Infrastructure - Task #2670

Story # 2661 (Closed): handling complicated identity-equivalencies for authorization

check for character limit of customMessages within certificates

2012-04-30 20:10 - Rob Nahf

Status:	Closed		**Start date:**	2012-04-30
Priority:	Normal		**Due date:**	
Assignee:	Rob Nahf		**% Done:**	100%
Category:	Authentication, Authorization		**Estimated time:**	0.00 hour
Target version:	Sprint-2012.39-Block.5.4			
Milestone:	CCI-1.0.0		**Story Points:**	
Product Version:	*			

Description
This could impact what's put in the certificate's subjectinfo

History

#1 - 2012-05-03 19:55 - Rob Nahf

- Category set to Authentication, Authorization

- Status changed from New to Closed

- % Done changed from 0 to 100

I could not find anything on the web that refers to size restrictions placed on custom messages in x.509 certificates, so instead turned to live testing. Using the d1_certificate_manager package, I successfully created a certificate containing a 602 KB serialized ObjectList (taken from cn-stage). The resulting cert is a surprising 819 KB (~33% larger than the original file).

Is this an adequate test?
size of other test certificates: ~4 KB
number of Persons in other test certificates: 2-5
character length of those Person records: ~300 characters
complexity of Person records - relatively simple

In the 602KB ObjectList:
* num of ObjectInfos = 2035
* char per ObjectInfo ~280

A more complicated Person object (many mappings and groups) would probably be 2-4x the size of the ones measured.

If:
* size(Person record) = 4 * size(ObjectInfo):
* and given a tested capacity for ~2000 ObjectInfos

We can safely assume that a SubjectInfo with 500 Persons (= 2000 ObjectInfos / 4) would not be problematic to put into a certificate.
It is difficult to imagine a graph of equivalent identities being larger than 20 Persons, so I think we are more than ok for certificate creation.

Not tested was the transmission and use of these certificates.

#2 - 2012-10-03 15:40 - Chris Jones

- Target version changed from Sprint-2012.35-Block.5.2 to Sprint-2012.39-Block.5.4