Infrastructure - Task #3576

Task # 3394 (Closed): Deploy Shibboleth provider for KNB LDAP accounts

Investigate using alternative CILogon DN format

2013-02-14 22:32 - Ben Leinfelder

Status:	Closed	**Start date:**	2013-02-14
Priority:	Normal	**Due date:**	
Assignee:	Ben Leinfelder	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2013.10-Block.2.1		
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

We are currently looking at values akin to:

CN=Ben Leinfelder T6468,O=DataONE Test,C=US,DC=cilogon,DC=org

But we were curious if instead of a common name + random string you could just use the uid for our identities (mine is 'leinfelder'):

UID=leinfelder,O=DataONE Test,C=US,DC=cilogon,DC=org

Our main concern is that the DN we get back from you contains random information that we do not have control over. I've also noticed some character encoding issues for our international users that have accents and such in their names:

CN=Fl&Atilde\;&iexcl\;via Pezzini T6456,O=Google,C=US,DC=cilogon,DC=org (Flávia Pezzini)
CN=Jos&Atilde\;&copy\; Augusto Salim T6455,O=Google,C=US,DC=cilogon,DC=org (José Augusto Salim)

When I changed my name in Google for testing purposes, both of these issues were highlighted in the CILogon warning screen:

One or more of the attributes released by your organization has changed since the last time you logged on to the CILogon Service. This will affect your certificates as described below. The above changes to your attributes will cause your certificate subject to change. You may be required to re-register with relying parties using this new certificate subject.
Previous Subject DN: CN=ben leinfelder A756,O=Google,C=US,DC=cilogon,DC=org
Current Subject DN: CN=benjamÃn leinfelder A1806,O=Google,C=US,DC=cilogon,DC=org

Perhaps that is just par for the course and what we have signed up to deal with by using CILogon, but it seems like people could freely edit their names if we used UID in the DN instead of CN.

History

#1 - 2013-02-15 06:49 - Ben Leinfelder

From Jim Basney:

Under our current policy for the DataONE Test IdP we could do:

CN=Ben Leinfelder (leinfelder),O=DataONE Test,C=US,DC=cilogon,DC=org

or

CN=leinfelder,O=DataONE Test,C=US,DC=cilogon,DC=org

but we aren't allowed to use "UID=" in the DN per http://www.ogf.org/documents/GFD.125.pdf.

Good questions about the UTF8 encoding. I need to defer to Terry on what's going on there. I agree it looks like a bug.

#2 - 2013-02-18 15:56 - Ben Leinfelder

From J Basney:

C=US is part of the registered unique distinguished namespace for our Certification Authority and can not be changed. It indicates that our CA is operated in the US. It is not meant to imply anything about the nationality of the user.

#3 - 2013-02-18 16:01 - Ben Leinfelder

- Status changed from New to Closed

- translation missing: en.field_remaining_hours set to 0.0

We've settled on the following DN format for our identities. This will only apply to accounts that use our IdPs:

CN=uidFromLdap,O=ourIdpName,C=US,DC=cilogon,DC=org

#4 - 2013-03-01 18:55 - Ben Leinfelder

- Target version changed from 2013.2-Block.1.1 to 2013.10-Block.2.1

#5 - 2013-04-26 18:17 - Ben Leinfelder

- Target version set to 2013.10-Block.2.1

#6 - 2013-04-26 18:17 - Ben Leinfelder

- Target version deleted (2013.10-Block.2.1)