OpenDNSSEC

Matthijs Mekking

NLnet Labs

DNSSEC

NSD

IPv6 shim6

ldns

Autotrust

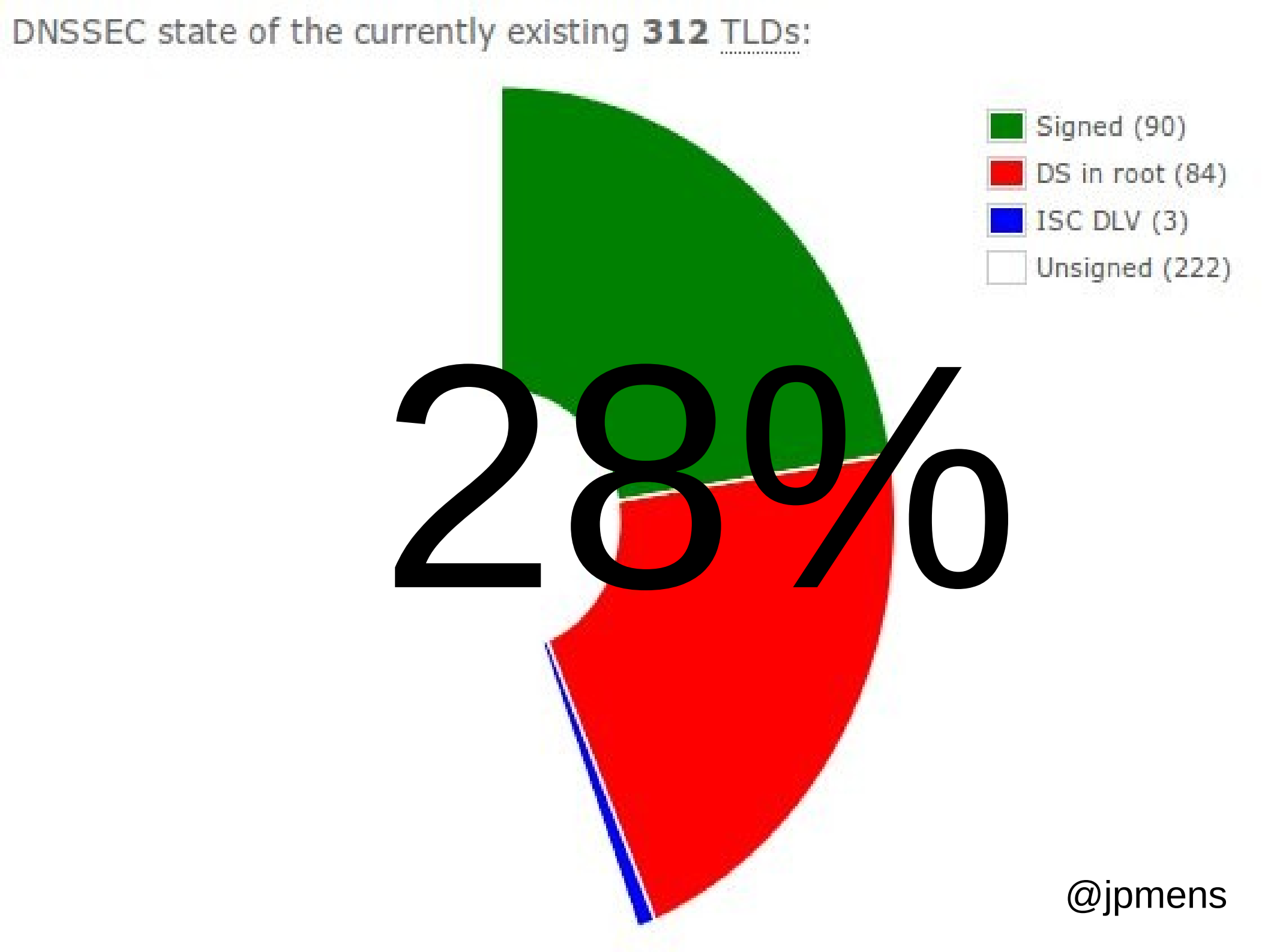
DNSSEC

PKI on top of DNS

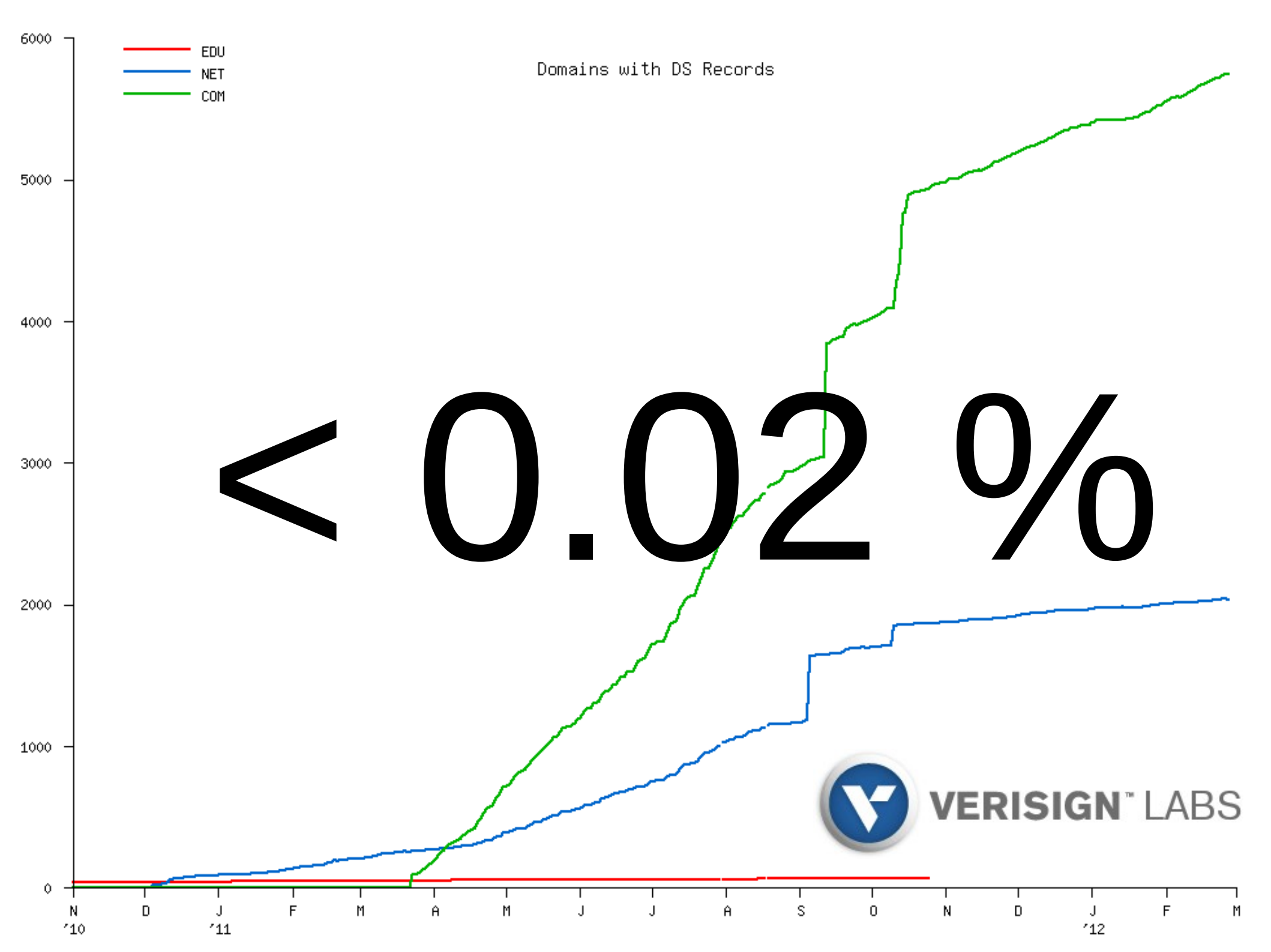
To protect against Cache Poisoning

Kaminsky Attack boosts DNSSEC Deployment

DNSSEC state of the currently existing **312** TLDs:



@jpmens


EDU
NET
COM
Domains with DS Records
6000
5000
4000
3000
2000
1000
0
N
D
J
F
M
A
M
J
J
A
S
O
N
D
J
F
M
'10
'11
'12
< 0.02 %
VERISIGN™ LABS

DNSSEC

comcast

T · ·Mobile·

DNSSEC

New opportunities for innovation of trust on the network

- DANE

DNSSEC

Maintaining DNSSEC != Maintaining DNS

- Signature renewal
- Key rollover
- Bigger impact on error

DNSSEC

Thanks Carsten Strotmann (Men and Mice)
for this analogy


Open
DNSSEC

What?

OpenDNSSEC is a complete DNSSEC zone signer that automates the process of keeping track of DNSSEC keys and the signing of zones.

Who?

.se

kirei

nominet

sinodun

SIDN

NLnet Labs

SURF NET

Why?

The available DNSSEC tools were lacking

- Key management
- Policy handling
- Hardware acceleration

Easy to deploy, increase number of users

BCP based on previous experiences

OpenDNSSEC

Open Source

BSD Licensed

Simplifies signing zones

Reduce work load of DNS administrator

Fits in existing infrastructure

Bump in the wire

Key Storage

Hardware acceleration

PKCS#11

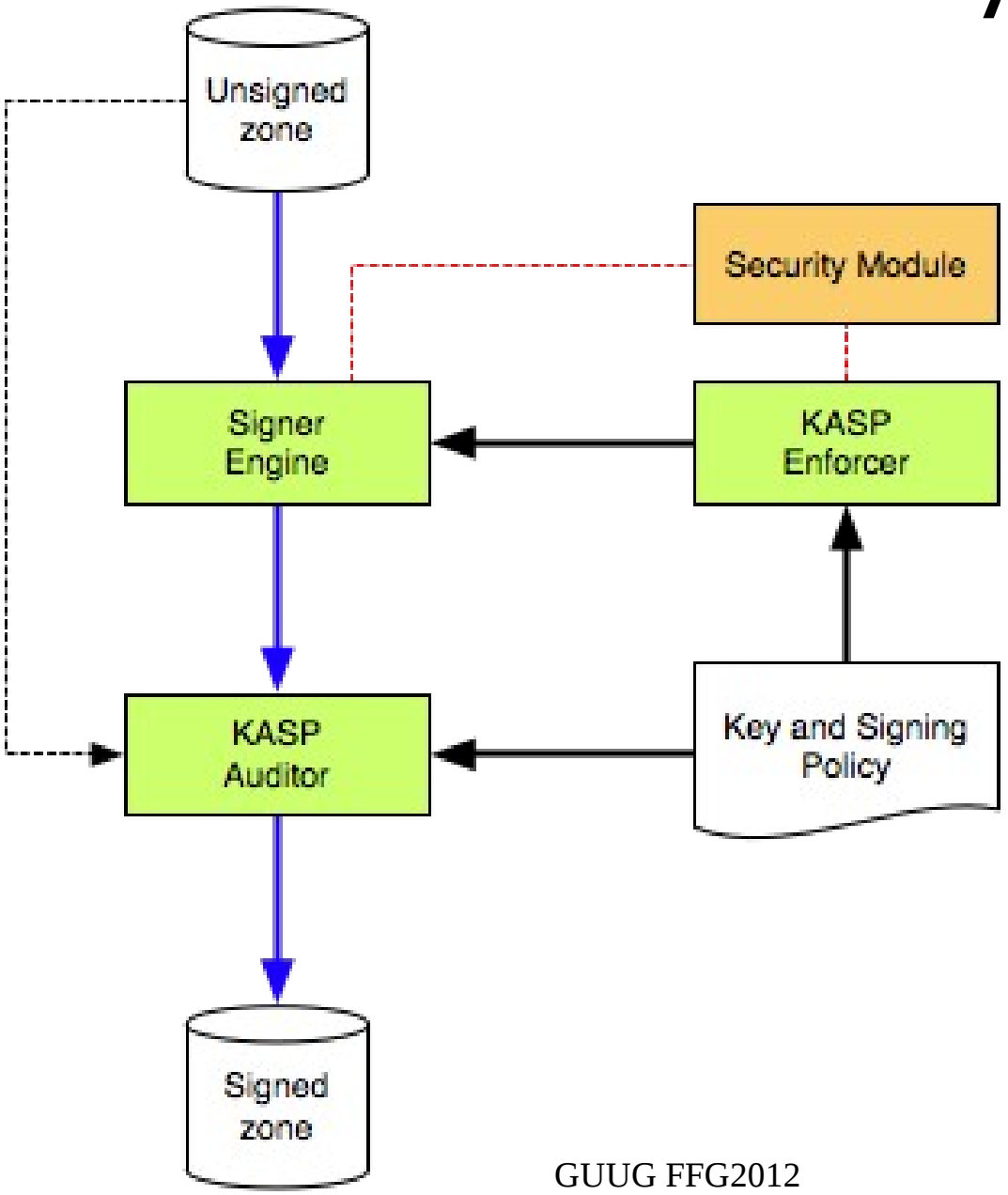
Bump in the wire

Hidden Primary Master (unsigned)

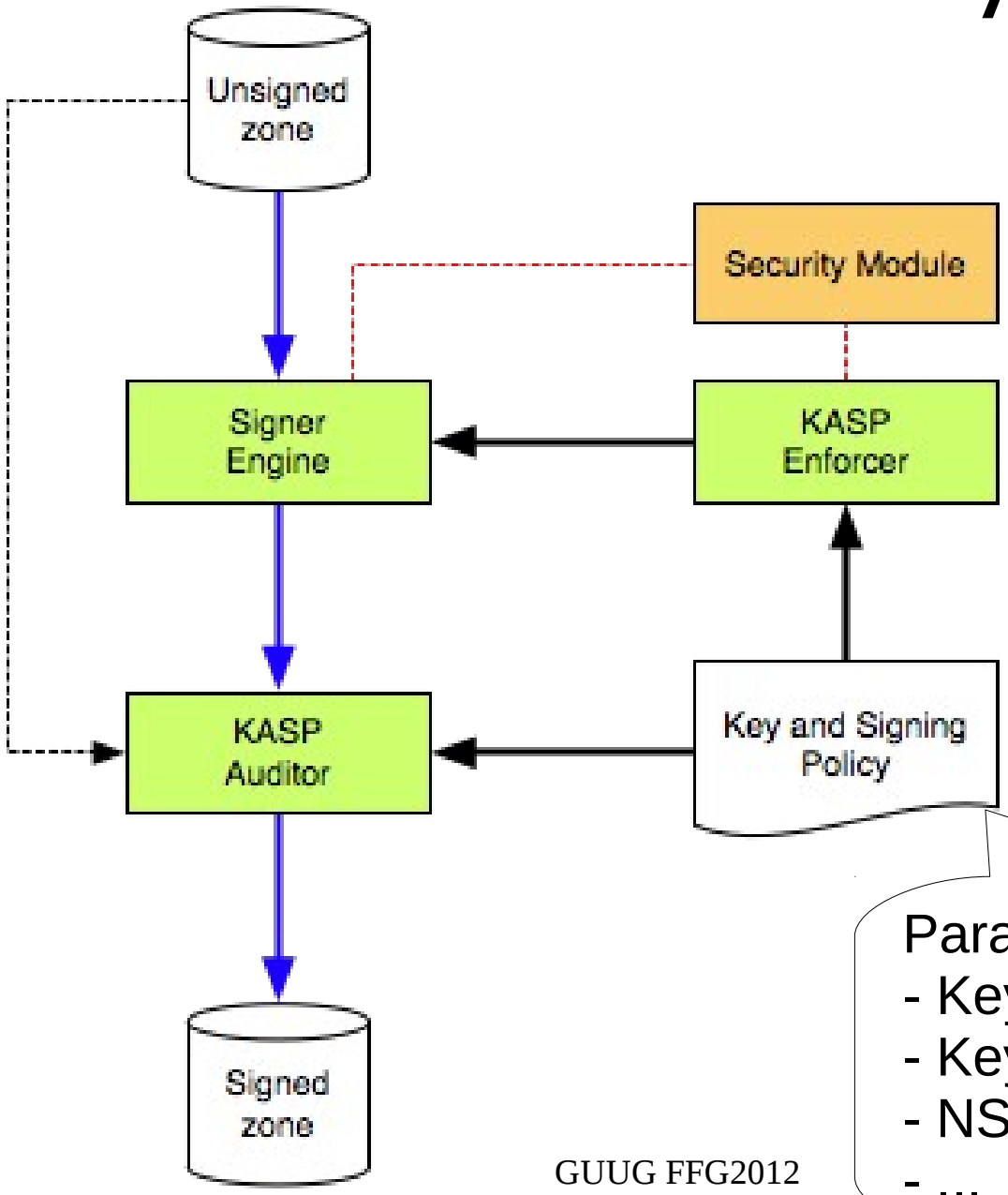
OpenDSSEC

Secondary Servers (DNSSEC)

Architecture

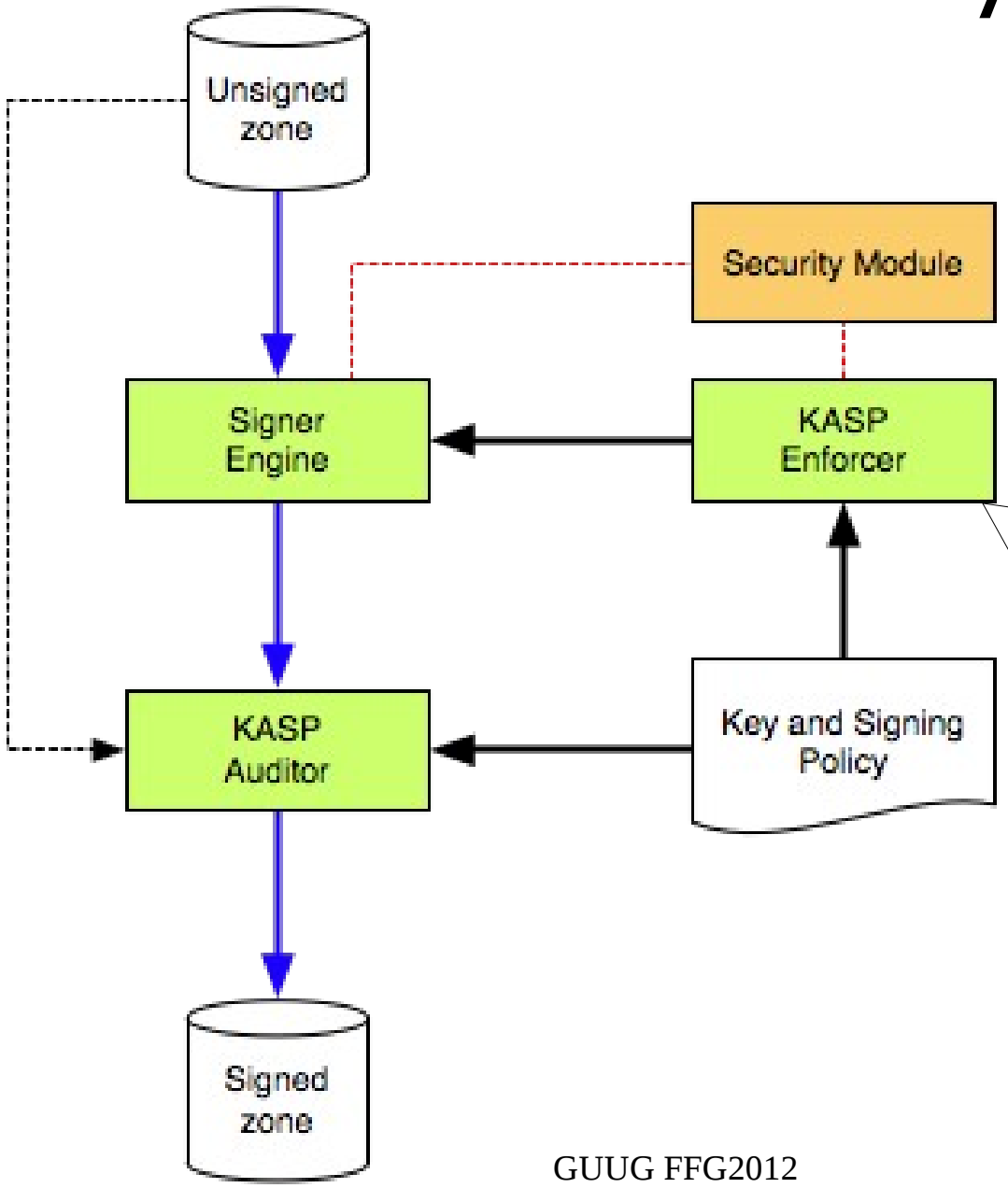


Architecture



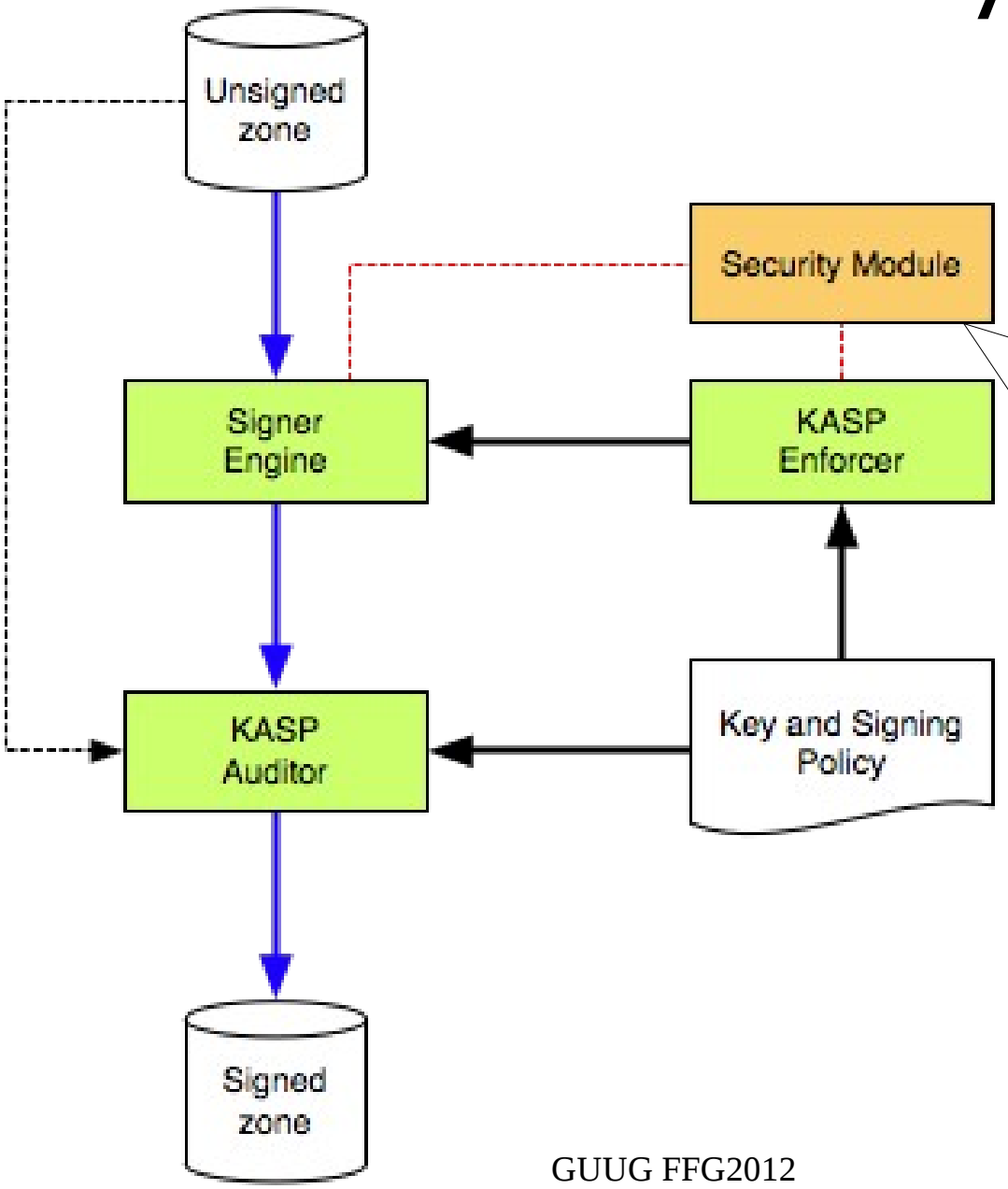
Parameters for zone signing:
- Key algorithm, strength
- Key rollover frequency
- NSEC/NSEC3
- …

Architecture



- Implements policy
- Key maintenance
- Creates keys
- Key rollover

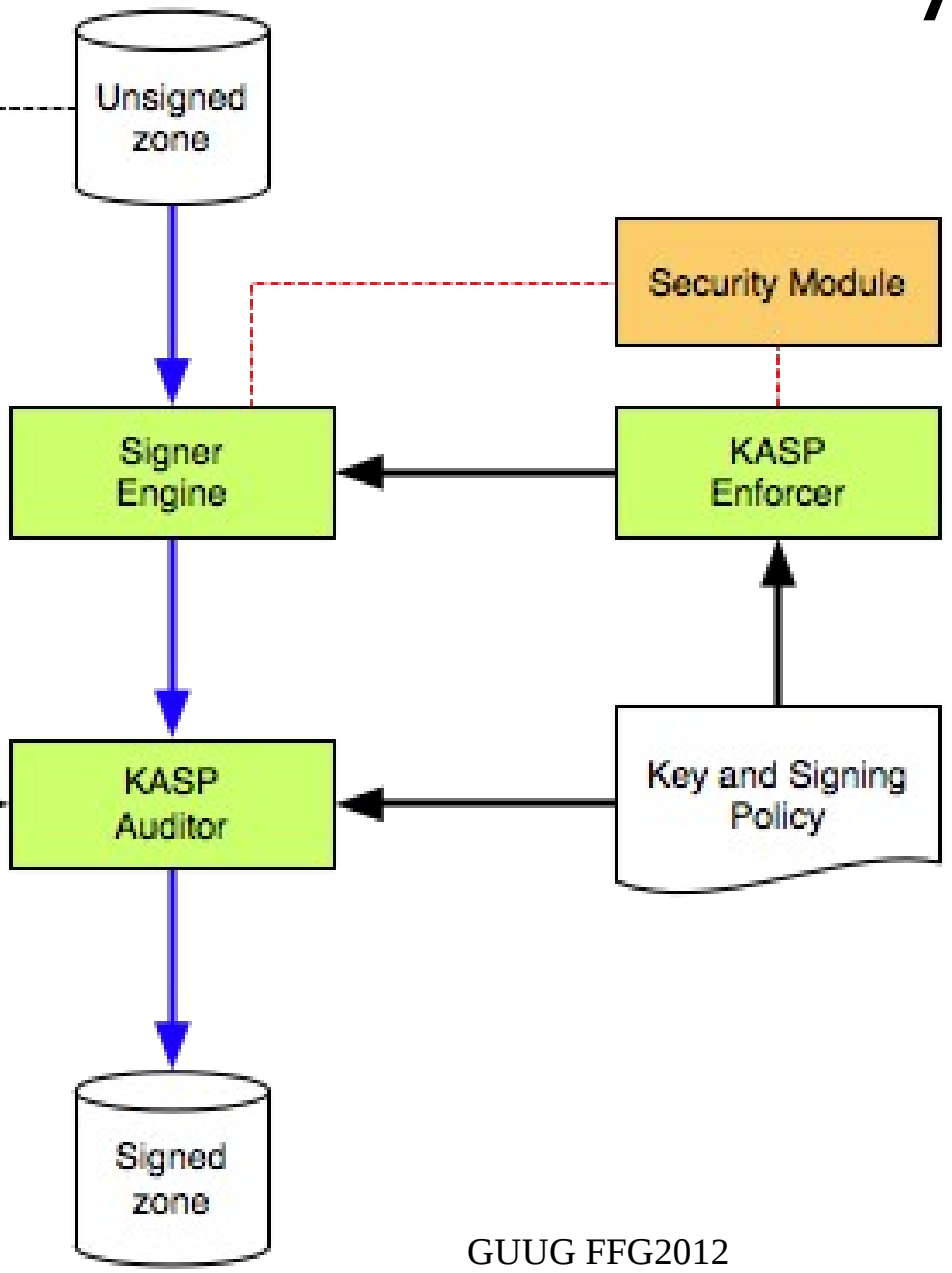
Architecture



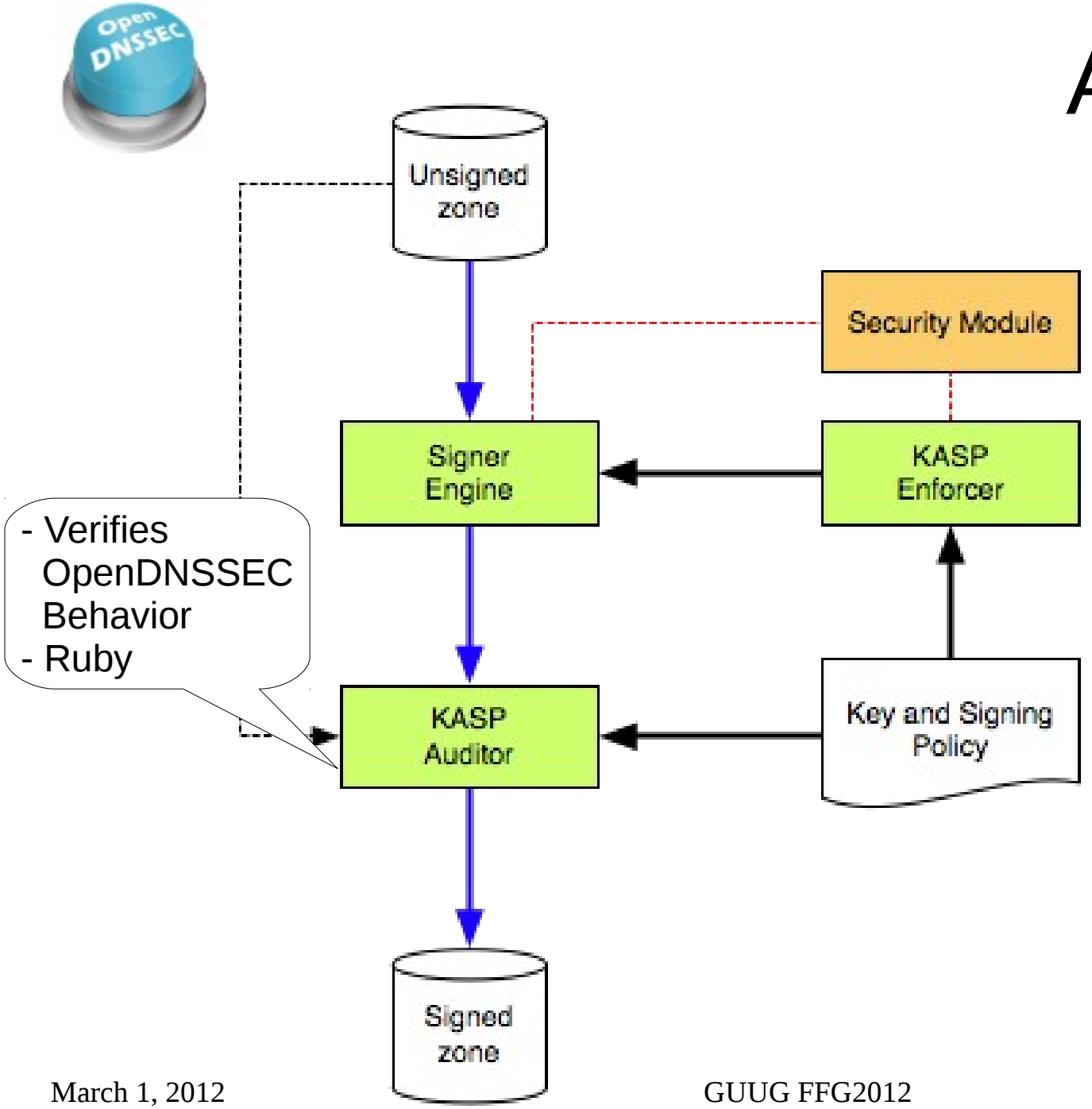
- Key Storage
- Hardware acceleration
- PKCS#11
- SoftHSM

Architecture

- Auto (re)sign
- Incremental
- Reuse Signatures
- Jitter expiration
- Maintains NSEC(3)
- Updates SOA

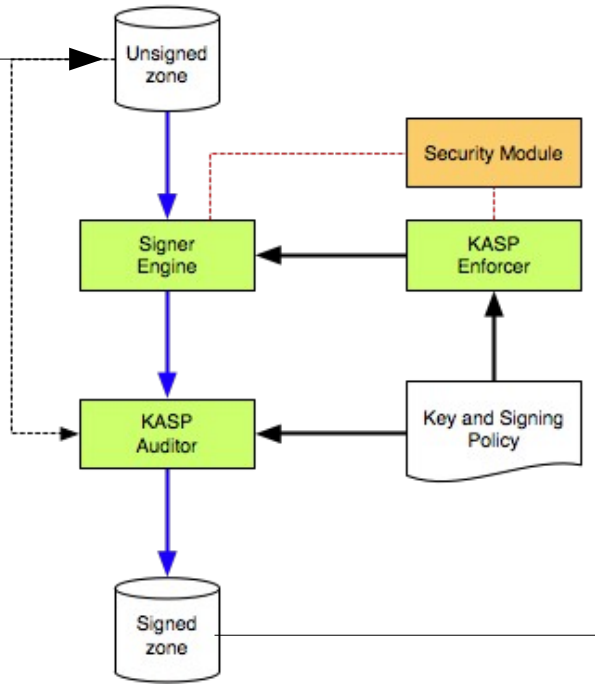


Architecture



Input and Output Adapters

Input Adapter:
- Zone file
- Zone fetcher



Output Adapter:
- Zone file + DNS server

Status

Jul 2009:
- 1.0 alpha

Feb 2010:
- 1.0
- C + Python

May 2010:
- 1.1
- First bugfix release

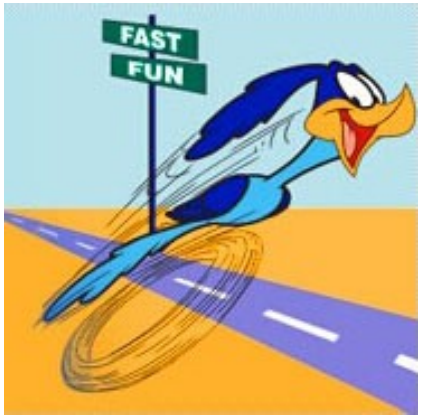
Feb 2011:
- 1.2
- New Signer, drop Python

Jul 2011:
- 1.3
- Signing performance

Mar 2012:
- 1.4 alpha

Meep, Meep!

- SCA6000 HSM
  - “Up to 13,000 RSA operations per second”
- OpenDNSSEC 1.2.X Performance
  - ~2100 RRSIG / second
- OpenDNSSEC 1.3.X Performance
  - 13552 RRSIG / second



1.4 (Q2 2012)

AXFR + IXFR Input/Output Adapters

- Deprecates Zone fetcher and DNS Server

Remove KASP Auditor

PIN Daemon

2.0 (Q4 2012)

New KASP Enforcer

- Various types of Rollover
- Algorithm Rollover
- Single Type Signing Scheme
- Easy to make policy changes
- Performance update for #zones

Support for unsigned zones

2.X

Dynamic Update

Database Adapters

GOST, ECDSA

GUI

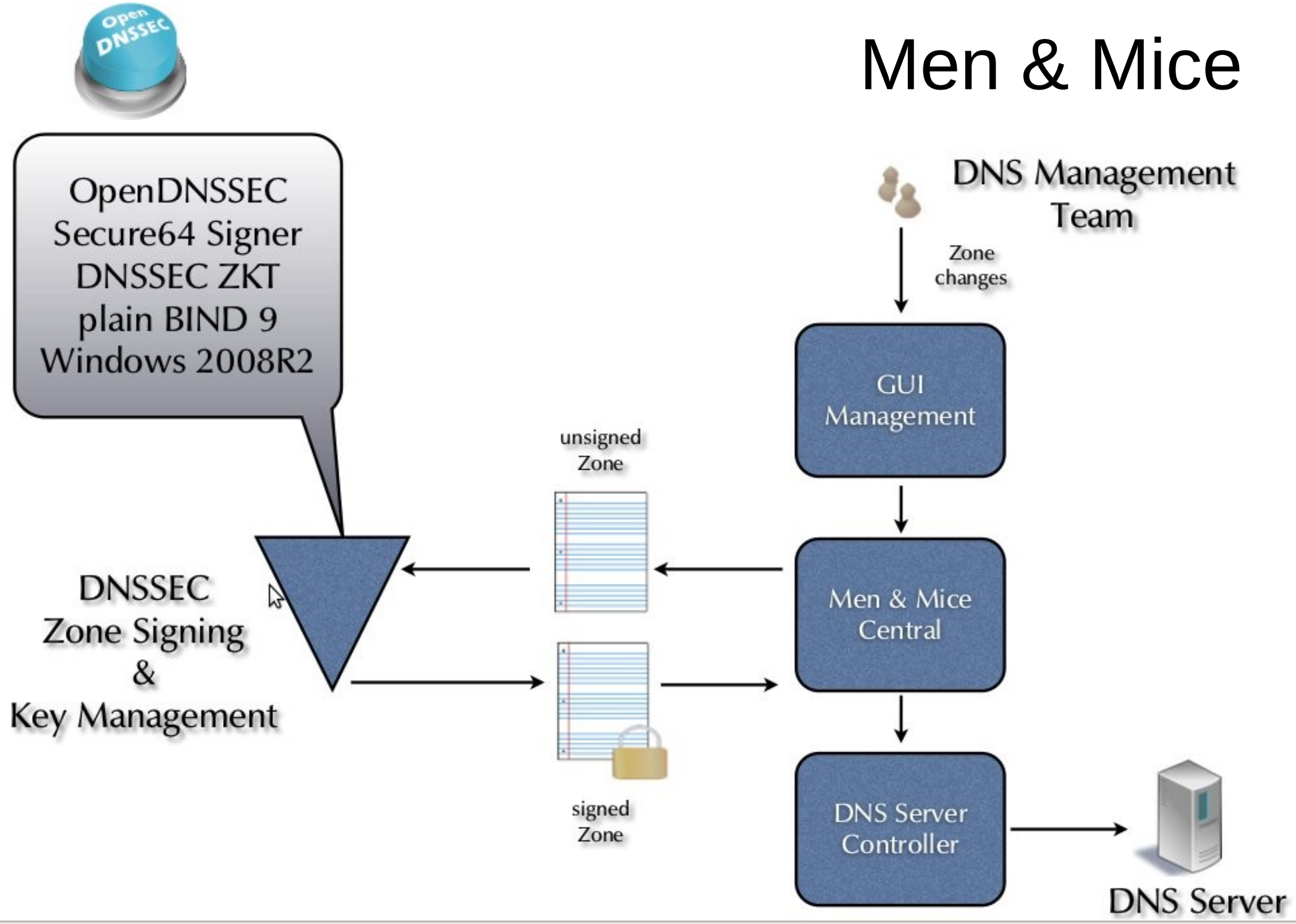
Offline Keys

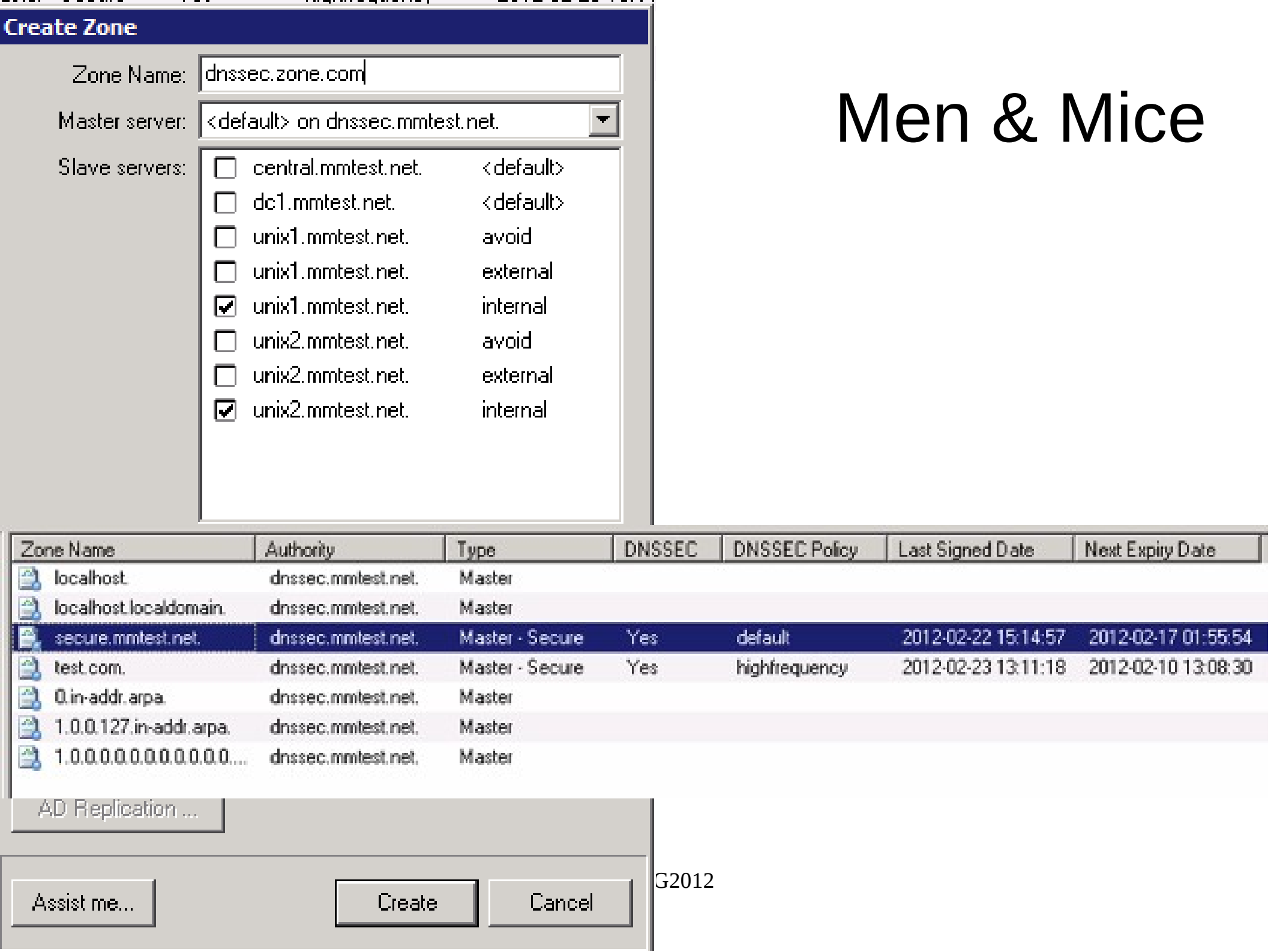
Push the Button

MEN&MICE

SURF NET

Men & Mice


Open DNSSEC
OpenDNSSEC
Secure64 Signer
DNSSEC ZKT
plain BIND 9
Windows 2008R2
DNS Management Team
Zone changes
GUI Management
unsigned Zone
Men & Mice Central
DNSSEC Zone Signing & Key Management
signed Zone
DNS Server Controller
DNS Server


Create Zone
Zone Name: dnssec.zone.com
Master server: <default> on dnssec.mmtest.net.
Slave servers:
central.mmtest.net. <default>
dc1.mmtest.net. <default>
unix1.mmtest.net. avoid
unix1.mmtest.net. external
unix1.mmtest.net. internal
unix2.mmtest.net. avoid
unix2.mmtest.net. external
unix2.mmtest.net. internal
Men & Mice
Zone Name | Authority | Type | DNSSEC | DNSSEC Policy | Last Signed Date | Next Expiry Date
localhost. dnssec.mmtest.net. Master
localhost.localdomain. dnssec.mmtest.net. Master
secure.mmtest.net. dnssec.mmtest.net. Master - Secure Yes default 2012-02-22 15:14:57 2012-02-17 01:55:54
test.com. dnssec.mmtest.net. Master - Secure Yes highfrequency 2012-02-23 13:11:18 2012-02-10 13:08:30
0.in-addr.arpa. dnssec.mmtest.net. Master
1.0.0.127.in-addr.arpa. dnssec.mmtest.net. Master
1.0.0.0.0.0.0.0.0.0.0.... dnssec.mmtest.net. Master
AD Replication ...
Assist me...
Create
Cancel

Surfnet

- Push-the-button signing:

- Unsigned to signed in 15 minutes

- http://www.opendnssec.org

- SoftHSM 
  - http://www.softhsm.org