OpenDNSSEC Integration

.se

Integration into an existing system

- Adding/removing zones
- Zone distribution
- Send the public keys to the parent zone

.se

Adding/removing zones

- Edit the zone list
  - Update the information in zonelist.xml
  - Trigger OpenDNSSEC to re-read the zonelist (ods-ksmutil update zonelist)
- Or only use CLI
  - ods-ksmutil zone add --zone <name of zone>
  - ods-ksmutil zone delete --zone <name of zone>
  - If the extra arguments are not used, then the system defaults will be used
  - Will edit the zonelist.xml for you

.se

Zone distribution

- OpenDNSSEC currently only support AXFR in, file in, and file out
- Remember to trigger OpenDNSSEC to re-read the zone file if you use file in
- Future versions will have better support
- You can use your favorite nameserver to serve the signed zone file
  - Use <NotifyCommand>rndc reload %zone</NotifyCommand> in conf.xml

.se

Sending keys to the parent zone

- Manually
  - Extract the keys from OpenDNSSEC or the signed zone
- Automatic
  - Use <DelegationSignerSubmitCommand> in conf.xml
  - OpenDNSSEC sends the current set of DNSKEY RR which should have a corresponding DS RR in the parent zone
  - A command which can receive DNSKEY RRset on stdin
  - The command has to do its own conversion to DS RR
  - Write your own plugin or use the ones provided by OpenDNSSEC

.se

EPP client

- Will use EPP to send DS RR to the parent
- Add --enable-eppclient to ./configure
- You also need to install libcurl

.se

EPP client - configuration

```
<database>/var/opendnssec/eppclientd.sqlite</database>
<pipe>/var/run/opendnssec/eppclientd.pipe</pipe>
<pidfile>/var/run/opendnssec/eppclientd.pid</pidfile>
<ackcommand>echo %s</ackcommand>
```

- The database is for the EPP queue
- The CLI needs to be able to talk to the daemon
- Once the key has been uploaded, then it can send back an acknowledge

.se

EPP client - configuration

```
 <registry>
   <suffix>.se</suffix>
   <host>epptest.iis.se</host>
   <port>700</port>
   <clID>iisrod1</clID>
   <pw>inU{r1jzN0rf</pw>
   <clientcert>
     <file>mycert.pem</file>
     <type>PEM</type>
   </clientcert>
   <clientkey>
     <file>mykey.pem</file>
     <type>PEM</type>
     <password>foo</password>
   </clientkey>
   <svcExtension>
<![CDATA[
     <extURI>urn:se:iis:xml:epp:iis-1.1</extURI>
]]>
   </svcExtension>
   <maxrate>360</maxrate>
   <expirytime>3600</expirytime>
 </registry>
```

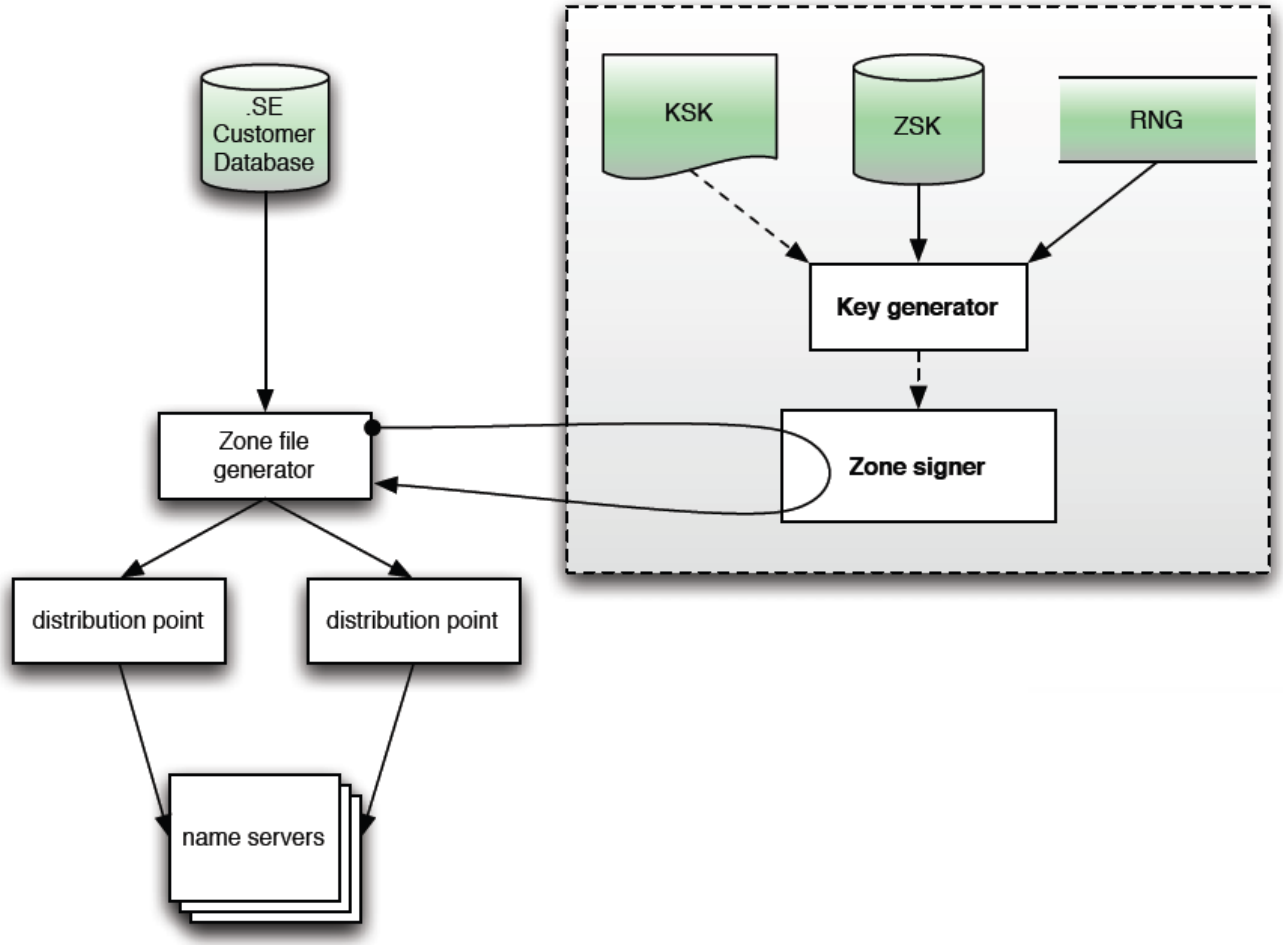
simple-dnskey-mailer

- A simple plugin to send the DNSKEYs to your email

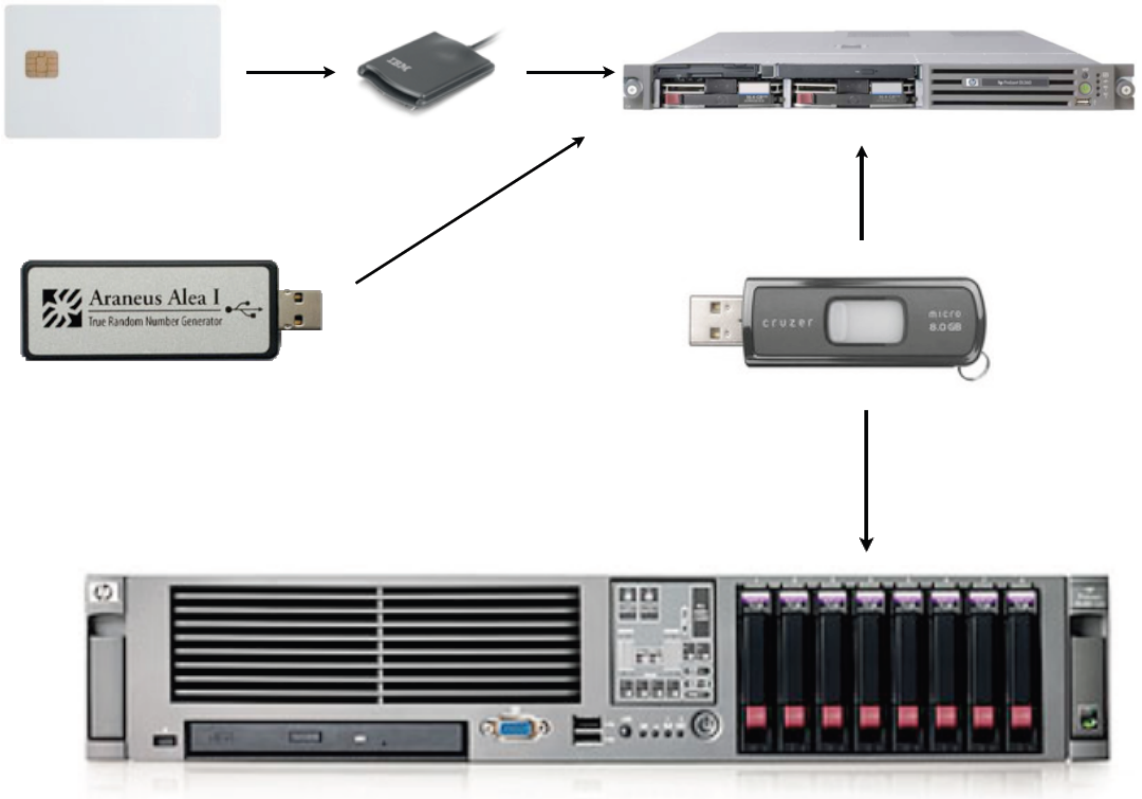
OpenDNSSEC at .SE

.se

The old system

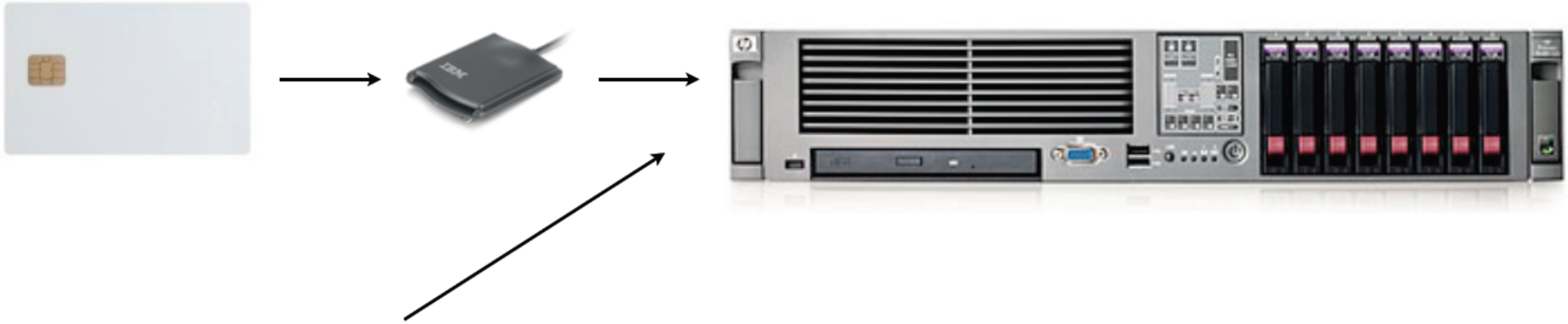


The old system



.se

The new system



The new system

- Old KSK is on a smartcard, but will be replaced by the end of the year. Stored in a safe.
- New keys are stored in an HSM
  - SCA 6000
- The keys are now always online

.se

SCA 6000
Sun Crypto Accelerator 6000

Interface	PCI-Express x8
Certification	FIPS 140-2 level 3
Performance (RSA-1024)	13,000 sign/s
System support	Solaris, RHEL, SUSE
Price	$ 1,350

.se

Interface

- The server fetch and deliver the zone file using SCP
- Using cronjobs to trigger the events
- New overlapping KSK is introduced in the beginning of each year
- The key is manually extracted

Backup

- No need to continuously do backup of the keys
  - Pre-generated keys for 10 years
- We only synchronize the KASP database to the standby site

.se

Thank you

- How do you administrate your zones?
- Zone distribution?
- Other questions?

.se