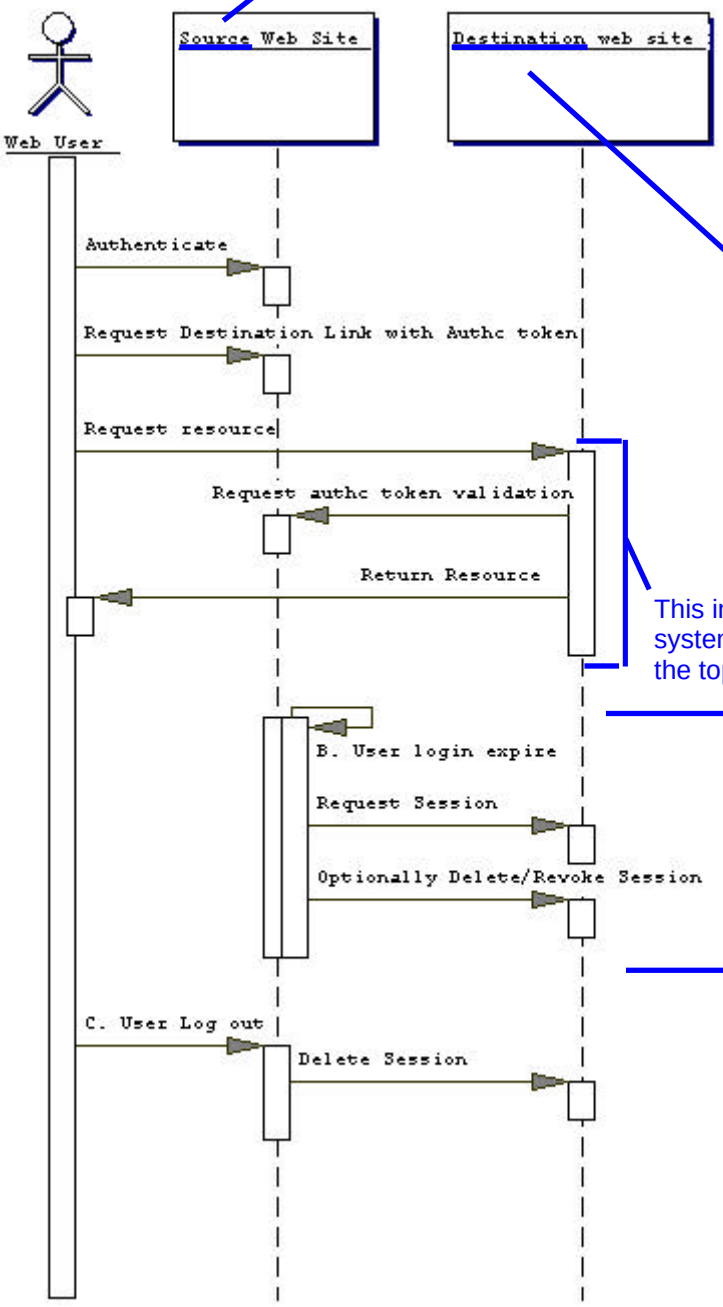
Session Management Scenarios

The following diagram illustrates the sign-on, time-out and log-out session management scenarios.



I feel we need to define our terms more precisely. By "source web site" I believe we actually mean something more akin to a "home domain" (as we've used it in some other conversations) and/or "orgin site", which is a build on RFC2616's definition of "origin server". And, we're making the assumption that the "home domain/origin site" has some authentication service that the "web user" authenticates with.

By "destination web site", we perhaps actually mean something more akin to "affiliated web site" and "origin site" all rolled into one. The term "origin site" being appropriate here because that is where the resource(s) reside or are created, in this scenario.

"home domain" is seems likely to be a contraction of "user's home administrative domain" or "user's authoritative administrative domain".

Also, perhaps we should just refer to the two sites as "the first site" and "the second site".

This indicates state is established and maintained on system entities within the site represented by the box at the top of the dashed line, yes?

?? where is state maintained? On BOTH sites?

A Single Sign-on and hand-off

Perhaps we should say "user authenticates with their home domain" or perhaps "user authenticates with the first site".

Note that this is a duplicate of Oasis security Services Scenario #1

A user logs onto the source Web site. ~~This results in the creation of a session on the source web site.~~ resulting in establishing a "session" with the home domain.

User requests a link to a destination web site. This link contains an authentication reference/token/ticket.

User requests resource represented by link on destination web site, including reference

Perhaps we should say this in this fashion: After authenticating with the first site, and perhaps after N operations on resources at the first site, the user performs some operation causing their system to connect to the second site. The authentication reference/token/ticket is conveyed to the second site as a reult of, or along with, this connection.

Destination web site requests validation of authentication reference from source web site.
Source web site returns success or failure, optionally additional session information.
Destination web site returns web site to user

what do we mean by this? "the user has not interacted with the first site for timeout amount of time"?

B. Timeout
Assume that the user has gone beyond the timeout limit on the source web site.
The source web site will query each participating web site to determine if the user has been active on their web site.
If the user has not been active on any of the destination web sites within the timeout period, the destination web sites are instructed to delete the session.

I am concerned with (a) assuming too much about the actual underlying mechanisms here (while realizing we're doing this to try to explain what we mean by "session timeout"), and (b) that this particular example scenario has scaling issues, and so is unlikely to be actually realized.

C. Logout
User logs out of the source web site.
Each of the destination web sites are instructed to delete the session.

Perhaps we should say something like "user causes their authentication credentials to become invalid or deleted (i.e. performs a "logout")". This may or may not involve communication with the first site.

Issue: [UC-3-1:UserSession] Should the use cases of log-off and timeout be supported? These result in the notion of session management. Advantage: Allows complete web user experience across multiple web sites. If not done as part of this specification, then some other body or work will have to standardize this functionality. Disadvantage: More complex than just passing authentication references between source and destination. Will slow down Technical committees work on specification of authentication/authorization only queries.

Candidate Requirement:
CR-3-1:UserSession: [OSSML] shall ~~support web user~~ session(s).

..specify a notion of end user..

Possible Resolutions:
1. Add this requirement and/or use cases to [OSSML]
2. Do not add this requirement and/or use cases

i.e. we should look into incorporating AuthXML's session notion.

Yes, I nominally think so. See the discussion in http://lists.oasis-open.org/archives/security-use/200102/msg00015.html ; BUT, there's been several subthreads on "session" on the list, and I don't feel we have a well-thought-out consensus on the set of issues, and thus I'm prepared to be convinced otherwise on this point.

ISSUE:[UC-3-02:ConversationSession] Is the concept of a session between security authorities separate from the concept of a user session? If so, should use case scenarios or requirements supporting security system sessions be supported? [DavidO: I don't understand this issue, but I have left in for backwards compatibility]. [DarrenP: I think this issue arose out of a misunderstanding/miscommunication on the mailing list and has been resolved. This is more of a formality to vote this one to a closed status.]

Possible Resolutions:
1. Do not pursue this requirement as it is not in scope.
2. Do further analysis on this requirement to determine what it is specifically.

ISSUE:[UC-3-03:Logout] Should [OSSML] support transfer of information about logout (e.g., a principal intentionally ending a session)? [DavidO: Isn't this covered in UC-3-1?. I've kept here for backwards compatibility]

Candidate Requirement:
CR-3-3:Logout: [OSSML] shall support web user logout.

perhaps we should say "session expiry or termination".

Possible Resolutions:
1. Add this requirement and/or use cases to [OSSML]

2. Do not add this requirement and/or use cases — as it is properly a part of UC-3-1.

Issue: [UC-3-6:Destination Logout] Should logging out of a destination web site be supported? Advantage: allows web sites control over their local domain, current model implemented on the web. Disadvantage: potentially more interactions between source and destination web sites

Candidate Requirement:
[CR-3-6:Destination Logout] [OSSML] shall support logout at destination web sites

Possible Resolutions:
1. Add this requirement and/or use cases to [OSSML]
2. Do not add this requirement and/or use cases — as it is properly a part of UC-3-1.

Issue: [UC-3-7:Logout Extent]. What is the impact of logging out at a destination web site?

Possible Resolution:
1. Logout from destination web site is local to destination [DavidO recommendation]
2. Logout from destination web site is global, that is destination + source web sites.

ISSUE:[UC-3-04:StepUpAuthc] "Step-up" authentication is when a receiving party refuses to accept an authentication from an authenticating party and asks for a higher level of authentication. For example, the RP can refuse password authc and require certificate authc. Should [OSSML] support step-up authentication? Should a use case be developed illustrating step-up authc?[DavidO: I don't think this is applicable to the session requirements, but I've kept here for backwards compatibility].

Possible Resolutions:
1. Move this issue to the AuthC issue group and leave open for discussion and voting.
2. Step up Authentication is not a requirement. Close the issue.

ISSUE:[UC-3-05:SessionTimeout] Should timeout be supported?

..a notion of session..

Candidate requirement:
[CR-3-5-Timeout]. [OSSML] shall support timeout ~~of a user log-on.~~

Possible Resolutions:
1. Add this requirement and/or use cases to [OSSML]
2. Do not add this requirement and/or use cases — as it is properly a part of UC-3-1.

Issue: [UC-3-8:Destination Timeout] Should timing out of a session at a destination web site be supported?

Candidate requirement:
[CR-3-8-DestinationTimeout]. [OSSML] shall support ~~destination web site timeout.~~ ..a notion of site- and/or service-specific session timeout and/or termination..

Possible Resolutions:
1. Add this requirement and/or use cases to [OSSML]
2. Do not add this requirement and/or use cases as it is properly a part of UC-3-1.