Infrastructure - Story #1123

Define the authentication token

2010-11-30 20:07 - Dave Vieglais

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Matthew Jones	**% Done:**	100%
Category:	Documentation	**Estimated time:**	0.00 hour
Target version:	Sprint-2011.14-Block.2		
Story Points:			

Description

We currently use an "authtoken" or "token" as placeholder in all api definitions for authentication information that needs to be passed in a method call.

It is necessary to further define what is meant by an authentication token so that methods dependent on principal and other authentication information can be more fully defined and at least stubbed out in the code base.

Subtasks:

Task # 1457: Document AuthToken and AuthSession objects	**Closed**

History

#1 - 2010-12-07 19:04 - Mark Servilla

- Status changed from New to In Progress

- Category set to d1_identity_manager

- % Done changed from 0 to 10

As per requested by Dave Vieglais, investigate the structure of a DataONE authentication token for use by DataONE services during the verification of a user's credential. A discussion regarding a proposed token structure (that being prototype for the LTER Network Information System) occurred during the 1 December CCIT call focused on whether the X.509 certificate was adequate for replacing a token? Missing from the certificate, however, are any attributes that define a user's group affiliation(s). Jim Basney was asked whether additional attributes may be injected into the certificate just prior to the CILogon digital signing of the certificate - his response follows:

> The core question is attribute push versus pull, i.e., whether you
> inject user attributes into the token, and then push the token with
> those attributes around, or you just have an identifier in the token and
> pull (query for) attributes from the appropriate attribute store on
> demand when/where they're needed. In the GridShib project we did a lot
> of work with both approaches, and every time we did attribute push, we
> later regretted it.
>
> The problems with attribute push are knowing in advance what attributes
> to put in the token and where to get them from and whether they're still
> current. It's difficult for CILogon or any general-purpose identity
> provider to gather the VO-specific (i.e., DataONE-specific) attributes
> to put in the token. CILogon would need to figure out that the user
> needs DataONE attributes (and not OOI attributes or iPlant attributes or
> ...) and then figure out if there are any attributes specific to the
> DataONE Member Node that the user wants to access versus DataONE-general
> attributes. The result is CILogon ends up asking the user for
> information and things end up breaking mysteriously because CILogon made
> a bad decision about which attributes to put in. For example, a
> researcher is involved in both DataONE and iPlant, and CILogon made the
> mistake of putting in DataONE attributes when the researcher wanted to
> do iPlant things.
>
> In contrast, the DataONE Member Node knows what the user is trying to do
> and knows what attributes it needs (from where) to make the local
> authorization decision. Maybe it wants to combine attributes from the
> central DataONE group service plus its local LDAP in case the user has
> some local privilege assignments. Therefore, the Member Node is in a
> much better position to pull in the attributes than CILogon is.
>
> So... the short answer is that it's possible for CILogon to inject

> attributes into the certificate. We've got the code to do it. I just think we shouldn't, based on past experience.... Of course I'm willing to keep an open mind and discuss further...

At issue, I believe, is whether the content in a certificate would become stale if it were to have an extended lifetime; this possibility, and its user dissatisfaction implications (where the user would be required to regenerate a new certificate with up-to-date information) would have to be weighed against any performance reduction if all DataONE services would be required to dynamically query a "group service" for affiliation information of a user. It appears, however, that CILogon would accomodate DataONE's needs as necessary.

#2 - 2010-12-13 18:34 - Dave Vieglais

- Position set to 5

- Target version changed from Sprint-2010.48 to Sprint-2010.50

#3 - 2011-01-03 03:11 - Dave Vieglais

- Target version changed from Sprint-2010.50 to Sprint-2011.04

#4 - 2011-02-01 17:14 - Dave Vieglais

- Position deleted (49)

- Position set to 1

- Position changed from 1 to 126

- Target version changed from Sprint-2011.04 to Sprint-2011.09-Block.2

#5 - 2011-03-07 17:43 - Dave Vieglais

- Position deleted (159)

- Position set to 10

- Target version changed from Sprint-2011.09-Block.2 to Sprint-2011.10-Block.2

#6 - 2011-03-15 16:23 - Matthew Jones

- Position set to 5

- Target version changed from Sprint-2011.10-Block.2 to Sprint-2011.11-Block.2

- Position deleted (17)

#7 - 2011-03-22 14:00 - Dave Vieglais

- Target version changed from Sprint-2011.11-Block.2 to Sprint-2011.12-Block.2

- Position deleted (19)

- Position set to 6

#8 - 2011-03-28 16:36 - Dave Vieglais

- Position deleted (13)

- Target version changed from Sprint-2011.12-Block.2 to Sprint-2011.13-Block.2

- Position set to 5

#9 - 2011-04-04 17:16 - Matthew Jones

- Target version changed from Sprint-2011.13-Block.2 to Sprint-2011.14-Block.2

- Position set to 2

- Position deleted (6)

#10 - 2011-04-07 02:36 - Matthew Jones

- Category changed from d1_identity_manager to Documentation

- Milestone changed from CCI-0.6 to 2011-Block-2

- Assignee changed from Mark Servilla to Matthew Jones

- Status changed from In Progress to Closed

Completed by deciding to use SAML2 Assertions as the structure for session descriptions. These contain user identity, groups, and identity mappings for the session. See the description in the Authentication sections of the Architecture documents for details.