

client -> SAML -> SP (Web SSO) & identity provider (IdP) -> IDP

Single Sign On SSO

Browser Enterprise -> client -> SP (Web SSO) & IDP (Identity Provider)

- Client sends SAML login request to SP
- SP sends SAML response to client
- Client sends SAML response to IDP
- IDP sends SAML response to client
- Client logs in to SP

Web -> SP 5 phases: 1. User logs in, 2. SP auth, 3. SP to IDP, 4. IDP auth, 5. IDP to SP

- User logs in (User enters credentials)
- SP auth (SP checks user's password)
- SP to IDP (SP sends SAML request to IDP)
- IDP auth (IDP checks user's password)
- IDP to SP (IDP sends SAML response to SP)

Phishing -> SP (User enters credentials)

- User logs in (User enters credentials)
- SP auth (SP checks user's password)
- SP to IDP (SP sends SAML request to IDP)
- IDP auth (IDP checks user's password)
- IDP to SP (IDP sends SAML response to SP)

Client logs in (User enters credentials)

- User logs in (User enters credentials)
- SP auth (SP checks user's password)
- SP to IDP (SP sends SAML request to IDP)
- IDP auth (IDP checks user's password)
- IDP to SP (IDP sends SAML response to SP)

(Client logs in) <--> (SP) <--> (IDP) <--> (Client logs in)

- Client logs in (User enters credentials)
- SP auth (SP checks user's password)
- SP to IDP (SP sends SAML request to IDP)
- IDP auth (IDP checks user's password)
- IDP to SP (IDP sends SAML response to SP)
- Client logs in (User enters credentials)

SSO -> SP -> IDP -> Client

Client -> SP -> IDP

SP -> IDP -> SP -> Client

SAML

(Assertion) <--> SP (Identity Provider) <--> IDP (Assertion)

Assertion <--> SP (Identity Provider)

SP -> IDP (Assertion) <--> IDP (Assertion)

Assertion <--> IDP (Assertion)

Assertion <--> SP (Assertion)

הנתקן ID-8 גורם ID-7 ו-ID-6 למשתמשים או Service Provider
Under the provider SP

הנתקן ID-8 גורם ID-7 ו-ID-6 למשתמשים או Service Provider

ID-3351 מודולו SP Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black

SSO -> Authorization Can be done SAML

SAML מילוי

הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black

הנתקן Subject = ID-3351 - Authorization - SP - white - black
הנתקן Subject = ID-3351 - Authorization - SP - white - black

SP → (Assertion) → (Auth Assertion) → (Assertion)
 Assertion → (assertion) → (Post) → (Assertion) → (Assertion)
 SP → (Assertion) → (Assertion)

Vid → (Phone) → (SP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 (assertion) → (assertion) → (IP) → (Assertion) → (Assertion) → (Assertion)

IP → (Site First) → (Assertion) → (IP) → (Site First) → (Assertion) → (Assertion)

(Source Side First) → (SP) → (SP) → (SP) → (Assertion) → (Assertion)

ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)

ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)

(Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)

ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)

(Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)
 ITS → (Session cookie) → (IP) → (IP) → (Assertion) → (Assertion) → (Assertion)

(IP->SP) \rightarrow SP initiated post-to-post
 (IP->SP) Post -> SAML assertion -> SP initiated post-to-post
 (IP->SP) Assertion -> SAML response -> SP initiated post-to-post

SP initiated post-to-post

Post-to-post assertion pull -> pull-to-push. Push -> pull (push assertions are triggered by push and pull initiated by external parties).
 Pull-to-push assertion is triggered by pull initiated by external parties.
 Pull-to-push assertion is triggered by push initiated by external parties.
 Pull-to-push assertion is triggered by push initiated by external parties.

SSL -> IP-> SP. (IP->SP) \rightarrow (IP->SP) Pull -> SP. Man-in-the-middle (MITM) can intercept the message between SP and IP. MITM can intercept the message between SP and IP. MITM can intercept the message between SP and IP. MITM can intercept the message between SP and IP. MITM can intercept the message between SP and IP.

SP -> SP initiated post-to-post. Man-in-the-middle (MITM) can intercept the message between SP and SP. MITM can intercept the message between SP and SP. MITM can intercept the message between SP and SP. MITM can intercept the message between SP and SP. MITM can intercept the message between SP and SP. MITM can intercept the message between SP and SP. MITM can intercept the message between SP and SP. MITM can intercept the message between SP and SP. MITM can intercept the message between SP and SP. MITM can intercept the message between SP and SP.

SP -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post.

SP -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post.

SP -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post. (Artifact -> SP) \rightarrow (SP->SP) Push -> SP initiated post-to-post.

3) מילוי אובייקט Assertion ב-WS-BEAN ב-WS-Security כ-XML SAML Assertion. בפונקציית `createAssertion()` ב-WS-Security ישנו מערך `assertions` שבו מוגדרת Assertion.

מ长时间

לפניהם מוגדרת Assertion. Assertion מוגדרת כ-XML SAML Assertion. בפונקציית `createAssertion()` ב-WS-Security ישנו מערך `assertions` שבו מוגדרת Assertion.

Open ID

4) מילוי אובייקט Assertion ב-WS-BEAN ב-WS-Security כ-XML SAML Assertion. בפונקציית `createAssertion()` ב-WS-Security ישנו מערך `assertions` שבו מוגדרת Assertion.