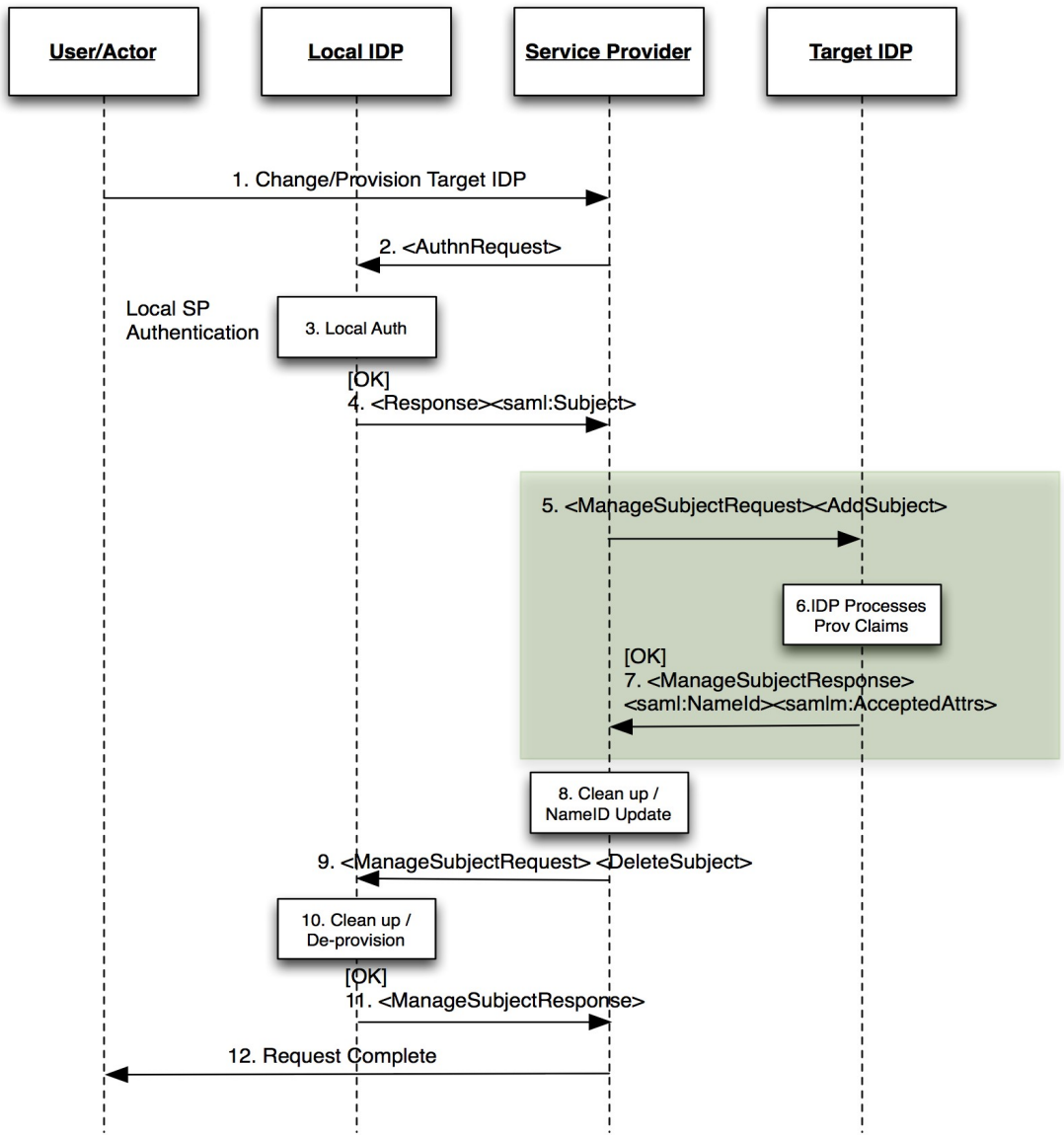
Discussion of section 2.4.1 of the Oracle/NSN sstc-saml2-management-protocol-02 proposal.

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
4. Notify Method

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

1 ManageSubject/Add Operation



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:

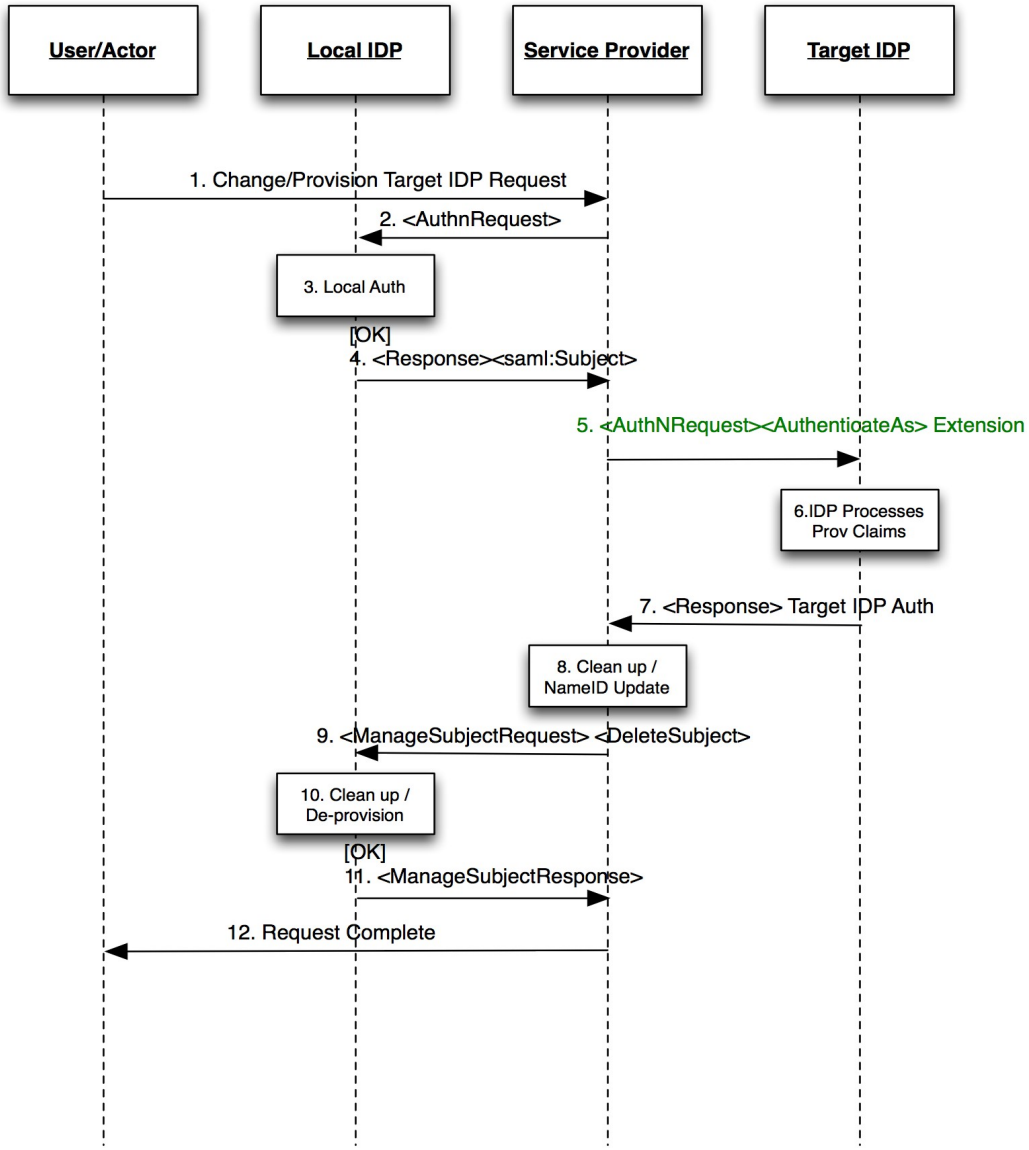
- Works for browser and offline profiles*
- Passes SSO session in browser profile if desired
- Distinct new operation.
- Operation may make more sense for SP “role”
- As a distinct operation, disposition of processing can be more detailed than typical with Authn Response
- Disposition of provisioning 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.

2 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.



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

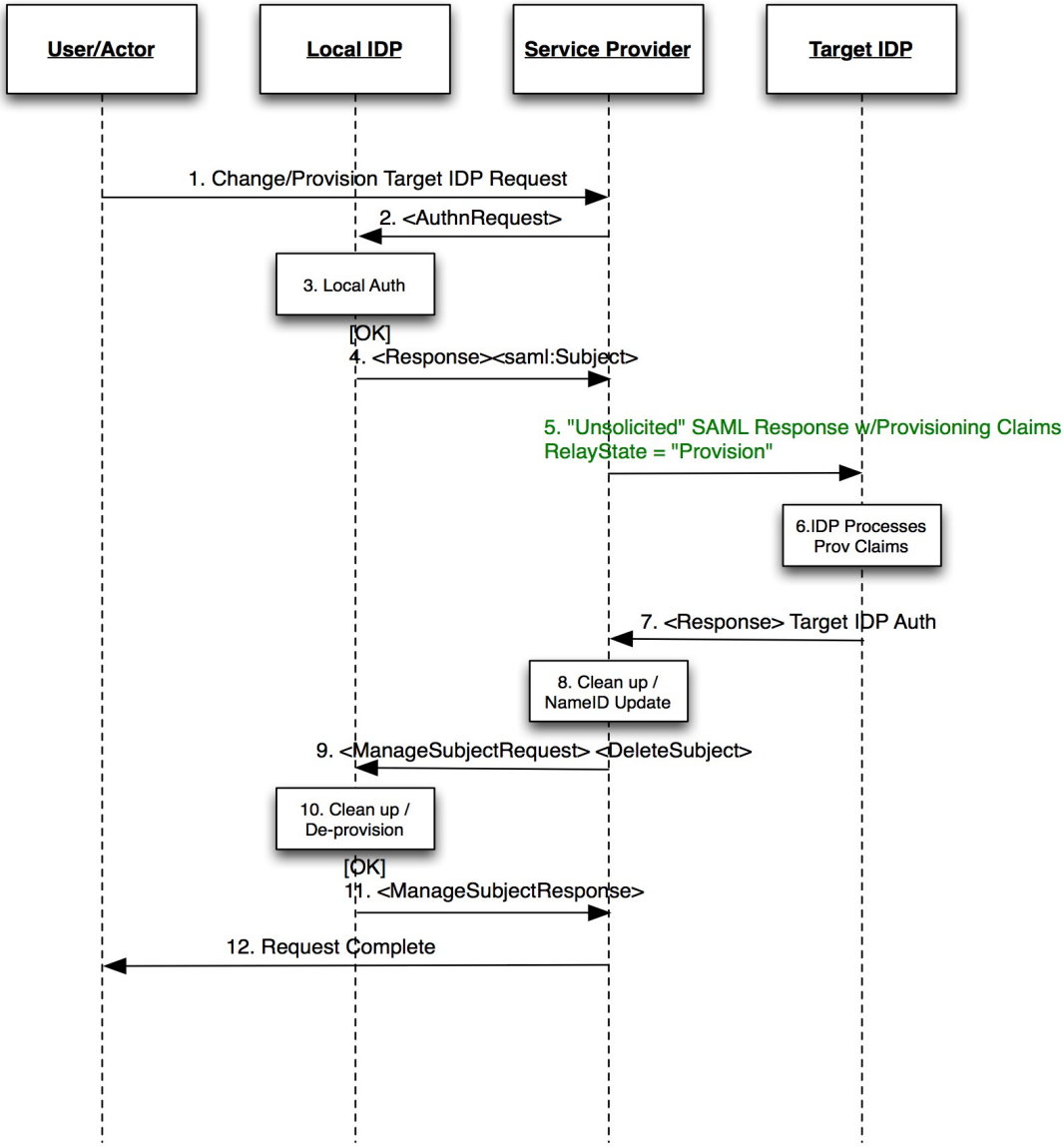
Disadvantage:

- 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.

3 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.



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:

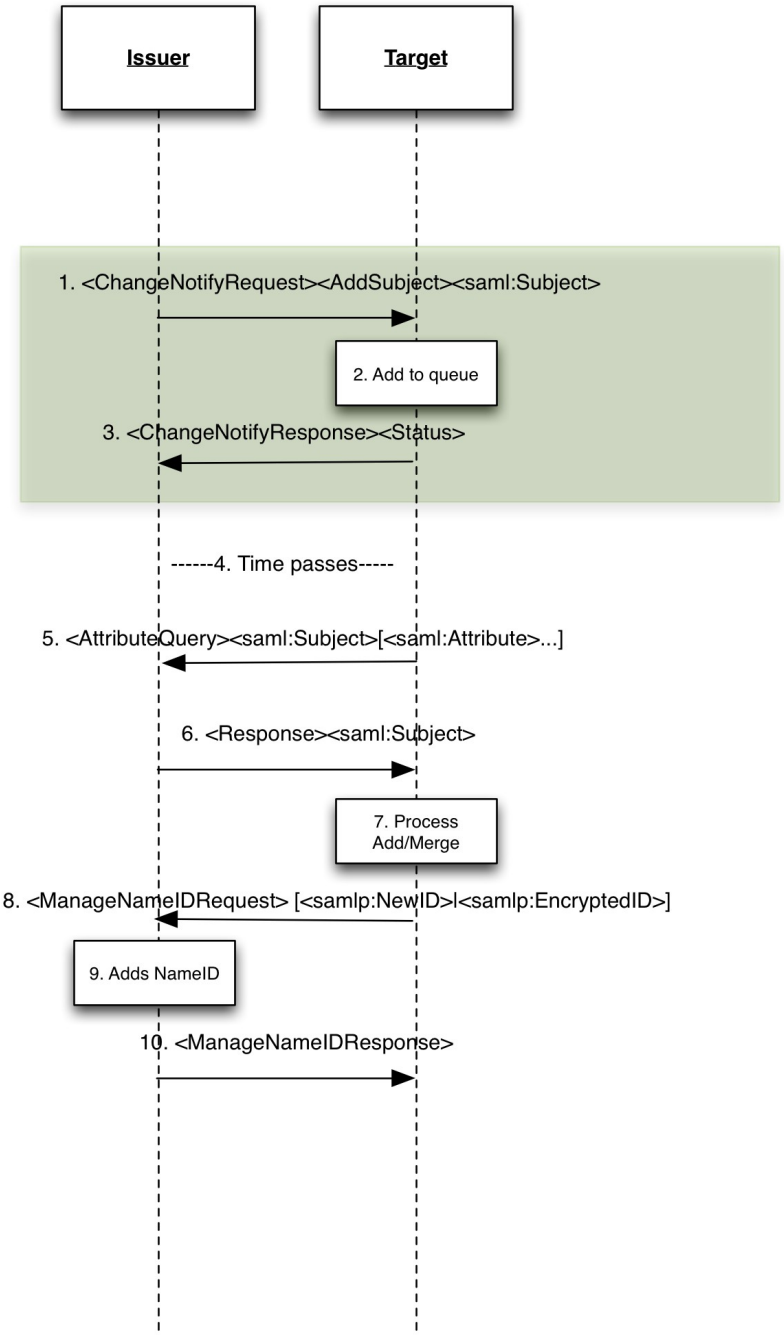
- Extension to <Response> or RelayState to indicate provisioning in step 5
- Reception of unsolicited response may be unexpected by IDPs

- 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.

4 Notify Method

In the notify method, the approach is taken that an issuer notifies a target of new information that is available. The target may then request the data via either an AttributeQuery or an AuthnRequest in the case of the browser profile.

Offline/Backchannel Mode:*



1. The issuer notifies the target of some updated information regarding a particular subject. In this case an addsubject indicates that the issuer believes this subject is new to the target (which may

or may not be true). The assertion only includes the issuers nameidentifier. The issuer can indicate multiple requests in the same message. The issuer may indicate what attributes are available in the message.

2. The target receives the request and either adds it to its queue processing (immediate or delayed). The target may also choose to ignore the request, but MUST acknowledge the receipt of the request (step 3).
3. The target acknowledges the request. The target may indicate OK, or indicate declined. A response of OK does not oblige the target to do anything further.
4. The target may optionally delay processing (the process is asynchronous)
5. The target issues an attributeQuery for each nameidentifier supplied by the issuer. If no attributes are named, the attributes provided shall be the ones indicated in step 1, or all attributes as per the normal AttributeQuery processing. OR, if arranged by prior agreement, the target may use a different protocol to effect transfer (e.g SPML, OpenID, etc).
6. Issuer responds with the attributes requested.
7. The target may optionally update the issuer with its local name identifier depending on the relationship between issuer and target.

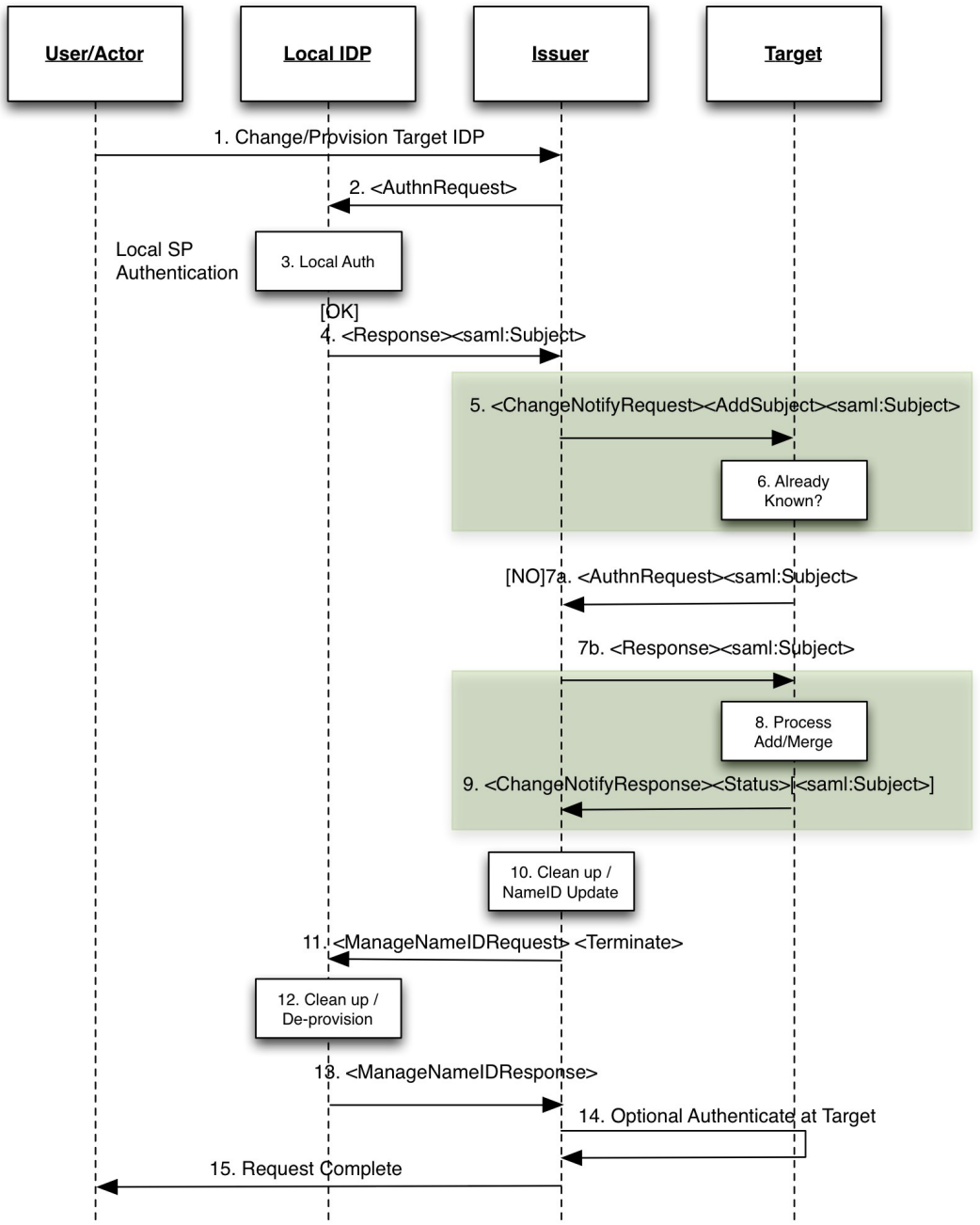
Note: for the purpose of this profile, issuer or target end-points can refer to either SP or IDP. E.g. An SP notifying an IDP of a new user transfer, or an IDP notifying an SP of a new user (e.g. Employee in an enterprise IDP).

Browser/Front-channel Profile

In the front-channel, information transfer is accomplished via browser SSO. This may be useful in cases where SSO transfer of context is desirable.

1. Issuer optionally obtains local SSO token for user (NSN scenario)
2.
3.
4.
5. The issuer notifies the target of some updated information regarding a particular subject. In this case an addsubject indicates that the issuer believes this subject is new to the target (which may or may not be true). The assertion only includes the issuers nameidentifier. The issuer can indicate multiple requests in the same message. The issuer may indicate what attributes are available in the message.
6. The target receives the request and determines what it wants to do (e.g. process as add, modify, or ignore). The target may also choose to ignore the request, but MUST acknowledge the receipt of the request by issuing a response (step 9).
7. If the target chooses to proceed, in the online mode it issues an AuthnRequest. If no attributes are named, the attributes provided shall be the ones indicated in step 5, or all attributes as per the normal AuthnRequest processing. The Issuer responds with the attributes requested.
8. The target processes the claims.

9. The target responds by closing the NotifySubject request. The target may provide in its response the local nameidentifier used by the target. Status may be simple ok, or fail.
10. Based on the response, the Issuer may then choose to deprovision the subject as desired.



Advantages of online/offline notify profiles:

- Works for browser and offline profiles*
- Passes SSO session in browser profile if desired
- Distinct new operation.
- Bi-directional
- 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.
- Offline profile can support bulk operations
- Asynchronous processing is possible
- Receiver always pulls information in response to notify.
- Not state-based.
- Issuer's access control is more easily integrated as the transfer operation is a normal AttributeQuery/AuthnRequest.
- Transfer mechanism could be another protocol if desired (e.g. SPML)

Disadvantage:

- Distinct new operation
- Provisioning occurs in 2 steps rather than one in ManageSubject operation.
- May still require another authentication step. (largest number of exchanges).