GOST Cryptoalgorithms in DNSSEC
Seamless Integration

V.Dolmatov

September 2010

DNSSec at glance

- Root is signed and deployed
- Some TLDs are signed
- Some (few!) registrars are DNSSEC-aware

Hosting Community

R01 / РЕГИСТРАТОР

Cryptic cryptos

- Cryptography is a sensitive field
- Cryptography is monitored and controlled by governments
- There are different specific laws and rules in different countries which should be followed simultaneously

КРИПТОКОМ

GOST cryptography

- ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94
- Certified implementations should be used for public services and/or personal data handling in Russia
- RFCs 5830, 5831, 5832

GOST in DNSSEC

- RFC 5933 – Standard Track
- RRSIG algorithm code – 12
- DS algorithm code – 3
- Fully featured DNSSEC set of GOST algorithms

Hosting Community

криптоком

GOST implementation

- OpenSSL 1.0.0a and later (implemented by Cryptocom)
- Unbound 1.4.6 – enabled by default
- Bind 9.7.0-P2 – with Cryptocom patch

DNSSEC with GOST in the wild

- . (root is RSA signed)
- TLD .org (is RSA signed)
- dnssec-with-gost.org (is GOST signed)
  - gost.dnssec-with-gost.org (is GOST signed)
  - rsa.dnssec-with-gost.org (is RSA signed)

R01 / РЕГИСТРАТОР

RSA-GOST chain – OK!

```
; <<>> DiG 9.4.-ESV-R2 <<>> ns +dnssec +trace +multiline gost.dnssec-with-
gost.org
.                  272177 IN RRSIG  NS 8 0 518400 20100924000000 (
;; Received 493 bytes from 195.208.192.18#53(195.208.192.18) in 0 ms

org.               86400 IN RRSIG DS 8 1 86400 20100926000000 (
;; Received 699 bytes from 192.58.128.30#53(j.root-servers.net) in 22 ms

dnssec-with-gost.org.  86400 IN DS 44448 12 1 (
                       63D18EB3CBEBB313C8F93D03EA3463F4B9A5A436 )
dnssec-with-gost.org.  86400 IN DS 44448 12 2 (
                       0633F04487283DFB1C3C1A106B5201CA59995BF13A98
                       B64DB3C8D906BE711F7C )

;; Received 348 bytes from 199.19.57.1#53(d0.org.afilias-nst.org) in 43 ms

dnssec-with-gost.org.  21600 IN SOA ns1.gost.gpt.ru. noc.gpt.ru. (
                       2010091701 ; serial
                       10800      ; refresh (3 hours)
                       1800       ; retry (30 minutes)
                       604800     ; expire (1 week)
                       21600      ; minimum (6 hours)
                       )
dnssec-with-gost.org.  21600 IN RRSIG SOA 12 2 21600 20101017181549 (
                       20100917181549 27710 dnssec-with-gost.org.
                       9JeSbnjqvfyqclFRAl2Cnrnm0+h/KcpSfrXWlQCdIwZ3
                       xpBiiKKnQJSw4T4jgVky8Zwi5bz76phbJBjUap5heg== )
dnssec-with-gost.org.  21600 IN NSEC RSA.dnssec-with-gost.org. A NS SOA RRSIG
NSEC DNSKEY
dnssec-with-gost.org.  21600 IN RRSIG NSEC 12 2 21600 20101017181549 (
                       20100917181549 27710 dnssec-with-gost.org.
                       R8qnJKNB3gan/QmuCJbiOvhuTQOclP6XeFJoDs6Y1lC5
                       cXgR1AUHbgyTbTXdxIBLG1fD7VA6UG6lku84ABZlEw== )
;; Received 388 bytes from 89.111.167.42#53(ns2.gost.gpt.ru) in 5 ms
```

RSA-GOST-RSA chain – OK!

```
; <<>> DiG 9.4.-ESV-R2 <<>> ns +dnssec +trace +multiline rsa.dnssec-with-
gost.org
.                  272138 IN RRSIG  NS 8 0 518400 20100924000000 (
;; Received 493 bytes from 195.208.192.18#53(195.208.192.18) in 0 ms

org.               86400 IN RRSIG DS 8 1 86400 20100926000000 (
;; Received 701 bytes from 193.0.14.129#53(k.root-servers.net) in 47 ms

dnssec-with-gost.org.  86400 IN DS 44448 12 1 (
                       63D18EB3CBEBB313C8F93D03EA3463F4B9A5A436 )
dnssec-with-gost.org.  86400 IN DS 44448 12 2 (
                       0633F04487283DFB1C3C1A106B5201CA59995BF13A98
                       B64DB3C8D906BE711F7C )
;; Received 347 bytes from 199.19.54.1#53(b0.org.afilias-nst.org) in 169 ms

rsa.dnssec-with-gost.org. 21600   IN NS ns2.r01.ru.
rsa.dnssec-with-gost.org. 21600   IN NS ns1.r01.ru.
rsa.dnssec-with-gost.org. 21600   IN DS 50656 5 1 (
                       94E20FBF9908AEF605EFF83FEED591811B148B8B )
rsa.dnssec-with-gost.org. 21600   IN RRSIG DS 12 3 21600 20101017181549 (
                       20100917181549 27710 dnssec-with-gost.org.

;; Received 247 bytes from 89.111.167.40#53(ns1.gost.gpt.ru) in 5 ms

rsa.dnssec-with-gost.org. 21600   IN NS ns2.r01.ru.
rsa.dnssec-with-gost.org. 21600   IN NS ns1.r01.ru.
rsa.dnssec-with-gost.org. 21600   IN RRSIG NS 5 3 21600 20101017180752 (
                       20100917180752 31860 RSA.DNSSEC-WITH-GOST.ORG.

;; Received 279 bytes from 195.24.65.7#53(ns1.r01.ru) in 5 ms
```

How to switch it on?

- Unbound 1.4.6 + ldns – ready now!
- bind 9.7.0-P2 with Cryptocom patch (integrated in 2011)
- Cryptography
  - Open version – OpenSSL 1.0.0a
  - Certified version – **“MagPro DNS”** by Cryptocom
- OpenDNSSEC (support for GOST in 2011)

DNSSEC in Russia

- All main DNSSEC services with GOST are provided
- Certified GOST DNSSEC is also available
- Waiting for DNSSEC GOST-capable support in .RU, .SU and .РФ TLDs

Questions?

v.dolmatov@hostcomm.ru
www.cryptocom.ru/dnssec