Signature-Based Integrity

Mike West @ TPAC 2025

```
HTTP/1.1 200 OK
Date: Mon, 10 Nov 2025 01:00:00 GMT
Content-Type: application/json
Content-Length: 18
Unencoded-Digest: sha-256=:X48E9q...u9DBPE=:
Signature-Input:                        \
    signature=("unencoded-digest";sf);  \
    keyid="JrQLj5P/89...PPsw3c5D0bs=";  \
    tag="ed25519-integrity"
Signature: signature=:SbCdPU...pQGO+hrkAg==:

{"hello": "world"}
```

https://wicg.github.io/signature-based-sri/

```
HTTP/1.1 200 OK
Date: Mon, 10 Nov 2025 01:00:00 GMT
Content-Type: application/json
Content-Length: 18
Unencoded-Digest: sha-256=:X48E9q...u9DBPE=:
Signature-Input:                             \
    signature=("unencoded-digest";sf);  \
    keyid="JrQLj5P/89...PPsw3c5D0bs=";  \
    tag="ed25519-integrity"
Signature: signature=:SbCdPU...pQGO+hrkAg==:

{"hello": "world"}
```

ID.httpbis-unencoded-digest

```
HTTP/1.1 200 OK
Date: Mon, 10 Nov 2025 01:00:00 GMT
Content-Type: application/json
Content-Length: 18
Unencoded-Digest: sha-256=:X48E9q...u9DBPE=:
Signature-Input:                        \
    signature=("unencoded-digest";sf);  \
    keyid="JrQLj5P/89...PPsw3c5D0bs=";  \
    tag="ed25519-integrity"
Signature: signature=:SbCdPU...pQGO+hrkAg==:

{"hello": "world"}
```

RFC9421

```
Content-Security-Policy: \
    script-src 'ed25519-JrQLj5P/89...PPsw3c5D0bs='
```

```
<script src="https://my.cdn/script.js"
    crossorigin="anonymous"
    integrity="ed25519-JrQLj5P/89...PPsw3c5D0bs="
    ...></script>
```

Open Questions

1. Requirements for replacement, rollbacks, and redirects (wicg/signature-based-integrity#45)?

2. Do developers understand the delta between supply-chain and content integrity (wicg/signature-based-integrity#52)?

3. Does this assertion satisfy developer obligations (e.g. PCI DSS: wicg/signature-based-integrity#53)?

4. Can we improve the key rotation story (wicg/signature-based-integrity#43)?

```
<esi:include
    src="https://widgets.example/widget.include"
/>

<script
    integrity="ed25519-JrQLj5P/89...PPsw3c5D0bs="
    signature="ed25519-SbCdPU...pQGO+hrkAg==">
  console.log("Amazing functionality goes here.");
</script>
```

https://mikewest.github.io/inline-integrity/

Open Questions

1. Is the spelling reasonable? Perhaps the signature could be a parameter to the key rather than a distinct attribute (e.g. `integrity="ed25519-JrQL...0bs=?ed25519-SbCdP..."`)?

2. Could this be extended to cover assertions over external subresources that don't themselves assert a signature (mikewest/inline-integrity#8)?