ESA EO Identify Management

The ESA EO IM Infrastructure & Services

A. Baldi ESA: Andrea.Baldi@esa.int

M. Leonardi   ESA: m.leonardi@rheagroup.com

Issues @ ESA with legacy user management

- Users had multiple identity (Login/password)
- User information was unstructured (any system had its own different user profile structure)
- user information was stored in multiple registries and got unsynchronized and inconsistent.
- User information was stored in unsafe registry
- User information was exchanged un-securely
- Authorization across applications was impossible
- NO Single Sign On
- High operational cost to keep all under control

IM introduced in 2011

- Identity Management and the supporting AAI infrastructure for the creation, maintenance, and utilization of digital identities introduced in beginning of 2011 after an initial study:
  - Initially based on Shibboleth 1 and then ported on Shibboleth 2 (current baseline) with few extensions,
  - Consist of:
    - Redundant Identity providers (IDPs)
    - Redundant Identity Registries (LDAPs)
    - Multiple Service Provider (SPs) Check Points
  - Is based on a common "Minimal User Profile" derived from *inetOrgPerson* + a dedicated common SP profile for specific attributes.

IM Functions

- ESA EO IM includes processes for:
    - **Authentication** – Single SIgn On for all Web applications with inheritance of User community between SPs.
        - Master SPs, Community SPs
    - **Authorization** – exchange of attributes for granting user access to resources with SP profile synchronization with IDP.
        - SOAP Interface to updates local SP profile attributes on IDP.
        - **Chained Multi Step Self Registration** – Acquiring user's identity information by IDP and SPs before issuing user credential.
            - SP registrations chained to IDP registration

IM Functions

- ESA EO IM includes processes for:
  - **Credential Recovery:** The user is able to self recover a forgotten password autonomously:
    - Based on Secret Question - Secret Answer
  - **Administration** - Self users administration of key profile information. More advanced administration functions across the enterprise for IM administrators.
    - User: Passwords, email, Question/Secret Answer
    - Admin: all profile fields, and simple SP management

IM Functions

- **Secure Storage:** storage of sensitive identity information into secure registry (via encryption):
  - Encryption keys owned by the IDP.
- **Security Enforcement**: password strong security enforced upon registration and password management by the IDP.
- **Auditing**: auditing of user privileges, user access to resources, resource utilization (on going).
- **Reporting**: reporting of user information for statistical utilization via a dedicated BI tool .
  - Integration with Data Analisys Tool for EO statistics

IM Functions

- **Authentication for Java Applications:**
  - JCL (Java Client Library) designed to offer an SSO API to Java applications.
  - The JCL component is like an encapsulated browser module with key browser capabilities:
    - Interface the user for credentials exchange
    - Store and handle the cookies
    - Handle Redirections
    - Handle Query/Response to/from IDP & SPs
- **AAI Easy Deployment**: Virtual Environment with AAI infrastructure and IM template for SP.

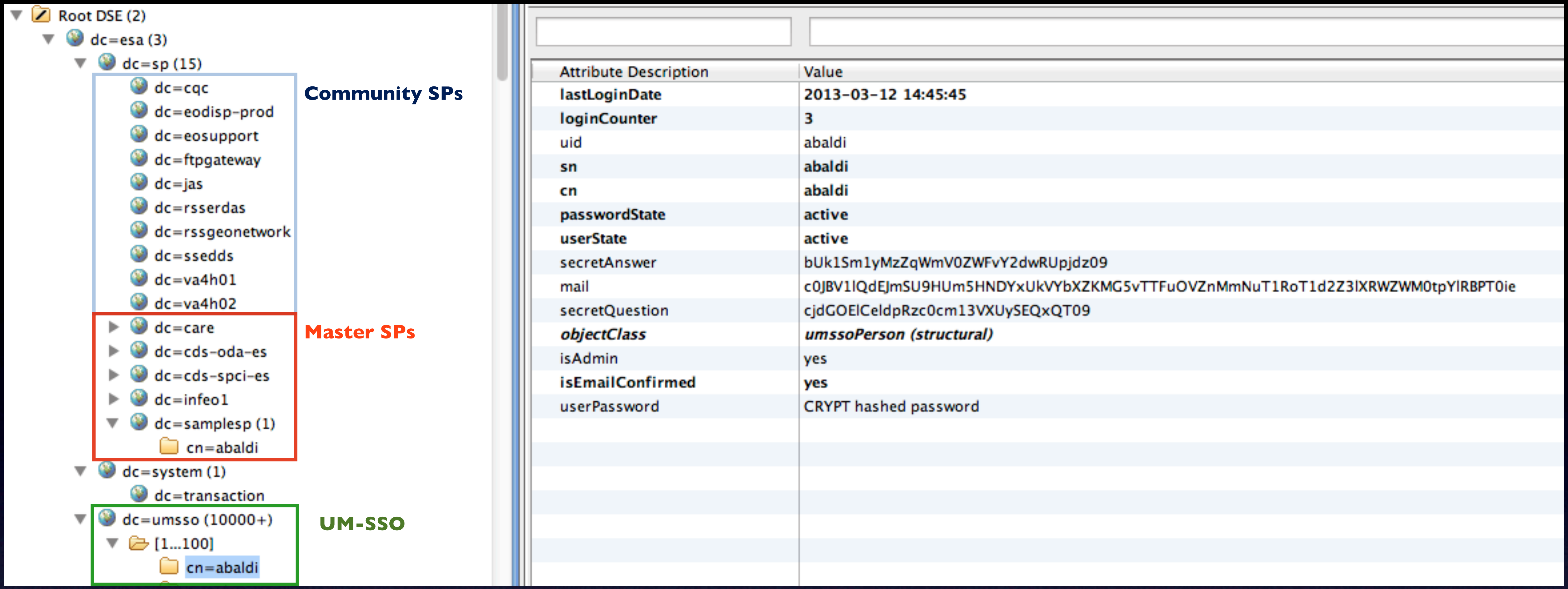
Short terms requirements

- Keep User registry smaller and manageable, minimizing administrative cost
- Enhance and streamline the EO User (Minimum) profile: necessary for harmonization of EO applications and to support new SPs AuthZ:
  - Term & Condition acceptance for access to EO data sets
  - Quality of Service associated to users' category to tune the resources availability
  - Opaque users' identifiers to enforce privacy rules
- Auditing and reporting about user access and resource utilization.
- Enhance operator's tools for supporting IM deployment and operations
- Allows even simpler integration and configuration of new EO Service Providers:
  - Evolution of the Virtual EO SSO
  - Simplify the exchange of metadata and configurations between parties.

Medium terms objectives

- Access resources operated by different organization (.e.g. EO SSO users accessing Nasa Resources)
- Create the foundation for Identity Federation:
    - Internal Federations: to split/model ESA user communities into smaller dedicate "domains" (i.e ESA projects, ESA/EU projects)
    - External Federations: with different Space organization to interoperate and share accounts (e.g NASA, EUMETSAT, ..)
- To be compliant with EC rules for data protection and privacy

Questions?



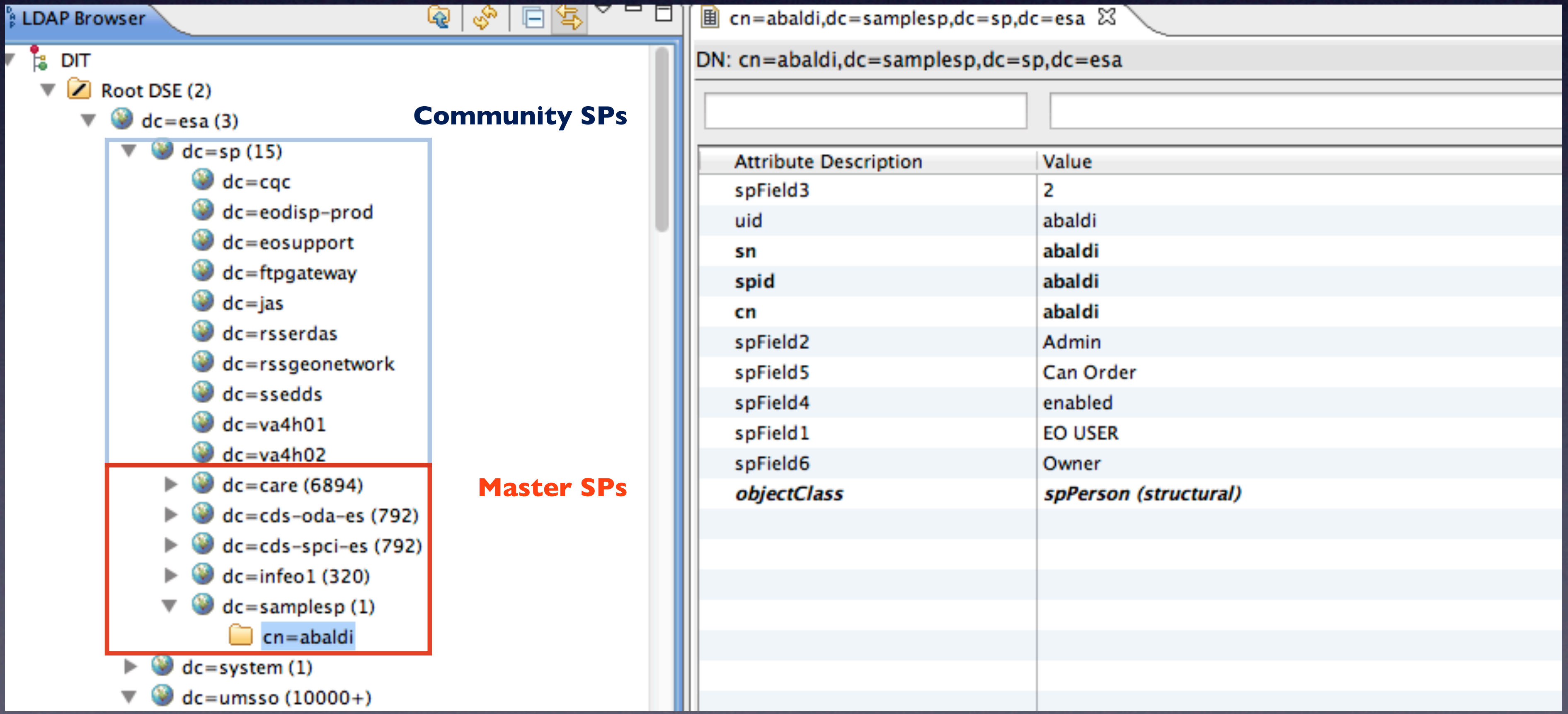
Root DSE (2)
dc=esa (3)
dc=sp (15)
dc=cqc
dc=eodisp-prod
dc=eosupport
dc=ftpgateway
dc=jas
dc=rsserdas
dc=rssgeonetwork
dc=ssedds
dc=va4h01
dc=va4h02
dc=care
dc=cds-oda-es
dc=cds-spci-es
dc=infeo1
dc=samplesp (1)
cn=abaldi
dc=system (1)
dc=transaction
dc=umsso (10000+)
[1...100]
cn=abaldi

Community SPs

Master SPs

UM-SSO

Attribute Description	Value
lastLoginDate	**2013-03-12 14:45:45**
loginCounter	**3**
uid	abaldi
sn	**abaldi**
cn	**abaldi**
passwordState	**active**
userState	**active**
secretAnswer	bUk1Sm1yMzZqWmV0ZWFvY2dwRUpjdz09
mail	c0JBV1lQdEJmSU9HUm5HNDYxUkVYbXZKMG5vTTFuOVZnMmNuT1RoT1d2Z3lXRWZWM0tpYlRBPT0ie
secretQuestion	cjdGOElCeldpRzc0cm13VXUySEQxQT09
objectClass	***umssoPerson (structural)***
isAdmin	yes
isEmailConfirmed	**yes**
userPassword	CRYPT hashed password



DIT
Root DSE (2)
dc=esa (3)
dc=sp (15)
dc=cqc
dc=eodisp-prod
dc=eosupport
dc=ftpgateway
dc=jas
dc=rsserdas
dc=rssgeonetwork
dc=ssedds
dc=va4h01
dc=va4h02
dc=care (6894)
dc=cds-oda-es (792)
dc=cds-spci-es (792)
dc=infeo1 (320)
dc=samplesp (1)
cn=abaldi
dc=system (1)
dc=umsso (10000+)

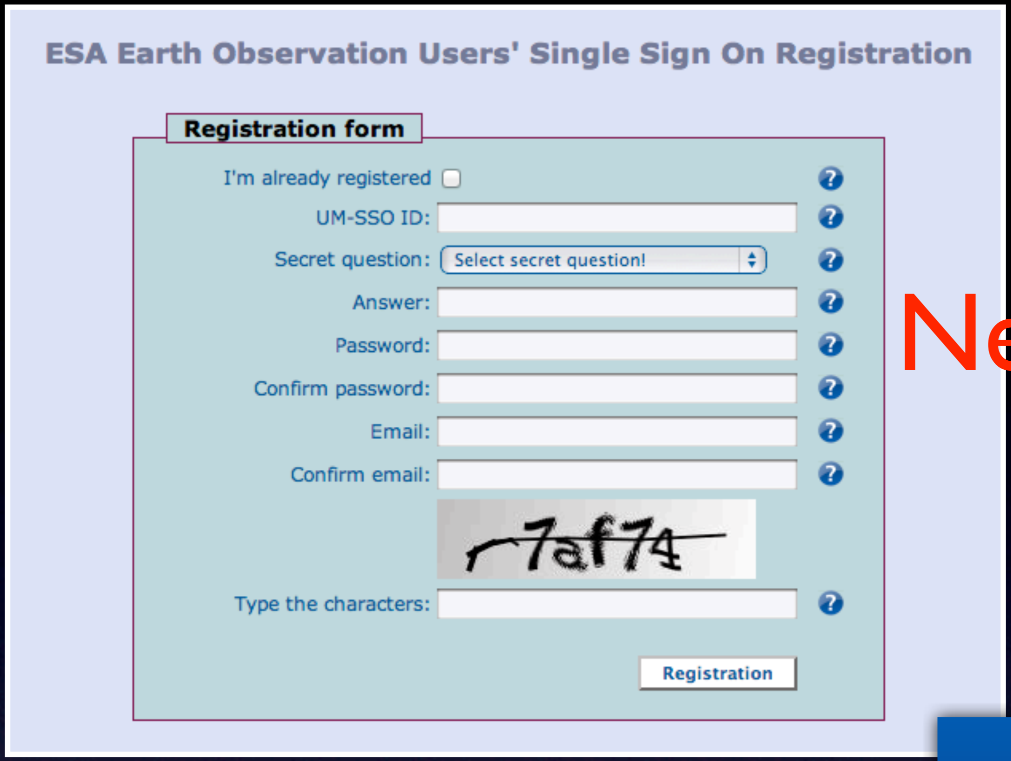
Community SPs

Master SPs

DN: cn=abaldi,dc=samplesp,dc=sp,dc=esa

Attribute Description	Value
spField3	2
uid	abaldi
sn	**abaldi**
spid	**abaldi**
cn	**abaldi**
spField2	Admin
spField5	Can Order
spField4	enabled
spField1	EO USER
spField6	Owner
objectClass	***spPerson (structural)***

Master SPs and Community SPs



ESA Earth Observation Users' Single Sign On Registration

Registration form

I'm already registered □

UM-SSO ID:

Secret question: Select secret question!

Answer:

Password:

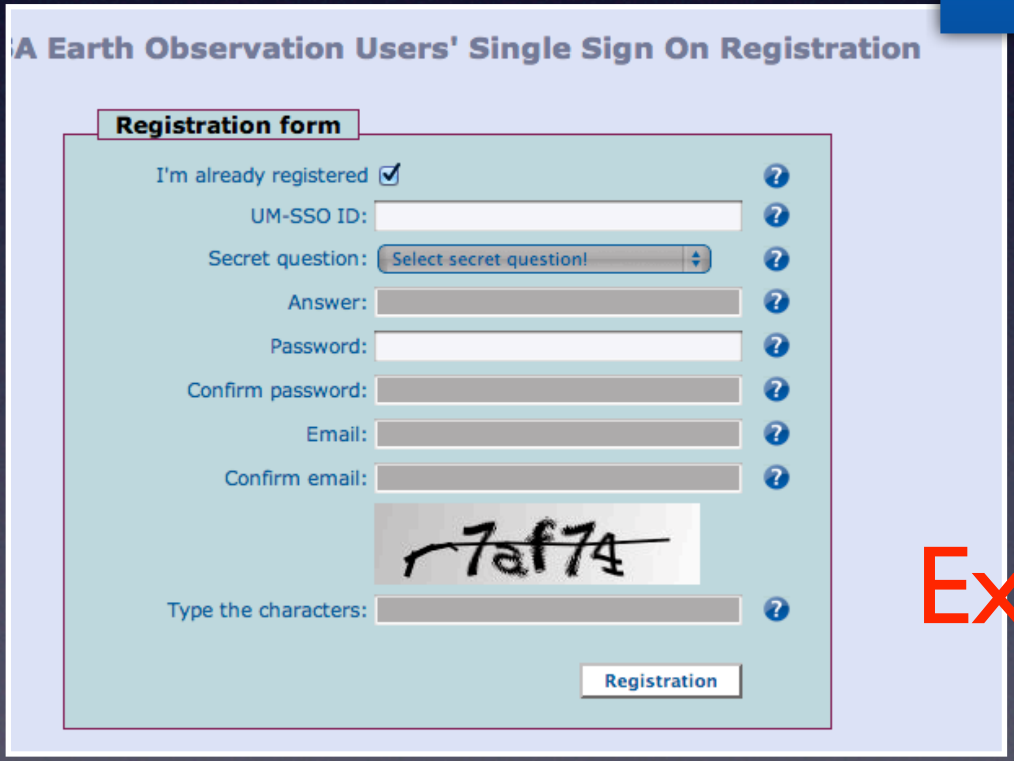
Confirm password:

Email:

Confirm email:

Type the characters:

New User



A Earth Observation Users' Single Sign On Registration

Registration form

I'm already registered ☑

UM-SSO ID:

Secret question: Select secret question!

Answer:

Password:

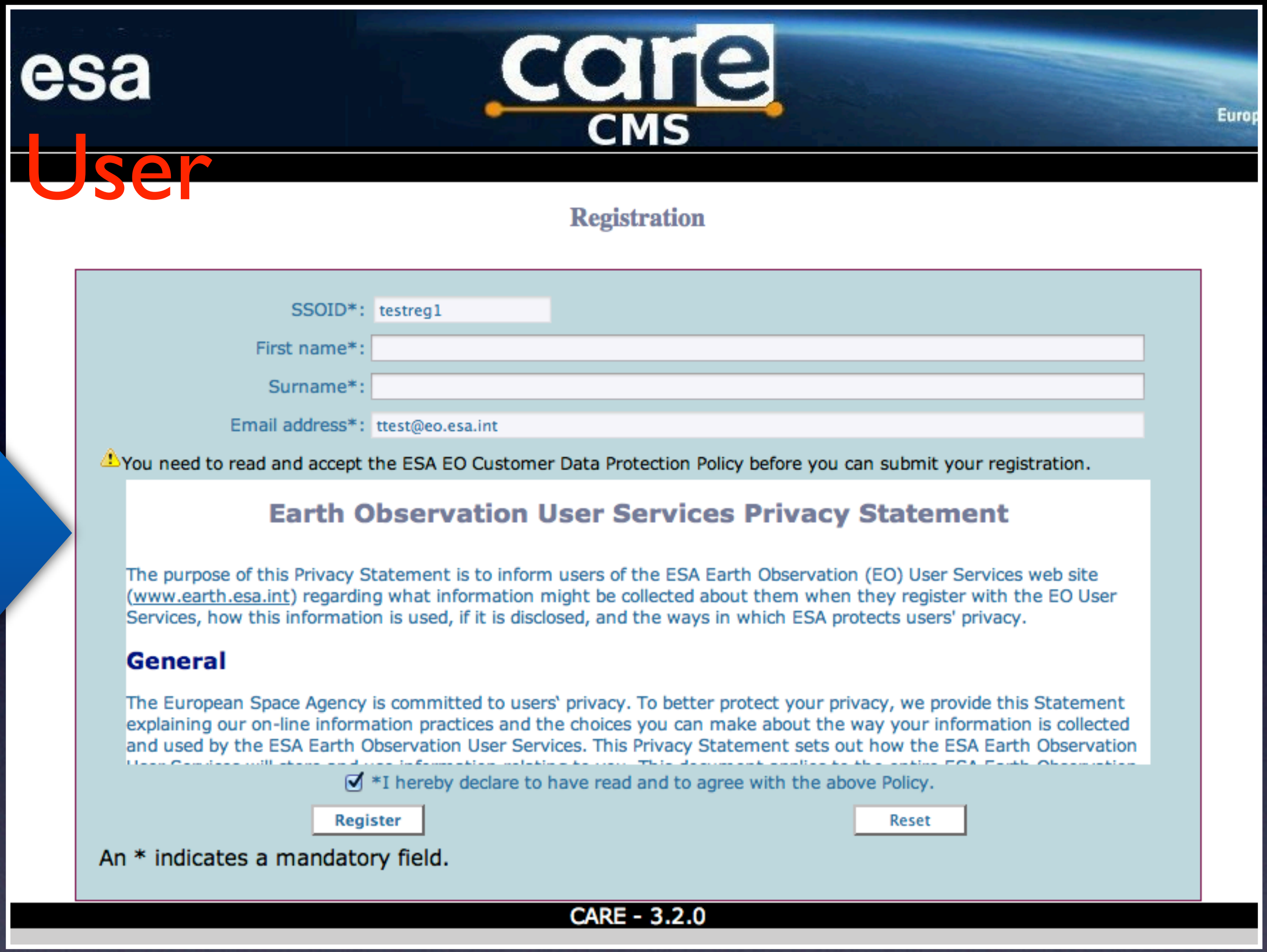
Confirm password:

Email:

Confirm email:

Type the characters:

Existing User



Registration

SSOID*: testreg1

First name*:

Surname*:

Email address*: ttest@eo.esa.int

⚠You need to read and accept the ESA EO Customer Data Protection Policy before you can submit your registration.

Earth Observation User Services Privacy Statement

The purpose of this Privacy Statement is to inform users of the ESA Earth Observation (EO) User Services web site (www.earth.esa.int) regarding what information might be collected about them when they register with the EO User Services, how this information is used, if it is disclosed, and the ways in which ESA protects users' privacy.

General

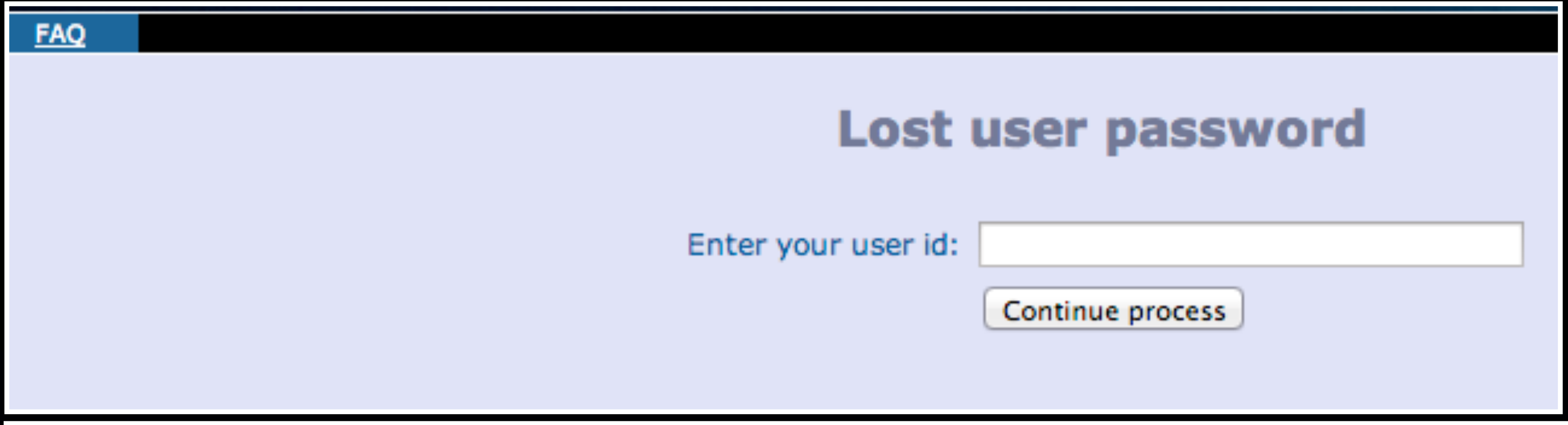
The European Space Agency is committed to users' privacy. To better protect your privacy, we provide this Statement explaining our on-line information practices and the choices you can make about the way your information is collected and used by the ESA Earth Observation User Services. This Privacy Statement sets out how the ESA Earth Observation

☑ *I hereby declare to have read and to agree with the above Policy.

An * indicates a mandatory field.

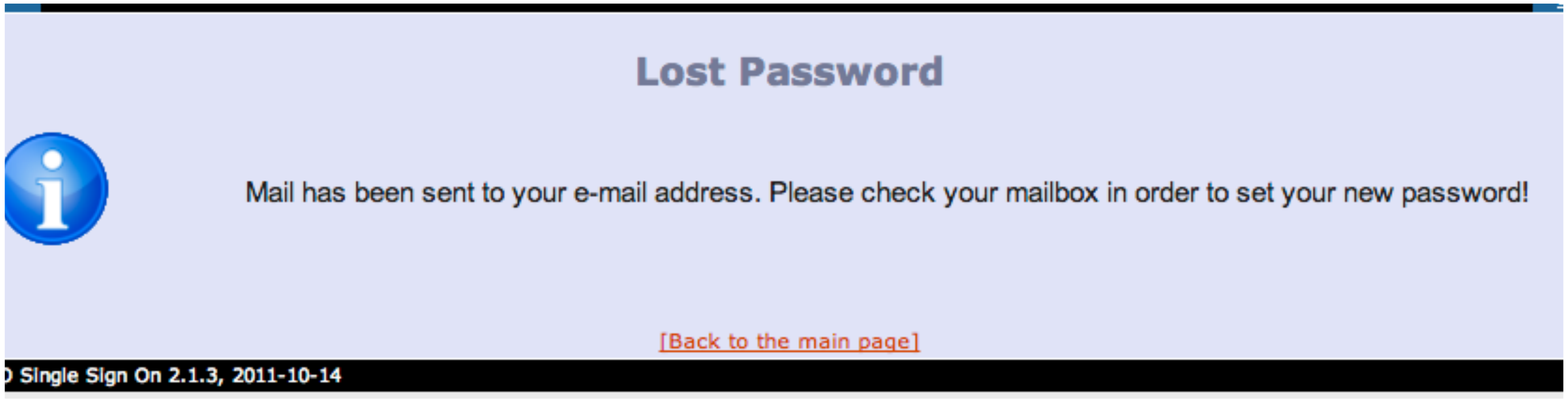
CARE - 3.2.0

Chained Users Registration



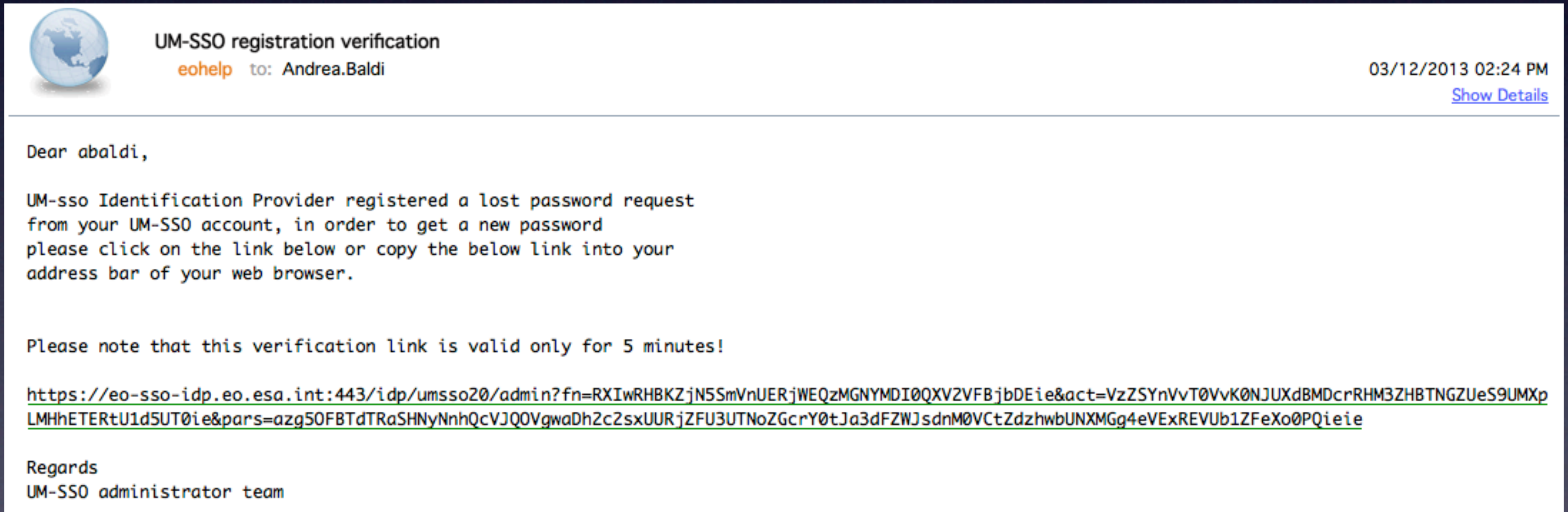
Lost user password

Enter your user id:



Lost Password

Mail has been sent to your e-mail address. Please check your mailbox in order to set your new password!

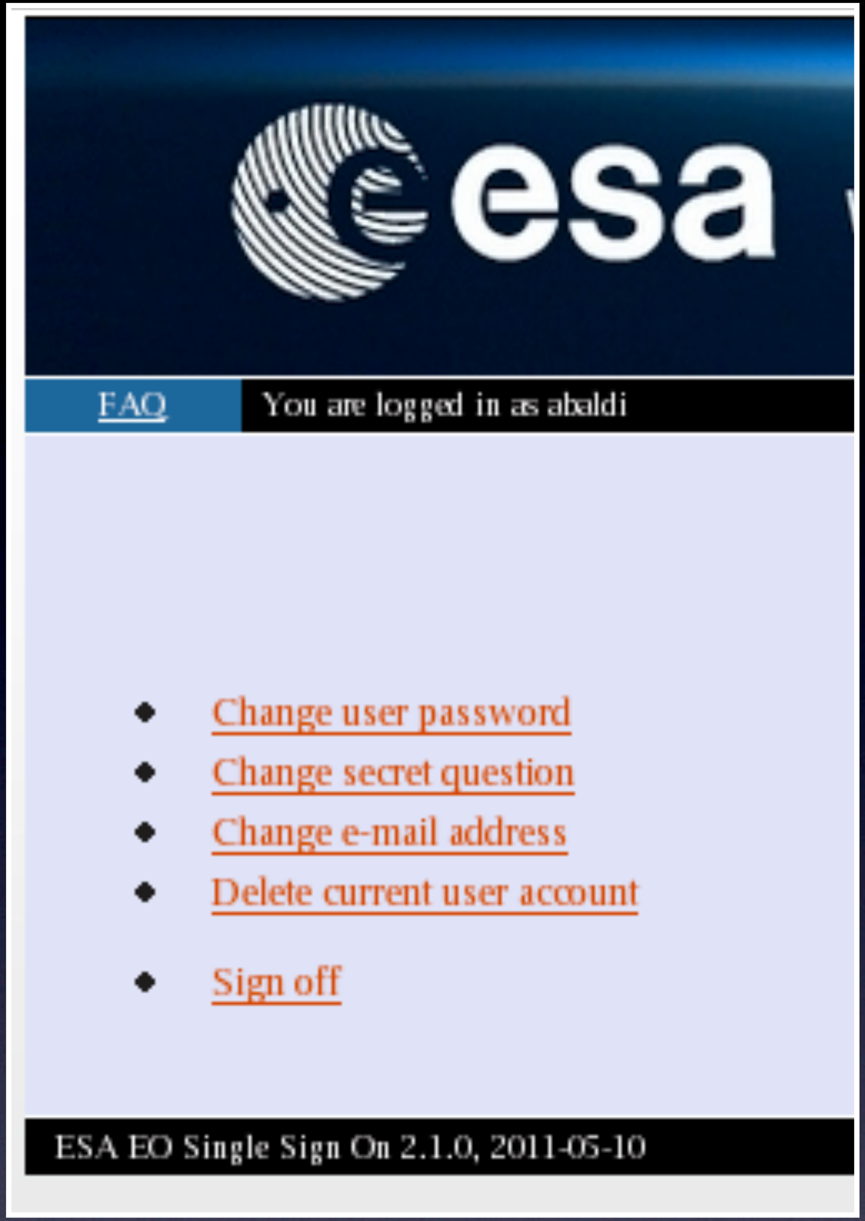


UM-SSO registration verification
eohelp to: Andrea.Baldi

03/12/2013 02:24 PM

```
Dear abaldi,

UM-sso Identification Provider registered a lost password request
from your UM-SSO account, in order to get a new password
please click on the link below or copy the below link into your
address bar of your web browser.


Please note that this verification link is valid only for 5 minutes!

https://eo-sso-idp.eo.esa.int:443/idp/umsso20/admin?fn=RXIwRHBKZjN5SmVnUERjWEQzMGNYMDI0QXV2VFBjbDEie&act=VzZSYnVvT0VvK0NJUXdBMDcrRHM3ZHBTNGZUeS9UMXp
LMHhETERtU1d5UT0ie&pars=azg5OFBTdTRaSHNyNnhQcVJQOVgwaDh2c2sxUURjZFU3UTNoZGcrY0tJa3dFZWJsdnM0VCtZdzhwbUNXMGg4eVExREVUb1ZFeXo0PQieie

Regards
UM-SSO administrator team
```

Lost Password

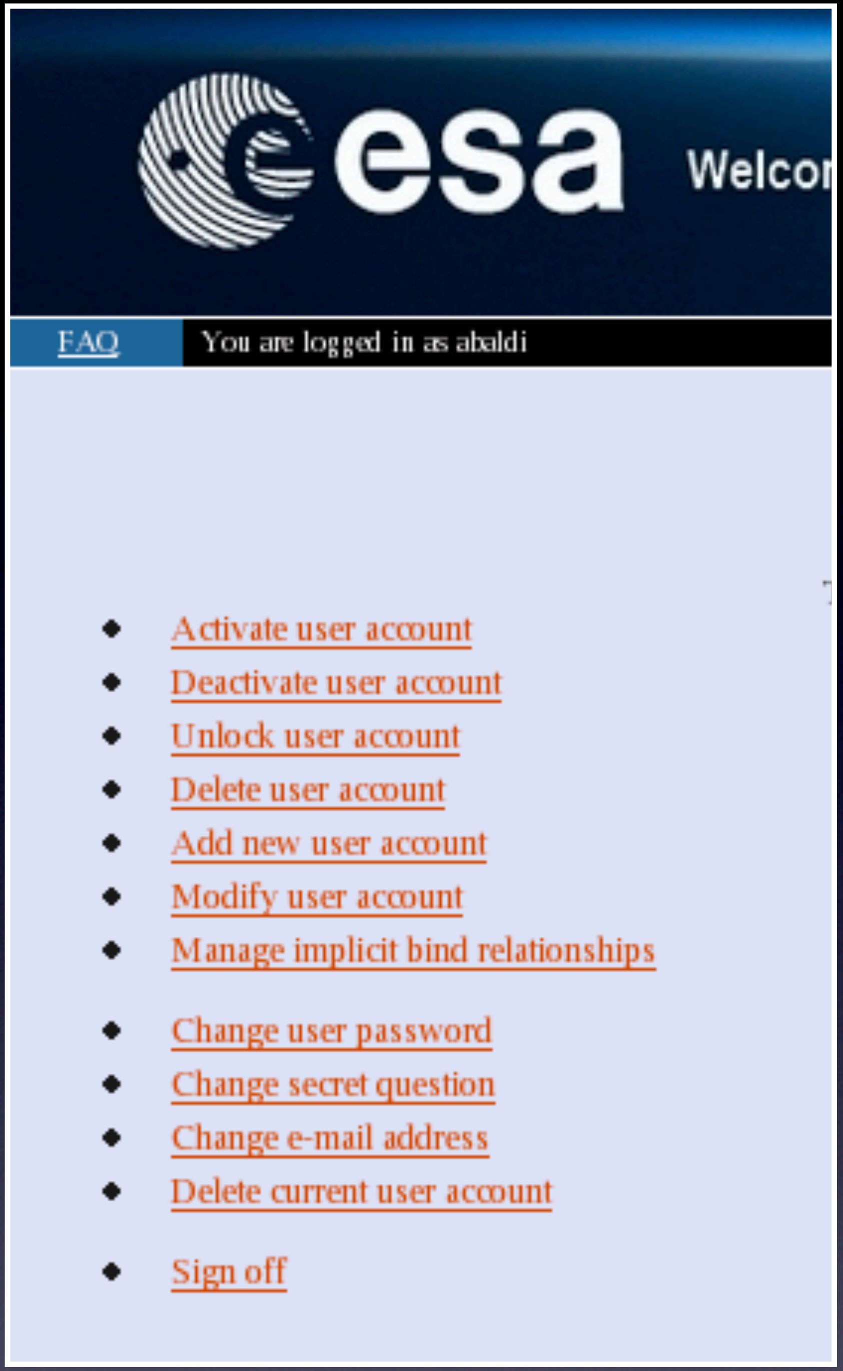


FAQ You are logged in as abaldi

- Change user password
- Change secret question
- Change e-mail address
- Delete current user account

- Sign off

ESA EO Single Sign On 2.1.0, 2011-05-10



FAQ You are logged in as abaldi

- Activate user account
- Deactivate user account
- Unlock user account
- Delete user account
- Add new user account
- Modify user account
- Manage implicit bind relationships

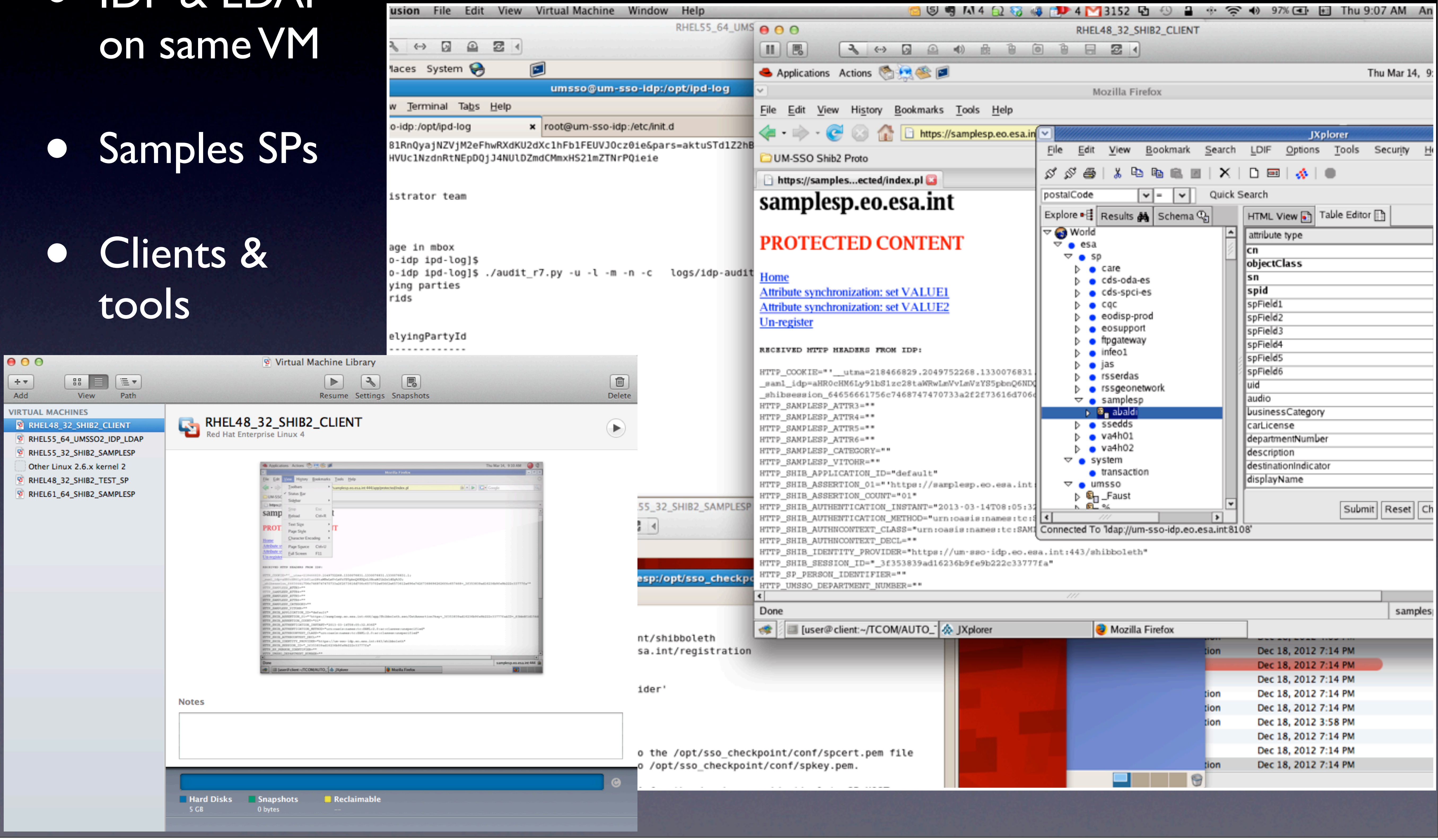
- Change user password
- Change secret question
- Change e-mail address
- Delete current user account

- Sign off

Administration

Virtual EO SSO

- IDP & LDAP on same VM
- Samples SPs
- Clients & tools



RHEL55_64_UMS

umsso@um-sso-idp:/opt/ipd-log

o-idp:/opt/ipd-log | root@um-sso-idp:/etc/init.d

```
81RnQyajNZVjM2eFhwRXdKU2dXc1hFb1FEUVJOcz0ie&pars=aktuSTd1Z2hB
HVUc1NzdnRtNEpDQjJ4NUlDZmdCMmxHS21mZTNrPQieie


istrator team



age in mbox
o-idp ipd-log]$
o-idp ipd-log]$ ./audit_r7.py -u -l -m -n -c   logs/idp-audit
ying parties
rids


elyingPartyId
-------------
```

RHEL48_32_SHIB2_CLIENT

Mozilla Firefox

https://samplesp.eo.esa.in

UM-SSO Shib2 Proto

https://samples...ected/index.pl

samplesp.eo.esa.int

PROTECTED CONTENT

Home
Attribute synchronization: set VALUE1
Attribute synchronization: set VALUE2
Un-register

```
RECEIVED HTTP HEADERS FROM IDP:

HTTP_COOKIE="'__utma=218466829.2049752268.1330076831
_saml_idp=aHR0cHM6Ly91bS1zc28taWRwLmVvLmVzYS5pbnQ6NDQ
_shibsession_64656661756c746874747470733a2f2f73616d706
HTTP_SAMPLESP_ATTR3=""
HTTP_SAMPLESP_ATTR4=""
HTTP_SAMPLESP_ATTR5=""
HTTP_SAMPLESP_ATTR6=""
HTTP_SAMPLESP_CATEGORY=""
HTTP_SAMPLESP_VITOHR=""
HTTP_SHIB_APPLICATION_ID="default"
HTTP_SHIB_ASSERTION_01="'https://samplesp.eo.esa.int
HTTP_SHIB_ASSERTION_COUNT="01"
HTTP_SHIB_AUTHENTICATION_INSTANT="2013-03-14T08:05:32
HTTP_SHIB_AUTHENTICATION_METHOD="urn:oasis:names:tc:S
HTTP_SHIB_AUTHNCONTEXT_CLASS="urn:oasis:names:tc:SAML
HTTP_SHIB_AUTHNCONTEXT_DECL=""
HTTP_SHIB_IDENTITY_PROVIDER="https://um-sso-idp.eo.esa.int:443/shibboleth"
HTTP_SHIB_SESSION_ID="_3f353839ad16236b9fe9b222c33777fa"
HTTP_SP_PERSON_IDENTIFIER=""
HTTP_UMSSO_DEPARTMENT_NUMBER=""
```

Done

JXplorer

postalCode = Quick Search

World
esa
sp
care
cds-oda-es
cds-spci-es
cqc
eodisp-prod
eosupport
ftpgateway
infeo1
jas
rsserdas
rssgeonetwork
samplesp
abald
ssedds
va4h01
va4h02
system
transaction
umsso
_Faust

attribute type
cn
objectClass
sn
spid
spField1
spField2
spField3
spField4
spField5
spField6
uid
audio
businessCategory
carLicense
departmentNumber
description
destinationIndicator
displayName

Connected To 'ldap://um-sso-idp.eo.esa.int:8108'

[user@client:~/TCOM/AUTO_ | JXplorer | Mozilla Firefox

Virtual Machine Library

VIRTUAL MACHINES
RHEL48_32_SHIB2_CLIENT
RHEL55_64_UMSSO2_IDP_LDAP
RHEL55_32_SHIB2_SAMPLESP
Other Linux 2.6.x kernel 2
RHEL48_32_SHIB2_TEST_SP
RHEL61_64_SHIB2_SAMPLESP

RHEL48_32_SHIB2_CLIENT
Red Hat Enterprise Linux 4

Notes

Hard Disks 5 GB | Snapshots 0 bytes | Reclaimable --

55_32_SHIB2_SAMPLESP

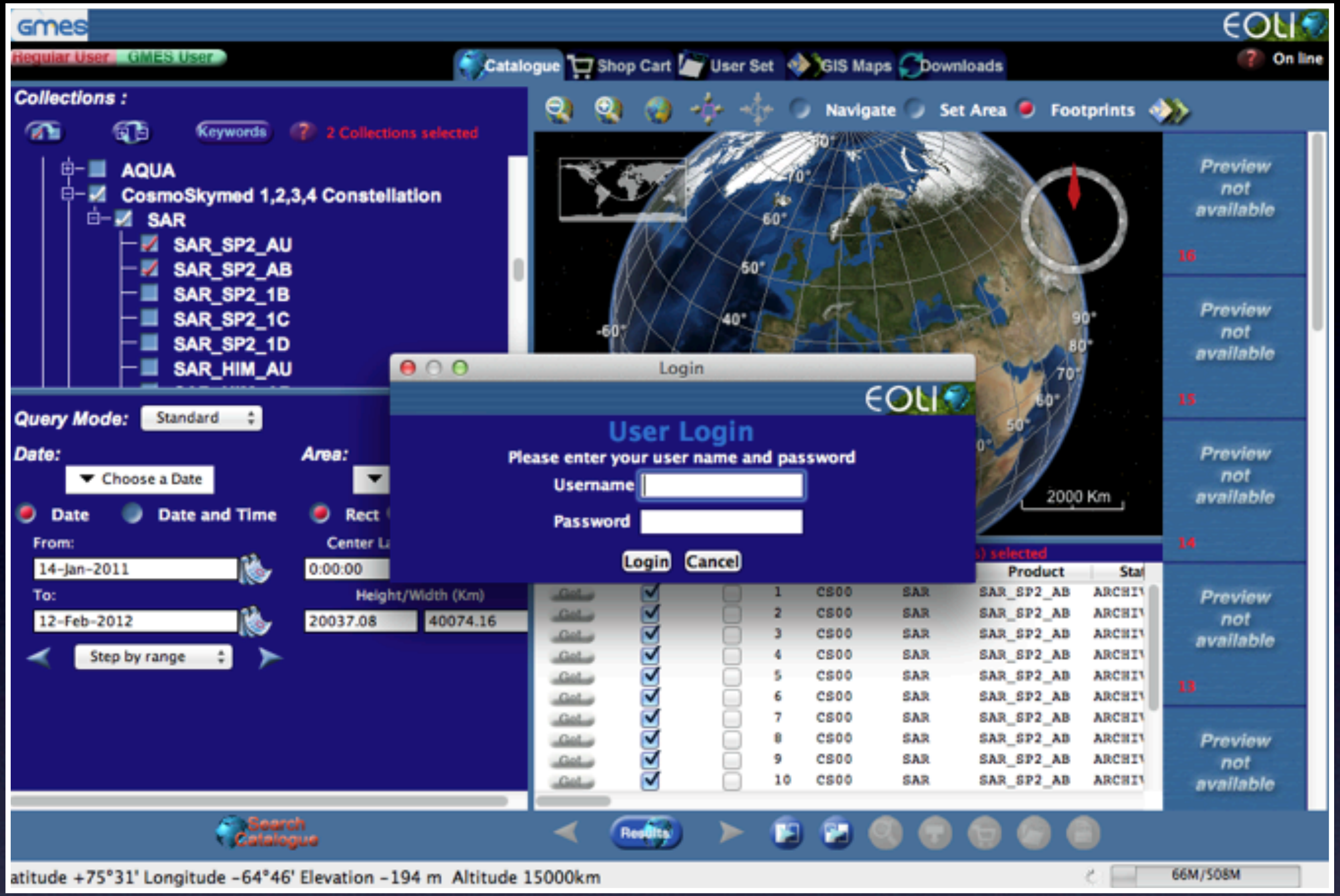
esp:/opt/sso_checkp

```
nt/shibboleth
sa.int/registration


ider'



o the /opt/sso_checkpoint/conf/spcert.pem file
o /opt/sso_checkpoint/conf/spkey.pem.
```

Dec 18, 2012 7:14 PM
Dec 18, 2012 7:14 PM
Dec 18, 2012 7:14 PM
Dec 18, 2012 7:14 PM
Dec 18, 2012 7:14 PM
Dec 18, 2012 3:58 PM
Dec 18, 2012 7:14 PM
Dec 18, 2012 7:14 PM
Dec 18, 2012 7:14 PM

usion File Edit View Virtual Machine Window Help
Thu 9:07 AM
Applications Actions
Thu Mar 14,
File Edit View History Bookmarks Tools Help
File Edit View Bookmark Search LDIF Options Tools Security
Explore Results Schema
HTML View Table Editor
Submit Reset
Add View Path Resume Settings Snapshots Delete

JCL Library for



User Login

Please enter your user name and password

Username

Password

Login Cancel

Query Mode: Standard

Date: Choose a Date

Area:

● Date ○ Date and Time ● Rect

From: 14-Jan-2011

To: 12-Feb-2012

Center L… 0:00:00

Height/Width (Km) 20037.08 40074.16

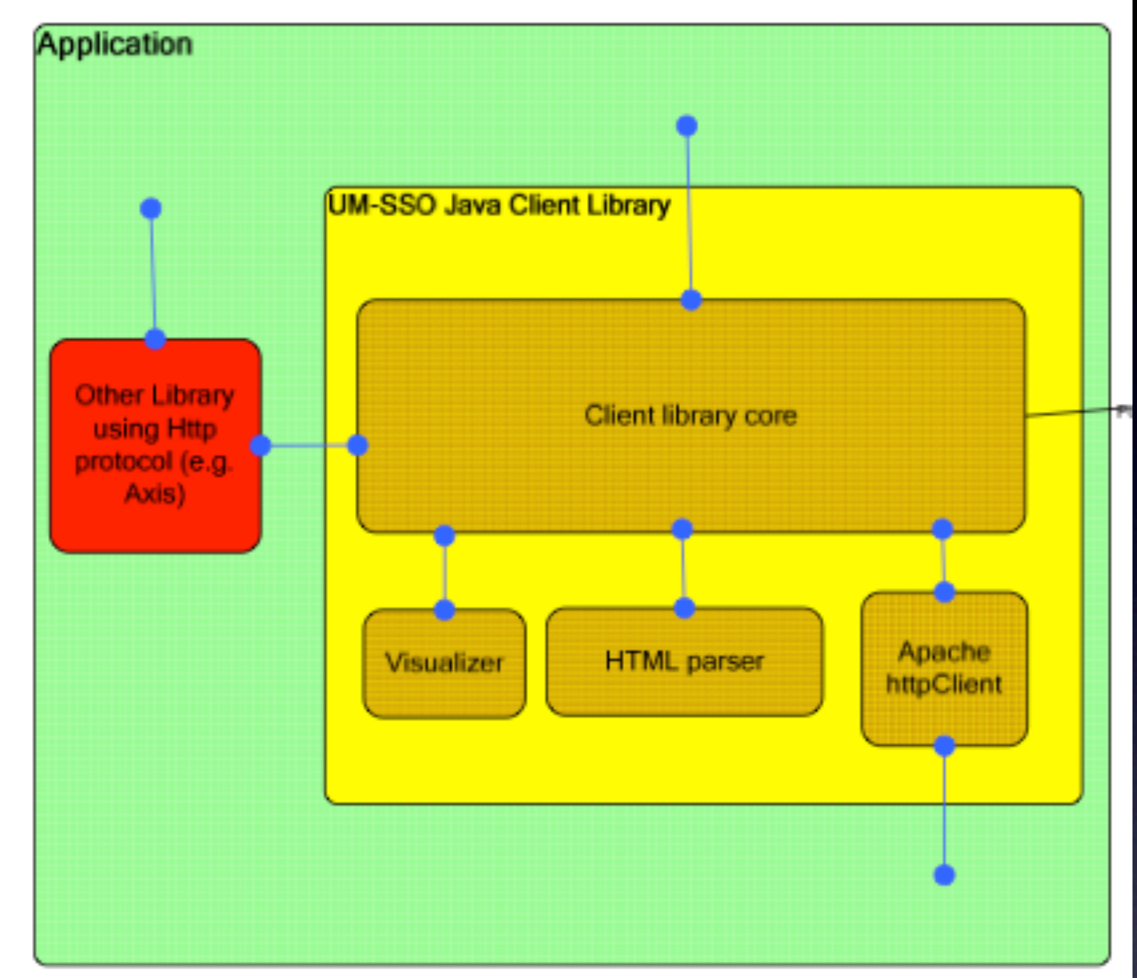
Step by range

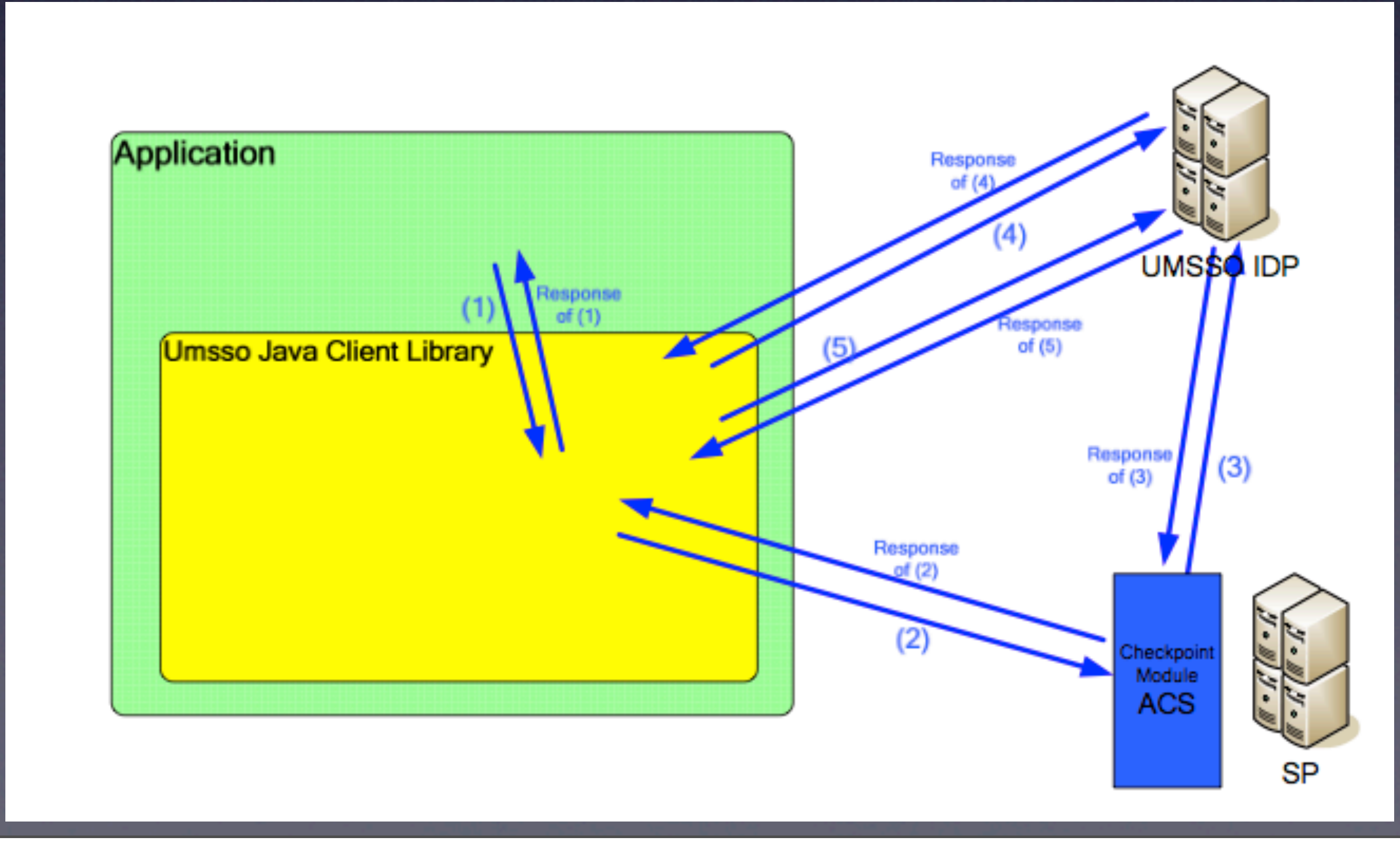
…) selected

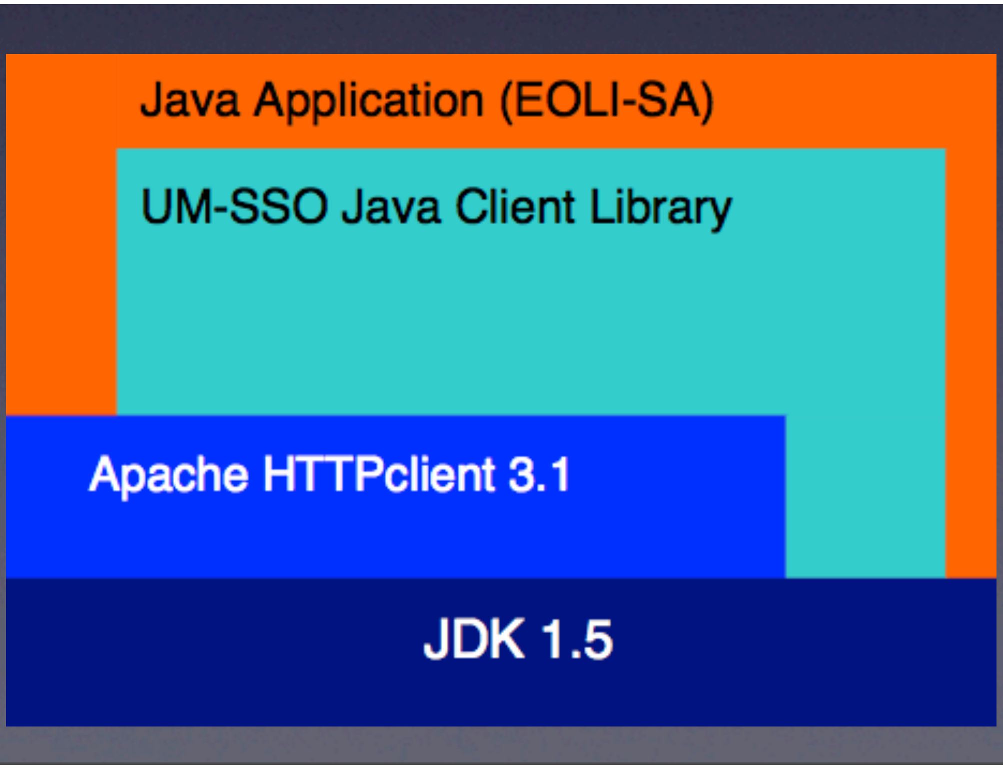
						Product	Stat
Get	☑	☐	1	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	2	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	3	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	4	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	5	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	6	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	7	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	8	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	9	CS00	SAR	SAR_SP2_AB	ARCHIV
Get	☑	☐	10	CS00	SAR	SAR_SP2_AB	ARCHIV

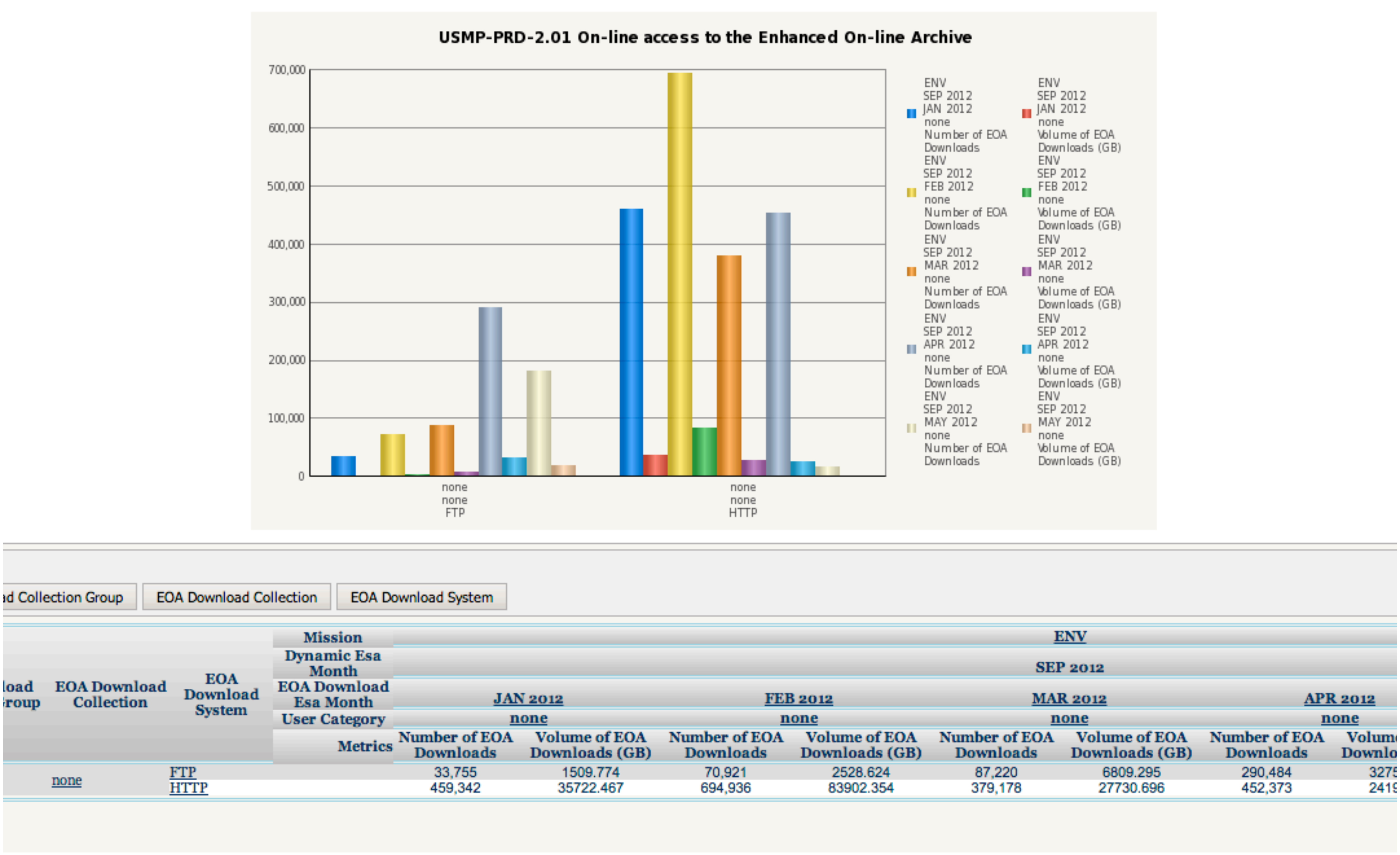
atitude +75°31' Longitude -64°46' Elevation -194 m Altitude 15000km

66M/508M


Application
UM-SSO Java Client Library
Other Library using Http protocol (e.g. Axis)
Client library core
Visualizer
HTML parser
Apache httpClient







USMP-PRD-2.01 On-line access to the Enhanced On-line Archive

700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
none none FTP
none none HTTP
ENV SEP 2012 JAN 2012 none Number of EOA Downloads
ENV SEP 2012 JAN 2012 none Volume of EOA Downloads (GB)
ENV SEP 2012 FEB 2012 none Number of EOA Downloads
ENV SEP 2012 FEB 2012 none Volume of EOA Downloads (GB)
ENV SEP 2012 MAR 2012 none Number of EOA Downloads
ENV SEP 2012 MAR 2012 none Volume of EOA Downloads (GB)
ENV SEP 2012 APR 2012 none Number of EOA Downloads
ENV SEP 2012 APR 2012 none Volume of EOA Downloads (GB)
ENV SEP 2012 MAY 2012 none Number of EOA Downloads
ENV SEP 2012 MAY 2012 none Volume of EOA Downloads (GB)
ad Collection Group
EOA Download Collection
EOA Download System

			Mission	ENV							
			Dynamic Esa Month	SEP 2012							
load roup	EOA Download Collection	EOA Download System	EOA Download Esa Month	JAN 2012		FEB 2012		MAR 2012		APR 2012	
			User Category	none		none		none		none	
			Metrics	Number of EOA Downloads	Volume of EOA Downloads (GB)	Number of EOA Downloads	Volume of EOA Downloads (GB)	Number of EOA Downloads	Volume of EOA Downloads (GB)	Number of EOA Downloads	Volum Downlo
	none	FTP		33,755	1509.774	70,921	2528.624	87,220	6809.295	290,484	3275
		HTTP		459,342	35722.467	694,936	83902.354	379,178	27730.696	452,373	2419

EO Statistics