to meet your update frequency needs.
  - Signatures have lifetime. No need to resign often.
  - ZSK key size influences performance greatly.
  - Sign the complete zone or asynchronously sign resource records.
  - Centralized or distributed signer architecture.
  - Commodity or specialized signing hardware.
- Choice of open source and commercial software available.

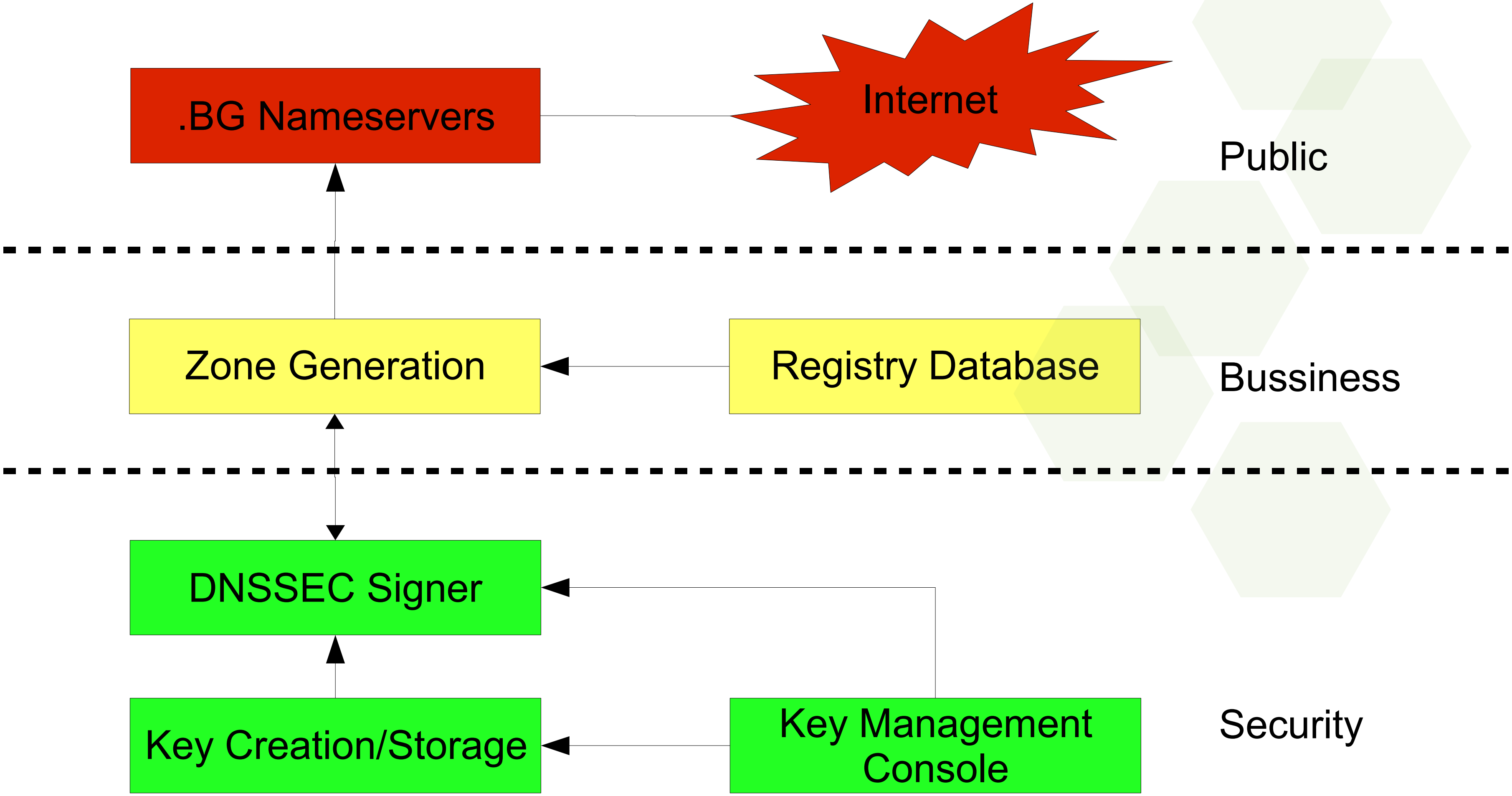
Automated key rollover process

- Automate as much as possible.
- Design appropriate database and tools to keep track of rollovers. Keep key history and status;
- Prevents/reduces human errors.
- Eases deployment, introduces security and stability.
- Easy to implement and strongly suggested for ZSK key rollover.
- If you do not automate: forget about DNSSEC!

Signature Delegation Policy

- DS records are DNS delegation records just like NS records.
- Similar procedures for authentication and handling as for NS records are expected.
- DNSSEC provides chain of trust – a form of open PKI based on the DNS hierarchy.
- Future might introduce new form of SSL certificates, integrated with DNSSEC delegations.
- Many new services made possible.

.BG zone
DNSSEC Signing Infrastructure



Thank You

Remember: DNSSEC does not bite!(c)

Daniel Kalchev
daniel@digsys.bg
https://www.register.bg