Lasso - Development #52

For ID-FF 1.2 and SAML 2.0, check that issuer of response is the one we are waiting for

22 May 2010 08:56 AM - Benjamin Dauvergne

Status:	Nouveau	**Start date:**	22 May 2010
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Core	**Estimated time:**	0:00 hour
Target version:	future		
Patch proposed:		**Planning:**	

Description

Currently it can happen that we accept a response, or an assertion not coming from the expected issuer. We should always check for it, if possible (for asynchronous binding, if the user did not keep the original profile object, we will not be able to know which provider was s targeted by a request).

It should be possible to desactivate this check for debugging purpose.

From the point of view of a caller using an asynchronous binding (redirect or POST) it should be simple, no dumping of the whole profile should be necessary. The two things to match are that the response is to a request we emitted (so check inResponseTo attribute) and that the issuer is the one targetted by the request.

The first can be done by the profile himself if the request is still present, if it's not an accessor must be provided to get to the inResponseTo field easily for ID-FF 1.2 and SAMLv2 (lasso_profile_get_in_response_to() would be ok).

The second one can also be done easily if the request is still in the profile object are by the caller through other means helped by an accessor.

A flag on the profile should indicate that the caller will do the job instead of Lasso, otherwise the absence of the request would result in a failure.

History

#1 - 27 July 2010 10:50 AM - Benjamin Dauvergne

- Category set to Core