

Web Packaging

draft-yasskin-dispatch-web-packaging-00

Jeffrey Yasskin, Chromium

IETF 99

July 2017

Outline

- Why?
- Requirements
- Format sketch
- Open questions

Why?

- Loading websites peer-to-peer instead of via expensive connections.
- A better MHTML
- CDNs without full control
- Vouched websites
- Easier-to-use HTTP2 Push?
- Node packages?
- Web publications?

Requirements

- P2P sites
 - Signed bundles
 - Certificate validation and downgrade protection
 - Random access allows transfer via SD cards
 - Multiple signatures allow algorithm upgrades
- A better MHTML
 - Unsigned bundles

Requirements

- CDNs without full control
 - Render packages as they download
 - Reorder/subset resources without breaking signatures
 - Maybe want a way to sign individual resources
- Vouched packages
 - Cross-signing

Sketch of the draft format

- CBOR base, but could be ASN.1/DER
- Optional signed list of resource hashes
- Sub-packages signed by other origins
- Content is an offset-indexed map from HTTP2 request headers -> responses.
- Certificate validation and downgrade protection will be based on OCSP and a signed minimum version, but we haven't designed how to attach this yet.

Open Questions

- Is the IETF the right venue for the format?
We plan to also specify how browsers load it via the W3C.
- Is a file format the right direction, or should we do something around just a new HTTP header?
- All of the details of the format are open to change.
- What else do you see?

Links

- <https://tools.ietf.org/html/draft-yasskin-dispatch-web-packaging-00>
- <https://github.com/WICG/webpackage>