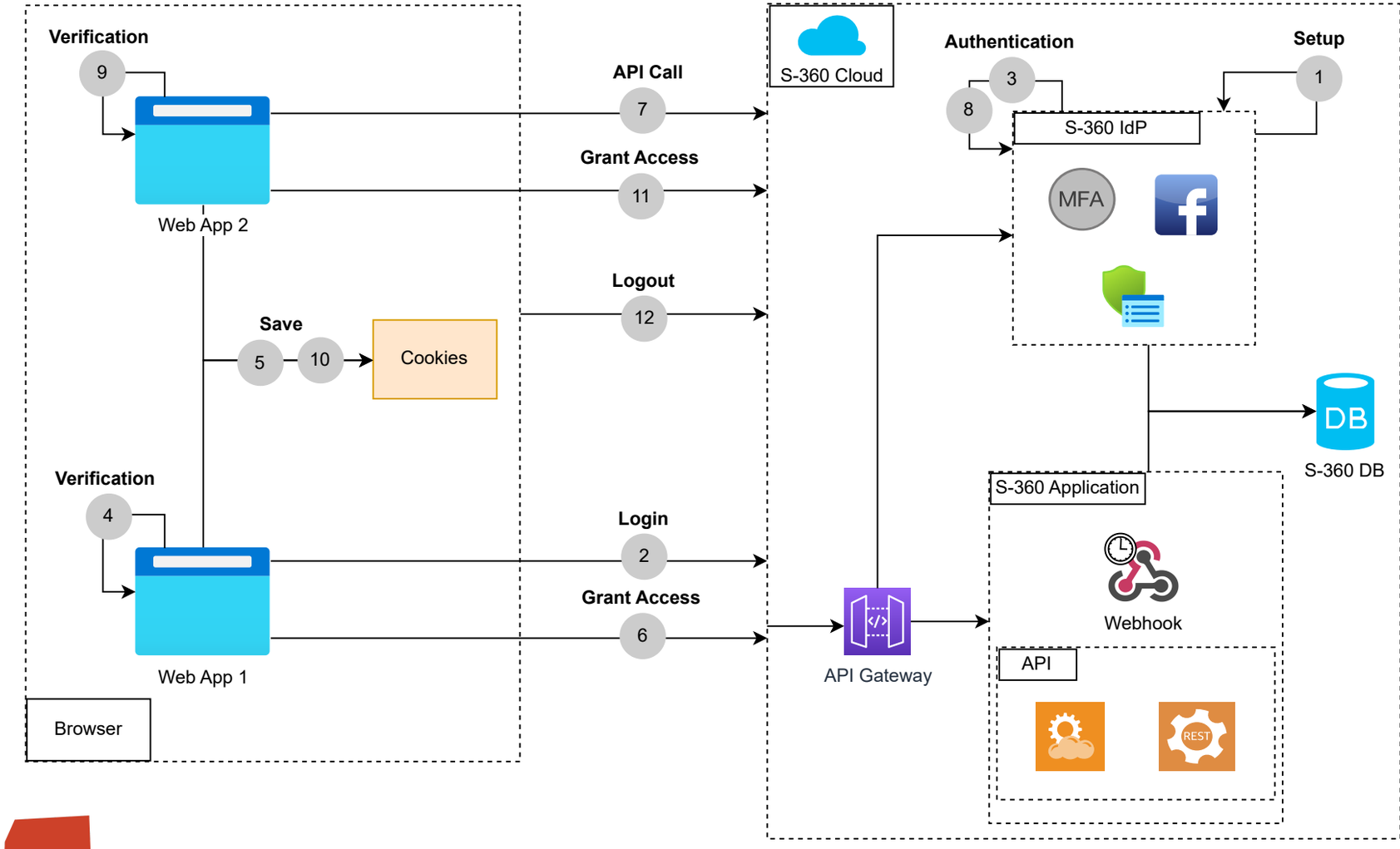
SSO integration as IdP using SAML

SecuTix platform provides an IdP for SSO authentication, using SAML technology.

The reference architecture explains the integration steps for different use cases.



1 **Setup :** The SSO needs configuration, in order to add the different sources as SP, to configure the certificates and points of sale.
Further details can be found following this link.

2 **Login :** User calls the API for the login (**/api/1/sso/saml/login**) , a POST of SAML request is performed and then the login form is displayed. The user identifies and the information are sent to the server.
The SAML request is created based on the PHP library provided by Secutix, for other language, the request should be built on the client side.

3 **Authentication :** The login details sent to the IdP server are used to authenticate the user, if the Login is correct, a SAML response is sent back to the user browser.

4 **Verification :** The SAML response sent back is verified and controlled, if it's ok, a new session is created on the customer website.
If the PHP library is used, the SAML response is easily decoded.

5 10 **Save :** Once the session is created, it will be stored within the cookies of the user's browser, so it will be used for further authentication and avoid loging-in multiple times.
This cookie contains user-related information. The domain to which this cookie is attached is the domain common to the organization's website and the purchase funnel.

6 11 **Grant Access :** Once the verification is done, the user is connected and can access all the services provided by the different applications that S-360 IdP gives access to.

7 **API Call :** To have access to App 2 services, a redirection is performed and a SAML request is sent to the IdP server along with the cookies of the last session.

8 **Authentication :** The Cookies sent to the IdP server are used to authenticate the user (Remember Me during the previous authentication should be activated), an assertion is sent back, a SAML response will contain the redirecting URL to the App2.

9 **Verification :** The SAML response sent back is verified and controlled, if it's ok, a new session is created on the customer website.
If the PHP library is used, the SAML response is easily decoded.

12 **Logout :** User calls the API to logout (**/api/1/sso/saml/logout**), a Get logout is performed and then the IdP server redirects to the URL specified for the consumer of the IdP. After logging out the different applications, the home page of the current application is then returned.

All the API definitions and limitations, can be found in the Secutix platform website.

SecuTix
THE TICKETING ENGAGEMENT PLATFORM

Reviewed for technical accuracy January, 2024

Secutix Reference Architecture