Framing questions - Force reauthN

n.b., These are less "questions" than "summuppance of email thread on the topic"

- We agreed that *__recommended__* IdP action for SLO notice is “kill IdP session, then do what you want”.
- We agreed that notwithstanding #1, an IdP can do nothing in response to SLO, and still be in compliance with the profile.
- Therefore, SPs need to assume that SLO/IdP Logout may not happen, even when talking to an IdP that conforms to the profile.
- From a risk perspective this is consistent.
    - From the SP’s risk and security standpoint (protecting the user’s access from being hijacked through unauthorized access to the current device), this behavior is consistent with supporting SSO, because the SP can’t know when the device is at risk/when an SSO session already exists anyway.
    - Ipso facto, if an SP allows SSO in any instance, it realistically can’t be concerned (relative to its own security) about whether SLO messaging actually ends any non-local sessions.
    - This means that effectively SLO represents a security hook for the IdP, not an SP security hook
- SPs that do not find the above “sufficient” need to consider requiring ForceAuthn.
    - Because the deployment profile calls out that IdPs must support ForceAuthn in a reasonable way (issue #35) and that SPs that request ForceAuthn must verify the “freshness” of the assertion they receive (issue #36), this is still supported under the profile.
- We all understand that in practice ForceAuthn may not really do anything meaningful either, though this is more a question of IdP’s “misbehaving” than an IdP “option”.
    - This *__may__* imply a need for entity tags to allow SPs to do something for non-conforming IdPs, even though it’s not clear what they could do in this case other than refuse logins from non-such IdPs.