**SSE Use Case Template**

**Title**

< Short one-line title of the use case >

**Authors (Affiliations)**

< Name and company affiliation of submitting author(s) >

**Short Description**

< Short description, 2-4 lines max. Can be used for building summary table of use cases, etc. >

**Transmitter**

<Who sends the signal/events >

**Receivers**

< Who receives these signals/events >

**Detailed Description**

< All details go here, we will still make write-up consistent between different use cases >

**Flow Diagram** (optional)

< Any flows to explain the use case >

**Notes/Open Questions** (optional)

< Any other pieces of information relevant for the use case, not covered above >

**SSE Use Case Example**

**Title**

G-Suite Security Scenario

**Authors (Affiliations)**

Atul Tulshibagwale (Google)

**Short Description**

G Suite can benefit from updated information from third-parties because it can adjust the access it provides to a session based on updated session attributes asserted by a third-party such as an identity provider or an endpoint protection service.

**Transmitter**

IdP (e.g. Ping, or Thales STA)

**Receivers**

SP (e.g. G-Suite)

**Detailed Description**

The specific use case detailed here is as follows:

1. A third-party IdP (referred to as “The IdP” here) creates a SAML assertion to login the user to G Suite. The user then is able to access various G Suite services such as Drive and Gmail.
2. The third-party IdP later realizes that the user is demonstrating suspicious behavior on other websites (i.e. attempting to login to multiple websites using The IdP’s gallery that they do not have access to)
3. Using CAEP the IdP signals to G Suite that the user is displaying suspicious behavior.
4. As a preventive measure G Suite turns off access to any file that has personally identifiable information in it.
5. At a later time, The IdP forces the user to re-login using a second factor. The user is able to successfully complete the 2-factor authentication.
6. The IdP then asserts to G Suite using CAEP that the user session has a higher assurance level.
7. G Suite then enables the user to access any file they normally have access to (including those with PII).

**Flow Diagram** (optional)

None, see steps in Detailed Description

**Notes/Open Questions** (optional)

To identify the specific session, the IdP includes a unique SAML Request ID in the SAML assertion used to establish federated session. This is included even if the SAML session was established without a SAML request from G Suite.

Due to network latencies or connectivity issues, it is possible that a message published earlier is received by a subscriber later than a later published message by the same publisher. When this happens with reference to the same user session, it can cause improper actions to be taken. Here’s how G Suite can handle these situations:

1. G Suite will ignore any messages that have a timestamp set in the future beyond some fuzz factor.
2. G Suite maintains a value for the latest CAEP timestamp per session, per publisher.
3. If G Suite receives a message relating to a session that is published earlier than the latest timestamp recorded for that session and publisher, it ignores the message.
4. If G Suite receives a message relating to a session that is published later than the latest timestamp recorded for that session and publisher, it will store the updated timestamp and process the message as described above.