Status

- Draft-hodges-strict-transport-sec-02 submitted on 11-Jul-2010
- Addressed (almost) all known open issues
Open Issues

• Julian notes that Effective Request URI is now manifested in HTTPbis (was leveraged from HSTS spec)
  • Should HSTS ref HTTPbis for this?
    • [ I think yes (assuming they are on-schedule for finishing HTTPbis before Sol engulfs Gaia :) ]

• Gerv suggested (a while back) a “LockCA” notion
LockCA

• Add directive to Strict-Transport-Security header field of “LockCA”

• Semantics are that UA remembers not only that site is secure-only, but also that its certs are issued by CA
  • From initial caching of HSTS info?
  • Supplied along with LockCA directive in header field?
Evonly

- Refinement of LockCA
- There's operational issues with LockCA
  - Eg what if site wishes to change their CA?
- With EV only, UA notes that site's cert MUST be an EV cert.
  - Leverages EV infrastructure (CA/Browser Forum)
  - Site can change CA
ToDo

- Remove Effective Request URI
- Add Evonly
- Publish HSTS spec as a WEBSEC WG draft