



---

# Fixing .nz DNSKEY encoding Technical report

Sebastian Castro  
sebastian@nzrs.net.nz

NZRS



# Chronology

---

- 1) Detection: 9-Dec-2011
- 2) Follow-up: 12-Dec 2011
- 3) Investigation: 13-Dec-2011
- 4) Software Patch: 16-Dec-2011
- 5) Realization: 11-Jan-2012
- 6) Remediation: 9-Feb-2012
- 7) Deployment: 23-Feb-2012

# 1) Detection

---

- Phil Regnauld and Andy Linton in Vietnam
  - Why .nz DNSKEY doesn't look like the rest
  - Email message to NZNOG
  - DNSKEY is encoded differently

```
From: Andy Linton  
Subject: [nznog] .nz zone DNSKEY
```

```
Is it just coincidence that the newly published DNSKEYs for .nz begin  
with the string BAABAA?
```

```
nz.          3600      IN  DNSKEY 256 3 8  
BAABAAGD+q3p2XDcb6SvAbACB/NPdIjxhpBx209ZnvF20Yb6kViMJ5dg  
xYDcFtvL5RW31Bc7UDvseoQPUK1wora3BtUTylo1xd5PN/lV600mrNGR  
xfmw77Hen/MXH5GQrjaj0+rFP1xce1/jdyvCciJzrYRcPL9p4c/eGoJK 3ZMubiu10Q==
```

## 2) Follow-up

---

- Duane Wessels
  - Your DNSKEY seems to generate different DS with BIND

```
NZ KSK has keytag 2517 yet dnssec-dsfromkey gives a DS with keytag 54026
$ dig nz dnskey | grep 257 > nz.key
$ dnssec-dsfromkey nz.key
nz. IN DS 54026 8 1 CC0EFEDAA4AA09CFB05E72E765A97BD5A9BFD1FE
nz. IN DS 54026 8 2
48B0A194EE26C9D59BCC683CBC7A3495BB0AAA51ECC75533DBC76408 F0F70458
```

- Mark Andrews
  - Your DNSKEY is wrongly encoded, contains a leading zero in the exponent, violating RFC 3110 Section 3.2, fix it

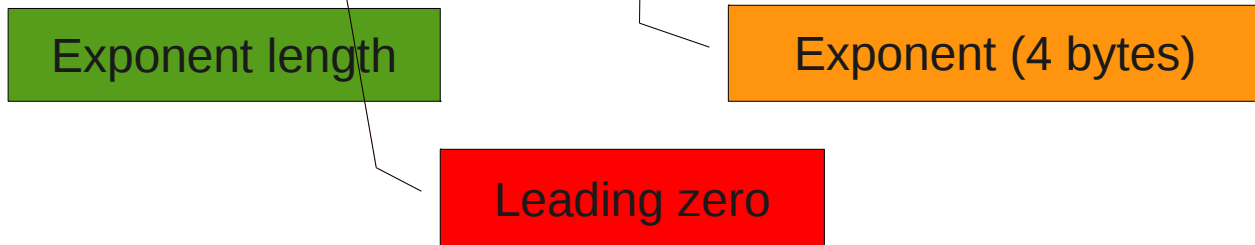
# 3) Investigation

- The version of Opencryptoki in use passes to libhsm an leading 0
- Libhsm doesn't validate the key contains an extra 0, encodes it as is.



```
drill -b2048 DNSKEY nz | grep -v '^$' | grep -v '^;' | awk '{ print $8}'  
| base64 -d | xxd -l 12 -b  
00000000: 00000100 00000000 00000001 00000000 00000001 10000011 .....  
00000006: 11111010 10101101 11101001 11011001 01110000 11000010 ....p.
```

According to RFC3110, Section 2, the decoded DNSKEY represents:



# 4) Software patch

```
--- libhsm/src/libhsm.c 2011-03-19 03:56:02.000000000 +1300
+++ /home/sebastian/src/opendssec-1.2.1/libhsm/src/libhsm.c
@@ -1261,6 +1261,18 @@
     return NULL;
 }

+static void
+__remove_leading_zeroes(CK_BYTE_PTR data, CK_ULONG *len)
+{
+    CK_BYTE_PTR p = data;
+    CK_ULONG l = *len;
+    while( 0 == (unsigned short int)(* p)) ++p, --l;
+    memmove(data, p, l);
+    *len = l;
+}
+
static ldns_rdf *
hsm_get_key_rdata(hsm_ctx_t *ctx, hsm_session_t *session,
                  const hsm_key_t *key)
@@ -1327,6 +1339,9 @@
     return NULL;
 }

+ // Remove leading zeroes for the public exponent
+ __remove_leading_zeroes(public_exponent, &public_exponent_len);
+
     data_size = public_exponent_len + modulus_len + 1;
     if (public_exponent_len <= 256) {
         data = malloc(data_size);
```

# 5) Realization

---

- Report from Comcast
  - Validation for .nz is not working, you have a problem, check dnsviz.net for diagnostics. We are disabling validation for .nz
- Reached Nominum for insight
- Conclusion: if we want to go ahead, we need to fix the DNSKEY

# 6) Remediation Plan

---

- Plan 1
  - Do a controlled manual KSK/ZSK rollover
  - Unusual: we are not changing the underlying keys, but their representation
  - Will need to feed old/new representation in the input zone
- Plan 2
  - Go unsigned
  - Deploy patched software
  - Clear status files
  - Re-sign
  - Test
  - Submit new DS



# 6) Deployment


- Go unsigned
  - Requested on 13-Feb
  - Completed on 16-Feb
- Deploy software
- Testing
- Submit new DS
  - Requested on 23-Feb
  - Completed on 26-Feb

 **Ondrej Filip**  
@ondrejfilip Follow ⌵


.NZ DS records removed from root zone. Whassup?

4 RETWEETS 

9:47 AM - 16 Feb 12 via web · Embed this Tweet  
← Reply ↻ Retweet ★ Favorite

 **Sebastian Castro**  
@secastro

say goodbye to the BAABAA .nz DNSKEY, please welcome the boring AwEAAY DNSKEY #DNS #DNSSEC

1 RETWEET 

10:48 AM - 17 Feb 12 via Hotot · Embed this Tweet  
← Reply 🗑 Delete ★ Favorite

 **Stéphane Bortzmeyer**  
@bortzmeyer Follow ⌵

DS record back in the root (first time it happened) RT: IANA whois: update for NZ Changes: [bit.ly/xpan9R](http://bit.ly/xpan9R) (via @ianawhois) #DNSSEC

3:18 AM - 27 Feb 12 via twmode · Embed this Tweet  
← Reply ↻ Retweet ★ Favorite

# Lessons learned

---

- Test using private implementation
  - We tested thoroughly using BIND/ldns
  - Thanks for Brian Wellington from Nominum for their help
- dnsviz.net didn't detect the wrong encoding
  - Notified Cassey Deccio
- IANA checks didn't detect the issue
  - Notified Kim Davies
- validns does detect the issue
- OpenDNSSEC devs very helpful
- Good response from IANA
  - DS removal triggered some alarms, manual verification was needed
  -

