DOEGrids CA Release Notes

Revision: 4/02/03

1 Introduction

The New DOEGrids Certificate Authority is ready for deployment by the operations staff. This document discusses the new service and the changes between the old DOEScienceGrid CA and the new DOEGrids CA. The document will cover: Service Features, Transition and Migration plan. This document must be reviewed by the DOEGrids PMA before community deployment can happen. The PMA has a fiduciary responsibility for the community that must be addressed before the new service is deployed. This will require a vote on the PMA to accept, modify or reject this new service.

1.1 New Features Available at Release

1.1.1 New Name Space

The "base name" of certificate subject names in certificates is DC=DOEGrids, DC=org.
Why has this been done? Linking the CA's name space to the DOE Science Grid project unnecessarily limited the scope of the CA in the minds of potential customers. Unfortunately this wasn't clear at the time the original CA was pressed into service.

1.1.2 New Community Certificate Authority

The old "community" certificate authority at pki1.doesciencegrid.org will be phased out. The new community CA's Subscriber and Agent UI are on pki1.DOEGrids.org. The new CA has several features:

- 2048 bit RSA key
- Hardware Security Module (HSM) managed signing key
- Physical security features
- New CP/CPS and PDS documents:

1.1.3 New Root Certificate Authority

The new ESnet Root Certificate Authority information can be found at: http://www.es.net/CA/ This CA is an offline CA that is only used to sign Subordinate CAs.

1.1.4 Naming standard / specification for features

1.1.5 LDAP published certificates

The new LDAP Server (ldap.doegrids.org) has the following attributes:-

- Common Name
- Email
- Phone Number
- Virtual Organization Name
- Sponsor Name
- Sponsor Email
- The Certificate.

1.1.6 Subscriber User Interface (UI) changes

1.1.6.1 Mandatory fields

The following fields must be filled in by the subscriber.

- Email address
- Sponsor name/contact information

1.1.6.2 Drop-down VO menu pick

The Virtual Organization (VO) field has been changed to a drop down menu that requires a subscriber to select a VO.

1.1.6.3 Size – limited fields

We have improved (not perfected) the validity checking of the email fields, enforced mandatory references, and limited the size of data to reduce the likelihood of attacks on the web server.

1.1.7 Transition UI

On the Enrollment tab of https:// PKI1.doegrids.org you will find the “Transition to DOEGrids” link. This page enables a subscriber with a certificate from the DOE Science Grid CA, installed in their browser, to acquire an equivalent certificate from the new DOEGrids community CA automatically.
This new certificate will retain the “Common Name” or CN field of the DOE Science Grid Certificate, but the rest of the subject name will be based in the new DOEGrids name space.

1.1.7.1 Transition UI workflow

DOEGrids Certificate Transition processing events occur in the following order; please check Appendix A for a flowchart of this process:

- Key Generation/Certificate Request Generation: - The web browser generates key pair and submits the certificate request with the public key. Kindly note that this certificate request doesn’t have any information about the user except the public key generated by the Web Browser. This is different than the customary process, such as that used on the (default)

manual enrollment page, where requests include various attributes like Common Name, Email etc.

- SSL Client Authentication: - The server initiates SSL client authentication with the web browser. The user has to have a DOESciencegrid certificate for this SSL client authentication. The server is set up to trust only DOESciencegrid certificates.
- Certificate Validation: - The server accepts client certificates that are still current, or *expired no more than 30 days*.
  For Example
  If today is April 2, 2003, then you cannot use a Certificate which has expired on OR before March 2, 2003.
  The server validates the DOESciencegrid Certificate against the current DOESciencegrid Certificate Revocation List. If the Certificate Serial Number is present in the CRL, then the server rejects the request.
- Subject name Transition: - The common name (CN) attribute, and the contents of the SubjectAltName extension from the DOESciencegrid certificate, are added to the DOEGrids certificate request. The CN attribute is added to the base name appropriate to the new name space used by the DOEGrids CA.
  For Example
  If **'CN=Fname Lname 12345, OU=people, O=doesciencegrid.org'** is the Subject name of your DOESciencegrid certificate, then your new Subject name in the DOEGrids certificate will be **"CN=Fname Lname 12345, OU=People, DC=DOEGrids, DC=org"**.
- The server automatically issues a new DOEGrids Certificate. Services UI

1.1.7.2 Host SubjectAltName added to certificate

This will align us with future developments expected in IETF specifications.

1.1.7.3 Drop-down VO menu pick

This is intended to make life easier for the RA agents.

1.1.8 Renewal Interface

We continue to support the renewal interface provided by the SunONE CMS product. This product now fully supports renewals from Microsoft Internet Explorer. This feature also has been retrofitted to the DOE Science Grid community CA.

1.1.9 CRL distribution

The service supports several methods of acquiring CRL information:

- LDAP retrieval
- Retrieval from CMS web page (Retrieval tab)
- Direct retrieval from CMS web site: https://pki1.doegrids.org/CRL/doegridsca.crl.

These features are subject to change.

1.1.10 Agent capability

All the currently-enabled DOE Science Grid agents are enabled as agents on the DOEGrids CA at time of release.

1.2 Features Not Available at Release

1.2.1 New Root CA PMA/CP/CPS

This project is under development. The preliminary information is available at: www.ES.net/CA

1.2.2 Redundant LDAP servers

1.2.3 Merged LDAP servers

We intend to support both community CA's by common LDAP servers and distributed slave servers.

1.2.4 LDAP Published Certificates

The following attributes will not be available for anonymous access:

- Email
- Phone number
- Sponsor Name
- Sponsor Email.

1.2.5 Community CA Remote Registration Manager

We intend to move the UI functions for both agents and subscribers to a "Remote Registration Manager", and progressively limit access to the CA itself.

1.2.6 CRL distribution

It doesn't conform to name space specifications yet.

1.2.7 OCSP

Untested OCSP service is available from the CMS web site. A full OCSP service will be tested and made available at a later date.

1.2.8 Services UI – automatic issuance

We intend to offer automatic issuance of grid services (SSL-host-like) certificates in the near future, if policy issues permit – requires DOEGrids and International PMA approvals. We will restrict the availability of this page to authenticated certificate holders in the near future.

1.2.9 Services UI – multiple host/email names

1.2.10 Transition UI – options

We have planned to add options to the transition UI page, to allow multiple or replacement email addresses to be added to new certificates' SubjectAltName field. This flexibility might be extended to other X.509 fields as well.

1.2.11 New subscriber UI

The option to delete email address from certificate (equivalent to making it non-S/MIME capable), and the option to add multiple email addresses is planned. We are not sure the current set of email client software is capable of dealing with this and need to test it.

1.2.12 All Certificates – missing extensions

- CRL publishing points
- Policy OID
- Policy URL
- OCSP Responder URL

These features await technical clarifications and policy discussion with the DOEGrids PMA, other communities, and the GGF CAOPS working group.

2 Migration: DOE Science Grid to DOEGrids CA

2.1 Migration Plan

The DOE Science Grid community CA signing certificate expires on 10 Jan 2004. We will not renew or extend it. Roughly one month before this date it will no longer be possible to renew existing certificates or acquire new certificates from the DOE Science Grid CA.
We would like to stop issuing new certificates from DOE Science Grid CA as soon as we possibly can – 01 May 2003 would be better than 10 Dec 2003.
We will not support the old name space (O=doesciencegrid.org, and DC=doesciencegrid, DC=org). Everyone must eventually migrate to the new name space (DC=DOEGrids, DC=org).

2.1.1 Model Plan

- Acquire the new CA's signing certificates and signing policy files at: www.doegrids.org/CA.
- Distribute these files to clients and service locations as appropriate
- Acquire new grid-cert-request and openssl.cnf files http://www.DOEGrids.org/CA.
- Begin directing new services signing requests to DOEGrids CA immediately
- END accepting service requests at DOE Science Grid CA – 28 Apr 2003 -- redirect these requests to DOEGrids CA

- END accepting new subscriber requests at DOE Science Grid CA – 01 June 2003 – redirect these requests to DOEGrids CA
- END renewal requests at DOE Science Grid – 01 Jul 2003

Other services will continue on DOE Science Grid CA until the expiration of its signing certificate in January 2004. After this date the servers will be retired and the records archived.

2.1.2 Agent Migration

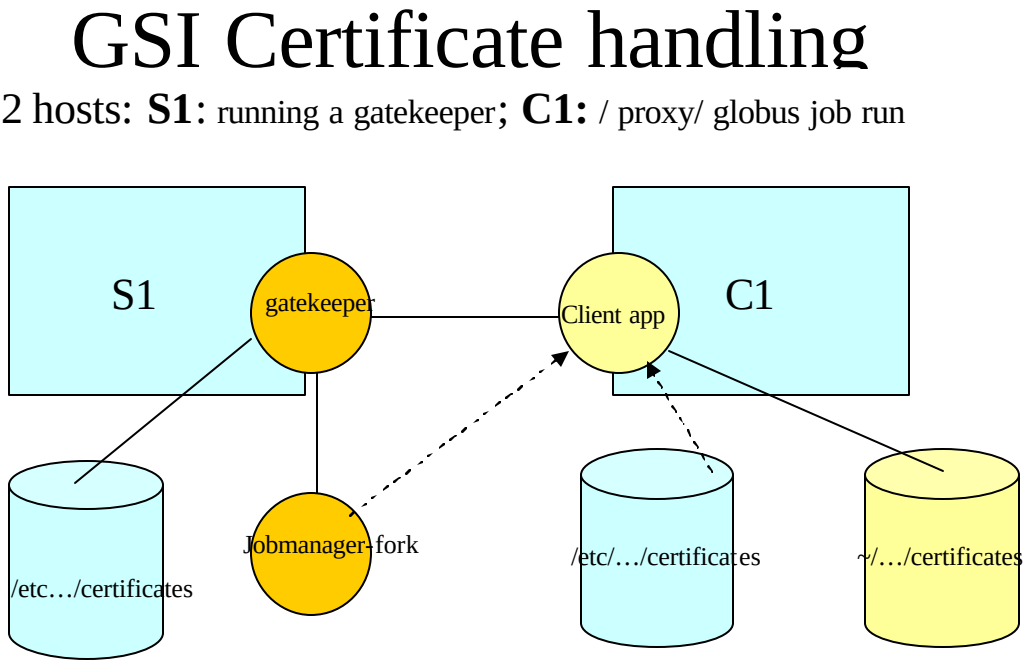
Agents should follow the DOE Science Grid CA renewal policy HERE; agents need to keep their DOE Science Grid certificate up-to-date. Do this in order to deal with duties related to the DOE Science Grid CA even after you have transitioned your users to the new CA: you may need to revoke older certificates.

- Copy all the existing agents' certificates to the new DOE Grids CA.
- Agents should create NEW certificates for themselves in the DOE Grids CA, and follow the renewal policy to enable these certificates for the agent role.

We recommend that agents do this as quickly as possible.
Agents should encourage their clientele to replace personal and services certificates. There is ample time to accomplish this, but customers will require assistance integrating the new certificates and policy files, and adjusting mapping files. Procrastination will result in a very unpleasant second week of January for those who have not yet changed over certificates to the new CA.

3 Testing of new CA certificates

To insure that the new CA and its associated certificates will work in our community a number of tests were conducted. The following is a diagram of the testing environment that was used.



TBD

3.1 Test Cases

TBD: Testing is underway; as results are available they will be posted here.

3.2 FAQ

TBD:

Appendix A Transition UI workflow

The following diagram illustrates the steps in the transition between DOEScienceGrid Certificates and DOEGrids certificates.