Infrastructure - Task #2279

Story # 2277 (Closed): GMN authn and authz

Support for Person::verified flag

2012-02-01 02:42 - 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 Person that has the verified flag set, "verifiedUser" should be added to the list of subjects for which they have permissions.

History

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

- Category changed from d1_mn_GMN to d1_identity_manager

- Assignee changed from Roger Dahl to Ben Leinfelder

Verification is a task that should ONLY be handled by the Identity management service on the CN. MNs do not have a mechanism to determine if a user has been verified or not, which is tracked in the CN user registration data. If a MN receives a certificate with a Person object that is not in fact marked as VerifiedUser, then the user is not verified and it should not be changed at the MN level. I think this is a duplicate of another ticket that addresses how to verify users at the CN level, but I can't immediately find that ticket, so I will leave this open until we determine if its a duplicate. I am also reassigning it to the CN identity service, and to Ben who has implemented this logic.

#2 - 2012-02-01 22:17 - Ben Leinfelder

- Category changed from d1_identity_manager to d1_mn_GMN

- Assignee changed from Ben Leinfelder to Roger Dahl

The MN has two options when checking that a Subject is verified or not:
1. call CN.getSubjectInfo for the given Subject which will contain a Person.verified flag
2. inspect the given certificate for the SubjectInfo block that CILogon has inserted into the certificate when it called CN.getSubjectInfo() when it generated the certificate, and then check the Person.verified flag as in #1.

It's true that the MN "authorization" implementation needs to check the Person.verified flag in order to allow or deny access to objects that include an AccessRule for the "authenticatedUser" constant. This appears to correctly be a ticket about the GMN implementation needing to check for this case and does not change the d1_identity module in any way. Assigning back to Dahl.

#3 - 2012-02-06 05:48 - Roger Dahl

- Status changed from New to Closed

Ben, you are correct, and I have implemented this in the algorithm that converts a SubjectInfo into a list of subjects to use for access checks.