Australian Government
Digital Transformation Agency

dta

Single Sign-On

GovPass Platform Architecture Group Item #X

Advocate

The advocate for this item is Ben Bildstein (DTA).

Background

Single sign-on: Single sign-on (SSO) refers to the ability for a user to make use of their digital identity at multiple services in a short period of time, with only a single user authentication. I.e. where two or more services or transactions would normally each require a user authentication event, if these transactions are completed within a reasonable timeframe (session timeout), and within the same web browser session, then their digital identity information can be cached in an authentication session, and reused, to avoid the inconvenience of additional authentication.

Single log-off: Single log-off (SLO) refers to the ability for a user, who has used single sign-on to connect to multiple services within a session, to be able to log out of all services with a single action. I.e. so that the user is not expected to re-visit each service they have interacted with, just to log-off of each service. It is important to note that SLO is generally the hardest part of an SSO solution to implement. However, it is generally not appropriate to implement any support for SSO without including some support for SLO, and so in general the term SSO usually refers to both collectively.

Single Sign-On problem statement: SSO is more than just a nice-to-have convenience feature, but rather a significant user experience requirement for any complex transaction that includes login to more than one component as part of the user journey. For example, within GovPass, this happens when a user attempts to log in to a relying party in a business context, but has not yet configured ABNs in RAM. In this case, the user will complete their login before the Exchange determines that no ABNs are configured, at which point the user will be prompted to log in to RAM to configure an ABN.

Without SSO, this will be experienced by the user as follows:

1. start the login process for a business service
2. complete myGovID login
3. be sent to RAM to configure an ABN
4. complete myGovID login
5. consent to share attributes with RAM
6. create ABN relationships in RAM
7. restart the login process for the business service
8. complete myGovID login
9. consent to share attributes with the business service
10. access the service

Single Sign-On solution:

With SSO, this user experience may be as simple as:

1. start the login process for a business service

2. complete myGovID login
3. be sent to RAM to configure an ABN
4. consent to share attributes with RAM
5. create ABN relationships in RAM
6. restart the login process for the service (e.g. Grants)
7. consent to share attributes with the service
8. access the service

The simplest possible implementation to achieve this is for Exchange to create an authentication session for the user, storing their core identity attributes (as sent by the identity provider) for the duration of the session.

The simplest way for the Exchange to store the identity attributes is in an encrypted cookie in the user's browser, which ensures that no party is vulnerable to compromise to extract these attributes from storage.

Single Log-Off solution:

When a user has authenticated to multiple relying parties (e.g. a business service, and RAM), the user needs a way to sign out of both relying parties. Importantly, the user will have navigated away from one of these relying parties (e.g. RAM), but may still be signed in. Therefore, for the best possible user experience and security posture, we will provide a method for the user signing out of both services.

Any implementation to achieve this requires all systems to provide some level of support.

Each relying party in the federation must implement a method of logging off the user. The simplest implementation is to have a URL with the sole purpose of killing the browser session of the user. (Note that this has been implemented in myGov.)

Following on from this minimal implementation at the relying parties, the Exchange will need to support the invocation of these session killing URLs. The simplest user experience would then be enabled by the Exchange providing a landing page for sign-out, with a confirmation step for the user to sign out of all other relying parties.

The resulting user experience is (after completing business at the target business service):

1. user clicks "log out" at the business service
2. user is logged out of the current business service and redirected to Exchange logout page
3. Exchange shows the user the other services they have logged in to
4. user confirms logout of all displayed services
5. user is logged out of all services, and a message to this effect is displayed

Australian Government
Digital Transformation Agency

dta

Recommendation

I recommend that the GPAG agree that:

1. The above solutions for SSO be taken as a candidate solution for the feature
2. This proposal be sent to the GovPass User Experience Group for validation
3. Subject to UXG validation, this proposal be reviewed by the various product teams for viability