Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 5 December 2025

W. Hardaker
USC/ISI
W. Kumari
Google

3 June 2025

Deprecate usage of ECC-GOST within DNSSEC
draft-ietf-dnsop-must-not-ecc-gost-07

Abstract

This document retires the use of GOST R 34.10-2001 (mnemonic "ECC-GOST") within DNSSEC.

RFC5933 (now historic) defined the use of GOST R 34.10-2001 and GOST R 34.11-94 algorithms with DNS Security Extensions (DNSSEC). This document updates RFC5933 by deprecating the use of ECC-GOST.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 December 2025.

Copyright Notice

Table of Contents

1. Introduction

The use of the GOST R 34.10-2001 and GOST R 34.11-94 algorithms with the DNS Security Extensions (DNSSEC) [RFC9364] was documented in [RFC5933]. These two algorithms were deprecated by the Orders of the Federal Agency for Technical Regulation and Metrology of Russia (Rosstandart) in August 2012, and were superseded by GOST 34.10-2012 and GOST 34.11-2012 respectively. The use of these newer two algorithms in DNSSEC is documented in [RFC9558] and their associated requirement levels are not changed by this document.

Thus, the use of GOST R 34.10-2001 (mnemonic GOST-ECC) and GOST R 34.11-94 is no longer recommended for use in DNSSEC [RFC9364].

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Deprecating ECC-GOST algorithms in DNSSEC

The GOST R 34.11-94 [RFC5933] algorithm MUST NOT be used when creating DS records. Validating resolvers MUST treat GOST R 34.11-94 DS records as insecure. If no other DS records of accepted cryptographic algorithms are available, the DNS records below the delegation point MUST be treated as insecure.

The ECC-GOST [RFC5933] algorithm MUST NOT be used when creating DNSKEY and RRSIG records. Validating resolvers MUST treat RRSIG records created from DNSKEY records using these algorithms as an unsupported algorithm. If no other RRSIG records of accepted cryptographic algorithms are available, the validating resolver MUST consider the associated resource records as insecure.

3. Security Considerations

This document potentially increases the security of the DNSSEC ecosystem by deprecating algorithms that are no longer recommended for use.

4. Operational Considerations

This document removes support for ECC-GOST. Zone operators currently making use of ECC-GOST based algorithms should switch to algorithms that remain supported. DNS registries should prohibit their clients from uploading and publishing ECC-GOST based DS records to ensure that they are using algorithms which are supported by DNSSEC validators, and so can be DNSSEC validated.

5. IANA Considerations

[Note to IANA, to be removed by the RFC Editor: the registry fields listed above will be created by draft-ietf-dnsop-rfc8624-bis.]

IANA is requested to set the "Use for DNSSEC Signing", "Use for DNSSEC Validation", "Implement for DNSSEC Signing", and "Implement for DNSSEC Validation" columns of the DNS Security Algorithm Numbers registry [DNSKEY-IANA] [draft-ietf-dnsop-rfc8624-bis] for ECC-GOST (12) to MUST NOT. Note that previously the "Use for DNSSEC Signing" and "Implement for DNSSEC Delegation" columns were already MUST NOT.

IANA is requested to set the "Use for DNSSEC Delegation", "Use for DNSSEC Validation", "Implement for DNSSEC Delegation", and "Implement for DNSSEC Validation" columns of the "Digest Algorithms" registry [DS-IANA] for GOST R 34.11-94 (3) to MUST NOT. Note that previously the "Use for DNSSEC Signing" and "Implement for DNSSEC Delegation" columns were already MUST NOT.

6. References

6.1. Normative References

[DNSKEY-IANA]
IANA, "Domain Name System Security (DNSSEC) Algorithm Numbers", n.d., <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml>.

[draft-ietf-dnsop-rfc8624-bis]
W., K., "DNS Security Algorithm Numbers", n.d., <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-rfc8624-bis>.

[DS-IANA] IANA, "Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms", n.d., <http://www.iana.org/assignments/ds-rr-types>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC5933] Dolmatov, V., Ed., Chuprina, A., and I. Ustinov, "Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5933, DOI 10.17487/RFC5933, July 2010, <https://www.rfc-editor.org/rfc/rfc5933>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/rfc/rfc9364>.

6.2. Informative References

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9558] Makarenko, B. and V. Dolmatov, Ed., "Use of GOST 2012 Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 9558, DOI 10.17487/RFC9558, April 2024, <https://www.rfc-editor.org/rfc/rfc9558>.

Appendix A. Acknowledgments

The authors appreciate the comments and suggestions from the following IETF participants in helping produce this document: Mark Andrews, Steve Crocker, Brian Dickson, Thomas Graf, Russ Housely, Shumon Huque, Paul Hoffman, S Moonesamy, Peter Dickson, Peter Thomassen, Stefan Ubbink, Paul Wouters, Tim Wicinski, and the many members of the DNSOP working group that discussed this draft.

Appendix B. Current algorithm usage levels

The DNSSEC scanning project by Viktor Dukhovni and Wes Hardaker highlights the current deployment of various algorithms on the https://stats.dnssec-tools.org/ website.

<RFC Editor: please delete this section upon publication>

Appendix C. Github Version of this document

While this document is under development, it can be viewed, tracked, fill here:

https://github.com/hardaker/draft-hardaker-dnsop-must-not-gost

<RFC Editor: please delete this section upon publication>

Authors' Addresses

Wes Hardaker
USC/ISI
Email: ietf@hardakers.net

Warren Kumari
Google
Email: warren@kumari.net