Russian GOST profile for DNSSEC

Dmitry Belyavskiy, TCI

DNSOP Virtual Meeting,

April 23, 2020

TCI

History

RFC 5933 — 2010
Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC

Digital signature: GOST R 34.10-2001

Message digest: GOST R 34.11-94

Both algorithms are (incompletely) described in RFC 4490

Deprecated in Russia since 2019

New profile

Draft:

https://datatracker.ietf.org/doc/draft-belyavskiy-rfc5933-bis/

Implementation:
https://github.com/beldmit/ldns/tree/gost2012

Digital signature:

GOST R 34.10-2012 256 bit, RFC 7091

Digital signature parameters:

RFC 7836

Message digest:

GOST R 34.11-2012, RFC 6986

Requested status

Updates: RFC 5933

DNS Security Algorithm Numbers — RFC required

Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms — Standard Action

Does not fit Independent stream requirements

Requested status: Adopt as WG document

Thank you.

Questions?

Dmitry Belyavskiy
beldmit@tcinet.ru
beldmit@gmail.com