Cookies: HTTP State Management Mechanism
draft-ietf-httpbis-rfc6265bis-10

Feb 28, 2022

Recent changes: -10 draft

- Standardize Max-Age/Expires upper bound: #1732, #1980
  - Expiry date now SHOULD be capped at 400 days in the future
- Expand on privacy considerations and third-party cookies: #1878
  - Expands spec's opinion on the privacy concerns of cookies
- Specify that no decoding of Set-Cookie line should occur: #1902
  - UA should not attempt to decode percent encoded character
- Require ASCII for domain attributes: #1969
  - The value of the Domain attribute must be a string of ASCII characters
- Editorial Changes:
  - #1789, #1858, #2069

Recent changes since -10

- Remove note to ignore Domain attribute with trailing dot: #2087, #2092
  - Correction that trailing ‘.’s should be ignored
- Remove an inadvertent change to cookie-octet: #2090
  - For 2 years servers were incorrectly advised to include %x80-FF
- Remove note regarding cookie serialization: #2165
  - The note wasn’t quite correct and could be better handled by the HTML spec
- Add case insensitivity note to Set-Cookie Syntax: #2167
  - Clarify that attribute names are case insensitive
- Add note not to send invalid cookies due to public suffix list changes: #2215
  - Discourage sending cookies that are part of a public suffix
- Add warning to not send nameless cookies: #2220
  - Discourage nameless cookies of any sort
- Improved max-age attribute parsing: #2214
  - Notes that values are base 10. Handle missing and invalid values.

Current Issue Status

4 open issues

- Currently in Scope
  - cookie-octet reality check: #2185
    - Spec’s current structure is confusing and prone to incorrect implementation.
  - Same-Site cookies and redirects: #2104
    - Enforcement of same-site redirect chains results in copious site breakage
- Maybe should defer
  - Parser for Domain attributes: #1939
    - How does the domain sub-algorithm know if something is an IP address
  - RFC 6265bis: Set-Cookie parsing algorithm should enforce more of the syntax requirements: #1399
    - UAs should start to enforce the more stricter Server syntax requirements
- An additional 14 deferred issues