What Does Logout Mean?

Michael B. Jones, Identity Standards Architect, Microsoft

Brock Allen, Software Security Consultant, Solliance

January 26, 2018

Submission to March 2018 OAuth Security Workshop at Trento, Italy

1 OVERVIEW

Digital identity systems almost universally support end-users logging into applications and many also support logging out of them. But while login is reasonable well understood, there are many different kinds of semantics for "logout" in different use cases and a wide variety of mechanisms for effecting logouts.

It's telling that OpenID Connect has three different specifications for different logout mechanisms:

- OpenID Connect Session Management 1.0 [OpenID.Session]
- OpenID Connect Front-Channel Logout 1.0 [OpenID.FrontChannel]
- OpenID Connect Back-Channel Logout 1.0 [OpenID.BackChannel]

SAML 2.0 similarly had multiple different logout mechanisms that were used in different contexts.

Differences in logout mechanisms include (but are not limited to):

- Whether logout is reliable or best-effort
- Whether only the application is logged out or also the identity provider
- Whether only web applications are logged out or also native applications
- Which authorizations created by login, such as refresh tokens, access token, HTML5 local state, etc. are revoked and cleared by logout and which are not

Logouts can be invoked for these and other reasons:

- End-User action
- Application time-out
- Identity Provider time-out
- Due to detection of anomalous behavior or account compromise
- Due to account termination

During the workshop, we will lead a discussion on what "logout" means in different contexts and what the usability, application, and security implications of the different meanings and mechanisms are. ***Logout definitely isn't "one size fits all"!***

2 REFERENCES

[OpenID.Session] de Medeiros, B., Agarwal, N., Sakimura, N., Bradley, J., Jones, M, "OpenID Connect Session Management 1.0 - draft 28", openid-connect-session-1_0-28 (Implementer's Draft), January 2017.

[OpenID.FrontChannel] Jones, M., "OpenID Connect Front-Channel Logout 1.0 - draft 02", openid-connect-frontchannel-1_0-02 (Implementer's Draft), January 2017.

[OpenID.BackChannel] Jones, M. and J. Bradley, "OpenID Connect Back-Channel Logout 1.0 - draft 04", openid-connect-backchannel-1_0-04 (Implementer's Draft), January 2017.