DNSSEC in the .UA Domain

Dmitry Kohmanyuk

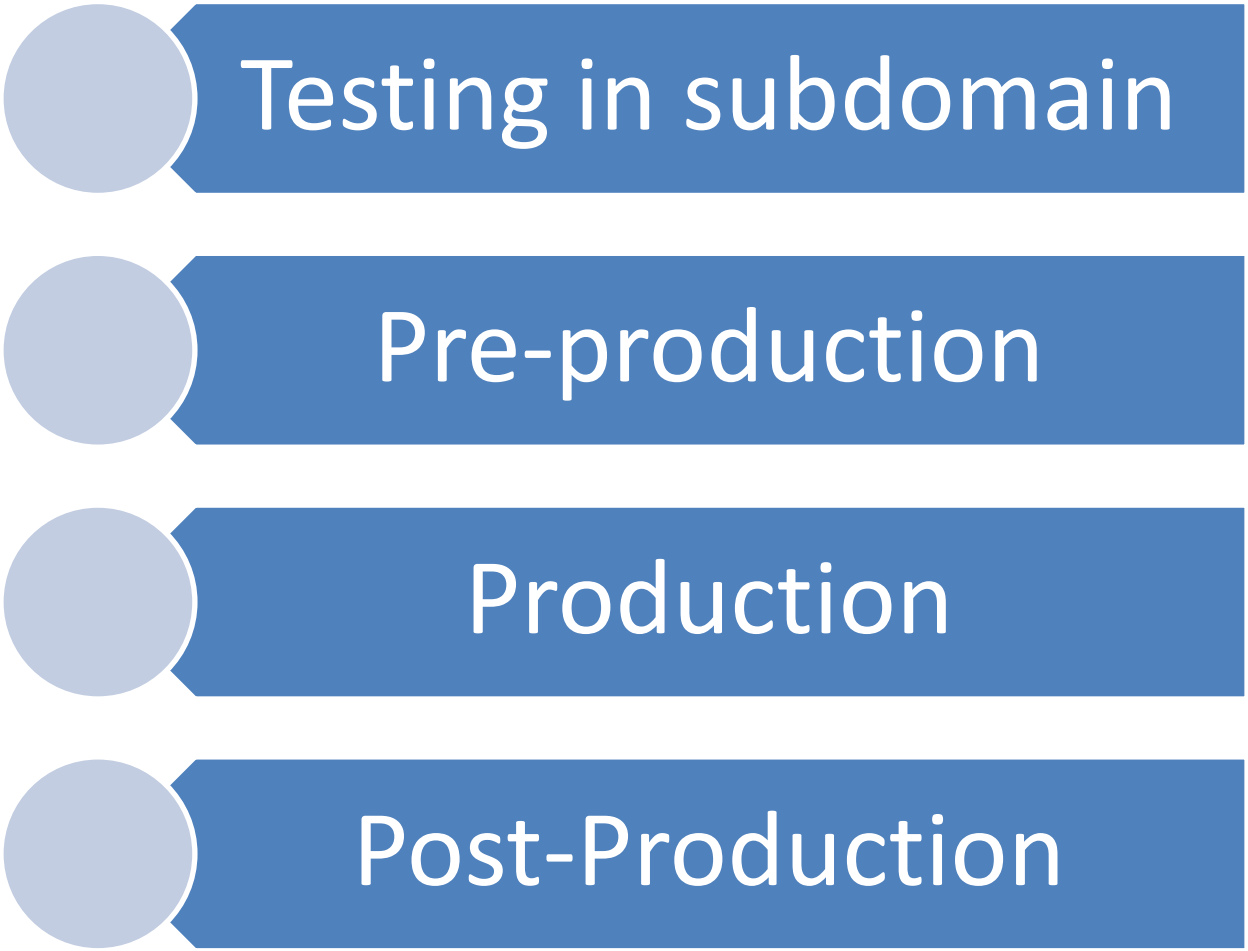
ENOG2

2011

Some facts

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

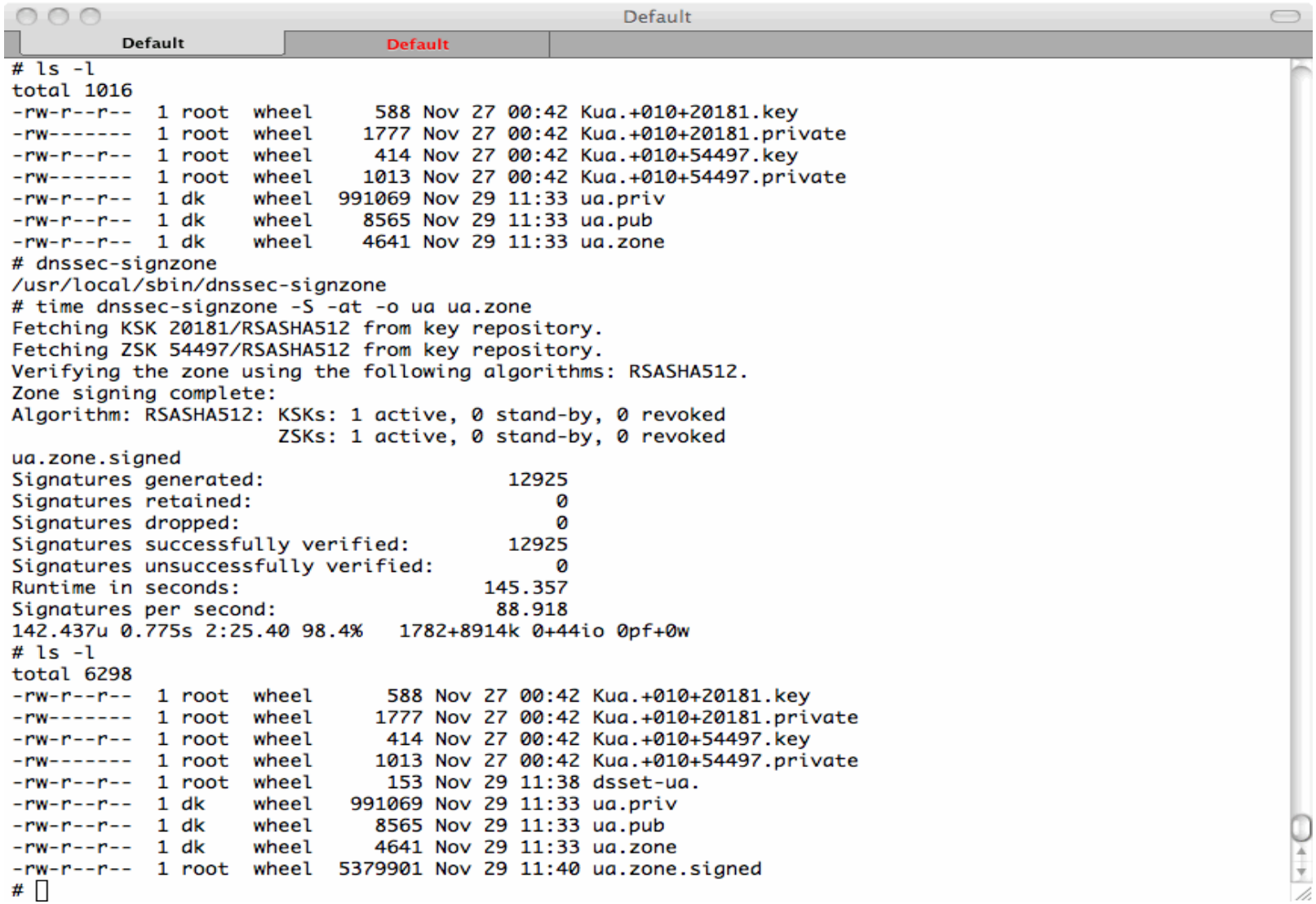
The Plan


Testing in subdomain
Pre-production
Production
Post-Production

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



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