



DNSSEC in the .UA Domain

Dmitry Kohmanyuk

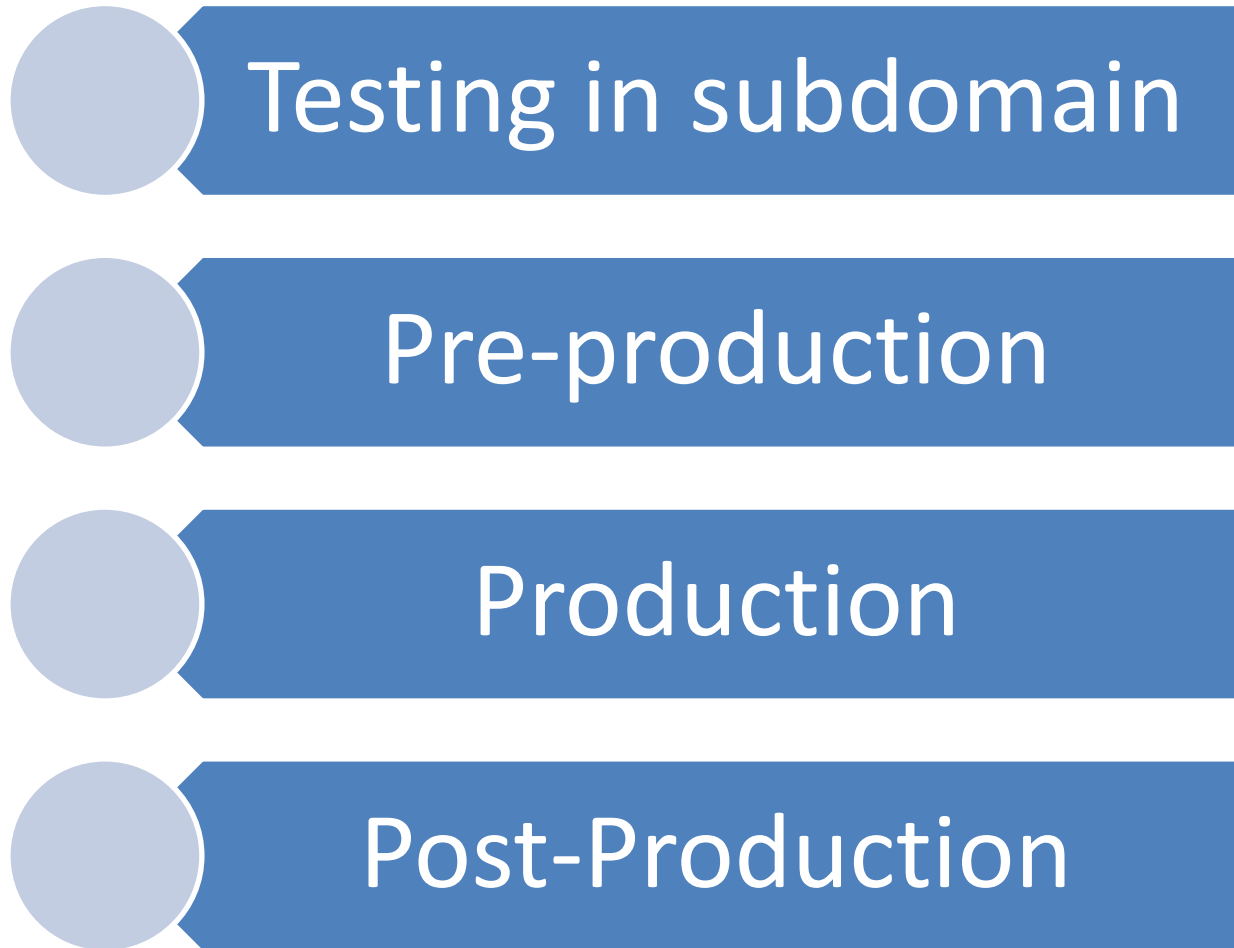
ENOG2

2011

Some facts

- UA total domains: 616523
- UA zone itself: 12672
- UA public subdomains: 76

The Plan



Testing in UA.UA

- Special domain - some strange resolver traffic
- Key generated at IPv6 Workshop #4 - November 8th, 2011
- Public key published
<http://hostmaster.ua/dnssec>
- Zone signed using bind 9.7 toolset (DNSSEC for Humans)

Testing signing UA, on private copy

```
Default
Default
Default
# ls -l
total 1016
-rw-r--r--  1 root  wheel   588 Nov 27 00:42 Kua.+010+20181.key
-rw-----  1 root  wheel  1777 Nov 27 00:42 Kua.+010+20181.private
-rw-r--r--  1 root  wheel   414 Nov 27 00:42 Kua.+010+54497.key
-rw-----  1 root  wheel  1013 Nov 27 00:42 Kua.+010+54497.private
-rw-r--r--  1 dk   wheel 991069 Nov 29 11:33 ua.priv
-rw-r--r--  1 dk   wheel  8565 Nov 29 11:33 ua.pub
-rw-r--r--  1 dk   wheel  4641 Nov 29 11:33 ua.zone
# dnssec-signzone
/usr/local/sbin/dnssec-signzone
# time dnssec-signzone -S -at -o ua ua.zone
Fetching KSK 20181/RSASHA512 from key repository.
Fetching ZSK 54497/RSASHA512 from key repository.
Verifying the zone using the following algorithms: RSASHA512.
Zone signing complete:
Algorithm: RSASHA512: KSKs: 1 active, 0 stand-by, 0 revoked
                        ZSKs: 1 active, 0 stand-by, 0 revoked
ua.zone.signed
Signatures generated:          12925
Signatures retained:           0
Signatures dropped:            0
Signatures successfully verified: 12925
Signatures unsuccessfully verified: 0
Runtime in seconds:            145.357
Signatures per second:         88.918
142.437u 0.775s 2:25.40 98.4% 1782+8914k 0+44io 0pf+0w
# ls -l
total 6298
-rw-r--r--  1 root  wheel   588 Nov 27 00:42 Kua.+010+20181.key
-rw-----  1 root  wheel  1777 Nov 27 00:42 Kua.+010+20181.private
-rw-r--r--  1 root  wheel   414 Nov 27 00:42 Kua.+010+54497.key
-rw-----  1 root  wheel  1013 Nov 27 00:42 Kua.+010+54497.private
-rw-r--r--  1 root  wheel   153 Nov 29 11:38 dsset-ua.
-rw-r--r--  1 dk   wheel 991069 Nov 29 11:33 ua.priv
-rw-r--r--  1 dk   wheel  8565 Nov 29 11:33 ua.pub
-rw-r--r--  1 dk   wheel  4641 Nov 29 11:33 ua.zone
-rw-r--r--  1 root  wheel 5379901 Nov 29 11:40 ua.zone.signed
# □
```

Pre-production

- Migration of all infrastructure to bind 9.8 (or later when stable)
- Separate signing and publication servers
- DUAZ - probably just single signed zone instance
- Possible use of DLV with pre-production keys

Algorithm selection

RSAMD5	DSA
RSASHA1	DSA-NSEC3-SHA1
RSASHA1-NSEC3-SHA1	DH
RSASHA256	ECC
RSASHA512	ECC-GOST

Potential issues

- GOST - no final opinion on validator support
- Algorithm support in IANA RZM system
- Storing key material - hard to split with bind
- Hardware certification - easier to do in software (and cheaper)

Production

- Key generation - scheduled for December 2nd 2011
- Key parameters - RSASHA512, 2048/1024 bits
- Deployment of key data in pre-production system replica
- Publishing records with IANA and our own web resources

Post-production

- Key rotation schedule - 3 years for KSK, 3 months for ZSK
- Reconsider algorithms: use Ukrainian own elliptical curve encryption - needs RFC



Questions?

www.hostmaster.ua

Whois.ua

info@hostmaster.ua