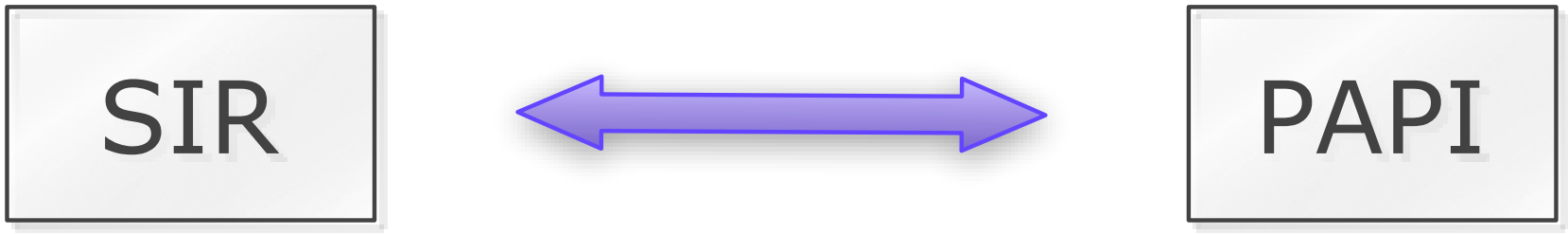
Metadatos
Control de atributos

Cándido Rodríguez
candido.rodriguez@rediris.es

Metadatos

- Metadatos en PAPI
  - Necesidad de formalizar
  - Facilita configuración entre instituciones
  - Evolución de la tecnología
- Metadatos en SIR
  - Gestión de Proveedores de Servicio
  - Gestión de conectores (proveedores de identidad)
- Basado en metadatos según SAML



- Proveedor de Identidad PAPI
  - Describe un proveedor de identidad en un entorno PAPI
  - Elementos principales:
    - ID del proveedor de identidad
    - URL donde está disponible el IdP
    - Clave pública
    - Nombre
  - Elementos opcionales:
    - Lista de comunidades autonómicas
    - Cookie global o por proveedor de servicio

- Proveedor de Identidad PAPI

```
<md:EntityDescriptor
  entityID=”…">

  <md:Extensions>
    <attr:EntityAttributes>
    […]
    </attr:EntityAttributes>
  </md:Extensions>

  <md:RoleDescriptor xsi:type="papi:AuthServerDescriptorType”
protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">
    […]
  </md:RoleDescriptor>

  <md:Organization>
    […]
  </md:Organization>

</md:EntityDescriptor>
```

- Proveedor de Identidad PAPI

```
<md:RoleDescriptor xsi:type="papi:AuthServerDescriptorType"
protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">
  <md:KeyDescriptor use="signing">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:KeyValue>
         <ds:RSAKeyValue>
            <ds:Modulus>…</ds:Modulus>
            <ds:Exponent>AQAB</ds:Exponent>
         </ds:RSAKeyValue>
      </ds:KeyValue>
    </ds:KeyInfo>
  </md:KeyDescriptor>

  <papi:IdPService AS_ID="aesir"
        Binding="urn:mace:rediris.es:papi:binding:browser-sso"
        Location="https://www.rediris.es/PAPIAESIR/AuthServer"/>
  </md:RoleDescriptor>
```

- Proveedor de Identidad PAPI

```
<md:RoleDescriptor xsi:type="papi:AuthServerDescriptorType"
protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">
  <md:KeyD
    <ds:Ke                                              dsig#">
      <ds:KeyValue>
        <ds:RSAKeyValue>
          <ds:Modulus>…</ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
    </ds:KeyInfo>
  </md:KeyDescriptor>

  <papi:IdPService AS_ID="aesir"
        Binding="urn:mace:rediris.es:papi:binding:browser-sso"
        Location="https://www.rediris.es/PAPIAESIR/AuthServer"/>
  </md:RoleDescriptor>
```

Indica que es un proveedor de identidad PAPI

- Proveedor de Identidad PAPI

```
<md:RoleDescriptor xsi:type="papi:AuthServerDescriptorType"
protocolSupportEnumeration="urn:mace
1.0">
  <md:KeyDescriptor use="signing">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:KeyValue>
         <ds:RSAKeyValue>
            <ds:Modulus>…</ds:Modulus>
            <ds:Exponent>AQAB</ds:Exponent>
         </ds:RSAKeyValue>
      </ds:KeyValue>
    </ds:KeyInfo>
  </md:KeyDescriptor>

  <papi:IdPService AS_ID="aesir"
        Binding="urn:mace:rediris.es:papi:binding:browser-sso"
        Location="https://www.rediris.es/PAPIAESIR/AuthServer"/>
  </md:RoleDescriptor>
```

Clave pública del conector

- Proveedor de Identidad PAPI

```
<md:RoleDescriptor xsi:type="papi:AuthServerDescriptorType"
protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">
  <md:KeyDescriptor use="signing">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:KeyValue>
        <ds:RSAKeyValue>
          <ds:Modulus>…</ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
    </ds:KeyInfo>
  </md:KeyDescriptor>

  <papi:IdPService AS_ID="aesir"
        Binding="urn:mace:rediris.es:papi:binding:browser-sso"
        Location="https://www.rediris.es/PAPIAESIR/AuthServer"/>
  </md:RoleDescriptor>
```

ID y URL

- Proveedor de Identidad PAPI
  - Definición de la entidad que despliega el proveedor de identidad

```
<md:Organization>
  <md:OrganizationName xml:lang="es">AESIR</md:OrganizationName>
  <md:OrganizationDisplayName xml:lang="es">AESIR</
md:OrganizationDisplayName>
  <md:OrganizationURL xml:lang="es">
    http://www.rediris.es/sir/aesir/
  </md:OrganizationURL>
</md:Organization>
```

  - Nombre a visualizar en el WAYF a través de `<OrganizationDisplayName>`
  - Incluso por idioma

- Proveedor de Identidad PAPI
  - Comunidad autónoma en el WAYF

```
<md:Extensions>
  <attr:EntityAttributes>
    <saml:Attribute
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
     Name="urn:oid:2.5.4.7"
     FriendlyName="l">
      <saml:AttributeValue xsi:type="xs:string">
        Andalucía
      </saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string">
        Comunidad de Madrid
      </saml:AttributeValue>
    </saml:Attribute>
  </attr:EntityAttributes>
</md:Extensions>
```

- Proveedor de Identidad PAPI
  - Cookie en el SIR GPoA global o por SP

```
<md:Extensions>
  <attr:EntityAttributes>
    <saml:Attribute
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
     Name="urn:oid:1.3.6.1.4.1.7547.4.3.2.14”
     FriendlyName="irisUserStatus">
       <saml:AttributeValue xsi:type="xs:string">
         urn:mace:rediris.es:papi:protocol:gpoaCookie:global
       </saml:AttributeValue>
    </saml:Attribute>
  </attr:EntityAttributes>
</md:Extensions>
```

  - Si lo incluye será global
  - Cookie por proveedor de servicio por defecto

- Proveedor de Servicio PAPI (PoA)

```
<md:EntityDescriptor
  entityID="http://www.rediris.es/sir/monitor/">

  <md:RoleDescriptor xsi:type="papi:PoADescriptorType"
   protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">

    <papi:PoAService
      Binding="urn:mace:rediris.es:papi:binding:browser-sso"
      RegExpLocation="true"
      Location="http://www.rediris.es:80/sir/monitor/.*"/>

  </md:RoleDescriptor>

</md:EntityDescriptor>
```

- Proveedor de Servicio PAPI (PoA)

```
<md:EntityDescriptor
  entityID="http://www.rediris.es/sir/monitor/">

  <md:RoleDescriptor xsi:type="papi:PoADescriptorType"
   protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">

    <papi:PoAService
      Binding="urn:mace:rediris.es:papi:binding:browser-sso"
      RegExpLocation="true"
      Location="http://www.rediris.es:80/sir/monitor/.*"/>

  </md:RoleDescriptor>

</md:EntityDescriptor>
```

URL basado en expresión regular

- GPoA

```
<md:EntityDescriptor entityID="http://test/gpoa">
  <md:RoleDescriptor xsi:type="papi:GPoADescriptorType"
   protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyValue>
          <ds:RSAKeyValue>
            <ds:Modulus>…</ds:Modulus>
            <ds:Exponent>AQAB</ds:Exponent>
          </ds:RSAKeyValue>
        </ds:KeyValue>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <papi:GPoAService
      Binding="urn:geant:rediris:papi:browser-sso"
      Location="http://test/gpoa"/>
  </md:RoleDescriptor>
</md:EntityDescriptor>
```

- GPoA

```
<md:EntityDescriptor entityID="http://test/gpoa">
  <md:RoleDescriptor                                    iptorType"
   protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyValue>
          <ds:RSAKeyValue>
            <ds:Modulus>…</ds:Modulus>
            <ds:Exponent>AQAB</ds:Exponent>
          </ds:RSAKeyValue>
        </ds:KeyValue>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <papi:GPoAService
      Binding="urn:geant:rediris:papi:browser-sso"
      Location="http://test/gpoa"/>
  </md:RoleDescriptor>
</md:EntityDescriptor>
```

Clave pública del GPoA

- GPoA

```
<md:EntityDescriptor entityID="http://test/gpoa">
  <md:RoleDescriptor xsi:type="papi:GPoADescriptorType"
   protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:
1.0">
   <md:KeyDescriptor use="signing">
     <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       <ds:KeyValue>
         <ds:RSAKeyValue>
           <ds:Modulus>…</ds:Modulus>
           <ds:Exponent>AQAB</ds:Exponent>
         </ds:RSAKeyValue>
       </ds:KeyValue>
     </ds:KeyInfo>
   </md:KeyDescriptor>
   <papi:GPoAService
     Binding="urn:geant:rediris:papi:browser-sso"
     Location="http://test/gpoa"/>
  </md:RoleDescriptor>
</md:EntityDescriptor>
```

URL del GPoA

- Actualización en SIR
  - Nuevos GPoAs para SIR y SIRtest
    - Basado en php-easygpoa
    - https://forja.rediris.es/projects/papi-easygpoa/
  - Proveedores de Identidad y Proveedores de Servicio
    - Sólo mediante metadatos
  - Primeras pruebas en SIRtest
    - Nuevo GPoA:
    - http://sir.rediris.es/sirtestgpoa/index.php

- Nueva gestión de cookie de sesión en el GPoA
  - Antes
    - Cookie de sesión para todo el SIR
    - Es necesario recibir todos los atributos del proveedor de identidad
  - Ahora
    - Dos modos
      - Cookie de sesión para todo el SIR
      - Cookie de sesión por cada recurso
    - Configurable mediante los metadatos

- Cookie por SP

```
PAPI_LCOOK_sirtestgpoa-d60eb13c8ef199b32e03a4a3dc34d0da
```

  - Nombre de la cookie + md5 (ID del SP)
  - Facilita la aparición del Servicio de Logout

Atributos

- Emisión de atributos para cada SP
  - Conector recibe petición ATTREQ
  - Parámetro PAPIOPOA
    - URL del SP a la que el usuario está intentando acceder
- Utilizando PAPIOPOA se emiten atributos sólo para dicho SP
- Metadatos facilitan la identificación del SP
- Emisión en Proveedores de identidad PAPI
  - icGPoA
    - No incluye de serie esta posibilidad
  - adAS (**ad**vanced **A**uthentication **S**erver)

http://www.rediris.es/sir/

www.red.es

Edificio CICA, Campus Universitario
Avenida Reina Mercedes s/n
41012 Sevilla. España

Tel.: 95 505 66 00
Fax: 95 505 66 27
www.red.es
www.rediris.es