

HMA for Science Kickoff Meeting

KO Meeting
24 January 2013, ESRIN Frascati

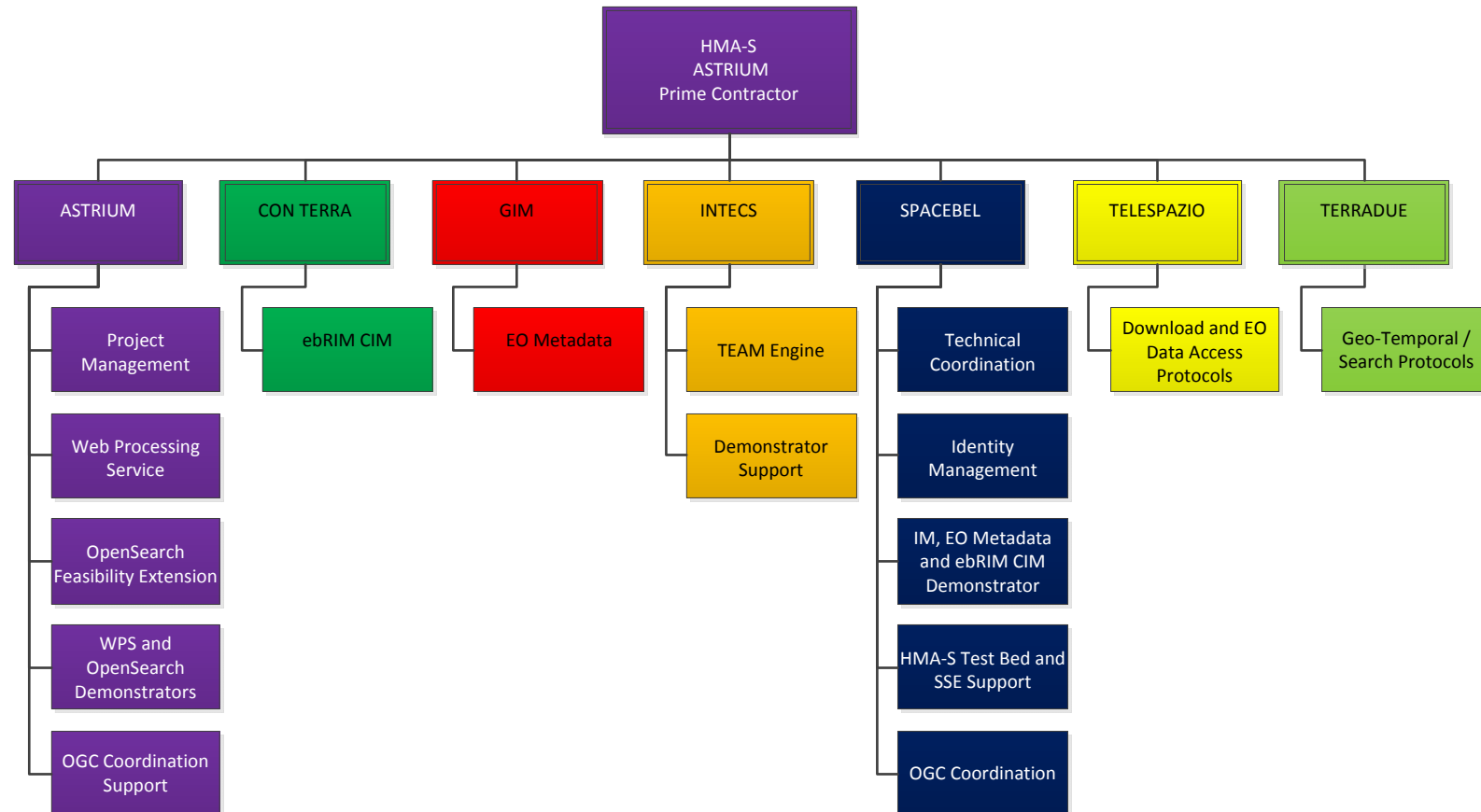
Yves Coene, SPACEBEL
Pierre Denis, SPACEBEL

- Specification Activities
 - Task 2: Identity Management

- Demonstrators
 - **Task 2: Identity Management**
 - Task 3: EO Metadata
 - Task 5: Enhancement ebRIM EP

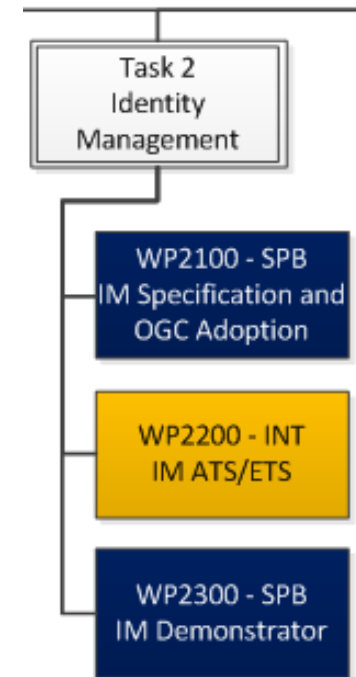
- Task 8: HMA-S Testbed

- Technical Coordination
 - Task 9: Coordination and harmonisation



➤ Task inputs:

- OGC 07-118 v1.1 (see Task 2 specification activity)
- HMA-T Identity and Access Management Guidance Document v 1.0
- HMA Skeleton 2.2
- Intecs Policy Enforcement Point
- Spacebel STS Implementation



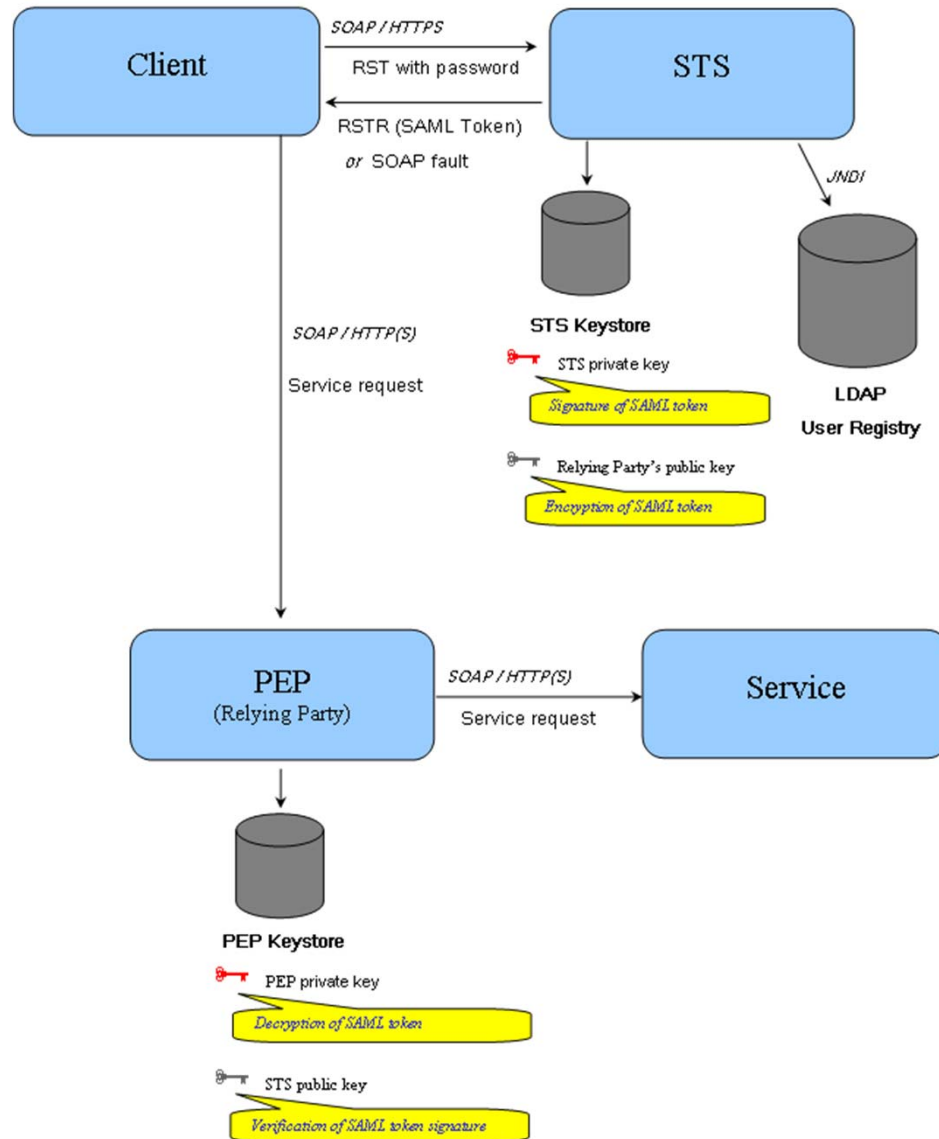
➤ Goal:

- Demonstrator for the 3 use cases of OGC 07-118:

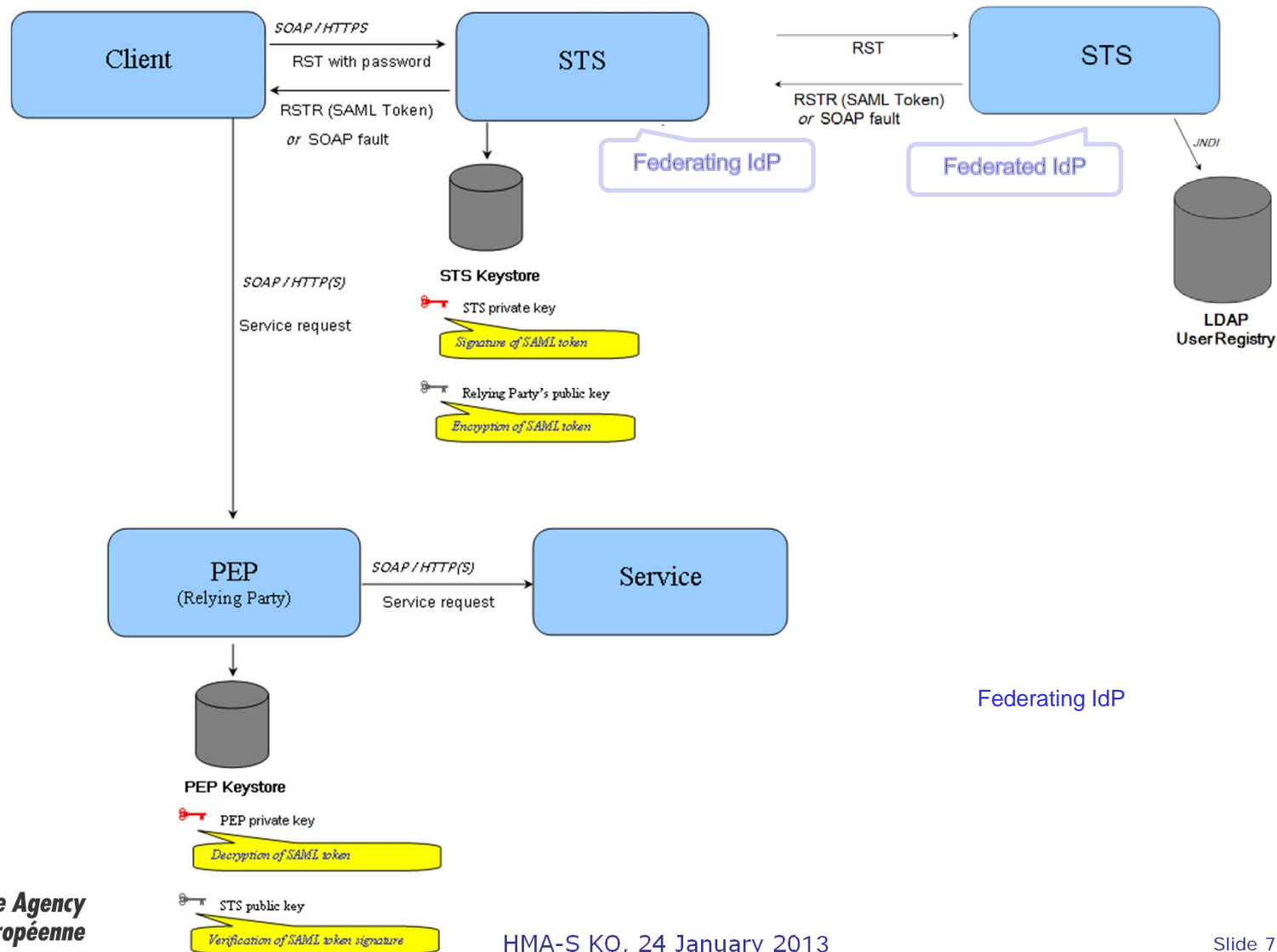
1. STS as local IdP
 2. STS as Federating IdP
 3. STS with trusted IdP (e.g. Web-SSO)
- } RST with *password*
- } RST with *signature*

- STS implementation shall be updated to cover use case 2.
- need to validate the correction of "DelegateTo" issue

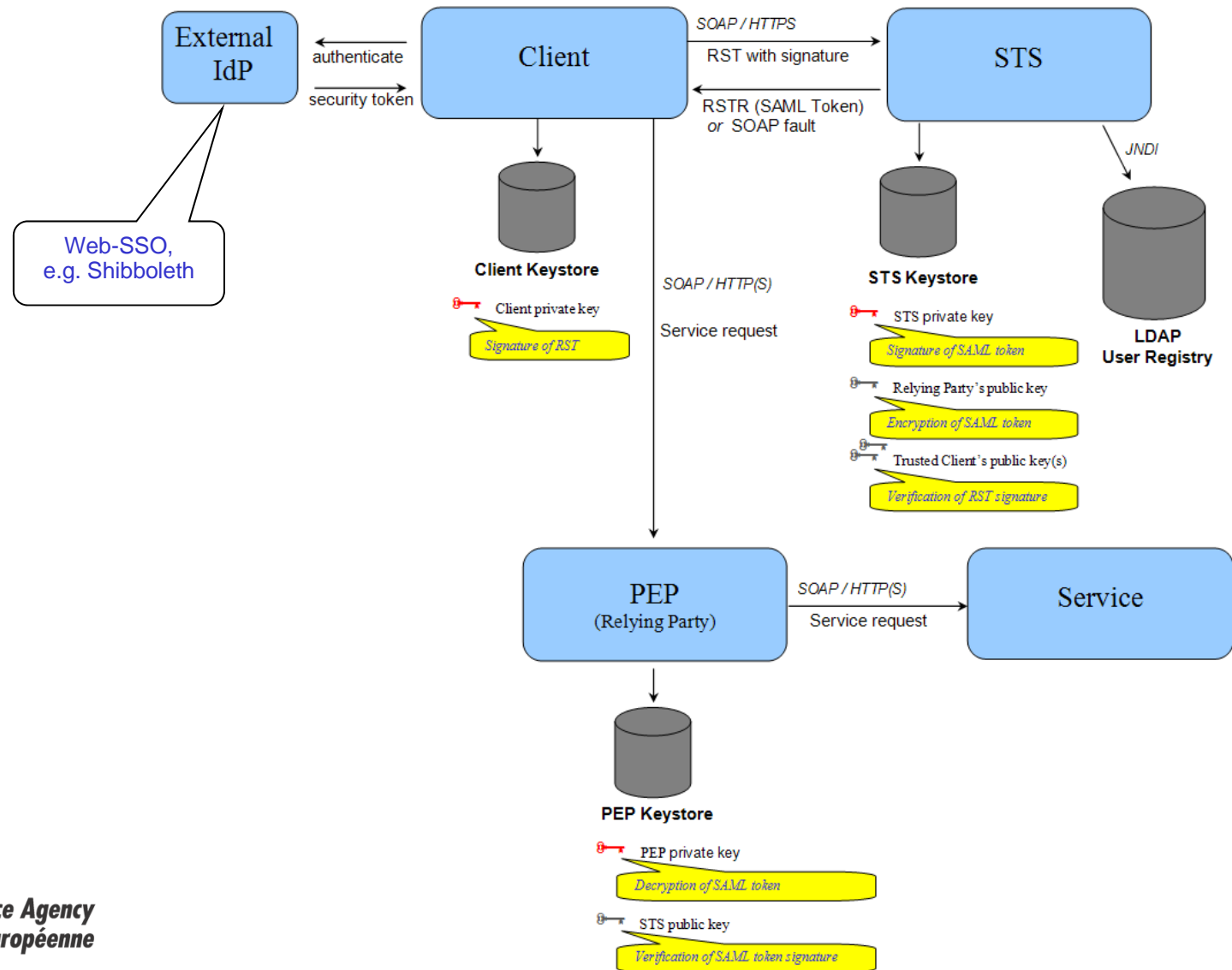
- Use case 1 : STS as local IdP





➤ Use case 2 : STS as Federating IdP (DelegateTo)



➤ Use case 3 : STS with trusted IdP





➤ HMA Skeleton (OGC 07-118 - RST)


HMA Skeleton (version 2.2 build 1004131448)


[Log](#)
[Help](#)

Service	authentication_OGC-07-118_version-0.1.0 ?
Operation	authenticate ?
Sample Request	authenticate-TestUser1 ?
Service Address	http://ssews1.esrin.esa.int/axis2/services/AuthenticationService ?
Request ?	<pre><ns1:RequestSecurityToken xmlns:ns1="http://docs.oasis-open.org/ws-sx/ws-trust/200512/"> <ns1:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1</ns1:TokenType> <ns1:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</ns1:RequestType> <ns2:UsernameToken xmlns:ns2="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"> <ns2:Username>TestUser1</ns2:Username> <ns2:Password>TestUser1</ns2:Password> </ns2:UsernameToken> </ns1:RequestSecurityToken></pre>
Send Request ?	
Response	<pre><!--> <wst:RequestSecurityTokenResponse xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512/"><wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1</wst:TokenType><wst:RequestedSecurityToken> <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"> <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <xenc:EncryptedKey><xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/><xenc:CipherData> <xenc:CipherValue>UPYCy6x0/gKcG0Ckg1jxHtW0CW1qh57m2hC8+0MpBIA6oPkXFbkcLmNOZCA2GPFxgHMS5eG8oJ9IT H0mtsAdBY91/qhOn7eF01+iasb6DwQAppQwYnrVMF1ORSkqCHaNVLB04fqWcmkHHS5u61WZfAwghZ nBhmPA0L50k2/Y0Wusk=</xenc:CipherValue></xenc:CipherData></xenc:EncryptedKey></ds:KeyInfo><xenc:CipherData> <xenc:CipherValue>/td2dQMFrg5KLNPF0+46ffES+MNCKbvB/vTS2T177sRT7WkomJN6QhKD1QWhCNAxWoo+u0vr0cv t0RWhQvITKojYiImgB82kwBhKtWjc5Twn2bPGLDJVoz8esdI8j2KYkustiB2w+Xnd0yC/ZWE2R+1 PrOzN5V+XFMwfKa2FCy7XsFpe9yInwdykb7z7cqp2K2KPKxv12TjbI6JRxV4MOQZURPesWBVXgo tult/wL6iYtBh+P6z5s05DesdzdEkBa9xPFUbDMomZr/QzTunLV7sRjMh+SqJDZ/BDLZzX09WV0L xpCBbzXkDKw33iN5s1MpWjSpIbbH3ZMFYQPz01VD0CepJY8zdvd8I2ywmQfAg5+G/cyEwBwalQPkW evXXyQutEraSR+idQ6+6xWs9mg1031T6K/RMPTC/A01G3W1Fyxz8wHGh9+tc70JS4eclYk/5LNNJS N8WTE/AFM1kRjQr8nj6aEhJcnpIvzUTUdlWuMSVhYe2Q0cWaL9ctwsZK1yEfoftrgWaQx+TnyJ6YEp ldWvivCd4otOmp79Y52YueQhOm/G8n/gyoNnmP2eAN2LcMATzB0iXChUPQ7FDhC8G2pEuMoK2fWc aWu5lh45xVYKLxf4cZekeuAmi11LoI7Xal+Y7izmzdSMEIJB6xz+HkAKwjmuMnzpGknsWK3ArPV 80LfpXWSEK8/1/Rum6XRMMNnV3NSoqS0atckIo/24XDjRLV1qlwg9Vv4luHRm8v0VQcPnRrk5hr 41Yz3RHx+62qKLZnoU5/ps12ABOF7DVgCX1PQ/gy+nwOCA4K+t1RNNZLj7LQYfqlkIdkZnBCUGD/</pre>

➤ HMA Skeleton (OGC 06-131 GetRecords)


HMA Skeleton (version 2.2 build 1006171048)


[Log](#)
[Help](#)

Service	catalogue_OGC-06-131_version-0.1.9 ?
Operation	GetRecords ?
Sample Request	GetRecords_Nominal_EOP ?
Service Address	http://django.esrin.esa.int:80/TOOLBOX/services/secured_EOP-Catalogue ?
Authentication Service Address	http://ssews1.esrin.esa.int/axis2/services/AuthenticationService ?
User name	TestUser2 ?
Password ?
Request ?	<pre><!-- \$Id: GetRecords_Nominal_EOP.xml 3904 2009-07-24 15:35:24Z tnn \$ --><GetRecords maxRecords="10" outputFormat="application/xml" outputSchema="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" requestId="" resultType="results" service="CSW" startPosition="1" version="2.0.2" xmlns="http://www.opengis.net/cat/csw /2.0.2" xmlns:aoi="http://www.esa.int/xml/schemas/mass/aoifeatures" xmlns:gml="http://www.opengis.net/gml" xmlns:ogc="http://www.opengis.net/ogc" xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" xmlns:serviceNs="http://www.esa.int/sse_ebrim" xmlns:sse="http://www.esa.int/mass" xmlns:wrs="http://www.opengis.net/cat/wrs/1.0"> <csw:Query typeName="rim:ExtrinsicObject rim:ExtrinsicObject_acquisitionPlatform rim:ExtrinsicObject_dataLayer rim:Association_acquisitionPlatAsso rim:Association_dataLayerAsso rim:Classification rim:ClassificationNode" xmlns:csw="http://www.opengis.net/cat/csw/2.0.2"> <csw:ElementSetName typeName="rim:ExtrinsicObject">full</csw:ElementSetName> </csw:Query> </GetRecords></pre>
Send Request ?	
Response	<pre><!--> <ns4:GetRecordsResponse xmlns="http://www.opengis.net/ows" xmlns:ns10="http://earth.esa.int/atm" xmlns:ns11="http://earth.esa.int/opt" xmlns:ns12="http://earth.esa.int/sar" xmlns:ns13="urn:oasis:names:tc:ebxml- regrep:xsd:rim:3.0" xmlns:ns2="http://www.w3.org/1999/xlink" xmlns:ns3="http://www.opengis.net/ogc" xmlns:ns4="http://www.opengis.net/cat/csw/2.0.2" xmlns:ns5="http://purl.org/dc/elements/1.1/" xmlns:ns6="http://purl.org/dc/terms/" xmlns:ns7="http://www.opengis.net/gml" xmlns:ns8="http://www.opengis.net /cat/wrs/1.0" xmlns:ns9="http://earth.esa.int/eop"> <ns4:SearchStatus/> <ns4:SearchResults nextRecord="0" numberOfRecordsMatched="0" numberOfRecordsReturned="0"/> </ns4:GetRecordsResponse></pre>

➤ Outputs:

- D2000.2: Open-source Demonstrator
 - Policy Enforcement Point (Intecs)
 - Client – HMA Skeleton (Spacebel)
 - Updated Security Token Service (Spacebel)
- D2000.3: Demonstrator TN including
 - Description of native interfaces
 - User Manual

H2.1 –
HMA Skeleton (Client)

H2.2 – STS

H2.3 – PEP

} Updated HMA-T Guidance Document

➤ Issues:

- Integration with Web SSO as part of Demonstrator ?
- Alternatives:
 - Online (test) UM-SSO IDP available at ESA to connect to ?
 - UM-SSO IDP to be made available by ESA ?
 - Shibboleth IDP instead of UM-SSO IDP ?