SECDISPATCH
@IETF123

Unobtrusive End-to-End Signatures for Email

`draft-gallagher-email-unobtrusive-signatures`

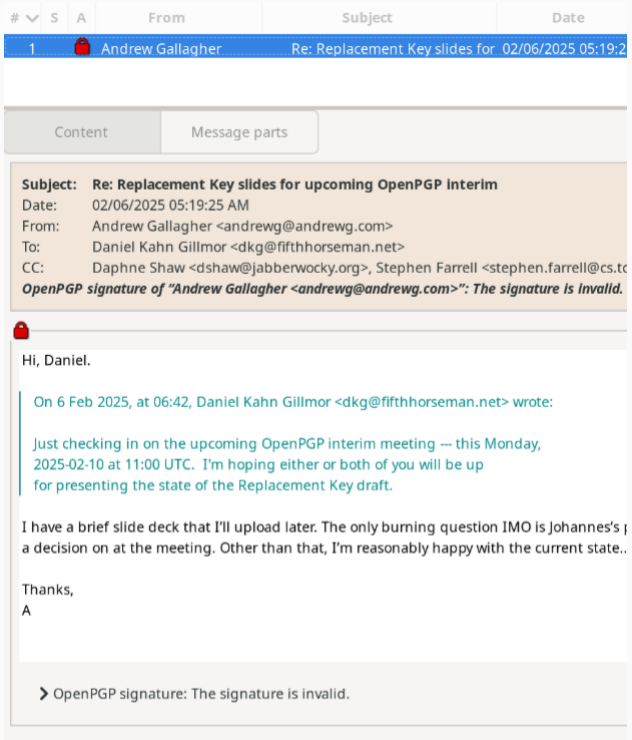
Andrew Gallagher (*pgpkeys.eu*), Kai Engert (*Thunderbird*), **Daniel Kahn Gillmor** (*ACLU*)

Motivation

It would be nice to not have to think about signing every e-mail I send. *But...*

- Some signed e-mail formats can't be read at all by legacy recipients (e.g., PKCS #7 signed-data)
- Other e-mail formats show legacy recipients an "unknown attachment"
- For non-legacy recipients, when a signature gets broken in transit, the recipient sees a scarier warning than an unsigned e-mail.

"Do I want to deal with the hassle of signing this message?"



What is it?

New format for signing an e-mail message end-to-end.

- Invisible to legacy MUAs.
- Appears unsigned to existing cryptographically aware MUAs.
- Signature failures are mandated to have no-scarier-than-unsigned results.

Bonus: *header fields are also covered by the e2e signature*

How is it done?

Message is a **`multipart/mixed`** object with a single child node.

The headers of **`multipart/mixed`** object start with one (or more) **`Sig:`** header fields.

The **`Sig:`** header field identifies itself as OpenPGP, and contains a base64-encoded OpenPGP signature, covering the entire rest of the object.

```
Content-Type: multipart/mixed; boundary="a21"
MIME-Version: 1.0
From: David Deluxe <david@openpgp.example>
To: Alice Lovelace <alice@openpgp.example>
Subject: Checking in
Date: Fri, 02 May 2025 13:01:07 -0400
Message-ID: <uosig-1@openpgp.example>


--a21
Sig: t=p; b=wpIGABsIAAAAKSIhBkGZ2eqmaCp41aU09iv3YiKlTk3rx4Xb
 5qbFs0WGAm/iBQJoFPpTAAAACgkQQZnZ6qZoKnhDIRA9tgkt50eA1ckzilm
 9KndQt3t4iYlab66bvtP+kP9D7zaNzvC1vE+B6jPY1gUBOQMyF5CK3yC/xZ
 Ol2ww+x8Y3PZ7OpZ1dPUlshDL5gA7ZAw==
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
From: David Deluxe <david@openpgp.example>
To: Alice Lovelace <alice@openpgp.example>
Subject: Checking in
Date: Fri, 02 May 2025 13:01:07 -0400
Message-ID: <uosig-1@openpgp.example>
Content-Type: text/plain; charset="us-ascii"; hp="clear"


Alice!


So good to see you earlier.


I hope you will have a chance to check out
our new website: https://openpgp.example/
and tell me what you think.


All the best,


David


--a21--
```

Wrinkles

Currently only OpenPGP (authors' interests, could be extended)

Just for signed-only messages (when encrypting and signing, use existing standards).

Dispatching Outcome

OpenPGP working group could do a small recharter to include it.

LAMPS, MAILMAINT, elsewhere?