EGI-InSPIRE

UMD Security Capabilities Quality Criteria v1.3

Document identifier:	EGI-SECURITY-QC-V1.3.doc
Date:	**09/02/2011**
Document Link:	https://documents.egi.eu/document/240

Abstract

This document describes the UMD Security Capabilities Quality Criteria.

Copyright notice

Document Log

Issue	Date	Comment	Author/Partner
1.0	15/11/2010	First draft	Enol Fernández
1.1	19/11/2010	Added criteria for more capabilities.	Enol Fernández
1.2	17/01/2011	Completed criteria for Credential Management, User Management and Authorisation.	Enol Fernández
1.3	09/02/2011	Added delegation criteria, Authorisation review	Enol Fernández

TABLE OF CONTENTS

1 AUTHENTICATION

An authentication token that is strongly bound to an individual must be applied consistently across the software used within the production infrastructure. The authentication system must be capable of supporting a delegation model.

1.1 Authentication Interface

X.509 Certificate support	
ID	**AUTHN_ IFACE_1**
Mandatory	
Applicability	Authentication Appliances
Related Requirements	None

Description The primary authentication token within the infrastructure is the X.509 certificate and its proxy derivatives. The certificates and any proxy schemes must follow specifications that are fully integrated into the https protocol (as opposed to the httpg protocol).
Input from TP Testsuite for the use of X.509 proxy support for authentication If the component exposes a WebService that requires authentication, it must use the X.509 certificates/proxies with the https protocol. The exact content of the testsuite depends on the component interface.
Pass/Fail Criteria X.509 proxies are accepted for authentication. WebServices use https.
Related Information
History

SAML assertions support	
ID	**AUTHN_ IFACE_2**
Not Mandatory	
Applicability	Authentication Appliances
Related Requirements	None

Description Components that perform authentication may use SAML 2.0 interface.
Input from TP Testsuite for the use of SAML 2.0 support for authentication. The exact contents of the testsuite depend on the component interface.
Pass/Fail Criteria Pass if the SAML2.0 authentication is supported.
Related Information
History

1.2 Delegation Model

Authentication Appliances that implement delegation must implement one of the two interfaces proposed in the following criteria.

GridSite Delegation	
ID	**AUTHN_ DELEG_1**
Mandatory	
Applicability	Authentication Appliances that require delegation with GridSite
Related Requirements	None

Description Components that require delegation of credentials must provide delegation using the GridSite delegation interface.
Input from TP Testsuite for the GridSite Delegation that includes all functions in the WSDL. Test erroneous input and generation of error messages.
Pass/Fail Criteria Pass if the GridSite delegation protocol is supported and properly tested.
Related Information GridSite Delegation Protocol.
History

Globus 4 Delegation	
ID	**AUTHN_ DELEG_2**
Mandatory	
Applicability	Authentication Appliances that require delegation with Globus
Related Requirements	None

Description Components that require delegation of credentials must provide delegation using the Globus delegation interface.
Input from TP Testsuite for the Globus Delegation that includes all functions in the WSDL. Test erroneous input and generation of error messages.
Pass/Fail Criteria Pass if the Globus delegation protocol is supported and properly tested.
Related Information Globus Delegation Protocol.
History

1.3 CAs root certificates Distribution

These QC deal with the distribution of the EuGridPMA [R 5] root certificates.

CA checksum	
ID	**AUTHN_CA _1**
Mandatory	
Applicability	CA Distribution
Related Requirements	None

Description

Test the correctness of each of the CAs certificates included in the distribution.

Input from TP

Checksum test of each of the root certificates distributed.

Test 1

Pre-condition	None
Test	Test checksum of the CA certificates.
Expected Outcome	All checksums are correct.

Pass/Fail Criteria

Pass if the test is provided and passes.

Related Information

History

CA valid dates	
ID	**AUTHN_CA _2**
Mandatory	
Applicability	CA Distribution
Related Requirements	None

Description

Test that the dates of the CA certificates are valid for the current date.

Input from TP

Data validity test of each of the root certificates distributed.

Test 1

Pre-condition	None
Test	Check the current date is in the range of the valid dates of the certificate.
Expected Outcome	All dates are valid.

Example test code

```
#!/bin/sh
check_dates() {
    certfile=$1
    start=`openssl  x509  -in  $certfile  -noout  -startdate  |  cut  -f2  -
d"="`
    if [ $? -ne 0 ] ; then
        echo "Error while processing $certfile"
        return 1
    fi
    now=`date +%s`
    start_sec=`date +%s -d"$start"`
    if [ $now -lt $start_sec ] ; then
        echo "$start is before now in $certfile!"
        return 1
    fi
    end=`openssl x509 -in $certfile -noout -enddate | cut -f2 -d"="`
    if [ $? -ne 0 ] ; then
        echo "Error while processing $certfile"
        return 1
    fi
    end_sec=`date +%s -d"$end"`
    if [ $end_sec -lt $now ] ; then
        echo "$end is after now in $certfile!"
        return 1
    fi
    return 0
}

ret=0
```

```
for cert in /etc/grid-security/certificates/*.0; do
    check_dates $cert
    if [ $? -ne 0 ] ; then
        pkg=`rpm -qf $cert`
        echo "Package $pkg is not valid"
        ret=1
    fi
done

exit $ret
```

Pass/Fail Criteria

Pass if the test is provided and passes.

Related Information

History

CA CRL check	
ID	**AUTHN_CA _3**
Mandatory	
Applicability	CA Distribution
Related Requirements	None

Description

The CRL of the CAs must be available for download and must be valid.

Input from TP

Test that the CRL of the CA is available for download and it's valid.

Test 1

Pre-condition List of URLs for each CRL is available.

Test Download CRL and load it with openssl.

Expected Outcome All CRLs can be downloaded and load correctly with openssl.

Example test code

```
#!/bin/sh

check_crl() {
    url_file=$1
    url=`cat $url_file`
    crl=`mktemp`
    wget -q $url -O $crl
    if [ $? -ne 0 ] ; then
        echo "Unable to download crl from $url"
        rm  $crl
        return 1
    fi
    openssl crl -in $crl -noout &> /dev/null
    if [ $? -ne 0 ] ; then
        # try in other format
        openssl crl -inform der -in $crl -noout &> /dev/null
        if [ $? -ne 0 ] ; then
            echo "Unable to load crl"
            rm $crl
            return 1
        fi
    fi
    rm $crl
    return 0
}

ret=0
for cert in /etc/grid-security/certificates/*.crl_url; do
    check_crl $cert
    if [ $? -ne 0 ] ; then
        pkg=`rpm -qf $cert`
        echo "Package $pkg is not valid"
        ret=1
    fi
done

exit $ret
```

Pass/Fail Criteria

Pass if the test is provided and passes.

Related Information

History

2 ATTRIBUTE AUTHORITY

Resources within the production infrastructure are made available to controlled collaborations of users represented in the infrastructure through Virtual Organisations (VOs). Access to a VO is governed by a VO manager who is responsible for managing the addition and removal of users and the assignment of users to groups and roles within the VO.

2.1 Attribute Authority Interface

An interface is needed to issue proxy certificates relating to the roles and groups that an individual has within a VO. The corresponding attributes may also be delivered back to the client through SAML assertions.

Proxy Issue	
ID	**ATTAUTH_ IFACE_1**
Mandatory	
Applicability	Attribute Authority Appliances
Related Requirements	None

Description Users must be able to get proxies with VO related information.	
Input from TP Test the creation of proxies for different users, roles and groups. Test for error situations (not registered user, unknown VO, non existing role/group, unreachable server)	
Test 1	
Pre-condition	Valid user certificate, user registered in VO
Test	Create proxy for user in the given VO.
Expected Outcome	Valid proxy created.
Test 2	
Pre-condition	Valid user certificate, user registered in VO, user in a given group/role
Test	Create proxy for user in the given VO and group/role
Expected Outcome	Valid proxy created with correct group/role information.
Test 3	
Pre-condition	Valid user certificate, user not registered in VO
Test	Create proxy for user in the given VO.
Expected Outcome	Issue a error message stating that the user is unknown to the VO.
Pass/Fail Criteria Pass if the testsuite is provided and passes.	

Related Information
History

Proxy Information	
ID	**ATTAUTH_ IFACE_2**
Mandatory	
Applicability	Attribute Authority Appliances
Related Requirements	None

Description Users must be able to get information about their proxies.	
Input from TP Test the tool for getting proxy information.	
Test 1	
Pre-condition	Valid user proxy
Test	Get information from proxy.
Expected Outcome	Return proxy information.
Test 2	
Pre-condition	Nonexistent user proxy
Test	Get information from proxy
Expected Outcome	No information returned and error message issued.
Pass/Fail Criteria Pass if the testsuite is provided and passes.	
Related Information	
History	

Proxy Destroy	
ID	**ATTAUTH_ IFACE_3**
Mandatory	
Applicability	Attribute Authority Appliances
Related Requirements	None

Description

Users must be able to destroy a previously created proxy

Input from TP

Test the proxy destroy.

Test 1

Pre-condition	Valid user proxy
Test	Destroy user proxy.
Expected Outcome	Proxy is destroyed.

Pass/Fail Criteria

Pass if the testsuite is provided and passes.

Related Information

History

2.2 VO management

VO Creation	
ID	**ATTAUTH_ MGMT_1**
Mandatory	
Applicability	Attribute Authority Appliances
Related Requirements	None

Description	
The service administrator must be able to create new VOs in the service.	
Input from TP	
Test the creation of VOs, test for incorrect input. Test for all the supported databases.	
Test 1	
Pre-condition	Administrator privileges in VO service. Configured service.
Test	Create a new VO
Expected Outcome	New database is created and initialized.
Test 2	
Pre-condition	Administrator privileges in VO service. Configured service. Existent VO name
Test	Create a VO with already existent name.
Expected Outcome	No action performed, warning message issued.
Pass/Fail Criteria	
Pass if the testsuite is provided and passes for all the supported databases.	
Related Information	
History	

VO Administrators	
ID	**ATTAUTH_ MGMT_2**
Mandatory	
Applicability	Attribute Authority Appliances
Related Requirements	None

Description

The service administrator must be able to define who are the VO administrator

Input from TP

Test adding VO administrators, test for incorrect input.

Test 1

Pre-condition	Administrator privileges in VO service. Configured service. User certificate of new admin.
Test	Define VO administrator with user certificate.
Expected Outcome	User is added as VO administrator.

Test 2

Pre-condition	Administrator privileges in VO service. Configured service. User certificate of already existent admin.
Test	Define VO administrator with user certificate.
Expected Outcome	No action performed, warning message is issued.

Test 3

Pre-condition	Administrator privileges in VO service. Configured service. User certificate of new admin.
Test	Define VO administrator with user certificate for a nonexistent VO.
Expected Outcome	Error message stating that the VO is not existent.

Pass/Fail Criteria

Pass if the testsuite is provided and passes.

Related Information

History

VO Role/Group/Attribute Management	
ID	**ATTAUTH_ MGMT_3**
Mandatory	
Applicability	Attribute Authority Appliances
Related Requirements	None

Description Authorized users must be able to define roles, groups and attributed and manage the users with those assigned.	
Input from TP Test creation of roles, groups, attributes and the assignment and de-assignment of users to those.	
Test 1	
Pre-condition	Authorized user to manage VO role/group/attribute. Role/Group/Attribute name.
Test	Create a new role/group/attribute in the VO.
Expected Outcome	New role/group/attribute is created in the VO
Test 2	
Pre-condition	Authorized user to manage VO role/group/attribute. Already existent Role/Group/Attribute name.
Test	Create role/group/attribute in the VO.
Expected Outcome	No action performed, issue warning message about the role/group/attribute already existing.
Test 3	
Pre-condition	Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name.
Test	Create a new role/group/attribute in the VO.
Expected Outcome	No action performed, issue error message.
Test 4	
Pre-condition	Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. VO User to add
Test	Assign role/group/attribute to user.
Expected Outcome	User has the role/group/attribute assigned.
Test 5	
Pre-condition	Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. VO User to add
Test	Assign role/group/attribute to user.

Expected Outcome	No action performed, issue error message.
Test 6	
Pre-condition	Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign
Test	De-assign role/group/attribute to user.
Expected Outcome	Role/Group/Attribute is de-assigned.
Test 7	
Pre-condition	Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign without assigned role/group/attribute
Test	De-assign role/group/attribute to user.
Expected Outcome	No action performed, warning message issued.
Test 8	
Pre-condition	Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign
Test	De-assign role/group/attribute to user.
Expected Outcome	No action performed, issue error message.
Pass/Fail Criteria Pass if the testsuite is provided and passes for roles, groups and attributes.	
Related Information	
History	

VO User Management	
ID	**ATTAUTH_ MGMT_4**
Mandatory	
Applicability	Attribute Authority Appliances
Related Requirements	None

Description

Authorized users must be able to add and remove users to the VO

Input from TP

Test the adding/removing users to the VO.

Test 1

Pre-condition	Authorized user to manage VO users. User to add to VO.
Test	Add user to VO
Expected Outcome	User is correctly added to the VO.

Test 2

Pre-condition	Non-Authorized user to manage VO users. User to add to VO.
Test	Add user to VO
Expected Outcome	No action performed, issue error message.

Test 3

Pre-condition	Authorized user to manage VO users. User to add to VO that already belongs to the VO.
Test	Add user to VO
Expected Outcome	No action performed, issue a warning message.

Pass/Fail Criteria

Pass if the testsuite is provided and passes.

Related Information

History

ACL Management	
ID	**ATTAUTH_ MGMT_5**
Mandatory	
Applicability	Attribute Authority Appliances
Related Requirements	None

Description

Authorized users must be able to change the ACLs of the VO.

Input from TP

Test for changing ACLs of users of the VO.

Test 1

Pre-condition	Authorized user to manage ACLs.
Test	Change ACL for a given user.
Expected Outcome	ACL is correctly changed.

Test 2

Pre-condition	Non-Authorized user to manage ACLs.
Test	Change ACL for a given user.
Expected Outcome	No action performed, error message issued.

Pass/Fail Criteria

Pass if the testsuite is provided and passes for all the kind of ACLs:

- browse users of VO
- management of groups
- management of roles
- management of attributes
- management of ACL
- add/remove users

Related Information

History

2.3 VO Management Web Interface

VO list view	
ID	**ATTAUTH_ WEB_1**
Mandatory	
Applicability	Web Interface of Attribute Authority Appliances
Related Requirements	None

Description Users connecting to the web interface should be able to list the VOs handled by the server.	
Input from TP Provide a page with the list of VOs in the server.	
Test 1	
Pre-condition	VO Web server running
Test	Access VO list page.
Expected Outcome	Web page with a list of all VOs in supported by the server.
Pass/Fail Criteria Pass if the test is provided and passes.	
Related Information	
History	

VO Membership Request	
ID	**ATTAUTH_ WEB_2**
Mandatory	
Applicability	Web Interface of Attribute Authority Appliances
Related Requirements	None

Description

Users should be able to request membership to a VO from the web interface.

Input from TP

Provide a page for requesting VO membership and test its functionality. This page must ask for the following information:

- Full name
- Institution
- Contact details (phone, e-mail, address)

Once the information is entered, users receive an email to confirm the membership request. Once confirmed, VO Admins should receive a notification of the new request.

Test 1

Pre-condition	VO Web server running, valid credentials of user.
Test	User requests membership from VO.
Expected Outcome	User gets an email to confirm the membership request.

Test 2

Pre-condition	VO Web server running, valid credentials of user, membership confirmation link.
Test	User accesses the membership confirmation link.
Expected Outcome	VO admin(s) receive a notification of the new request.

Pass/Fail Criteria

Pass if the VO membership request page provides the requested functionality.

Related Information

History

VO Membership Authorisation	
ID	**ATTAUTH_ WEB_3**
Mandatory	
Applicability	Web Interface of Attribute Authority Appliances
Related Requirements	None

Description

Admins should be able to allow or deny pending membership request from the web interface.

Input from TP

Provide a page for listing pending membership requests and allowing or denying them.

Test 1

Pre-condition	VO Web server running, valid admin credentials, membership request.
Test	Admin accepts the membership request.
Expected Outcome	User is added to the VO. Notification email is sent to user.

Test 2

Pre-condition	VO Web server running, valid admin credentials, membership request.
Test	Admin rejects the membership request.
Expected Outcome	User is not added to the VO.

Pass/Fail Criteria

Pass if the test is provided and passes.

Related Information

History

VO Administration	
ID	**ATTAUTH_ WEB_4**
Mandatory	
Applicability	Web Interface of Attribute Authority Appliances
Related Requirements	None

Description

Authorized used should be able to manage VO groups, roles, attributes and ACLs from the web interface.

Input from TP

Provide pages for managing the groups, roles, attributes and ACLs of the VO. They must allow the creation of new items, assigning and removing users for those items, deleting items.

Test 1

Pre-condition	VO Web server running, valid credentials.
Test	Create new group/role/attribute using web interface.
Expected Outcome	The new group/role/attribute is created.

Test 2

Pre-condition	VO Web server running, valid credentials.
Test	Remove existing group/role/attribute using web interface.
Expected Outcome	The group/role/attribute is deleted.

Test 3

Pre-condition	VO Web server running, valid credentials.
Test	Assign group/role/attribute to user using web interface.
Expected Outcome	The group/role/attribute is assigned to user.

Test 4

Pre-condition	VO Web server running, valid credentials.
Test	Remove user from group/role/attribute using web interface.
Expected Outcome	User no longer has group/role/attribute assigned.

Pass/Fail Criteria

Pass if the VO management pages are provided with the expected functionality.

Related Information

History

VO Browse	
ID	**ATTAUTH_ WEB_5**
Mandatory	
Applicability	Web Interface of Attribute Authority Appliances
Related Requirements	None

Description Authorized used should be able to browse the VO members, groups, roles or attributes.	
Input from TP Provide pages for listing the VO members, groups, roles and attributes for a given VO.	
Test 1	
Pre-condition	VO Web server running, valid credentials.
Test	Browse VO members by groups/roles/attributes.
Expected Outcome	Web pages with list of users for groups/roles/attributes is delivered.
Pass/Fail Criteria Pass if the VO browsing pages are provided with the expected functionality.	
Related Information	
History	

3 AUTHORISATION

The implementation of access control policy – authorisation – needs to take place on many levels. Sites will wish to restrict access to particular VOs and individuals. Sites or VOs may wish to stop certain users accessing particular services. The infrastructure as a whole may need to ban particular users from the whole infrastructure. Policy Enforcement Points (PEPs) will be embedded into many components throughout the infrastructure and will use Policy Decision Points (PDPs) to drive access control decisions.

3.1 Policy Management

Policy Listing	
ID	**AUTHZ_ MGMT_1**
Mandatory	
Applicability	Authorisation Appliances with PAP.
Related Requirements	None

Description Administrators must be able to list the policies stored in the service.
Input from TP Test of policy listing
Test 1 **Pre-condition** Policy repository available. **Test** List policies **Expected Outcome** List of stored policies.
Pass/Fail Criteria Pass if the testsuite is provided and passes.
Related Information
History

Policy Repositories Management	
ID	**AUTHZ_ MGMT_2**
Mandatory	
Applicability	Authorisation Appliances with PAP.
Related Requirements	None

Description Administrators must be able to manage the remote Policy Repositories to be used by the service.	
Input from TP Test for the management of Policy Repositories that will be used in the service.	
Test 1	
Pre-condition	Remote policy repository available.
Test	Add remote policy repository.
Expected Outcome	Remote repository added, remote policies retrieved.
Test 2	
Pre-condition	Configured Remote policy repository.
Test	Remove remote policy repository.
Expected Outcome	Remote repository removed, policies no longer available.
Test 3	
Pre-condition	Configured Remote policy repository
Test	Update remote policies.
Expected Outcome	Remote policies retrieved.
Test 4	
Pre-condition	Enabled policy repository.
Test	Disable policy repository.
Expected Outcome	Policies from repository no longer used.
Test 5	
Pre-condition	Disabled policy repository.
Test	Enable policy repository.
Expected Outcome	Policies from repository used.
Test 6	
Pre-condition	Several policies repositories configured.

Test	Show policy repository order.
Expected Outcome	Policy repository order shown.
Test 7	
Pre-condition	Several policies repositories configured.
Test	Set policy repository order.
Expected Outcome	New policy repository is set.
Pass/Fail Criteria Pass if the testsuite is provided and passes.	
Related Information	
History	

3.2 Policy Definition

(un) Banning Policies	
ID	**AUTHZ_ PCYDEF_1**
Mandatory	
Applicability	Authorisation Appliances with PAP.
Related Requirements	None

Description Administrators must be able to define policies that ban users or FQANs.
Input from TP Test of banning for different user DNs and FQANs, test also restablishing already existing banning.
Test 1 **Pre-condition** Policy repository available. Banning policy for DN/FQAN not defined **Test** Define ban policy for DN/FQAN **Expected Outcome** Ban policy for DN/FQAN stored in policy repository.
Test 2 **Pre-condition** Policy repository available. Banning policy for DN/FQAN defined **Test** Unban policy for DN/FQAN **Expected Outcome** Ban policy for DN/FQAN no longer stored in policy repository.
Pass/Fail Criteria Pass if the testsuite is provided and passes for DNs and FQANs
Related Information
History

Policy Definition from file	
ID	**AUTHZ_ PCYDEF_2**
Mandatory	
Applicability	Authorisation Appliances with PAP.
Related Requirements	None

Description Administrators must be able to manage the policies in the service.	
Input from TP Test of policy definitions for different DNs and FQANs, test both *allow* and *deny* policies for different resources and actions.	
Test 1	
Pre-condition	Policy repository available. Policy file with policies.
Test	Add policies from file.
Expected Outcome	Policies from file now stored in repository.
Test 2	
Pre-condition	Policy repository available with a policy to update. Update description in policy file.
Test	Update policy from file.
Expected Outcome	Update policy stored in repository.
Test 3	
Pre-condition	Policy repository available with a policy to remove.
Test	Remove policy.
Expected Outcome	Policy no longer stored in repository.
Pass/Fail Criteria Pass if the testsuite is provided and passes for DNs and FQANs	
Related Information	
History	

Ban User/FQAN	
ID	**AUTHZ_ PCYDEF_3**
Mandatory	
Applicability	Authorisation Appliances without PAP.
Related Requirements	None

Description	
Administrators must be able to define policies that ban users or FQANs.	
Input from TP	
Test of banning for different user DNs and FQANs.	
Test 1	
Pre-condition	Configured system.
Test	Ban policy for DN/FQAN. Test access for DN/FQAN.
Expected Outcome	Ban policy is correctly enforced.
Test 2	
Pre-condition	Configured system. Banning policy for DN/FQAN defined
Test	Unban DN/FQAN. Test access for DN/FQAN.
Expected Outcome	DN/FQAN is allowed.
Pass/Fail Criteria	
Pass if the testsuite is provided and passes for DNs and FQANs	
Related Information	
History	

Access Policy Definition	
ID	**AUTHZ_ PCYDEF_4**
Mandatory	
Applicability	Authorisation Appliances without PAP.
Related Requirements	None

Description Administrators must be able to manage the policies in the service.	
Input from TP Test of policy definitions for different DNs and FQANs, test both *allow* and *deny* policies for different resources and actions.	
Test 1	
Pre-condition	Configured system.
Test	Allow DN/FQAN access into system. Test access fro DN/FQAN.
Expected Outcome	DN/FQAN is allowed in the system.
Test 2	
Pre-condition	Configured system.
Test	Deay DN/FQAN access into system. Test access fro DN/FQAN.
Expected Outcome	DN/FQAN is not allowed in the system.
Pass/Fail Criteria Pass if the testsuite is provided and passes for DNs and FQANs	
Related Information	
History	

3.3 Policy Decision Point

PDP API Testsuite	
ID	**AUTHZ_ PDP_1**
Mandatory	
Applicability	Authorisation Appliances with PDP.
Related Requirements	None

Description APIs and libraries are needed for the integration of PEPs into software and a defined interface for the PDP is needed to allow different PDPs to be deployed within the infrastructure. The API must provide support for contacting a PDP and get from it authorisation responses for a given user, service and action.	
Input from TP Testsuite of the complete API for accessing the PDP from clients. The testsuite must cover correct and erroneous input for the API, authorize and deny policies taking into account DNs, VOs, FQAN, and proxies.	
Test 1	
Pre-condition	Configured PEP and PDP.
Test	Complete testsuite of PDP API
Expected Outcome	Log of actions.
Pass/Fail Criteria Pass if the testsuite is provided and passes.	
Related Information	
History	

3.4 Policy Enforcement

Policy Enforcement	
ID	**AUTHZ_ PEP_1**
Mandatory	
Applicability	Authorisation Appliances.
Related Requirements	None

Description The defined policies in the authorisation capability must be enforced when needed.	
Input from TP Testsuite for the policy enforcement, test for user certificate with and without VOMS extensions and with policies expressed with DNs and FQANs.	
Test 1	
Pre-condition	Configured system. User certificate chain of user allowed to perform action.
Test	Test if the user can perform action
Expected Outcome	Permission is granted to user.
Test 2	
Pre-condition	Configured system. User certificate chain of user NOT allowed to perform action.
Test	Test if the user can perform action
Expected Outcome	Permission is NOT granted to user.
Pass/Fail Criteria Pass if the testsuite is provided and passes.	
Related Information	
History	

User Mapping with gridmap	
ID	**AUTHZ_ PEP_2**
Mandatory	
Applicability	Authorisation Appliances.
Related Requirements	None

Description

The authorisation capability should provide mapping of authorized users to local accounts with the gridmap.

Input from TP

Testsuite for the mapping of users to local accounts, test with and without VOMS extensions, and with/without pool accounts.

Test 1

Pre-condition	Configured system. No previous mapping for user.
Test	Accepted authorisation.
Expected Outcome	GID/UID of the mapping returned. Primary group determined by FQAN if available. New entry in grid map is created.

Test 2

Pre-condition	Configured system. Previous mapping for user existing.
Test	Accepted authorisation.
Expected Outcome	GID/UID of the previous mapping returned.

Pass/Fail Criteria

Pass if the testsuite is provided and passes.

Related Information

History

4 CREDENTIAL MANAGEMENT

The Credential Management capability provides an interface for obtaining, delegating and renewing authentication credentials by a client using a remote service.

One of the key functionalities in this area is the linking of institutional authentication systems (e.g. Kerberos, Shibboleth) to the transparent issuing of certificates for use in the infrastructure through identity federations. This should be provided for operational deployment through the use of web portals and web service interfaces.

4.1 Credential Management Interface

Credential Storage	
ID	**CREDMGMT_IFACE_1**
Mandatory	
Applicability	Credential Management Appliances
Related Requirements	

Description The Credential Management capability should provide an interface for storing user credentials in the service.		
Input from TP Testsuite for storing user credentials in the service (with and without VOMS extensions).		
Test 1		
Pre-condition	Valid user credentials (X509 certificate), user allowed in the service.	
Test	Store user credential in the service	
Expected Outcome	Credential is stored in the system	
Test 2		
Pre-condition	Valid user credentials (X509 certificate), user not allowed in the service.	
Test	Store user credential in the service	
Expected Outcome	Error message is issued; no credentials are stored.	
Pass/Fail Criteria Testsuite is provided and passes for user credentials with and without VOMS extensions.		
Related Information		
History		

Credential Retrieval	
ID	**CREDMGMT_IFACE_2**
Mandatory	
Applicability	Credential Management Appliances
Related Requirements	

Description

The Credential Management capability should provide an interface for retrieving user credentials in the service.

Input from TP

Testsuite for retrieving user credentials in the service (with and without VOMS extensions).

Test 1

Pre-condition	Valid user credentials stored in service, user allowed in the service.
Test	Retrieve user credential
Expected Outcome	User credentials returned.

Test 2

Pre-condition	No valid user credentials stored in the service.
Test	Retrieve user credential
Expected Outcome	Error message is issued; no credentials are returned..

Pass/Fail Criteria

Testsuite is provided and passes for user credentials with and without VOMS extensions.

Related Information

History

Credential Renewal	
ID	**CREDMGMT_IFACE_3**
Mandatory	
Applicability	Credential Management Appliances
Related Requirements	

Description

The Credential Management capability should provide an interface for renewing user credentials in the service.

Input from TP

Testsuite for renewing user credentials in the service (with and without VOMS extensions).

Test 1

Pre-condition	Valid user credentials stored in service, host allowed to renew credentials.
Test	Renew user credential
Expected Outcome	User credentials renewed.

Test 2

Pre-condition	Valid user credentials stored in service, host not allowed to renew credentials.
Test	Renew user credential
Expected Outcome	Error message is issued; no credentials are renewed.

Test 3

Pre-condition	No valid user credentials stored in the service.
Test	Renew user credential
Expected Outcome	Error message is issued; no credentials are renewed.

Pass/Fail Criteria

Testsuite is provided and passes.

Related Information

History

4.2 Institutional Authentication Systems Linking

Institutional Authentication Linking	
ID	**CREDMGMT_LINK_1**
Not Mandatory	
Applicability	Credential Management Appliances
Related Requirements	#701: SSO and other enhancements

Description

Users should be able to access grid resources using institutional authentication systems.

Input from TP

Testsuite for linking institutional authentication system with the Credential Management implementation

Test 1

Pre-condition	Valid institutional user credentials, user allowed in the service.
Test	User requests grid credentials using his/her institutional credentials
Expected Outcome	Short-lived X.509 credential for used created.

Pass/Fail Criteria

Testsuite is provided and passes for each of the institutional authentication systems supported (e.g. Kerberos, Shibboleth)

Related Information

History

5 REFERENCES

R 1	UMD roadmap: https://documents.egi.eu/public/ShowDocument?docid=100
R 2	Generic UMD Quality Criteria
R 3	GridSite Delegation Protocol: http://www.gridsite.org/wiki/Delegation_protocol
R 4	Globus Delegation Service: http://www.globus.org/toolkit/docs/4.0/security/delegation/
R 5	European Policy Management Authority for Grid Authentication (EuGridPMA): http://www.eugridpma.org/