Root Key Signing Ceremony X

26 July 2012

Andy Linton
<asjl@lpnz.org>

InternetNZ

What are you talking about?

- The process for signing the DNS root zone for DNSSEC
- I’m not going to talk about how DNSSEC works at the technical level – relief all round!
- Detailed business process designed to promote public confidence in the system
- Our system in New Zealand is not the same – that’s OK!

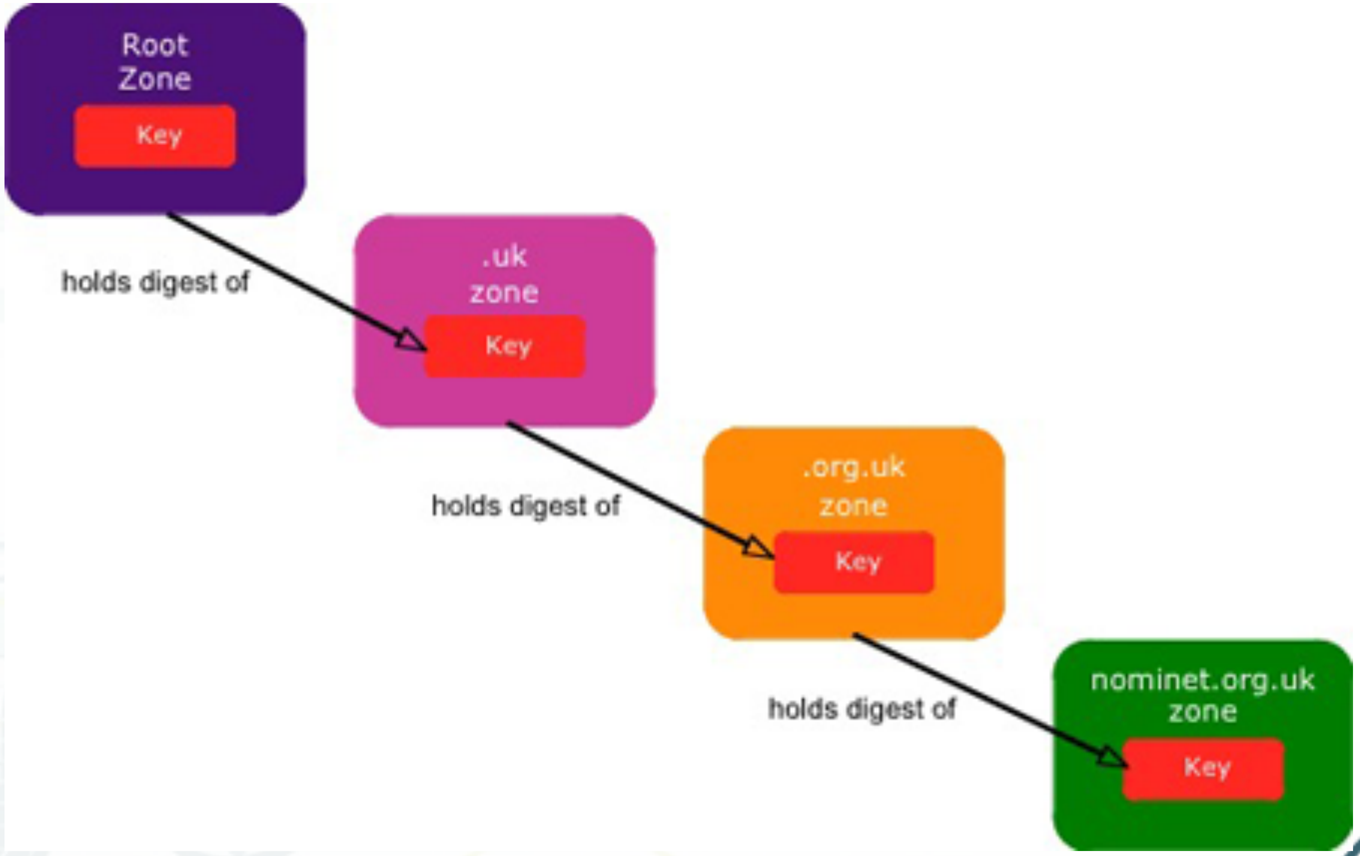
InternetNZ

Some definitions

- Root
  - The top of the DNS hierarchy
  - 13 name server instances globally provide the service
  - If we can't trust these servers then how can we trust services like .nz that depend on them
- KSK
  - Key Signing Key
  - Cryptographic key used to sign other keys
  - Not the German SAS - Kommando Spezialkräfte
- Chain of Trust
  - Established by validating each component of hardware and software from the bottom up

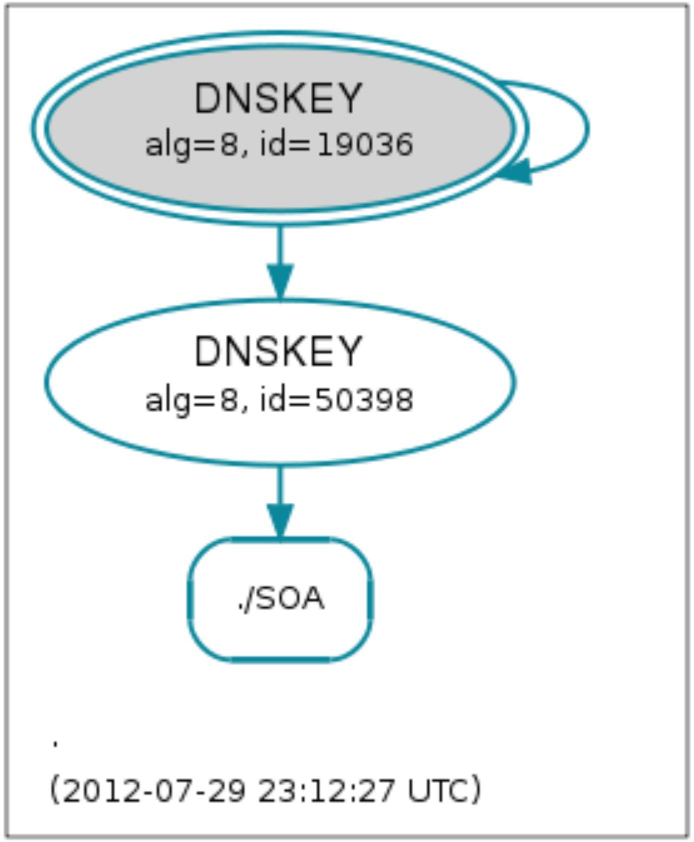
InternetNZ

Chain of Trust

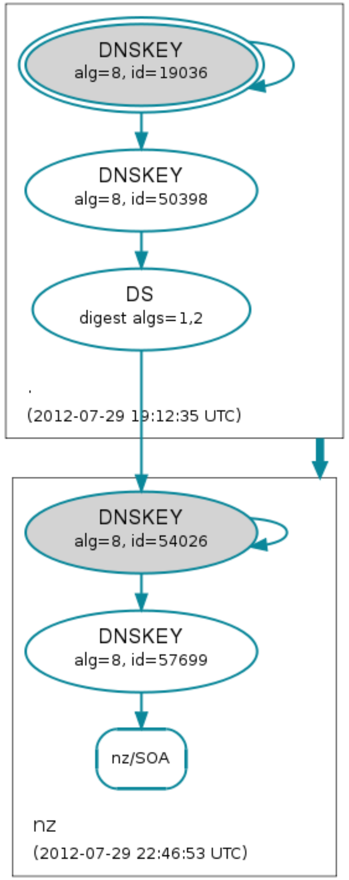


InternetNZ

Chain of trust for . (the root)



Chain of trust for .nz



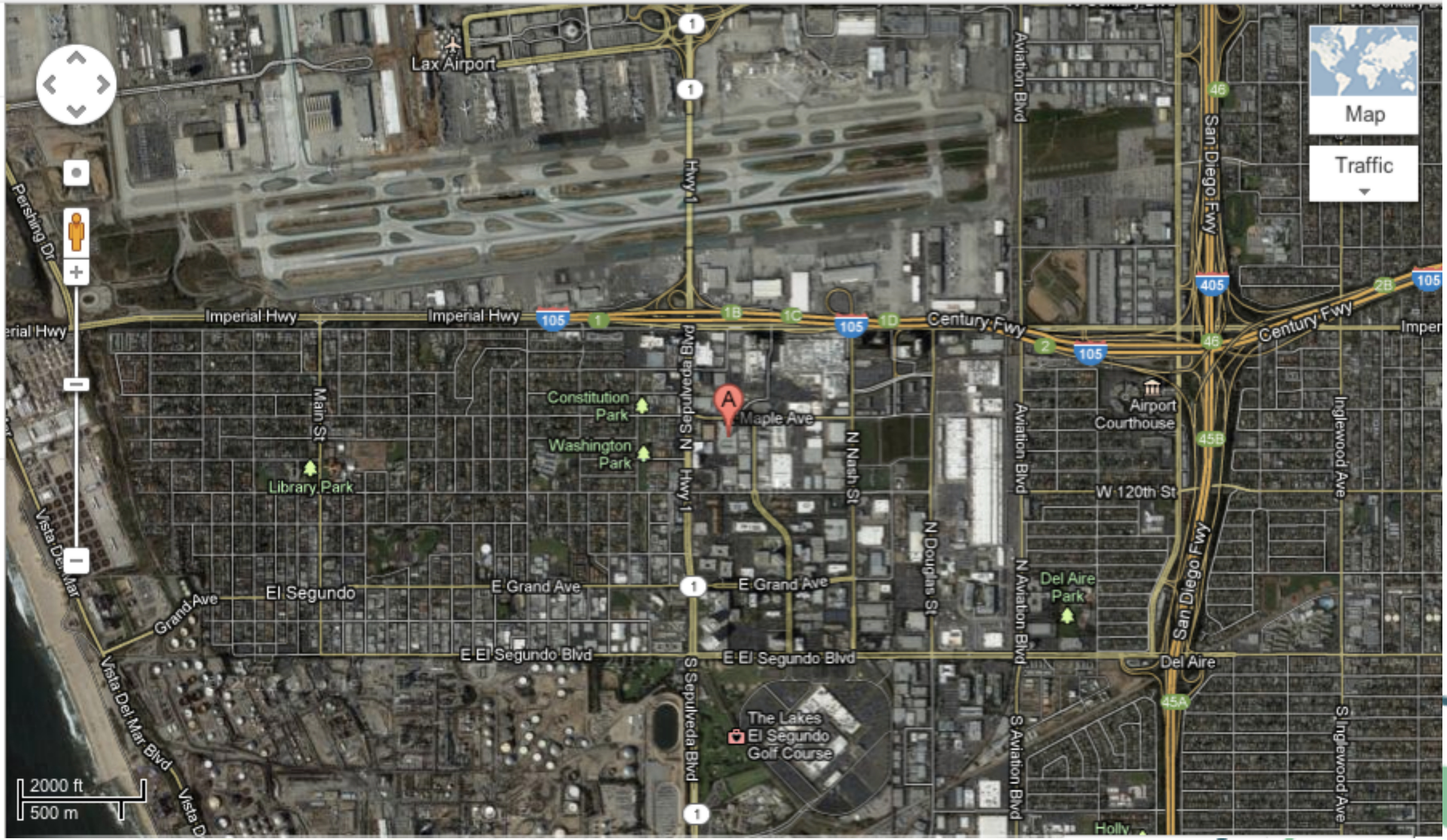
InternetNZ

Day trip to Los Angeles

- I left NZ on Wednesday evening
- Flew to LA arriving Wednesday afternoon
- Took part in Ceremony 10 on Thursday
- Flew home from LA on Thursday evening
- Breakfast in Wellington on Saturday
- Thanks to DNCL for supporting the travel!

InternetNZ

1920 E Maple Ave, El Segundo



InternetNZ

Key Management Facility House Rules

- The following rules applies to both ICANN Key Management Facilities. Please read them carefully before traveling to the facility.
  - You need two types of Government Issued Identification with Photo (e.g., Passport, Driver's License, Military ID) to enter the facility. You may be requested to leave one of the two ID's at facility security while you are on the premises.
  - Your bags are subject to scanned and/or searched by security personnel while entering the facility. You may also be requested to go thru a metal detector.
  - You are not allowed to use any cell phone, two-way pagers or radios in the ceremony room.
  - You are not allowed to record any audio and/or video on the premises.

Key Management Facility House Rules

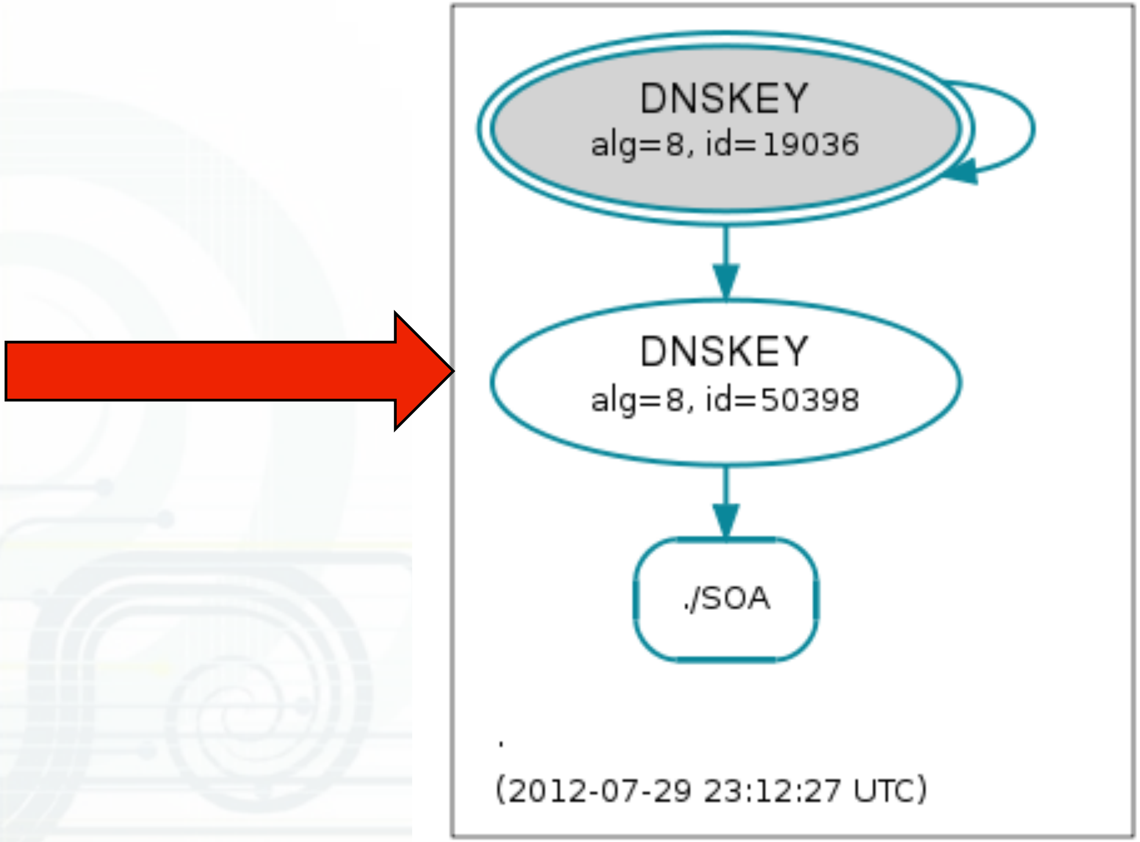
- You are not allowed to bring any laptop, personal digital assistant or the like in to the ceremony room. ICANN will provide storage for such items during the ceremony.
- Health and Safety regulations states that open toe shoes are not allowed on the premises.
- Weapons of any kind (e.g., Guns, Explosives, Knives, Pepper Sprays) are not allowed on the premises.
- Our facilities are smoke-free.

InternetNZ

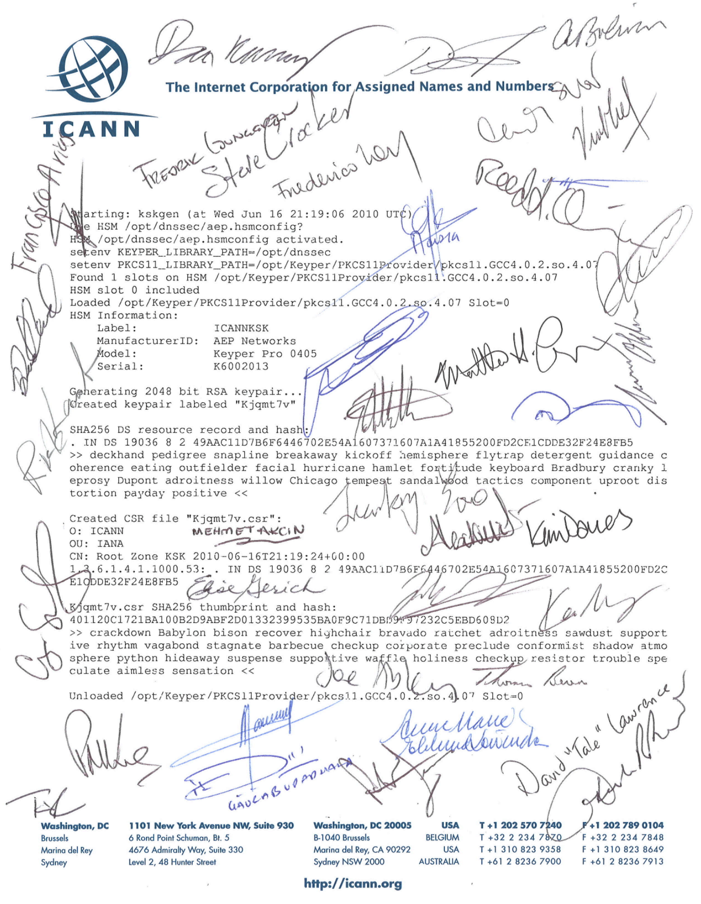
Ceremony 10

- 26 July 2010
- Ceremony script
  - http://data.iana.org/ksk-ceremony/10/KC10_Scripts.pdf
- 22 pages, 99 steps
- process takes nearly 3 hours
- ICANN staff + external witnesses + streamed on line
- 5 of 7 Crypto Officers present – minimum of 3 needed
- Verisign representative conveys keys for use in master root server

What are we producing?



Root KSK from Ceremony 1



The Internet Corporation for Assigned Names and Numbers

ICANN

```
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:
401120C1721BA100B2D9ABF2D01332399535BA0F9C71DBD9F97232C5EBD608D2
>> 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
```

Steve Crocker

Francisco Arias

MEHMET AKCIN

Kim Davies

Elise Gerich

Joe Abley

David "Tale" Lawrence

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

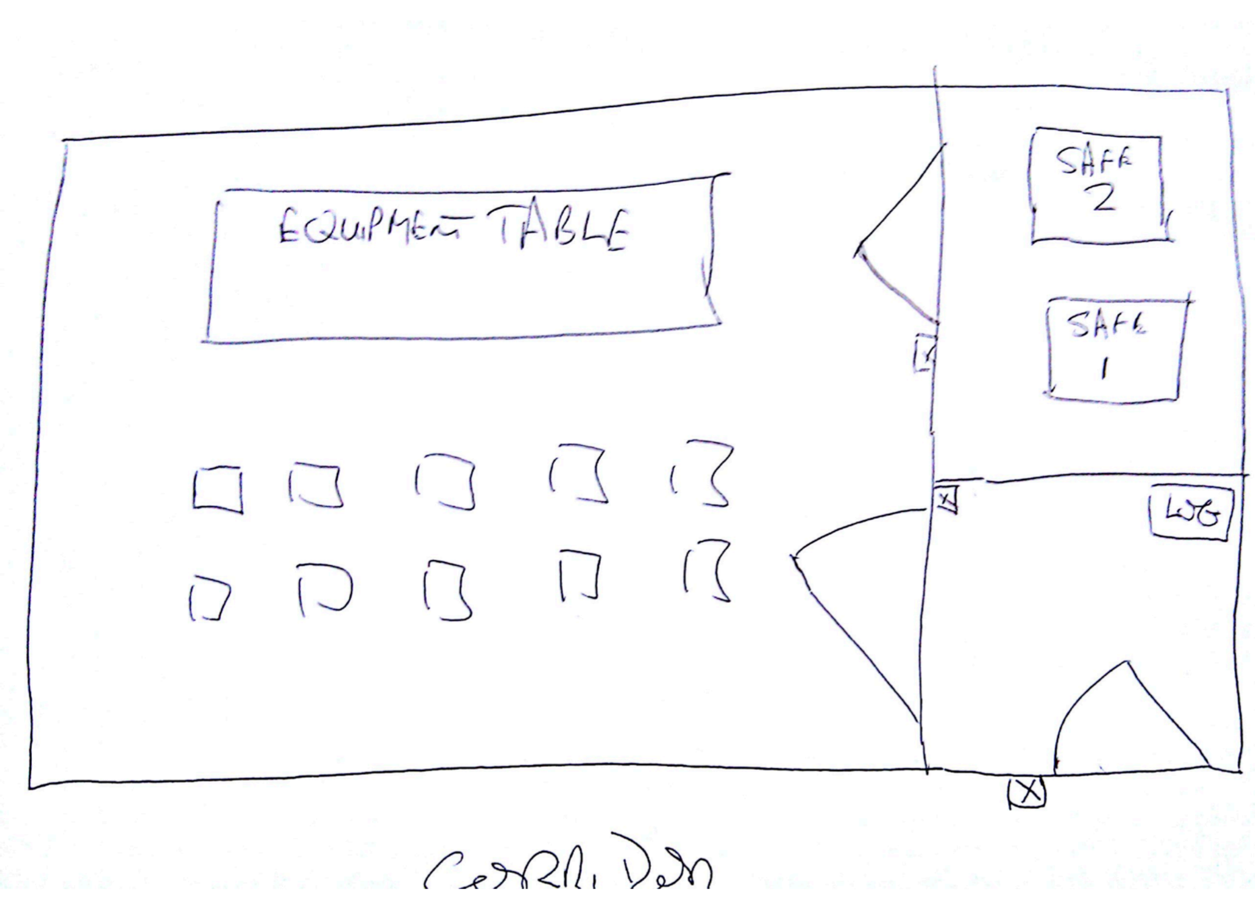
http://icann.org

InternetNZ

Some details from Ceremony 9

```
Validate and Process KSR /media/KSR/ksr-root-2012-q3-0.xml…
#  Inception            Expiration            ZSK Tags      KSK
     Tag(CKA_LABEL)
1  2012-07-01T00:00:00 2012-07-15T23:59:59  50398,56158
2  2012-07-11T00:00:00 2012-07-25T23:59:59  50398
3  2012-07-21T00:00:00 2012-08-04T23:59:59  50398
4  2012-07-31T00:00:00 2012-08-14T23:59:59  50398
5  2012-08-10T00:00:00 2012-08-24T23:59:59  50398
6  2012-08-20T00:00:00 2012-09-03T23:59:59  50398
7  2012-08-30T00:00:00 2012-09-13T23:59:59  50398
8  2012-09-09T00:00:00 2012-09-24T00:00:00  50398
9  2012-09-20T00:00:00 2012-10-05T23:59:59  24220,50398
...PASSED.
```

The Secret Chamber



Summary

- Robust process
- Publicly visible
- Collusion is possible but seems highly unlikely
- Keys are generated securely
- .nz signing is nearly complete
  - over to end users now
  - some INZ group work coming – another day!

InternetNZ