DNSSEC Developments

Internetdagarna 2010, Stockholm

kirei

Jakob Schlyter

kirei

jakob@kirei.se

kirei

IT Security Advisor

kirei

Crypto Plumber

kirei

IETF DNSSEC

Protocol Geek

kirei

.SE DNSSEC Mascot

kirei

Unbound

kirei

OpenDNSSEC

kirei

Root DNSSEC Design Team

kirei

jakob@schlyter.se

kirei

Chocoholic

kirei

Lindy Hop Dancer

kirei

Wife & two kids

kirei

One car

kirei

No dog

kirei

DNSSEC Yesterday

kirei

1983

Paul Mockapetris invents the DNS and implements the first server – JEEVES

kirei

1986

Formal IETF Internet Standard
RFC 1034 & 1035

kirei

1990

Steve Bellovin describes cache poisoning –
report is held back until …

kirei

1995

Steve Bellovin's article is published and
DNSSEC becomes a topic within the IETF

kirei

1997

1st generation of DNSSEC – RFC 2065

kirei

1997

Kashpureff of “AlterNIC” hijack the InterNIC website

kirei

1997

BIND 8 released

kirei

1999

First DNSSEC workshop in Sweden

kirei

1999

2nd generation of DNSSEC – RFC 2535

kirei

2000

BIND 9 released – with support for DNSSEC

kirei

2001

RFC 2535 key management did not work

kirei

2002 – 2004

"DNSSEC will be ready in 6 months"

kirei

2005

3rd generation of DNSSEC – RFC 4033/4034/4035

kirei

2005

.SE deploys DNSSEC

kirei

2006 – 2007

Others are thinking about deploying DNSSEC

kirei

2008

RFC 5155 brings us NSEC3

kirei

2008

The Kaminsky Bug

kirei

2009

Others are deploying DNSSEC

kirei

2010

The root zone is signed

kirei

Signing the Root

kirei

Root DNSSEC Design Team

kirei

Requirements

kirei

Transparency

Processes and procedures should
be as open as possible for the Internet
community to trust the signed root

kirei

Audited

Processes and procedures should
be audited against industry standards,
e.g. ISO/IEC 27002:2005

kirei

High Security

Root system should meet all NIST
SP 800-53 technical security controls required
by a HIGH IMPACT system

kirei

2048-bit RSA

SHA-256

kirei

Split KSK/ZSK management

kirei

ICANN manage the Key Signing Key

kirei

VeriSign manage the Key Signing Key

kirei

Incremental deployment

Deliberately Unvalidatable Root Zone (DURZ)

kirei

Trusted Community Representatives

kirei

Crypto Officers

7 people for each facility, controlling
access to the Cryptographic Modules

kirei

3 of 7 required

for access

kirei

Recovery Key Shareholders

7 people keeping the recovery key safe

kirei

5 of 7 required

to recover

kirei

Key Management Facilities

kirei

US East & West Coast

kirei

Multi-Tiered Security

kirei

m-of-n

kirei

SysTrust audit

kirei

Key Ceremonies

kirei

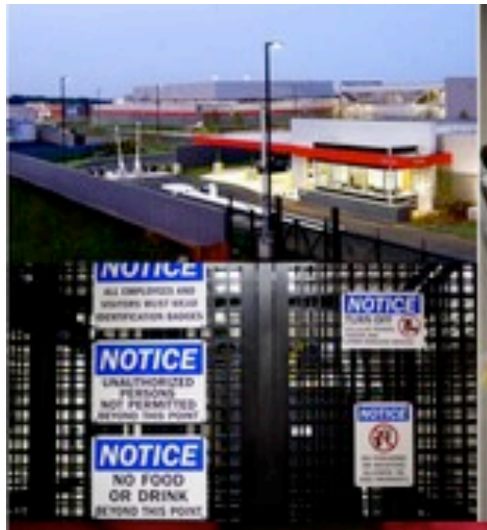
KSK Generation

kirei

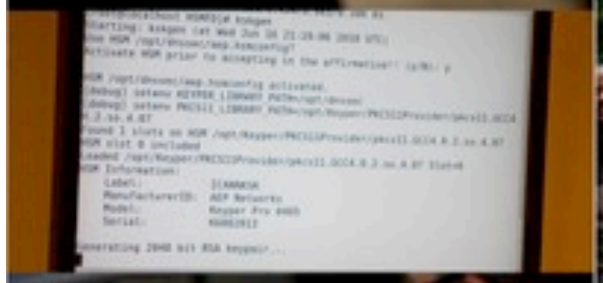
ZSK Signing

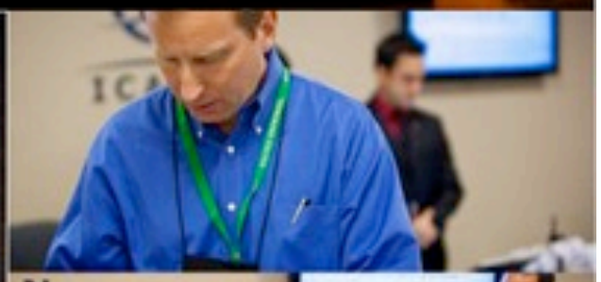
4 times a year

kirei

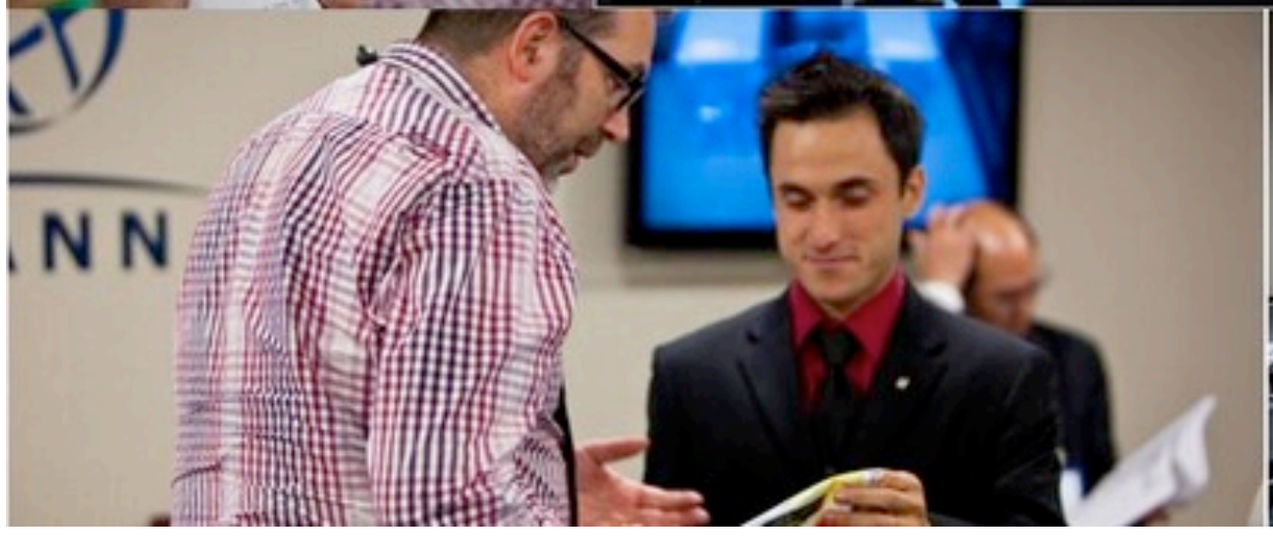

NOTICE
NOTICE
NOTICE
NO FOOD
OR DRINK
BEYOND THIS POINT


ICANN






N


NN


One World. One Internet. Everyone Connected.
19036

The Internet Corporation for Assigned Names and Numbers

```
Starting: kskgen (at Wed Jun 16 21:19:06 2010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:            ICANNKSK
    ManufacturerID:   AEP Networks
    Model:            Keyper Pro 0405
    Serial:           K6002013

Generating 2048 bit RSA keypair...
Created keypair labeled "Kjqmt7v"

SHA256 DS resource record and hash:
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
>> deckhand pedigree snapline breakaway kickoff hemisphere flytrap detergent guidance c
oherence eating outfielder facial hurricane hamlet fortitude keyboard Bradbury cranky l
eprosy Dupont adroitness willow Chicago tempest sandalwood tactics component uproot dis
tortion payday positive <<

Created CSR file "Kjqmt7v.csr":
O: ICANN
OU: IANA
CN: Root Zone KSK 2010-06-16T21:19:24+00:00
1.3.6.1.4.1.1000.53: . IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2C
E1CDDE32F24E8FB5

Kjqmt7v.csr SHA256 thumbprint and hash:
401120C1721BA100B2D9ABF2D01332399535BA0F9C71DB[illegible]97232C5EBD608D2
>> crackdown Babylon bison recover highchair bravado ratchet adroitness sawdust support
ive rhythm vagabond stagnate barbecue checkup corporate preclude conformist shadow atmo
sphere python hideaway suspense supportive waffle holiness checkup resistor trouble spe
culate aimless sensation <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```


Washington, DC	**1101 New York Avenue NW, Suite 930**	**Washington, DC 20005**	**USA**	**T +1 202 570 7240**	**F +1 202 789 0104**
Brussels	6 Rond Point Schuman, Bt. 5	B-1040 Brussels	BELGIUM	T +32 2 234 7870	F +32 2 234 7848
Marina del Rey	4676 Admiralty Way, Suite 330	Marina del Rey, CA 90292	USA	T +1 310 823 9358	F +1 310 823 8649
Sydney	Level 2, 48 Hunter Street	Sydney NSW 2000	AUSTRALIA	T +61 2 8236 7900	F +61 2 8236 7913

http://icann.org

```
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
```

kirei

DNSSEC Today

kirei

Top Level Domains

are deploying

kirei

60 of 294

TLDs are now signed

http://stats.research.icann.org/dns/tld_report/

kirei

41 of them has published DS in the root zone

kirei

.arpa .asia .be .bg .biz .br

.bz .cat .ch .cl .cz .dk

.edu .eu .fi .fr .gi .gov .hn

.info .jp .kg .lc .li .lk .me

.mn .museum .my .na .nl

.nu .org .pm .pr .pt .re

.sc .se .tf .th .tm .uk .us

.vc .yt .இலங்கை

kirei

ISPs are validating

kirei

Swedish ISPs deployed early

kirei

Comcast recently started its rollout

kirei

Secure by default

kirei

Key Management

You are doing it wrong

kirei

OKRS

Obsessive Key Rollover Syndrome

kirei

Yes, it is partly my fault

We didn't know better back in 2005

kirei

We know better now

kirei

Best Current Practice

is ≠ best nor current

kirei

Say hi to risk management

kirei

Calm down

kirei

Roll keys when needed

– not ‘cause you can

kirei

Rolling a key is associated with a risk

kirei

Still need to practice

… although not in the production environment

kirei

DNSSEC Tomorrow

kirei

Are we ready to rumble?

kirei

We still have needs

kirei

Tools are getting better

kirei

Appliances are finally getting up to speed

kirei

Open Source Software getting better

kirei

ISC BIND

kirei

OpenDNSSEC

kirei

… and others

kirei

DNSSEC for the masses

kirei

How do you sign 100’000 zones?

kirei

How do you sign dynamic zones?

kirei

Secure Key Management

which doesn't cost you a fortune

kirei

Sane Key Management

Obsessive Key Rollover Syndrome
should not be the default

kirei

DNSSEC-aware Applications

kirei

I proposed this

back in 2002

kirei

… and was told this

was NOT a good idea

kirei

8 years later, it's apparently kosher

kirei

KIDNS BOF

Cryptographically secured communication
by using information in DNS

kirei

SSH – Secure Shell

kirei

PKI

kirei

Domain Validation

vs

Extended Validation

kirei

If you control the DNS…

kirei

…you control the PKI

kirei

Can DNSSEC take care of domain validation?

kirei

Speed. I am Speed.

kirei

No more waiting for revocation verification

kirei

IPsec

kirei

DKIM

kirei

The future is bright

kirei

Don’t forget GIGO

kirei

Garbage in – Garbage out

kirei

The End

kirei