



CONTRACT NUMBER 508830

DEISA
**DISTRIBUTED EUROPEAN INFRASTRUCTURE FOR
SUPERCOMPUTING APPLICATIONS**

European Community Sixth Framework Programme
RESEARCH INFRASTRUCTURES
Integrated Infrastructure Initiative

SA5 third year report

Deliverable ID: DEISA-DSA5-3.2
Due date : April 30, 2007
Actual delivery date: May 25, 2007
Lead contractor for this deliverable: SARA, Netherlands

Project start date : May 1st, 2004
Duration: 4 years

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of Content

Table of Content.....	1
1. Introduction.....	2
1.1 Executive Summary.....	2
1.2 References and Applicable Documents	2
1.3 Document Amendment Procedure	2
1.4 List of Acronyms and Abbreviations	2
2. Developments for the security infrastructure	4
2.1 Introduction.....	4
2.2 User Administration	4
2.2.1 Introduction.....	4
2.2.2 Portal users	4
2.2.1.1 deisaGenericAccount.....	5
2.2.1.2 deisaPortalProject.....	5
2.2.1.3 deisaPortalUser	6
2.2.1.4 Use of information about portal users.....	6
2.2.3 Project administrators.....	6
2.3 Accounting.....	7
2.3.1 Introduction.....	7
2.3.2 Access to accounting data.....	8
2.3.1.1 WSRF access	8
2.3.1.2 Web server access	8
2.3.1.3 Client tools	9
2.4 Conclusions	11
3. Appendices	12
3.1 DEISA LDAP schema.....	12

1. Introduction

1.1 Executive Summary

The SA5 activity is responsible for the implementation and support of AAA (Authentication, Authorisation, and Accounting) facilities and for the implementation and maintenance of procedures for the operational security. The most important technical developments by this activity in the third project year are described in this document.

For the user administration facilities, enabling the authentication and authorisation services of DEISA, several enhancements have been added. First of all the registration of portal users, needed by the eSA3 activity which is setting up a portal service, has been made possible by extending the LDAP schema defined for the DEISA User Administration System (UAS). Secondly, the registration of supervisors of the application projects, e.g. the DECI projects, has also been made possible by the extension of the LDAP schema. The information about the supervisors is used for authorization purposes, both for granting new users to be registered as belonging to a DEISA project and for authorized access to accounting data for the project. These enhancements are described in section 2.2 **Erreur ! Source du renvoi introuvable.**

Most of the effort was this year put in the development and deployment of accounting tools for DEISA. The architecture for the accounting facilities is described in another deliverable, DSA5-3.1 "Accounting facilities for DEISA", published in November 2006. Here the most recent developments are presented, the further development of access facilities for the accounting data. The result of these developments is that now users and administrators (both from sites and DEISA projects) can access the accounting data for which they are authorized. This is discussed in section 2.3.

1.2 References and Applicable Documents

- [1] <http://www.deisa.org>
- [2] DEISA deliverable DSA5-3.1 Accounting facilities for DEISA
- [3] DSA5-2.1 User Administration in the DEISA Environment- version 2.2
- [4] Accounting Facilities in the European Supercomputing Grid DEISA - http://www.ges2007.de/fileadmin/papers/jreetz/GES_paper105.pdf

1.3 Document Amendment Procedure

1.4 List of Acronyms and Abbreviations

DART	DEISA Accounting Report Tool
GTK4	Globus Toolkit version 4
JKS	Java Key Store, a repository for X.509 certificates
LDAP	Lightweight Directory Access Protocol
MDS	Monitoring and Discovery System, a Globus Toolkit service
POSIX	The Portable Operating System Interface
UAS	User Administration System
UNICORE	UNiform Interface to Computing Resources

2. Developments for the security infrastructure

2.1 Introduction

The SA5 activity is responsible for the implementation and support of AAA (Authentication, Authorisation and Accounting) facilities and for the implementation and maintenance of procedures for the operational security, such as an acceptable use policy for users. The status of these facilities and the achievements for the third project year are given in the general management report. Here we give technical details for the most important developments within the security activity. We describe the changes in the user administration system (UAS), the facility which enables the authentication and authorisation services within DEISA. And we describe the developments on the accounting facilities which have taken place since the publication of the deliverable of November 2006 describing the architecture of the accounting facilities for DEISA [2].

2.2 User Administration

2.2.1 Introduction

The DEISA user administration system (UAS) is responsible for the registration of DEISA users and contains attributes which are needed to enable other DEISA specific services. The system enables the creation of user accounts at sites, the distribution of information from the X.509 certificates for the PKI based authorisation services, and the distribution of information needed for the generation of usage records. In addition the repository gives general information about DEISA users. Details of the system are described in the document "User Administration in the DEISA Environment- version 2.2"

In the third project year several enhancements have been added and these are presented here.

2.2.2 Portal users

In June 2006 with the start of eDEISA, an expansion of the DEISA activity [1], a portal working group started work on the introduction of a portal facility. Through discussions between SA5 and the portal working group, several decisions were made about the implementation of the registration of the users of these portal facilities. It was decided that jobs submitted through the portal will run under a common account for each portal application. These portal accounts are registered as standard DEISA accounts. They can be identified as a portal account because they are registered as members of the specific portal project name which is defined in the UAS. Because a common account is used for all portal users using the same application the portal facility does not need root permissions for switching between different user ids at DEISA sites.

The portal users are registered by the site running the portal server. However other sites also want to have access to information about these users because of local policies. DEISA sites want to be able to track the end user which is behind the job that is running under the common portal account. It was decided to add the needed information about the portal users to the UAS.

Portal users don't need user accounts or login credentials at the DEISA sites. The LDAP schema in use for registering DEISA users however defines the login name and uid as a mandatory attribute. If portal users were registered in the same way as normal DEISA users then additional information would be needed to indicate that no

login facilities would have to be created for these users. This was not regarded as a very transparent way of registering portal users and it was decided to add a separate branch in the LDAP schema for the registration of portal users.

Two new object classes, one for the registration of portal projects and the other for the registration of portal users, and several new attribute definitions were added to the DEISA LDAP schema. The complete DEISA LDAP schema is given in Appendix 3.1.

The use of these definitions will be illustrated by the following examples.

2.2.2.1 *deisaGenericAccount*

Before jobs can be run for a portal application an account must be created. This is a standard DEISA user account, however not associated with a real end user but with the portal server. So the LDAP entry looks a little different than one for a standard user, but the important result is that the specified uid and gid are created at all sites. An entry for an account that can be referenced as `deisaGenericAccount` will look like:

```

dn: uid=idr001ip,ou=People,ou=idris.fr,ou=ua,dc=deisa,dc=org
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
objectClass: deisaUser
uid: idr001ip
givenName: eSA3 portal Generic Account
ou: IDRIS
uidNumber: 399999
gidNumber: 399999
gecos: eSA3 Portal Generic Account
seeAlso: ou=IDRIS,ou=Organisation,ou=idris.fr,dc=deisa,dc=org
cn: eSA3 portal Generic Account
sn: eSA3 portal Generic Account
loginShell: /bin/bash
homeDirectory: GPFS
telephoneNumber: +33 1 69 35 84 38
deisaNationality: FR
deisaRegistrar: Nicole Lizambert
deisaDeactivated: FALSE
deisaScienceField: Life Sciences
title: Mr.
mail: Vincent.Ribaillier@idris.fr
shadowExpire: 1

```

As part of the registration this generic account must also be registered as a member of a DEISA project. For this purpose a project "portal-generic-accounts" is defined and `idr001ip` is registered as a member.

2.2.2.2 *deisaPortalProject*

The `deisaPortalProject` object class is used to register a specific portal application (portal project) and the portal users which can use this application. An example is given here:

```
dn: deisaPortalProjectId=portal-000001,ou=PortalServer,ou=idris.fr,ou=ua,dc=deisa,dc=org
objectClass: deisaPortalProject
deisaPortalProjectId: portal-000001
deisaReference: GENOPLUS
deisaGenericAccount: idr00lip
deisaPortalMember: portal-user1
deisaPortalMember: portal-user2
```

The deisaPortalMembers are the portal users which are registered using the deisaPortalUser object class.

2.2.2.3 *deisaPortalUser*

For each user which can make use of one or more portal applications, an entry must be given using the deisaPortalUser object class and some standard defined object classes. An example is given below:

```
dn: deisaPortalUserId=portal-user1,ou=PortalUser,ou=idris.fr,ou=ua,dc=deisa,dc=org
objectClass: deisaPortalUser
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: John Martin
title: Mr.
givenName: John
sn: Martin
telephoneNumber: +33 1 69 35 84 38
mail: john.martin@cnrs.fr
ou: IDRIS
postalAddress: IDRIS, Batiment 506, BP167, 91403 ORSAY, FRANCE
deisaPortalUserId: portal-user1
deisaNationality: FR
deisaRegistrar: Nicole Lizambert
deisaDeactivated: FALSE
deisaSubjectDN: CN=John Martin,OU=LAB,O=CNRS,C=FR,O=GRIDFR
```

2.2.2.4 *Use of information about portal users*

The deisaPortalProjectId and the deisaPortalUserId will be specified for jobs which are submitted by the portal server. With this information other sites can identify the user and the application for which the job has run and more details can be retrieved from the UAS. This information will also be used for the creation of usage records. The portal server will be able to collect the usage information using the DEISA accounting tools and with this information the server can control the usage by the different portal applications and individual portal users.

2.2.3 *Project administrators*

Recently it was decided to add the person(s) responsible for a DEISA project (e.g. DECI projects) to the UAS. This will be implemented early in the fourth project year. This information will support the authorisation process for users that must be added as project members.

To enable the registration of the project administrators a new object class `deisaProject` is defined which extends the information that is given about a DEISA project:

```
objectclass ( 1.3.6.1.4.1.20846.101.4
  NAME 'deisaProject'
  DESC 'DEISA Project'
  SUP top
  AUXILIARY
  MAY ( deisaScienceField $ deisaProjectSupervisor )
)
```

The `deisaProjectSupervisor` is the new attribute defined to specify the project administrator. There can be more than one supervisor registered. At the same time it was decided to move the existing attribute `deisaSciencefield` from the user registration to the project registration as this is more appropriate. The definition of the `deisaProjectSupervisor` attribute is given by:

```
attributetype ( 1.3.6.1.4.1.20846.101.1.12
  NAME 'deisaProjectSupervisor'
  DESC 'id of Project Investigator'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
)
```

An example of the addition of a project entry with the extensions given above will now look like:

```
dn: cn=example-project,ou=Project,ou=sara.nl,ou=ua,dc=deisa,dc=org
objectClass: posixGroup
objectClass: deisaProject
objectClass: top
cn: example-project
gidNumber: 90000
memberUid: sar00001
deisaScienceField: example
deisaProjectSupervisor: sar00004
```

In this example both a new member and a new supervisor are specified. Both these attributes are not mandatory. Supervisors are identified by their uid as specified by their user registration. It is assumed that supervisors will be registered in the UAS. More than one supervisor can be specified.

2.3 Accounting

2.3.1 Introduction

The architecture of the accounting facilities for DEISA is described in the deliverable DSA5-3.1, published in November 2006 [2]. An important property of the architecture is the distributed set up of the services as is shown in Figure 1. Each site has a local database which is filled with DEISA specific usage records from jobs which have run

locally. Other sites and persons can retrieve this information with authorisation based on their role. An administrator of site A can access all remote records for users which are registered by site A, the site accounting role and a project administrator can access all records belonging to that project, the project accounting role. And of course users will be able to access all the records belonging to the jobs they have run.

We will present more details about the access tools which have been developed.

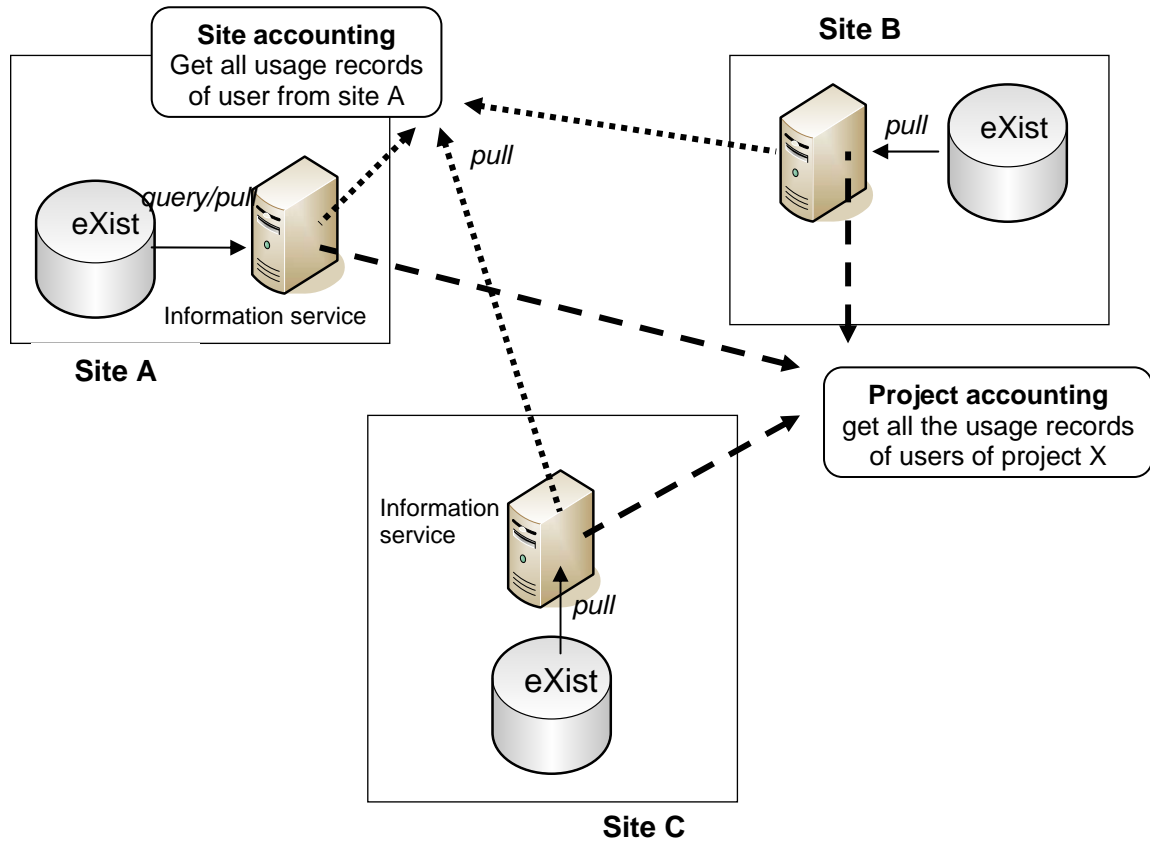


Figure 1 Architecture of accounting services

2.3.2 Access to accounting data

2.3.2.1 WSRF access

A WSRF (Web Services Resource Framework) based tool has been developed that can retrieve remotely the accounting data. The tool makes use of the GTK4 provided information service which is deployed by DEISA sites. The information service will check the authorisation and will provide the requested accounting information to a remote client. The testing of this facility takes more time than expected and it was decided to implement first access facilities based on web servers that will run a CGI script.

2.3.2.2 Web server access

For the web server access each site has to set up a web server and enable a CGI script which will handle incoming requests. Authorisation for access to the data is implemented using a file, acct-grid-mapfile, which maps the Subject Names from X.509 certificates to the roles that the owner of the certificate has (roles can be user, site administrator, project administrator and DEISA supervisor). The entries in this file look like

"/O=dutchgrid/O=users/O=sara/CN=First Last" site-SARA
"/O=dutchgrid/O=users/O=sara/CN=First Last" uid
"/O=dutchgrid/O=users/O=sara/CN=First Last" project-example
"/O=dutchgrid/O=users/O=sara/CN=First Last" site-all

The first entry grants access on a site for all SARA related records for the owner of the certificate with the Subject Name "/O=dutchgrid/O=users/O=sara/CN=First Last", the second entry for all records related to the DEISA user id uid, and the third entry grants access to all records for the example project. The last entry could be for a DEISA supervisor. It grants access to all records available on the site.

These entries can be generated automatically for the user and site entries from the information in the UAS. The Subject Name is part of the user registration and is associated with the DEISA uid. Site administrators can be identified as members of the DEISA staff project and the site is given by the organization they belong to. The project administrator entries can also be generated automatically after the new attribute deisaProjectSupervisor, which is described in section 2.2.3, is introduced in the UAS,

2.3.2.3 *Client tools*

Tools have been developed for the generation of reports based on the data retrieved from the accounting repositories. With these tools it is possible to select the data that the user is interested in and summary reports will be generated based on the authorization as determined by the role of the user.

As a fast available solution, a web based client, SimpleDART, was developed with Perl with which a user can display the information to which access is authorized based on the role of the user. This tool uses the web server and CGI script facilities described in section 2.3.2.2.

The SimpleDART tool is a command-line tool which can for example be used as an automated UNIX cron-job.

However the tool doesn't have an easy to use graphical interface and it also lacks the possibility to interface to the WSRF based access facilities. It was decided to develop an improved tool, DART (DEISA Accounting Reporting Tool), based on Java. With this tool both access facilities, WSRF and web server based, can be used.

The DART tool is a Java webstart application, which means that it can be started from a browser, and updates can easily be maintained centrally, but it has the power of a full featured Java application.

The DART tool is still under development, but a beta version is already deployed. The tool can be run on every client system, provided that a JKS is available with the necessary X.509 certificates loaded. For most users this will already be the case as the JKS is also needed for using the UNICORE client, which is the standard tool to access the DEISA infrastructure.

After the DART application is loaded the user has to provide on the first window the JKS location. The default location of the JKS as used by UNICORE will be displayed if found. In the next window, shown in Figure 2., the user can select the role, the time interval for which data is requested, and from which sites data will be requested.

Role selection

DEISA user sar00005

DEISA project

DEISA site SARA

DEISA supervisor

Date selection

Starttime (YYYY-MM-DD): 2007-05-01

Endtime (YYYY-MM-DD): 2007-05-15

Site selection

SARA LRZ RZG

FZJ CINECA IDRIS

CSC

BACK NEXT

INFO: Dart Revision 0.7 (Java Version 1.5.0_07)

Figure 2 DART selection window

Startdate: 2007-01-01 Enddate: 2007-05-15 New Report Save Settings Export

Total | May 2007

Project	User	Site / Machine	Jobs	Walltime [s]	Cpu Duration (norm) [h]	Cpu Duration [h]	Cpu Time (norm) [h]	Cpu Time [h]
ALL	ALL	SUMMARY	2	127	0,00		0,03	
staff	ALL	SUMMARY	2	127	0,00		0,03	
	Jules Wolfrat (sar00005)	RZG / RZG SP4	1	64	0,00	0,00	0,01	0,02
	Jules Wolfrat (sar00005)	SARA / ASTER	1	63	0,00	0,00	0,02	0,02

INFO: Dart Revision 0.7 (Java Version 1.5.0_07)

ERROR: Error while connecting https://norma4.idris.fr/cgi-bin/accounting
Connection timed out: connect

Figure 3 DART output window

With the “next” button the generation of the report is started. An example of an end user report is given in Figure 3. The output displays number of jobs run and several

timings for the jobs. The walltime is the wall clock time of the job in seconds, the CPU duration is the wall clock time multiplied with all CPUs which have been reserved for the job, and the CPU time is the total real CPU time as used by the job. For these two latter values both normalized as well as the original values are displayed. The normalized values are based on a conversion of the original values to values for a reference system. Currently the reference system is a IBM Power4 CPU running at 1.7GHz. The conversion factors are based on the results obtained by a benchmark suite of applications and they are maintained in a separate file in XML format. Changes in the conversion factors don't affect the original data, which makes it easy to apply changes.

At the bottom of the screen error messages are displayed, in this case about one of the accounting servers which could not be contacted.

2.4 Conclusions

The UAS has proven to be easily extendable with new functionality. Users of the portal facilities can now be registered using the new LDAP schema taken in production this year and this information is used for tracking the usage of DEISA resources by these users. Also the registration of supervisors or administrators of DEISA projects can be registered with the new schema and this enables authorization facilities for users having this role.

With the availability of the DART tool a complete set of accounting tools is available for the DEISA community. End users as well as site administrators and project administrators can retrieve the data in which they are interested. With DART the data can also be imported to a local file, which then can be used for further processing of the data. For instance the data can be exported to a local repository by site administrators.

The accounting facilities developed and implemented for DEISA have also been published in a paper [4].

3. Appendices

3.1 DEISA LDAP schema

```
# DEISA X.500 Schema
#
# This schema defines several object classes and attributes for DEISA
# The DeisaUser objectclass contains the following attributes:
#
# - deisaNationality      Nationality (e.g. NL)
# - deisaRegistrar       Full name of the administrator that
registered the user
# - deisaScienceField     Scientific field in which the user
operates
# - deisaDeactivated      True if account is deactivated
# - deisaDeactReason      Reason of account deactivation
# - deisaSubjectDN       Subject DN from user certificate
# - deisaUser             DEISA user
#
# PortalProject objectclass:
# - deisaPortalproject    DEISA Portal Project
# - deisaPortalProjectId  id of DEISA Portal Project
# -deisaGenericAccount    DEISA UNIX Generic Account mapped to
a deisaPortalProject
# - deisaPortalMember     deisaPortalUser member of a
deisaPortalProject
# - deisaReference        Acronym of a deisaPortalProject
#
# PortalUser objectclass
# - deisaPortalUser       DEISA PortalUser
# - deisaPortalUserID     id of DEISA Portal User
```

```
attributetype ( 1.3.6.1.4.1.20846.101.1.1
  NAME 'deisaNationality'
  DESC 'Nationality of user (see ISO 3166)'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.11
)
```

```
attributetype ( 1.3.6.1.4.1.20846.101.1.2
  NAME 'deisaRegistrar'
  DESC 'Registrar of user (full name)'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
  SINGLE-VALUE
)
```

```
attributetype ( 1.3.6.1.4.1.20846.101.1.3
  NAME 'deisaScienceField'
  DESC 'Scientific Field'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
  SINGLE-VALUE
)
```

```
attributetype ( 1.3.6.1.4.1.20846.101.1.4
  NAME 'deisaDeactivated'
```

```
DESC 'Account deactivated'
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE
)

attributetype ( 1.3.6.1.4.1.20846.101.1.5
  NAME 'deisaDeactReason'
  DESC 'Reason of account deactivation'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
  SINGLE-VALUE
)

attributetype ( 1.3.6.1.4.1.20846.101.1.6
  NAME 'deisaSubjectDN'
  DESC 'Subject DN from user certificate'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE
)

attributetype ( 1.3.6.1.4.1.20846.101.1.7
  NAME 'deisaPortalProjectID'
  DESC 'id of a portal project'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
  SINGLE-VALUE
)

attributetype ( 1.3.6.1.4.1.20846.101.1.8
  NAME 'deisaPortalUserId'
  DESC 'id of user of a portal project'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
  SINGLE-VALUE
)

attributetype ( 1.3.6.1.4.1.20846.101.1.9
  NAME 'deisaGenericAccount'
  DESC 'DEISA UNIX Generic Account mapped to a deisaPortalProject'
  EQUALITY caseExactIA5Match
  SUBSTR caseExactIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE
)

attributetype ( 1.3.6.1.4.1.20846.101.1.10
  NAME 'deisaPortalMember'
  DESC 'deisaPortalUser member of a deisaPortalProject'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
)
```

```
attributetype ( 1.3.6.1.4.1.20846.101.1.11
  NAME 'deisaReference'
  DESC 'Acronym of a deisaPortalProject'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
  SINGLE-VALUE
)

objectclass ( 1.3.6.1.4.1.20846.101.1
  NAME 'deisaUser'
  DESC 'DEISA user'
  SUP top
  AUXILIARY
  MUST ( deisaNationality $ deisaRegistrar $ deisaDeactivated )
  MAY ( deisaDeactReason $ deisaSubjectDN $ deisaScienceField )
)

objectclass ( 1.3.6.1.4.1.20846.101.2
  NAME 'deisaPortalUser'
  DESC 'DEISA Portal User'
  SUP top
  AUXILIARY
  MUST ( deisaPortalUserID $ deisaNationality $ deisaRegistrar $
  deisaDeactivated )
  MAY ( deisaDeactReason $ deisaSubjectDN )
)

objectclass ( 1.3.6.1.4.1.20846.101.3
  NAME 'deisaPortalProject'
  DESC 'DEISA Portal Project'
  SUP top
  STRUCTURAL
  MUST ( deisaPortalProjectId $ deisaGenericAccount )
  MAY ( deisaReference $ deisaPortalMember )
)
```