A failure to communicate…

AKA: draft-ietf-dnsop-rfc5933-bis

History

draft-ietf-dnsop-rfc5933-bis - "Use of GOST 2012 Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC"

- 2020-07-08 - WG -00 approved (adopted)
- 2022-07-28 - IETF WG state changed to WG Consensus: Waiting for Write-Up
- 2022-09-13 - IESG process started in state Publication Requested
- 2022-10-05 - IESG state changed to Last Call Requested
- 2022-10-25 - IESG state changed to IESG Evaluation
- 2022-12-01 - Telechat

Note: This is (obviously) a summary…

Roman Danyliw

Discuss

Discuss (2022-11-29 for -12)

Sent

(updated ballot)

The IETF has steered away from publishing protocol mechanisms with dependencies on national cryptography as we do not have the ability to validate their security properties ourselves. IETF stream documents typically rely on documents published in the Crypto Forum Research Group (CFRG) [1]; an open and peer-reviewed vetting process; or a review by the IRTF Crypto Panel [2] to give us confidence in cryptographic algorithm choices. Since the described GOST mechanism doesn't fit into these vetting criteria and the WG (based on the shepherd's report) has not provided alternative analysis, it is not appropriate to publish this document in the IETF stream.

11/28/2022: Suggested resolution per mailing list discussion: https://mailarchive.ietf.org/arch/msg/dnsop/XZoakWUDruPXylJ2wLIS4l4vevo/

[snip]

> It feels like this DISCUSS ballot is asking for a non-IETF-stream RFC to obsolete
> an IETF-stream RFC. Yuck. Instead, it might be better to publish this in the IETF
> stream; separately, the IESG could then publish a statement that future
> national algorithm documents should not come through the IETF stream.

I agree that we need to be careful on what a non-IETF stream document would do to an IETF-stream document. As a counter proposal, I would recommend that we use the flexibility afforded by RFC6014 and RFC9157 to address our current situation, and split the document.

The document has several components:

(a) Specification of and guidance for new DNSKEY and RRSIG behavior using GOST R 34.10-2012 and GOST R 34.11-2012 (i.e., Section 2 - 6, 9)

(b) Guidance to obsolete/update previous RFC5933/RFC8624 behavior per (a) (i.e., Section 7, 8)

(c) Request new IANA registry entries for (a) (i.e., Section 10)

(d) Request updates to IANA registries to deprecate older GOST code points specified by IETF-stream documents (i.e., Section 10)

Components (a) and (c) could be extracted from this document and added to a new document published by the ISE. This text is the new national crypto that the WG cannot render judgement on per my DISCUSS. The remaining text, components (b) and (d), would be the reduced draft-ietf-dnsop-rfc5933-bis document and would reference this new ISE document with the appropriate caveats on the confidence the WG in this new ISE reference. This reduced draft-ietf-dnsop-rfc5933-bis document would be the compromise where an IETF-stream document is needed to redefine previously specified behavior so that an ISE-stream document wouldn't have to obsolete an IETF-stream one. If (when) GOST R 34.10-2012/GOST R 34.11-2012 is superseded (and assuming it remains national crypto), algorithm revisions can be handled entirely by the ISE.

Regards,
Roman

And, of course, this was all discussed with the WG...

And, of course, this was all discussed with the WG...

Right?

Nope.

Somehow, somewhere, DNSOP fell of the thread, and I didn't notice.

See thread: "Warren did a bad (was Re: Datatracker State Update Notice: <draft-ietf-dnsop-rfc5933-bis-13.txt>)"

IETF conflict review for draft-makarenko-gost2012-dnssec

conflict-review-makarenko-gost2012-dnssec-00

Status | IESG evaluation record | Email expansions | History

Yes

Paul Wouters

Warren Kumari

No Objection

Erik Kline

Jim Guichard

John Scudder

Murray Kucherawy

Robert Wilton

Roman Danyliw

Zaheduzzaman Sarker

Éric Vyncke

Note: This ballot was opened for revision 00 and is now closed.

Ballot question: "Is this the correct conflict review response?"

Paul Wouters — **Yes**

Warren Kumari — **Yes**

Comment (2023-10-17) — Sent

Thank you everyone. A variation of this document was originally in the DNSOP WG, but, as it dealt with the definition of crypto algorithms, the Security ADs requested that it be progressed through the ISE.

Much thanks to the ISE, the Security ADs, and the authors for the delay / additional work, etc.

ISE doesn’t want to progress documents that step on WG toes…

Proposal / request:
We ask / let the ISE continue with publication.