

HTTP Session Continuation Problem Statement

IETF-87, Berlin



Status

- [draft-ietf-websec-session-continue-prob-00](#)
- Despite name, not a WG draft (yet)
- Several protocol proposals exist
- Out of scope for now

Motivation

- Variable auth token
 - To resist BEAST, CRIME etc.
 - Channel bound cookies are OK
- Explicit logout
- Manageability
 - E.g. query session state, report on open sessions, ...
- Negotiable replay protection
- Channel binding
- Make HTTP/Negotiate better (reduce freq. of authen.)

Requirements

- Support authenticated and unauthenticated sessions
- Support HTTP and HTTPS
- Implementable with no server state as an option
- Expressed via HTTP headers
- Crypto strength
- Cannot reuse TLS-protected SC values in unprotected context
- Protected against MITM when used with TLS, e.g. anonymous sessions
- Explicit logout
 - Initiated by either party
 - Will not be possible in truly stateless server use cases
- Works across proxies
- Sessions should be tied to Origins™ (with a good def. of “origin”)

Next Steps

- Adopt as WG document?
- Needs more review before we all go into solution space

Thank You!

yarolf.ietf@gmail.com

nico@cryptonector.com

