# SLO in JISF

## Why SLO (Single Logout) is important ?

SAML single sign-on (SSO) allows the end-user to securely authenticate across multiple applications by logging in once using one set of credentials.
However, authentication is only the first half of the story. Unless the user manually logs out of each session that they seamlessly accessed, they leave behind a trail of orphaned sessions. This is where single logout (SLO) comes in. SLO allows the end-user to terminate all sessions by initiating the logout process once. End-users rarely log out of every session established during SSO. All these orphaned sessions increase your attack surface, and ideally, this is something that you should attempt to fix for the user.

SLO is a SAML flow that allows the end-user to logout from a single session and be automatically logged out of all related sessions that were established during SSO.

### The Protocol:

The end-user can initiate the SLO process from within the Identity Provider (IdP) or one of the Service Providers (SP). We typically see SLO initiated from an SP; however, an IdP can also trigger SLO for other reasons, for example, if an agreed global timeout has been exceeded or if the user credentials have been compromised.

SLO can use asynchronous bindings (front-channel), such as the HTTP Redirect, POST, and Artifact bindings, to send logout messages via the user agent (a browser). Alternatively, synchronous bindings (back-channel), via SOAP, can be used for direct server-to-server communication bypassing the user agent.

#### The Flow:

When initiating SLO from a Service Provider, the following flow will take place:

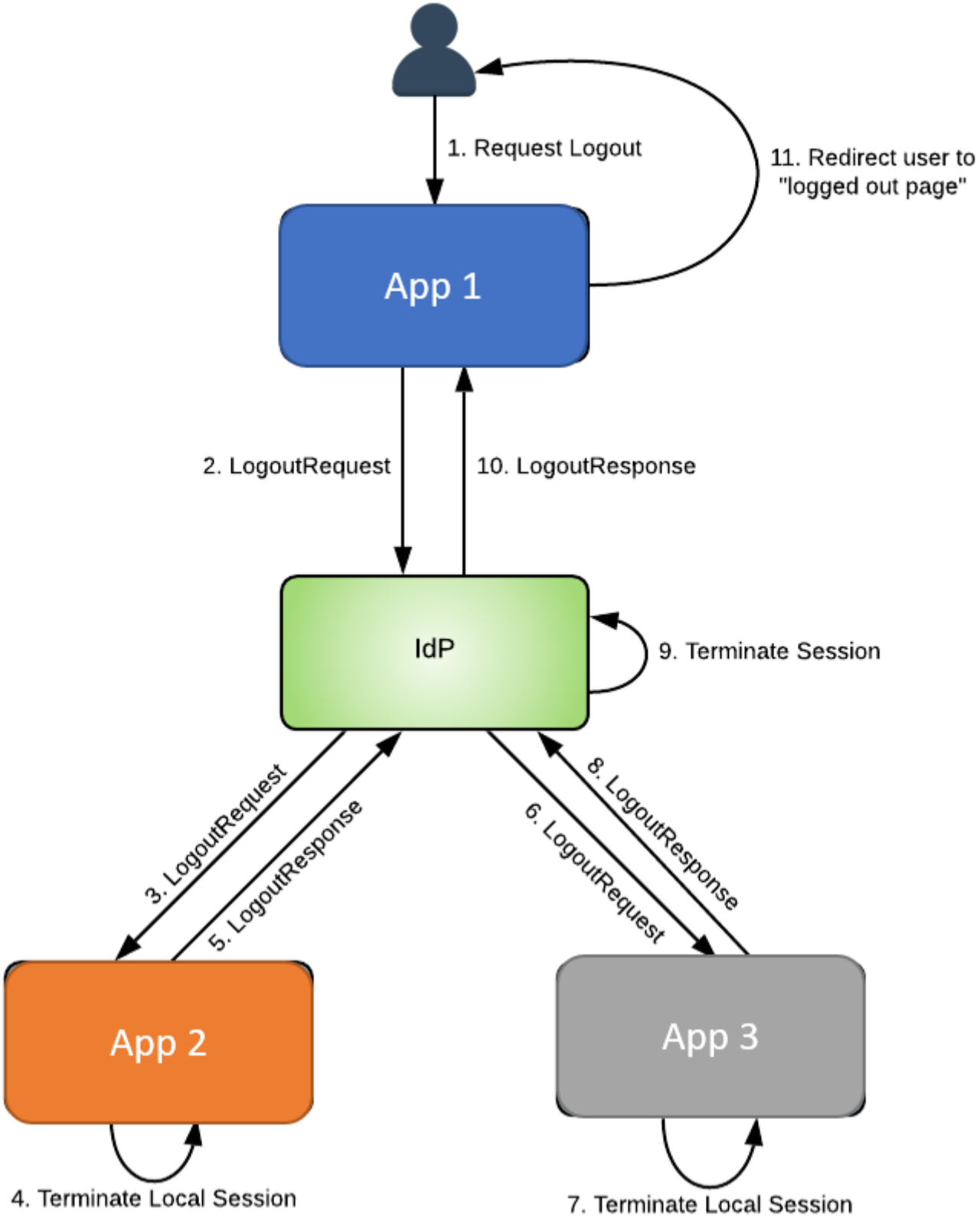


FIgure: SLO Process

- **Step 1:** The end-user initiates the SLO process by clicking a logout button within an SP
- **Step 2:** The SP terminates the user's session and triggers SP-initiated SLO by sending a logout request to the IdP
- **Step 3:** Upon receiving a logout request, the IdP first identifies all other SPs that are part of the current session, and iteratively performs the following steps for each SP. This is

known as IdP-initiated SLO
    1. IdP sends a logout request to the SP
    2. IdP redirects the user to the SP's SLO endpoint
    3. IdP waits for a logout response
- **Steps 4-8:** Each SP validates the logout request and terminates the user's session before returning a logout response to the IdP
- **Steps 9-10:** Once the IdP receives logout responses from all SPs, it terminates its own user session and sends a logout response to the originating SP. The logout response includes a status code which informs the originating SP whether SLO completed entirely or partially
- **Step 11:** The originating SP can then redirect the user to another page, such as a "logged out" page

# SAML SLO Request

A SAML logout request follows your typical SAML message structure, with an ID, lifetime data, and information about its origin and destination.

However, it also includes the name ID of the user who is being logged out. This allows the IdP or SP to confirm that they are logging out the correct user. For instance, if a logout request is received for Bob, but Alice is currently logged in, the IdP or SP would deny the request.

The logout request can optionally contain the reason for the logout, such as if it has been initiated by a user or an admin, or if a global timeout was exceeded:

```
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_9088cb8766164b149e63358b92ece1c3"
    Version="2.0"
    IssueInstant="2020-05-11T20:24:11Z"
    Destination="https://idp.identityserver.com/saml/slo"
    NotOnOrAfter="2020-05-11T20:26:11Z"
    Reason="urn:oasis:names:tc:SAML:2.0:logout:user">
   <saml2:Issuer>https://sp.identityserver.com/saml</saml2:Issuer>
   <saml2:NameID>d65a1ecb97404a988c0b9c18cc915e3b_scott</saml2:NameID>
</saml2p:LogoutRequest>
```

## SAML SLO Response

A SAML Logout response also follows your typical SAML message structure, with an ID and information about the message's origin and destination.

However, the SLO also includes the ID of the original SAML logout request message, which the Idp or SP can use to correlate responses with original requests to confirm that the response was

intended for it.

The logout response also contains a status code, which indicates whether SLO failed or completed successfully or partially:

```
<saml2p:LogoutResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_145745962cdb411d91d80967fb082643"
    Version="2.0"
    IssueInstant="2020-05-11T20:26:36Z"
    Destination="https://sp.identityserver.com/signout-saml"
    InResponseTo="_9088cb8766164b149e63358b92ece1c3">
  <saml2:Issuer>https://idp.identityserver.com</saml2:Issuer>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
</saml2p:LogoutResponse>
```

---

Revision #5
Created 27 September 2021 21:15:23 by Niton
Updated 28 September 2021 21:50:42 by Niton