Token Binding over HTTPS

I-D Changes Since IETF 94

Vinod Anupam, Google Inc.
Token Binding HTTP Header

- Changed name back to “Sec-Token-Binding”
- Carries the EncodedTokenBindingMessage as before
- Sec- prefix makes it a “forbidden header name”
  - Header stays completely under user agent control
- Key reason: Integrity Protection in user agents like Web Browsers
  - Disallows scripts etc. from directly manipulating that header
Privacy Considerations

● Expanded Section

● Key ideas (still) that UA should
  ○ Use different Token Binding Key for different public suffix (eTLD+1)
  ○ Provide privacy parity for existing behavior
    ■ Allow users to delete TB Keys like they can Cookies
    ■ Auto-delete TB Keys like Cookies at the end of Private Browsing Mode
Token Binding Federation

- Added Federation Example
  - Adding Token Binding Id into OpenID Connect ID Token

- Include-Referer-Token-Binding-ID header honored only if Token Binding in use

- Minor edits for clarity
Ongoing Discussion: Federation

1: “I want to log in”

2: “Go get an id token from idp.com”

5: “Here is the id token from idp.com”

6: “You’re logged in. Here is your cookie”

3: “Give me an id token for rp.com”

4: “Here is your id token for rp.com”

“Who are you??”

“username: bob & passwd: 12345”

Need: Client must tell IDP the binding key for client-RP TLS connection

Need: Token from IDP must be bound to client-RP TLS connection.
Links And Contact Information

• TLS Extension for Token Binding Negotiation: https://datatracker.ietf.org/doc/draft-ietf-tokbind-negotiation/

• The Token Binding Protocol Version 1.0: https://datatracker.ietf.org/doc/draft-ietf-tokbind-protocol/

• Token Binding over HTTPS: https://datatracker.ietf.org/doc/draft-ietf-tokbind-https/

• GitHub: https://github.com/TokenBinding/Internet-Drafts

• Dirk Balfanz balfanz@google.com

• Andrei Popov andreipo@microsoft.com