Infrastructure - Story #2548

recasting untrusted certs to public poses accessibility inconsistency to users

2012-03-27 21:55 - Rob Nahf

Status:	New	**Start date:**	2012-03-27
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Authentication, Authorization	**Estimated time:**	0.00 hour
Target version:			
Story Points:			

Description

KNB recasts a connection with an untrusted certificate to public, so that a client does not get "less than public" privileges.
GMN throws an InvalidToken in this situation.
both refuse connections from clients with expired certificates from trusted CAs.

This approach can cause confusion caused when the user unwittingly uses an untrusted certficate and doesn't get what they expected. If these connections were instead refused, the user would be alerted and could reconnect as a public user, if it chose.

brief discussion found at line 97 of : http://epad.dataone.org/20120131-authn-authz-questions

- when would honest users be in this situation?
- elicit advantages of recasting approach
- either way, dataone should implement uniform behavior across CN and MNs.

Subtasks:

Task # 2549: document the decision	**New**
Task # 2551: test feasibility of apache rejecting non-verified certificates	**Closed**

Related issues:

Related to Infrastructure - Bug #2411: knb MNs and CNs allow self-signed cert...	**In Progress**	**2014-10-01**	**2014-10-01**
Related to Java Client - Story #6570: libclient should give better indication...	**Closed**		

History

#1 - 2018-01-17 20:36 - Dave Vieglais

- Sprint set to Infrastructure backlog