Infrastructure - Bug #8045

certificateLocation not seeming to be utilized

2017-03-14 20:24 - Rob Nahf

Status:	New	**Start date:**	2017-03-14
Priority:	Normal	**Due date:**	
Assignee:	Rob Nahf	**% Done:**	0%
Category:	d1_libclient_java	**Estimated time:**	0.00 hour
Target version:	Maintenance Backlog		
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

A d1_libclient_java user (as repository owner) is trying to use libclient to submit content to GMN, and has had trouble configuring CertificateManager to find the long-lived client certificate. He has tried on both Windows (via Eclipse) and Linux (Play framework), and what has worked for him was putting his certificate in the default location (/tmp/x509_u1000).

We will need to monitor the connection / handshake to determine if the certificate is being sent and GMN ignoring it, or it's not getting sent.

History

#1 - 2017-03-14 20:45 - Rob Nahf

running with JVM arguments "-Djavax.net.debug=ssl:handshake" will give handshake information about whether or not a client certificate was exchanged"

(In Eclipse, the run configuration: Arguments tab, VM argument pane.)

A successful transmission of client certificate with the handshake debugging output includes this section (after a lot of preamble...)

---

found key for : cilogon
chain [0] = [0] Version: 3
SerialNumber: 148086
IssuerDN: DC=org,DC=cilogon,C=US,O=CILogon,CN=CILogon OpenID CA 1
Start Date: Tue Mar 14 13:34:33 MST 2017
Final Date: Wed Mar 15 07:39:33 MST 2017
SubjectDN: DC=org,DC=cilogon,C=US,O=Google,CN=Robert Nahf A579
Public Key: RSA Public Key
modulus:
a0d4769ffb35b9f8ff79d377ba549eb0ba369ebccf50deb6bbabdfe3ebd00b10ec6729506061730711c6b9a356b08efa4fc9bea14c2b8b9e58d744104fffd
9d907ac5c3ba3e292a5897907d5768de586d3df1e9a19029535394fe35206a707233b6c366a3088fcc8362ca944028bf11537bffe8bdfd6b7fe4e3e149a
94fd87d7d4ce8bb415a2bdfe28718dc6d2afbfa7b7dd5885f6f6d34f80f1d2bc4bd3b62a9e5f6d121b824a2bdf24bedda9697e4e34555792c9b82220bd86
74926b330acc896002bf4c5bd29ecb1f9e8968fdf2d40b44ca4727ac0118a15001b3be9597a1ce74753862fafe089e28dc4b2d8729a0e778df3e236adc7
3f371fafdbcf7beed
public exponent: 10001

Signature Algorithm: SHA256WITHRSA