SAML Authentication Sequence

Last Modified on 10/03/2019 12:48 pm EDT

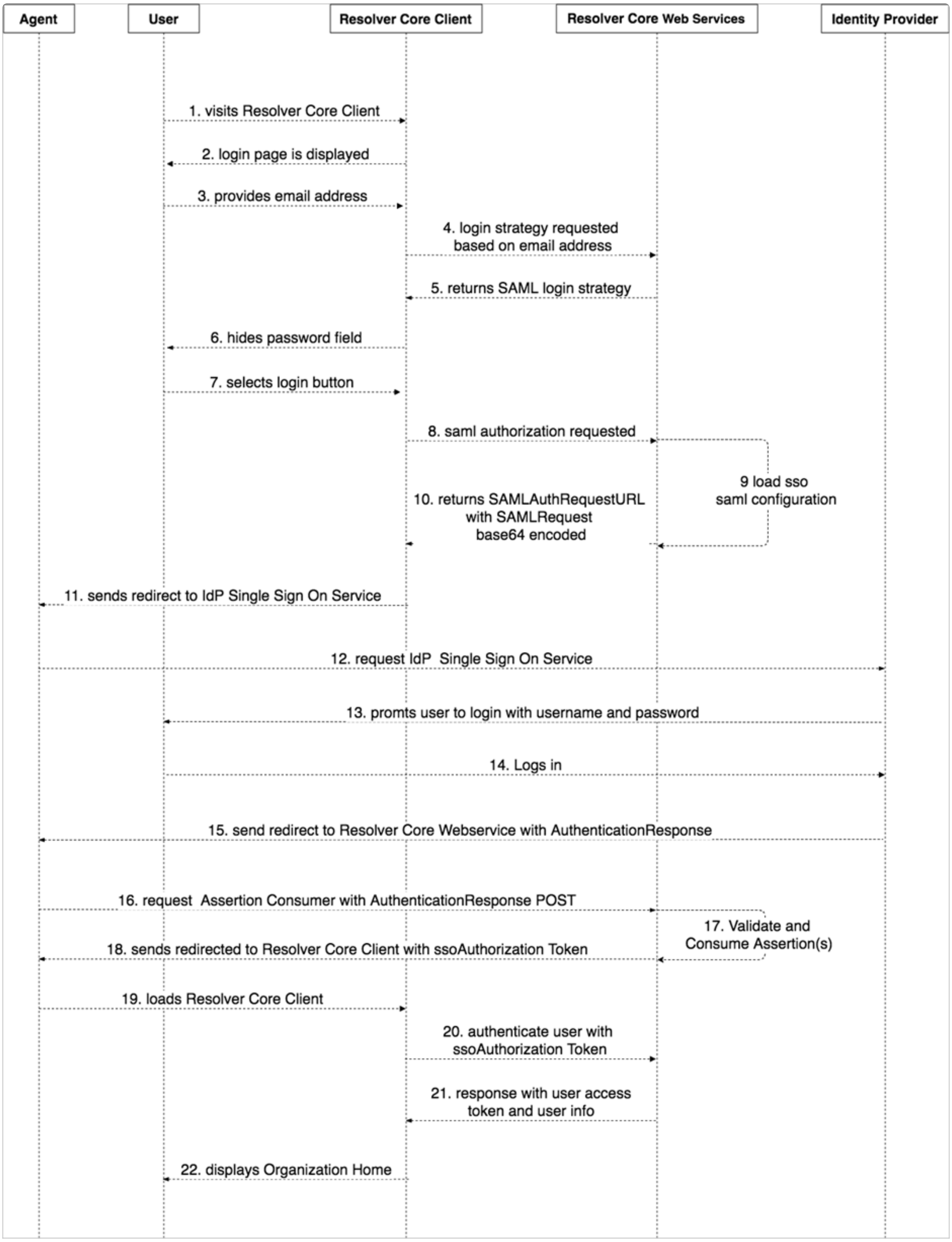
The roles in the below sequence include:

- **User:** Principal
- **Agent:** Web browser
- **Resolver Core Client (Client):** Web-based software GUI
- **Resolver Core Web Services (Web Services):** Service provider
- **Identity Provider (IdP):** ADFS, OneLogin, SiteMinder, CA, etc.

This sequence also assumes that:

1. The user exists in Core and is a member of at least one organization;
2. The user is not logged into Core;
3. SSO SAML configuration has been imported using the IdP metadata and the primary email domain name; and
4. The user is not logged into the IdP service.

SAML Sequence Diagram


Agent
User
Resolver Core Client
Resolver Core Web Services
Identity Provider
1. visits Resolver Core Client
2. login page is displayed
3. provides email address
4. login strategy requested based on email address
5. returns SAML login strategy
6. hides password field
7. selects login button
8. saml authorization requested
9 load sso saml configuration
10. returns SAMLAuthRequestURL with SAMLRequest base64 encoded
11. sends redirect to IdP Single Sign On Service
12. request IdP Single Sign On Service
13. promts user to login with username and password
14. Logs in
15. send redirect to Resolver Core Webservice with AuthenticationResponse
16. request Assertion Consumer with AuthenticationResponse POST
17. Validate and Consume Assertion(s)
18. sends redirected to Resolver Core Client with ssoAuthorization Token
19. loads Resolver Core Client
20. authenticate user with ssoAuthorization Token
21. response with user access token and user info
22. displays Organization Home

A sequence diagram showing the typical flow of SAML SSO authentication in Core.

1. User visits the Core client.
2. Client displays the login page.
3. User enters their email address.

4. Client requests the authentication strategy using the provided email address. Web Services loads and asserts SSO SAML configuration using the domain of the domain of the email address.
5. Web Services returns the authentication strategy to the Core Client.
6. Client hides the password field and sets its state into SSO SAML authentication strategy.
7. User clicks Login.
8. Client requests an SSO SAML authorization using the provided email address.
9. Web Services loads the SSO SAML configurations using the domain of the email address. The service uses the configuration to create a **SAMLRequestAuthentication**. The **SAMLRequestAuthentication** is a SAML 2.0 protocol XSD XML digitally signed deflated Base 64 encoded string.
10. Web Services returns the request URL, which is the Single Sign On service URL with the **SAMLrequest** query **PARAM** containing the **SAMLRequestAuthentication**.
11. Client sends a redirect to the Agent with the **SAMLAuthentication**.
12. Agent requests the SSO service with the **SAMLAuthentication**.
13. IdP service prompts the User to authenticate with their username and password.
14. User logs in and authentication is successful.
15. IdP sends a redirect to the Agent with the **SAMLResponse**.
16. Agent redirects to the consumer service in Web Services with the **SAMLResponse**.
17. Consumer service in Web Services validates the response and assertion, then retrieves the user identity from the assertion. The identity is the email address of the user who just logged in into the IdP. Web Services validates if the user exists. If the user exists and is active, an **ssoAuthorization** token will be created. This token is used by the Client to authenticate the user in Web Services and to obtain an access token.
18. Web Services sends a redirect to the Agent with the **ssoAuthorization** token.
19. Agent loads the Core client.
20. Client authenticates the user into Web Services using the **ssoAuthorization** token.
21. Web Services validates the token and authenticates the user into the Web Services. The Web Services then returns the user information and access token to the Client. The **ssoAuthorization** token is invalidated.
22. Client displays the homepage of the organization.