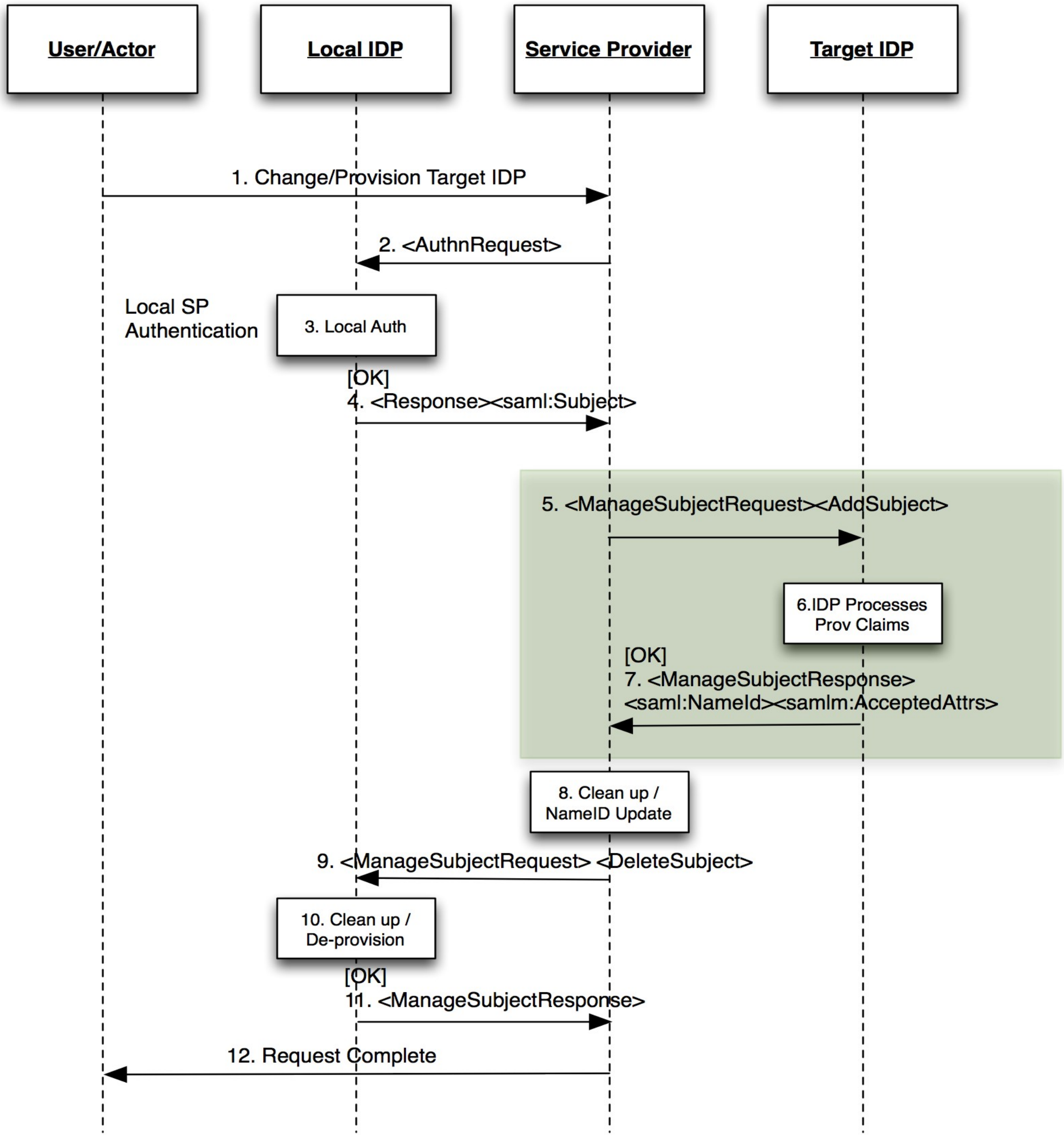
Discussion of section 2.4.1 of the Oracle/NSN sstc-saml2-management-protocol-02 proposal.

For the online profile of the AddSubject function, there appears to be 3 current alternatives.

1. ManageSubjectRequest/Add Operation
2. Extended AuthNRequest
3. Unsolicited Response

This document attempts to compare/contrast different options to identify the best solution.

ManageSubject/Add Operation


User/Actor
Local IDP
Service Provider
Target IDP
1. Change/Provision Target IDP
2. <AuthnRequest>
Local SP
Authentication
3. Local Auth
[OK]
4. <Response><saml:Subject>
5. <ManageSubjectRequest><AddSubject>
6.IDP Processes
Prov Claims
[OK]
7. <ManageSubjectResponse>
<saml:NameId><samlm:AcceptedAttrs>
8. Clean up /
NameID Update
9. <ManageSubjectRequest> <DeleteSubject>
10. Clean up /
De-provision
[OK]
11. <ManageSubjectResponse>
12. Request Complete

This method defines a new SAML operation "ManageSubjectRequest" as originally proposed in the SAML Mgmt Protocol Proposal. The AddSubject sub-element is defined either to carry a SAML Assertion or SAML EncryptedAssertion. As with a <Response> element, the AddSubject element can also carry SSO information.

Advantages:

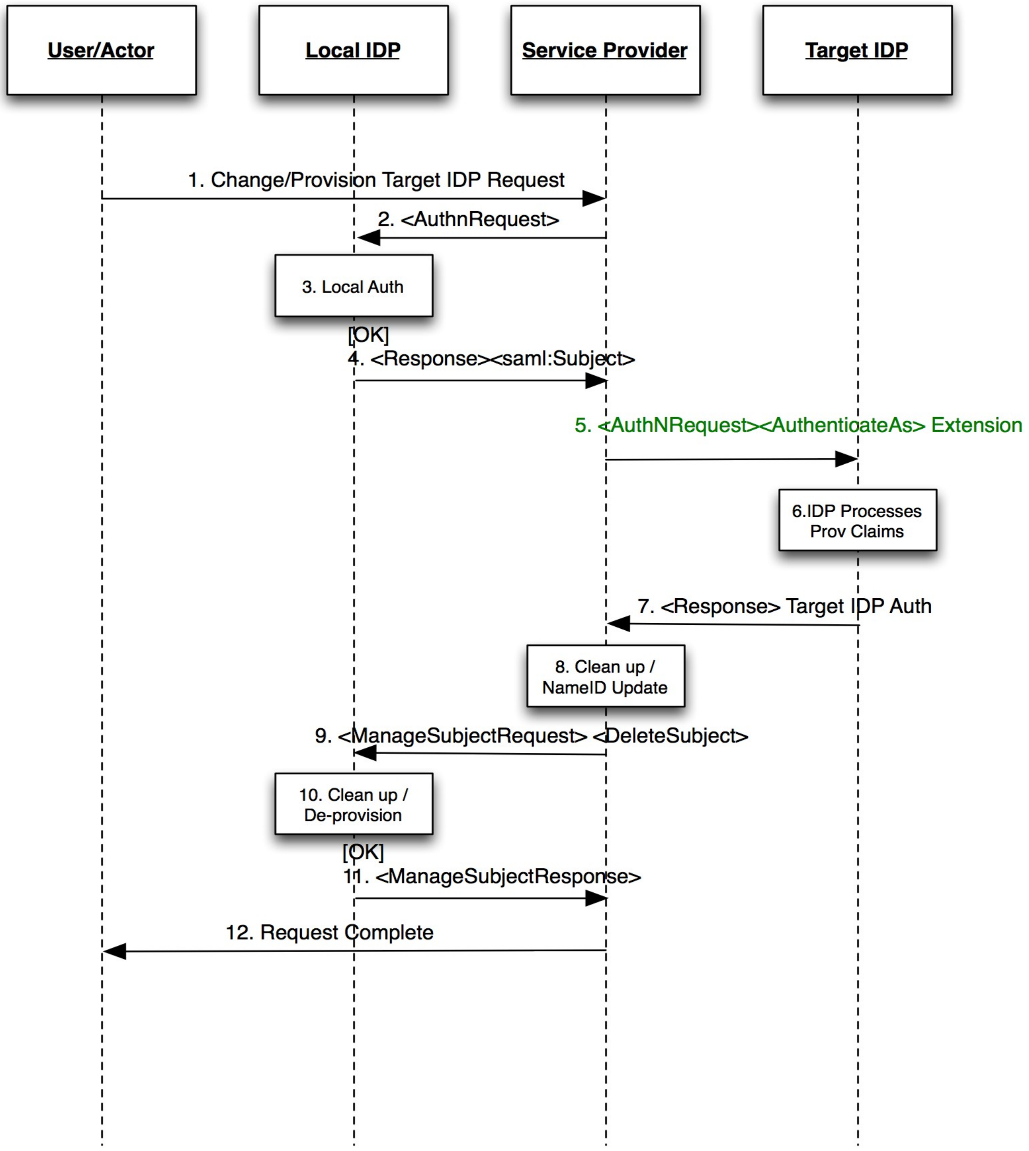
- Works for browser and offline profiles*
- Passes SSO session in browser profile if desired
- Distinct new operation.
- Operation may make more sense for SP “role”
- As a distinct operation, disposition of processing can be more detailed than typical with Authn Response
- Disposition of provisioning is understood.
- Can return extended information for extended workflows (e.g. URL for browser to follow, or email notification).
- An SSO Response is not needed in Step 7, this can happen later.

Disadvantage:

- Distinct new operation
- Authentication and provisioning is 2 steps
- Appears to duplicate functionality in current <Response> operation.

Authentication Request Method

This method takes the <AuthnRequest> and extends it to allow the requestor to include an existing SAML Assertion (<AuthenticateAs>) for the purpose of both passing along the authenticated session and to initiate a provisioning request. The Target, processes the request and returns its own SAML Assertion.


User/Actor
Local IDP
Service Provider
Target IDP
1. Change/Provision Target IDP Request
2. <AuthnRequest>
3. Local Auth
[OK]
4. <Response><saml:Subject>
5. <AuthNRequest><AuthenticateAs> Extension
6.IDP Processes Prov Claims
7. <Response> Target IDP Auth
8. Clean up / NameID Update
9. <ManageSubjectRequest> <DeleteSubject>
10. Clean up / De-provision
[OK]
11. <ManageSubjectResponse>
12. Request Complete

Advantages:

- SSO session from local passed to target
- Operation may make more sense for SP "role"
- RelayState can be used as normal
- Allows provisioning and re-authentication by Target to be handled in one step

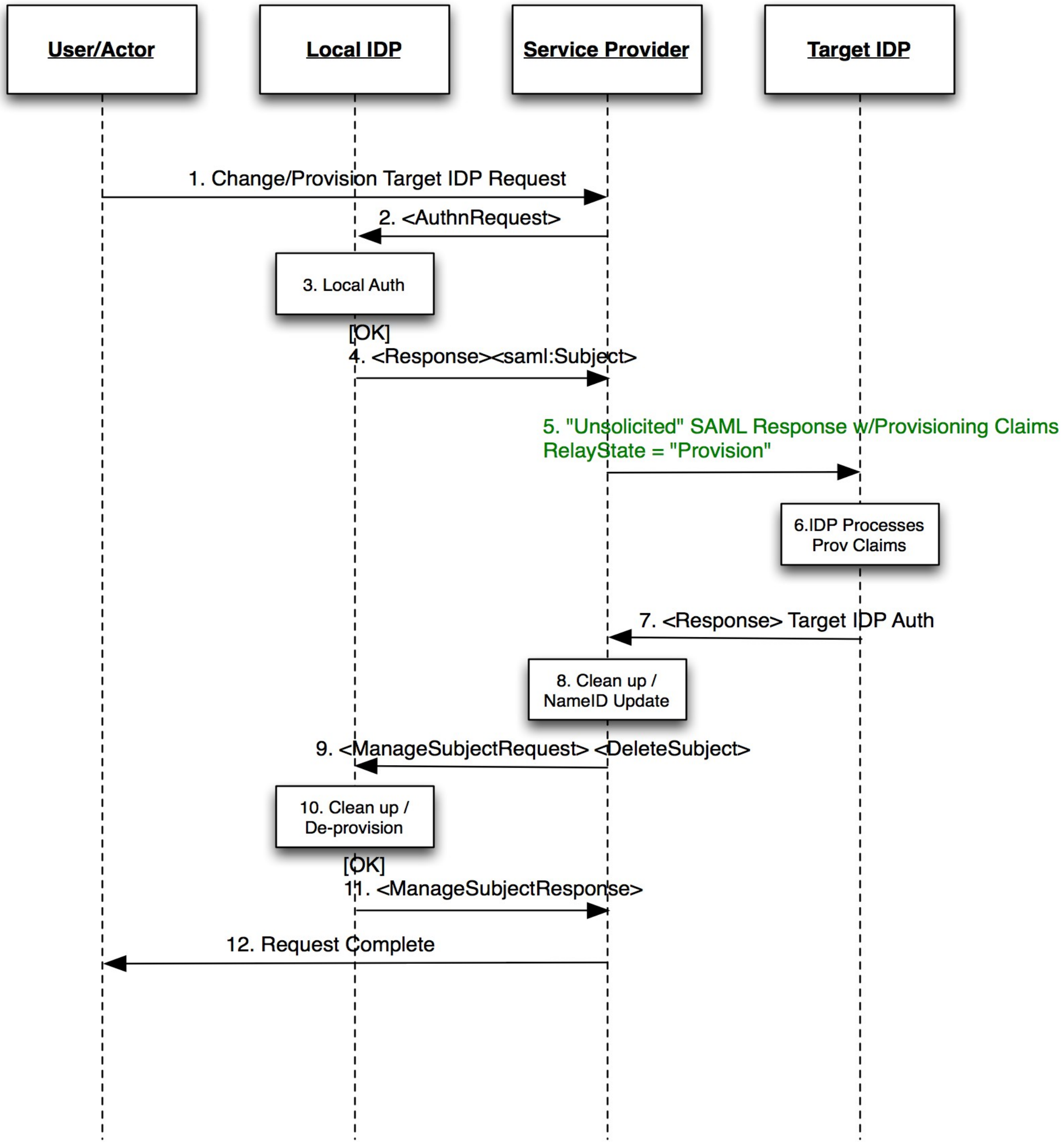
Disadvantage:

- Extension to <AuthnRequest> with <AuthenticateAs>

- Target IDP may not be able to return authentication in a single step (e.g. Due to extended workflow/approval requirement)
- How to differentiate between failed auth (e.g. Target may have secondary process to complete before it can authenticate) and failed provisioning?
- Different from offline profile
- Requires extended Status response definition to indicate provisioning as well as authentication status.

Response Request

The response request approach leverages the normal use of <Response> to pass along authenticated sessions from one IDP to the next. In using the "Unsolicited Response" profile, very little change (if any) is required to SAML Core spec.


User/Actor
Local IDP
Service Provider
Target IDP
1. Change/Provision Target IDP Request
2. <AuthnRequest>
3. Local Auth
[OK]
4. <Response><saml:Subject>
5. "Unsolicited" SAML Response w/Provisioning Claims
RelayState = "Provision"
6.IDP Processes Prov Claims
7. <Response> Target IDP Auth
8. Clean up / NameID Update
9. <ManageSubjectRequest> <DeleteSubject>
10. Clean up / De-provision
[OK]
11. <ManageSubjectResponse>
12. Request Complete

Advantages:

- SSO session from local passed to target
- Does not require modification of existing specification
- RelayState can be used as normal
- Allows provisioning and re-authentication by Target to be handled in one step

Disadvantage:

- Extension to <Response> or RelayState to indicate provisioning in step 5
- Reception of unsolicited response may be unexpected by IDPs

- A <response> to a <response> may be unexpected.
- Target IDP may not be able to return authentication in a single step (e.g. Due to extended workflow/approval requirement)
- How to differentiate between failed auth (e.g. Target may have secondary process to complete before it can authenticate) and failed provisioning?
- Different from offline profile
- Requires extended Status response definition to indicate provisioning as well as authentication status.