nominet

Crypto Hardware and Software for Signing .uk

John Dickinson

Crypto Hardware and Software for Signing .uk

Introduction

nominet

Signing .uk

nominet

.uk

- Very small zone
- Can be signed with regular DNSSEC (NSEC)
- We dont care about zone walking
- Could be done by hand with existing tools
- BUT...

Signing co.uk

nominet

co.uk

- Very large zone
- Requires NSEC3
- Requires hardware acceleration to sign in reasonable time
- Dynamically updated
  - Requires that we can continuously sign the zone

Continuous signing

nominet

We use dynamic updates to update co.uk

- Updates every minute
- We do not want to stop updates to re-sign
- Need BIND to generate signatures as updates arrive
- Need BIND to maintain those signatures
  - resign before signatures expire
  - but not all at once

Signing Requirements

nominet

so

- Want a system for .uk that will still work with co.uk
- Able to use hardware acceleration
- Also want HSM functionality
- Need NSEC3 support
- Need continuous signing

Crypto Hardware and Software for Signing .uk

Hardware

nominet

Introduction

nominet

Crypto hardware is available in a variety of formats

- Network Devices
  - SafeNet Luna SA £££
    - Stores keys on box. Use SSL link to contact box
  - nCipher netHSM £££
    - Stores keys on client. Master key on box
- PCI cards
  - nCipher ££
  - Sun SCA6000 £
    - Keys stored on disk. Master key in firmware on card

Getting Started

nominet

There is a big learning curve

- Documentation can be very poor
  - Expects you already know all about things like
    - pkcs11, crypto, HSM's...
  - Expects you to be doing SSL termination or IPSec
  - Very few simple explanations of things like
    - How to generate a RSA key pair
    - Where the keys actually are!
    - How to use OpenSSL with them
- Support can be variable
- Much harder than we expected.

Crypto Hardware and Software for Signing .uk

Software

nominet

Talking to the hardware

nominet

Crypto hardware is accessed using pkcs11 standard

- Big learning curve
- 391 page specification:
  - `ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf`
- Provided as library with hardware.
- Needed for key generation.
- Could be used for signing.
- No PERL implementation.
- No existing dnssec tools support pkcs11.

Signing with OpenSSL

nominet

We wanted to use OpenSSL wherever possible

- Generally accepted Crypto library
- Used by all existing DNSSEC tools
- Not tied to any specific hardware
- Should be able to access hardware
- Again big learning curve
  - Hard technology
  - Incomplete documentation

nominet

OpenSSL and Hardware

- To access hardware from OpenSSL you need an engine
  - interface between OpenSSL and pkcs11 library
  - Comes with hardware, OS or 3rd party
  - Support often locked to specific version of OpenSSL
  - Solaris engine is incomplete
- We used one from OpenSC
  - http://www.opensc-project.org/engine_pkcs11
- To sign with an engine you need to use the EVP API
  - Can not use lower level functions like RSA_sign()

nominet

Engines and EVP

- Very easy once you get used to it.
- Lack of documentation

```
OPENSSL_config(config_name);
e = ENGINE_by_id(engine_id);
ENGINE_init(e)
ENGINE_register_RSA(e)
priv_key = ENGINE_load_private_key(e, key_id, ui_method, &cb_data);

OpenSSL_add_all_digests();
md_type = EVP_get_digestbyname(argv[1]);
EVP_SignInit(&ctx, md_type);
EVP_SignUpdate(&ctx, message, strlen(message));
EVP_SignFinal(&ctx, sig, &s, priv_key);
```

OpenSSL

nominet

OpenSSL and DNSSEC tools

- All existing tools expect private keys to be in unencrypted files on disk!
- None of the existing tools use EVP API
  - use lower level calls to OpenSSL
- We were amazed to find no PERL implementation of EVP
- Again – Much harder than we expected

Where we are

nominet

We have written **proof of concept** tools

- An EVP perl implementation
  - Using Inline::C
- A perl based signer that uses EVP
- Support in LDNS for EVP
- A signer that uses LDNS and EVP
- pkcs11 key generator

Where we are

nominet

We are working with

- NLNet Labs to get production EVP support in LDNS
  - beta code now available in subversion
- ISC to get EVP, NSEC3 and continuous signing in BIND

We plan to

- Complete the EVP Perl Module
- Develop a pksc11 Perl module

More info

nominet

Find out more at

- Our blog
  - `http://blog.nominet.org.uk/tech`