Infrastructure - Task #2280

Story # 2277 (Closed): GMN authn and authz

Support for authenticatedUser

2012-02-01 02:58 - Roger Dahl

Status:	Closed	**Start date:**	2012-02-01
Priority:	Normal	**Due date:**	
Assignee:	Roger Dahl	**% Done:**	100%
Category:	d1_mn_GMN	**Estimated time:**	0.00 hour
Target version:	Sprint-2012.05-Block.1.3		
Milestone:	CCI-1.0.0	**Story Points:**	
Product Version:	*		

Description

When someone connects with a valid cert, add authenticatedUser to the list of subjects for which they have permissions.

History

#1 - 2012-02-01 07:11 - Matthew Jones

- Category changed from d1_mn_GMN to d1_identity_manager

- Assignee changed from Roger Dahl to Ben Leinfelder

Similar to #2279, this should be set in the certificate for the subject, and not modified. Unlike verifiedUser, though, the MN can tell if a user is properly authenticated if they have a valid certificate from CILogon. So, its more reasonable for the MN to update this value. But it would be best practice if the CN identity service set the authenticated user in the equivalent identities list for consistency and to ease implementations for MNs. Reassigning to identify service and to Ben.

#2 - 2012-02-01 22:27 - Ben Leinfelder

- Category changed from d1_identity_manager to d1_mn_GMN

- Assignee changed from Ben Leinfelder to Roger Dahl

I disagree with Matt here. The identity manager does not know when or whether a Subject is "authenticated" -- this is entirely in the hands of CILogon. If the user can authenticate with CILogon, CILogon generates a certificate for the user. If the MN receives a valid [CILogon] certificate it should safely assume that the user is indeed "authenticated" since that is the point of utilizing certificates and CILogon.
The MN should then allow access to objects that have AccessRules defined for the "authenticatedUser" constant. It's true that this is similar to interpreting "equivalent identities" but since authentication is temporally dependent, we cannot safely encode that in the identity manager as an innate attribute of the given Person (as was hinted by Matt's suggestion that it be part of the SubjectInfo encoded in the certificate). I believe this ticket is correctly placed as a feature of [G]MN -- back to Dahl.
Note: this does not mean the MN is editing attributes of the Person, just to be clear. It's only about *interpretation*.

#3 - 2012-02-06 16:05 - Roger Dahl

- Status changed from New to Closed

Implemented. Sorry for the confusion caused by the vague description in this ticket.