

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

Oct 5, 2022

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.

Recent changes since -10 Continued

- Offload Service Worker SFC computation to spec: [#2217](#)
- Compare cookie name prefixes case-insensitively: [#2236](#)
- Prevent nameless cookies with prefixed value: [#2251](#)
- Editorial Change: [#2244](#)

Current Issue Status

12 open issues

- Currently in Scope
 - Same-Site cookies and redirects: [#2104](#)
 - Enforcement of same-site redirect chains results in copious site breakage
 - Set-Cookie parsing algorithm should enforce more of the syntax requirements: [#1399](#)
 - nameless cookies, client/server inconsistencies: [#2229](#)
- An additional 18 deferred issues