SIGNED EXCHANGES IN CHROME

IPFS Camp

Kinuko Yasuda
@kinu

Jim Pick
@jimpick

Signed HTTP Exchanges

Lightning talk for IPFS Camp
June 2019

Kinuko Yasuda, Google
kinuko@chromium.org, @kinu

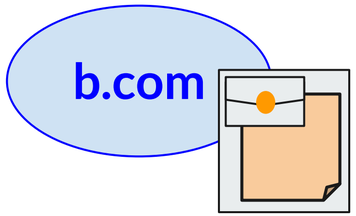
Overview of Signed HTTP Exchanges (or “SXG”)

An HTTP exchange, or request/response, that is **cryptographically signed** so that browsers can verify:

- True origin of the content: “it was signed and provided by the origin X”
- Integrity of the content: “it is not modified from the original one”

What does this enable? → Distribution!

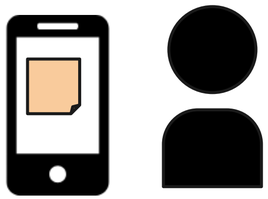
A resource on a.com



Served as a SXG on b.com
with signature from a.com

Note: currently there's no general mechanism to go from a URL on a.com to find the signed copy on b.com

UA verifies that a.com signed the resource, and then treats it as coming from a.com



Decouples the origin of the content and who distributes it.

Content, once published and signed, can be loaded from anywhere, **including IPFS**, and the browser will execute it under its true origin.

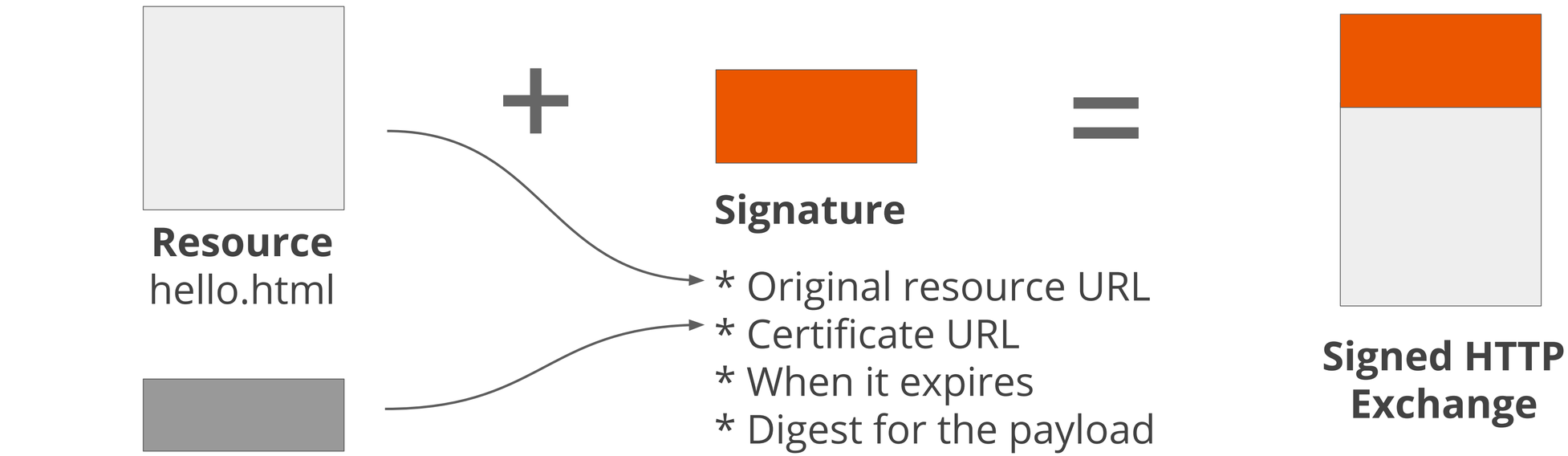
Exchanges can be “Bundled”

Exchanges, or SXGs, can be also **bundled**, so that an entire web page / site can be packaged up and can be distributed. Like books!

(* Note: Bundled exchange is NOT implemented in any browsers YET)

Visit bit.ly/webpackaging to find more about “Web Packaging” proposal

Signed HTTP Exchanges: More Details



- “Cacheable” content only, no Cookies or Authenticate headers allowed
- Intended for “public” content only
- Short expiry signature (max 7 days)

Trying SXG in Chrome

- Chrome **shipped SXG** in Chrome 73
- Google Search supports SXG for AMP results
  - For privacy-preserving prefetching, i.e. prefetching result pages w/o connecting to publisher
  - Try searching for “amp by example” on google on Android, click results with mark
- **Bundled exchange** is under development-- stay tuned!

Demo!