Entitlements at UMA.es

first steps into centralised AuthR

Victoriano Giralt

Central ICT Services
University of Málaga

Cork
May 19th, 2009

Entitlements

a definition

Entitlements

a definition

What’s an entitlement?

Entitlements
a definition

What’s an entitlement?
according to Oxford English Dictionary

Entitlements

a definition

What's an entitlement?
according to Oxford English Dictionary

entitlement |en'tïtlmənt|
noun
the fact of having a right to something : *full* ***entitlement to*** *fees and maintenance should be offered | you should be fully aware of your legal entitlements.*

- the amount to which a person has a right : *annual leave entitlement.*

Entitlements

a definition

Entitlements

a definition

What’s an entitlement?

Entitlements

a definition

What’s an entitlement?
according to the eduPerson specification

Entitlements

a definition

What’s an entitlement?
according to the eduPerson specification

eduPersonEntitlement URI (either URN or URL)
that indicates a set of rights to specific resources.

URNs
how do they look like

URNs

how do they look like

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

Assigns access rights to the designated application:

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

Assigns access rights to the designated application:

- Function

entitlement

the URN describes a right for a user or role

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

Assigns access rights to the designated application:

- Function

applAccess

kind of right, access to an application in this case.

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

Assigns access rights to the designated application:

- Function

SolicitudGasto

application the right is granted on.

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

Assigns access rights to the designated application:

- Function

LEVEL

granted access level, application specific:
RUG, ROU, RGE

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

- Function
- Usage

LDAP search

The application does a standard directory search to find out if the user that has been authenticated has the right to use it and the access level that has been granted to her.

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

- Function
- Usage

Query via web service

The application queries a web service with user and application identifier as inputs and obtains the access level or the absence of the right to use.

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

- Function
- Usage

WebSSO AuthR assertion

The authentication server has information about the accessed resource, once the user is AuthN'd, retrieves application specific AuthR information from the entitlements in the user's entry in the directory, and passes them onto the resource

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

- Function
- Usage

Federation

We insert the appropriate entitlement values into the SAML assertions for the applications, as SPs, to consume.

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

- Function
- Usage
- Advantages

Unique authorisation point

All of an object's authorisations,
both explicit and implicit,
are centrally kept in a directory entry.

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

- Function
- Usage
- Advantages

A sole authorisation model

URNs allow us to express all authorisation
in a common form,
with application specific semantics.

URNs in Entitlements for AuthR

as it is in use at UMA (by example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccess:SolicitudGasto:*LEVEL*

- Function
- Usage
- Advantages

Agent-Function-Qualifier

Who **can do** *What* **on** *Which object*

URNs in Entitlements for AuthR

as it is in use at UMA (a *hairier* example)

URNs in Entitlements for AuthR

as it is in use at UMA (a *hairier* example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccessAdmin:rectorado_convenios

Assigns permission granting rights in the designated application:

URNs in Entitlements for AuthR

as it is in use at UMA (a *hairier* example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccessAdmin:rectorado_convenios

Assigns permission granting rights in the designated application:

- Function

entitlement

the URN describes a right for a user or role

URNs in Entitlements for AuthR

as it is in use at UMA (a *hairier* example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccessAdmin:rectorado_convenios

Assigns permission granting rights in the designated application:

- Function

applAccessAdmin

kind of right, application access permission granting in this case.

URNs in Entitlements for AuthR

as it is in use at UMA (a *hairier* example)

irisUserEntitlement = urn:mace:rediris.es:uma.es:
entitlement:applAccessAdmin:rectorado_convenios

Assigns permission granting rights in the designated application:

- Function

rectorado_convenios

application the permission can be granted upon.

Demo time

ok?

like or not, it's going to happen

On URN handling problems

or, more precisely, their absence

On URN handling problems

or, more precisely, their absence

URNs usage problems are more perceived than real

On URN handling problems

or, more precisely, their absence

URNs usage problems are more perceived than real

- Searching for URNs

URN = text string

When properly indexed,
LDAP shines
for its speed in substring searching;
regardless of length.
(We have benchmarks to back this).

On URN handling problems

or, more precisely, their absence

URNs usage problems are more perceived than real

- Searching for URNs
- Entitlement processing

Entitlement = multivalued attribute

Processing is not more complex than any other multivalued attributes.

On URN handling problems

or, more precisely, their absence

URNs usage problems are more perceived than real

- Searching for URNs
- Entitlement processing
- URN processing

URN = text string

Searching for information inside a URN
is just string processing,
most programming languages in use
can easily accomplish.

On URN handling problems

or, more precisely, their absence

URNs usage problems are more perceived than real

- Searching for URNs
- Entitlement processing
- URN processing
- Value control

URNReg

A schema and application for registering URN values
in a distributed fashion

URNs
how do they look like

URNs

how do they look like

Thank you

Questions?

answers not assured