PAPI + openLDAP para control de acceso basado en *entitlements*

Victoriano Giralt José A. Accino

Servicio Central de Informática
Universidad de Málaga

Logroño, 24 de octubre de 2005

Índice

Control de solicitudes de gasto
(en producción)

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

Asigna niveles de acceso a la aplicación indicada:

- Función
- Modo de uso
- Ventajas

entitlement

el URN contiene un derecho del usuario o rol

Control de solicitudes de gasto
(en producción)

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

Asigna niveles de acceso a la aplicación indicada:

- Función
- Modo de uso
- Ventajas

applAccess

tipo de derecho, en este caso acceso a una aplicación.

Control de solicitudes de gasto
(en producción)

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

Asigna niveles de acceso a la aplicación indicada:

- Función
- Modo de uso
- Ventajas

SolicitudGasto

aplicación sobre la que se ejerce el derecho.

Control de solicitudes de gasto
(en producción)

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

Asigna niveles de acceso a la aplicación indicada:

- Función
- Modo de uso
- Ventajas

NIVEL

nivel de acceso concedido, específico de la aplicación:

RUG, ROU, RGE

Control de solicitudes de gasto
(en producción)

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

- Función
- Modo de uso
- Ventajas

Consulta LDAP

Consulta convencional al directorio desde la aplicación para averiguar si el usuario que se ha autenticado tiene derecho a usarla y el nivel de acceso que se le ha concedido.

Control de solicitudes de gasto
(en producción)

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

- Función
- Modo de uso
- Ventajas

Consulta vía servicio web

La aplicación consulta un servicio web dándole como entrada los identificadores del usuario y de la aplicación, y obteniendo el nivel de acceso o la ausencia de derecho.

Control de solicitudes de gasto
(en producción)

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

- Función
- Modo de uso
- Ventajas

PAPI (futuro)

El futuro, como tal, se verá más adelante.

Control de solicitudes de gasto
(en producción)

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

- Función
- Modo de uso
- Ventajas

Punto único de autorización

Todas las autorizaciones de un objeto, explícitas o implícitas, están centralizadas en una entrada del directorio.

Control de solicitudes de gasto
(en producción)

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

- Función
- Modo de uso
- Ventajas

Modelo único de autorización

El formato URN nos permite expresar todas las autorizaciones de la misma forma, dejando a cada aplicación su propia semántica.

Control de solicitudes de gasto
(en producción)

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

- Función
- Modo de uso
- Ventajas

Agente-Función-Calificador

Quién **puede hacer** *Qué* **sobre** *Qué objeto*

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

Gestión personal de permisos

Es el usuario quien da permisos a las aplicaciones sobre sus datos.
¿Podemos usar los *entitlements*?
¿Estamos dentro de la ortodoxia?
¿Un nuevo irisUserPrivateAttribute?

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

Control de acceso a atributos

Diversas aplicaciones pueden querer utilizar un atributo, el usuario puede decidir si permite o no el uso del atributo para el fin de cada una de ellas.

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

mobile

Este atributo se puede utilizar para diversas aplicaciones, como pueden ser:

+ cambio de claves olvidadas
+ envío de calificaciones
+ envío de notificaciones

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

VALOR = passwordChange

El usuario autoriza el uso de su número de móvil a la pasarela SMS para la función de cambio de claves. Visto de otra forma, el usuario permite que su número de móvil se pueda usar para iniciar un cambio de clave de acceso.

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

VALOR = marks

El usuario autoriza el uso de su número de móvil para el acceso a sus notas y para que se le envíen sus calificaciones.

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

VALOR = maySpam

El usuario autoriza el uso de su número de móvil para el envío de comunicaciones desde la Universidad.

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

irisUserEntitlement

Contiene permisos que se conceden al objeto (usuario).

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

irisUserPrivateAttribute

Contiene permisos que el objeto (usuario) concede para acceder a sus atributos.

Usos del número de móvil
(un caso más complicado)

irisUserEntitlement = urn:mace:rediris.es:uma.es:entitlement:attrAccess:mobile:*VALOR*

- Usuario a aplicación
- El problema
- Ejemplos
- Pero ...

¿Nuevo irisUserPrivateAttribute?

¿Cambiamos a un modelo de URN?

¿Podría funcionar?

Sobre los problemas de manejo de URN

o, en realidad, de la ausencia de ellos

Los problemas del uso de URNs son más de percepción que reales

- Búsqueda de URNs
- Procesamiento de Entitlements
- Procesamiento de URNs

URN = cadena de texto

Si se indiza adecuadamente, LDAP destaca por la rapidez de búsqueda de subcadenas; da igual la longitud de las mismas.

Sobre los problemas de manejo de URN
o, en realidad, de la ausencia de ellos

Los problemas del uso de URNs son más de percepción que reales

- Búsqueda de URNs
- Procesamiento de Entitlements
- Procesamiento de URNs

Entitlement = atributo multivaluado

Su tratamiento no es más complejo que el de otros atributos multivaluados.

Sobre los problemas de manejo de URN
o, en realidad, de la ausencia de ellos

Los problemas del uso de URNs son más de percepción que reales

- Búsqueda de URNs
- Procesamiento de Entitlements
- Procesamiento de URNs

URN = cadena de texto

La búsqueda de datos en un URN es un simple proceso de cadenas, que los lenguajes al uso realizan con gran facilidad.

El futuro
es hoy

- Eliminar acceso LDAP
- Servicios web
- PAPI

El futuro
es hoy

- Eliminar acceso LDAP
- Servicios web
- PAPI

El acceso, NO el directorio

Las aplicaciones no pueden tener el control de acceso.
El directorio no puede saber si la aplicación usa las credenciales que le corresponden.
Por ello, podrían usar información para la que no están autorizadas.

El futuro
es hoy

- Eliminar acceso LDAP
- Servicios web
- PAPI

Control de credenciales

Las aplicaciones NO DEBEN tener acceso a las credenciales.
¿Por qué?
¿Hay solución?

El futuro
es hoy

- Eliminar acceso LDAP
- Servicios web
- PAPI

Solución para el acceso

Son el interfaz entre las apllicaciones y el directorio.
Al ser pocos, permiten una revisión exhaustiva del código para verificar que es acorde a la política de acceso a los atributos.

El futuro
es hoy

- Eliminar acceso LDAP
- Servicios web
- PAPI

Atenticación **Y** Autorización

El AS es el único punto con acceso a las credenciales.
La aserción de PAPI puede contener los entitlements definidos por el administrador para cada POA (=aplicación).
El AS controla el acceso a los atributos.