Internet Engineering Task Force (IETF)
Request for Comments: 9906
Category: Standards Track
ISSN: 2070-1721

W. Hardaker
USC/ISI
W. Kumari
Google

November 2025

Deprecate Usage of ECC-GOST within DNSSEC

Abstract

This document retires the use of GOST R 34.10-2001 (mnemonic "ECC-GOST") and GOST R 34.11-94 within DNSSEC.

RFC 5933 (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 RFC 5933 by deprecating the use of ECC-GOST.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9906.

Table of Contents

1. Introduction

The GOST R 34.10-2001 and GOST R 34.11-94 algorithms are documented in [RFC5933] and their use with DNS Security Extensions (DNSSEC) is further described in [RFC9364]. 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the Orders of the Federal Agency for Technical Regulation and Metrology of Russia (Rosstandart) in August 2012 and were superseded by GOST 34.10-2012 and GOST 34.11-2012, respectively.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 two newer 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 "ECC-GOST") 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 algorithm [RFC5933] MUST NOT be used when creating Delegation Signer (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 GOST R 34.10-2001 algorithm [RFC5933] (mnemonic "ECC-GOST") MUST NOT be used when creating DNS Public Key (DNSKEY) and Resource Record Signature (RRSIG) records. Validating resolvers MUST treat RRSIG records created from DNSKEY records using these algorithms as unsupported algorithms. 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 that are supported by DNSSEC validators and thus can be DNSSEC validated.

5. IANA Considerations

IANA has updated the GOST R 34.10-2001 (12) entry in the "DNS Security Algorithm Numbers" registry [DNSKEY-IANA] [RFC9904] as follows:

Number: 12
Description: GOST R 34.10-2001 (DEPRECATED)
Mnemonic: ECC-GOST
Zone Signing: Y
Trans. Sec.: *
Use for DNSSEC Signing: MUST NOT
Use for DNSSEC Validation: MUST NOT
Implement for DNSSEC Signing: MUST NOT

Implement for DNSSEC Validation: MUST NOT
Reference: [RFC5933], Change the status of GOST Signature Algorithms in DNSSEC in the IETF stream to Historic (https://datatracker.ietf.org/doc/status-change-gost-dnssec-to-historic/), and RFC 9906

Note: The "Use for DNSSEC Signing" and "Implement for DNSSEC Delegation" columns were already set to MUST NOT.

IANA has updated the GOST R 34.11-94 (3) entry in the "Digest Algorithms" registry [DS-IANA] as follows:

Value: 3
Description: GOST R 34.11-94 (DEPRECATED)
Use for DNSSEC Delegation: MUST NOT
Use for DNSSEC Validation: MUST NOT
Implement for DNSSEC Delegation: MUST NOT
Implement for DNSSEC Validation: MUST NOT
Reference: [RFC5933], Change the status of GOST Signature Algorithms in DNSSEC in the IETF stream to Historic (https://datatracker.ietf.org/doc/status-change-gost-dnssec-to-historic/), and RFC 9906

Note: The "Use for DNSSEC Signing" and "Implement for DNSSEC Delegation" columns were already set to MUST NOT.

6. References

6.1. Normative References

[DNSKEY-IANA] IANA, "DNS Security Algorithm Numbers", <https://www.iana.org/assignments/dns-sec-alg-numbers>.

[DS-IANA] IANA, "Digest Algorithms", <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/info/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/info/rfc5933>.

[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/info/rfc8174>.

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

[RFC9904] Hardaker, W. and W. Kumari, "DNSSEC Cryptographic Algorithm Recommendation Update Process", RFC 9904, DOI 10.17487/RFC9904, November 2025, <https://www.rfc-editor.org/info/rfc9904>.

6.2. Informative References

[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/info/rfc9558>.

Acknowledgments

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

Authors' Addresses

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

Warren Kumari
Google
Email: warren@kumari.net