Certificate Policy and Certificate Practices Statement Template for ESGF CAs

Authors:
Lukasz Lacinski, ANL
Prashanth Dwarakanath NSC-LIU

Version: 2017-1.0

Argonne National Laboratory, Lemont, IL, USA
National Supercomputer Centre, Linköping, Sweden

Contents

Certificate Policy and Certificate Practices Statement Template for ESGF CAs

(In RFC 3647 format)

Date: January 30, 2017
Version: 2017-1.0

1 Introduction

The Earth System Grid Federation (ESGF), uses three internal Certification Authorities (CAs), to issue CA and identity certificates for the systems in ESGF. These CAs are operated by

1. Argonne National Laboratory (ANL), IL, Lemont, USA
2. Institut Pierre Simon Laplace (IPSL), Paris, France.
3. National Supercomputer Centre (NSC), Linköping, Sweden.

This document describes the set of rules and procedures established by ESGF, for the operation of its CAs. Structured according to RFC 3647 [RFC3647], this document describes policy and practices to be followed by ESGF CAs. Each individual CA is to have its own Certificate Policy and Certificate Practices Statement (CP/CPS) derived from this document. The CA/CPS is designed so that a Relying Party can look at them and obtain an understanding of the trustworthiness of credentials issued by the ESGF CAs.

1.1 Overview

The ESGF CA infrastructure supports grid and e-science activities in the Earth System Grid Federation (ESGF). This document describes the set of rules and procedures established by ESGF for the operations of its CAs. The purpose of the ESGF CAs is:

1. To sign host certificates for nodes operated by vetted members of the ESGF federation.
2. To sign subordinate CA certificates for nodes operated by vetted members of the federation, with the understanding that the subordinate CA may only be used to issue end-user credentials and short-lived credential proxies.

1.2 Document name and identification

This document is the CP and CPS Template of the ESGF CAs.

Document title: Certificate Policy and Certification Practice Statement Template for ESGF CAs

Document version: 2017-1.0

Document date: January 30, 2017

1.3 PKI participants

1. Certificate Authorities: ANL, IPSL, and NSC issue CA certificates and host certificates for the ESGF.
2. Registration Authorities: There are no RAs external to the issuing authorities. The individual CAs are responsible for all approvals and revocations that they perform.
3. Subscribers: Only institutions that participate in the ESGF receive certificates from the Root CA.
4. Relying Parties: No stipulation.

1.4 Certificate usage

The ESGF CA Root certificate may be used for the following purposes:

1. To validate the signature of a Subject CA
2. More generally, to validate any certificate chain ending with this Root, provided all certificates in the chain are used for permitted purposes
3. To validate the signature on a CRL issued by this Root. No other use of the ESGF CA Root certificate is permitted. The ESGF CA Root asserts that all Subordinate CAs serve the same community and they all issue in distinct namespaces.

1.5 Policy administration

The Argonne National Laboratory (ANL), and National Supercomputer Center (NSC) at Linköping University (LiU) are responsible for drafting, registering, maintaining and updating this CP/CPS template. The persons responsible for this policy and the practices of the CA are:

1. Lukasz Lacinski, Argonne National Laboratory (ANL), Building 240, 9700 Cass Avenue, Lemont, IL 60439, Email esgf-ca@lists.llnl.gov.
2. Prashanth Dwarakanath, National Supercomputer Center (NSC), House Galaxen, Entrance 83, Linköping University, Campus Valla, Olaus Magnus väg 42-44, Linköping, Email: esg-admin@nsc.liu.se.

1.6 Definitions and acronyms

1. ANL: Argonne National Laboratory, located in Lemont, IL, USA.
2. IPSL: Institut Pierre Simon Laplace, located in Paris, France.
3. NSC: National Supercomputer Center at Linköping University (LiU), located in Linköping, Sweden.
4. EE: Users obtaining credentials from a Subordinate/Subject CA are called End Entities (EE).
5. ESGF: is the Earth System Grid Federation.
6. RP: Relying party (RP) is a computer term used to refer to a server providing access to a secure software application. Claims-based applications, where a claim is a statement an entity makes about itself in order to establish access, are also called relying party applications.
7. For the purposes of this document, a Subject CA is a CA whose certificate was issued by the Root whose policy and practices are described in this document.
8. For the purposes of this document, a Subordinate CA is a Subject CA in a hierarchy whose root is described in this document.
9. For the purposes of this document, Profile refers to the content of the signed envelope within a certificate, but excluding the public key itself and the lifetime. Thus, Profile normally comprises extensions, the issuer and subject names, but also the type of keys and algorithms, and the version of the certificate.

2 Publication and repository responsibilities

It is the responsibility of each of the ESGF CA Root CAs to publish the following information on their respective websites

1. Its CP/CPS;
2. Its certificate;
3. All certificates issued by the ESGF CA Root CA and their status;
4. The signing policy of the hierarchy of which it forms the root;
5. Its Certificate Revocation List (CRL)

The ESGF CA Root CA grants the ESGF the right of unlimited redistribution of this information.

3 Identification and authentication

3.1 Naming

1. Each of the Subject CAs shall have a unique name;
2. Its Subject DN shall form the Subject name of each Subject CA to relate its purpose and distinguish it from others alone.
3. The Issuer name shall include /O=ESGF/OU=ESGF.ORG.
4. No subject name of a Subject CA shall be reused anywhere in the hierarchy.
5. Subject CA names have a fixed and a variable component. The certificate subject names start with the fixed component to which a variable component is appended to make it unique. The fixed component is as follows:

/O=ESGF/OU=ESGF.ORG

3.2 Initial identity validation

A certificate shall be issued to a Subject CA only when:

1. The requestor has been ascertained to be the responsible node administrator of the node the certificate is being sought for.
2. The requestor and his organization have been vetted to be a part of the ESGF federation.
3. The Subject CA promises to adhere to the policies and practices described in this document.
4. The Subject CA has submitted a certificate request and is able to prove to the Root CA possession of the corresponding private key.

Furthermore, the ESGF CA Root CA requires, as a condition for certificate issuance, that:

1. All Subject CAs make available to the ESGF CA Root CA results of CA audits and plans to remedy deficiencies
2. All Subject CA Managers and Operators agree to be signed up to a closed mailing list, maintained by the ESGF CA Root CA;
3. The Subject CA's certificate request (and hence certificate) contains no personal information.

3.3 Identification and authentication for re-key requests

ESGF CA Security Officers who manage the Subject CA shall prove possession of the private key corresponding to the certificate being renewed, and prove possession of the private key corresponding to the request being submitted.

3.4 Identification and authentication for revocation request

The certificate of a Subject CA will be revoked when:

1. A revocation request is received which is signed with the private key of the Subject CA; or,
2. An authenticated revocation request from the CA Manager of the Subject CA is received; or,
3. The ESGF CA Root CA has otherwise determined the need for revocation, e.g., if the Subject CA does not comply with the requirements imposed on it by the ESGF CA Root.

4 Certificate life-cycle and operational requirements

The ESGF CA should use a key of at least 2048 bits have a lifetime of at least five years. For Subject CAs, keys are generated by the requestors who are responsible for the security of the keys themselves. The Subject CAs shall have a lifetime not exceeding one year.

4.1 Certificate application

For an initial request, the Manager of the Subject CA shall agree to the namespace of the Subject CA with the Manager of the ESGF CA Root CA, and shall submit a CP/CPS under which the Subject CA will operate. It is the responsibility of the Manager of the Subject CA to ensure that it operates within the constraints imposed by the Policy of the Root.

4.2 Certificate application processing

When the ESGF CA Root CA Manager is satisfied that Subject CA will operate within the constraints imposed by the Root, The ESGF CA Root CA will issue and publish the certificate of the Subject CA.

4.3 Certificate issuance

The ESGF CA Root CA Manager makes the Subject CA available on its website.

4.4 Certificate acceptance

Both the ESGF CA Root CA Manager and the ESGF CA Subject CA Manager shall verify the content of the Subject CA certificate against the CP/CPS of the Subject CA and test its use (e.g. against grid middleware). If problems are discovered during testing, the certificate shall be revoked by the ESGF CA Root CA, and reissued with changes, provided that these changes are still compatible with the CP/CPSes of both the ESGF CA Root and Subject CAs.

4.5 Keypair and certificate usage

The certificates of all Subordinate CAs and those of the EEs issued by Subordinate CAs must be used only for purposes of direct academic science and grid work, or related incidental support (i.e. infrastructure, email). The certificates issued to Subject CAs may only be used as CA certificates, i.e., for validating certificates issued by them, and for validating CRLs. A Subordinate CA may impose further constraints on the use of certificates on, and only on, their EEs. Conversely, no Subordinate CA shall relax constraints imposed on its policy or operations by the CP/CPS of a CA of which it is itself Subordinate. It is the responsibility of the EE to use certificates for permitted purposes only. It is the responsibility of RPs to validate the certificate to their satisfaction at the time of reliance.

4.6 Certificate renewal

Issued certificates are never automatically renewed, and it is the responsibility of the certificate requestors to contact the ESGF CAs by emailing to esgf-ca.lists.llnl.gov and requesting for a new certificate. Requestors are expected to generate new keys and make a fresh request for a new certificate.

4.7 Certificate revocation and suspension

A Subject key CA shall be revoked if:

1. It is seen to consistently and willfully violate its own CP/CPS, or that the CA Manager of the Subject CA does not take steps to address such
2. It is seen to violate requirements imposed on it by the policy and practices of the Root; or
3. It can be shown that the private key has been compromised.

4.8 Certificate status services

The Root CA shall issue a CRL. Certificates and certificate status of Subject CAs are available on the Root CA's web site. See also section 5.7.

4.9 End of subscription

No stipulation.

5 Facility, management and operational controls

This section discusses specific ESGF CA procedures related to its facility and ESGF CA Root CA operation.

5.1 Physical security

The machine on which the Root signs its certificates and CRLs is expected to be installed in a facility which restricts physical access of the machine only to designated personnel.

5.2 Personnel controls

Training: The Root CA is OpenSSL based, and ESGF CA Managers must have sufficient experience with OpenSSL to be able to issue certificates and CRLs. ESGF CA Managers must be permanent staff of the respective institution.

5.3 Audit logging procedures

All OpenSSL operations and basic system logs for the signing machine will be saved in files that are periodically signed and backed up onto secondary storage media.

5.4 Records archival

Records are kept throughout the lifetime of the CA and for a period no less than three years after the termination of the CA.

5.5 Key changeover

At re-keying, the new Root public keys shall be published on the Root CA's web site, as certificates signed by both the old and the new private key. The transitional certificate, signed with the old key, shall expire at the same time as the old Root certificate, but shall otherwise have the same content as the new Root certificate. It shall be clearly marked as a transitional certificate, and instructions shall be provided for users explaining how to verify the transition.

5.6 Compromise and disaster-recovery

Following any compromise of the Root private key, The Root CA shall make this widely known to all peer CAs, Subject CAs and relying parties. Efforts to re-issue new Subject CA certificates will follow the method described in section 5.7.

5.7 CA or RA termination

Upon termination of the Root CA, a ESGF CA Manager shall communicate this in advance to peer CAs, Subject CAs and relying parties. The advance notice should be no less than the longest lifetime of any currently valid Subject CA.

6 Technical security controls

This section discusses technical aspects specific to the operation of the ESGF CA Root CA.

6.1 Key-pair generation and installation

The Root CA's key pair shall be generated with sufficient entropy, by the CA. It shall be the responsibility of a ESGF CA Manager to generate the key pair. The Root key pair shall be RSA and have a length of at least 2048 bits. Key pairs for Subject CAs are generated according to best practices. Each Subject CA key pair should have a length of at least 2048 bits.

6.2 Other aspects of key pair management

All Root CA certificates shall be kept and published throughout the lifetime of the CA, and a period no less than three years after the termination of the CA. Subject CAs' key pairs shall have a lifetime not to exceed one year.

6.3 Computer security controls

Only ESGF CA Security Officers and CA Managers may access the dedicated ESGF CA server.

6.4 Lifecycle technical controls

Only ESGF CA Security Officers or CA Managers may perform hardware maintenance or upgrade software on the dedicated ESGF CA server.

6.5 Network security controls

1. ESGF CA Root server should be on a private LAN with no other hosts on the same network, except the gateway host which it may use in order to download critical updates.

2. It's strongly advised that the gateway host only allow packet forwarding for the CA server, when updates are to be installed, ensuring that it is totally isolated from the internet at all other times.

3. A local firewall policy on the server that prohibits all machines other than the gateway host machine, to connect to it via ssh, is also recommended.

4. No other ports on the server should be open from any machine, including the gateway host machine. This ensures that the ESGF CA Root CA server is disconnected from the internet and all other machines, except the host machine, at all times, other than the time when it is being updated.

5. Even when the ESGF CA Root server is being updated, only outbound connection requests from the server ought to be permitted to receive responses, i.e. it cannot be contacted by any external machine, directly, at any time.

6.6 Time-stamping

The CA server is expected to maintain correct time using NTP service, to stay in sync with designated NTP servers. The selection of the NTP servers is managed by each individual CA, based on their network policies. The ESGF CA Root CA Manager shall periodically check the time on the server, to ensure that it is really in sync, and correct it, only if necessary.

7 Certificate, CRL and OCSP profiles

This section articulates details of certificates and certificate revocation lists issued by the ESGF CA Root CA. The ESGF CA Root CA does not currently provide OCSP support.

7.1 Certificate profile

All certificates issued by the ESGF CA Root CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280 [RFC3280].

The Root CA shall have the following Profile:

1. The certificate shall be version 3 (i.e., the version number shall be 2);

2. The issuer and subject name shall both contain the following: O = ESGF, OU = ESGF.ORG
3. The signature algorithm shall be sha256WithRSAEncryption, or sha1WithRSAEncryption;
4. The extensions shall contain:
   a) basicConstraints: CA=true, critical;
   b) keyUsage: certificate signing, CRL signing, critical;
   c) There shall be a subjectKeyIdentifier and it shall have the hash as a value;

The requirements on the Profile of the Subject CAs are as follows:

1. The certificate shall be version 3 (i.e., the version number shall be 2);
2. basicConstraints must be present and critical and must contain CA=true, (but may contain other constraints);
3. keyUsage must be present and critical and must have certificate signing and CRL signing set, and no other value;
4. There shall be a subjectKeyIdentifier containing the hash.
5. Other extensions are allowed.

7.2 CRL Profile

The Root CA issues CRL version 2 (i.e., the version number shall be 1). The “lifetime” of the CRL is 18 months and it is issued at least once every year.

7.3 OCSP Profile

Not applicable.

8 Compliance audit and other assesments

The ESGF CA Security Officer shall carry out a compliance audit of the Root CA once every year. The audit shall inspect the logs and check the security of the activation data and the copies of the encrypted private key.

9 Other business and legal matters

The section headers in section 9 are taken from RFC3647 and are kept as-is for ease of reference and comparison with other CAs. They must not be interpreted or construed in any way that will affect the interpretation or construction of the contents of the sections. Certificates and all other components of the CA must be used for lawful purposes only. CA Managers shall sign a document to the effect that they will comply with the procedures and requirements described in this document.

9.1 Fees

The ESGF CA Root CA charges no fees for its services.

9.2 Financial responsibility

No financial responsibility is accepted for certificates issued under this policy.

9.3 Confidentiality of business information

The ESGF CA Root CA will follow best practices to protect any confidential information as well as policies specified by the individual institutions.

9.4 Privacy of personal information

The ESGF CA Root CA does not process any personal data, except for the following:

1. The email addresses of the ESGF CA Security Officers and CA Managers. These are not published and are used only for announcements pertaining to the Root CA or announcements affecting all Subject CAs.

ESGF CA Root and Subject CAs publish a generic email address to contact ESGF CA Security Officers: esgf-ca@lists.llnl.gov.

9.5 Intellectual property rights

This document is based on RFC3647 and its application to the "UK e-Science Root Certificate Policy and Certification Practices Statement" by the UK e-Science CA run by CCLRC. The ESGF CA Root CA does not claim any IPR on certificates that it has issued. Anybody may freely copy from any version of the ESGF CA Root CA's Certificate Policy and Certification Practices Statement provided they include an acknowledgment of these sources.

9.6 Representations and warranties

When issuing a certificate to a Subject CA, the ESGF CA Root CA will have evaluated the CP/CPS of the Subject CA and is satisfied that the Subject CA, when operating according to its CP/CPS, complies with the requirements imposed on it by this document.

9.7 Disclaimers of warranties

ESGF CA makes no representation and gives no warranty, condition or undertaking in relation to the ESGF CA Root CA and its operation.

9.8 Limitations of liability

With respect of the information published by the Root CA, including, but not limited to certificates and CRLs, the Root CA shall make best endeavors to ensure the information is timely and accurate. ESGF CA shall be under no obligation or liability, and no warranty condition or representation of any kind is made, given or to be implied as to the sufficiency, accuracy or fitness for purpose of such information. The recipient party, whether CA, RP, EE, or anyone else, shall in any case be entirely responsible for the use to which it puts such information. The ESGF CA Root CA also declines any liability for damages arising from the nonissuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the designated RA acting in conformance with this CP/CPS.

9.9 Indemnities

The ESGF CA Root CA declines any payment of indemnities for damages arising from the use or rejection of certificates it issues. Each Subject CA and relying party shall indemnify and hold harmless ESGF CA and keep ESGF CA indemnified against any and all damages, costs, claims or expenses, which are awarded against, or suffered by the Subject CA or relying parties or their hosting institution or company, as a result of any act or omission of the relying party or Subject CA.

9.10 Term and termination

The initial lifetime of the ESGF CA is five years, and it is intended to be renewed for a similar period, prior to reaching expiration. Should the ESGF CA Root CA service be permanently discontinued, there shall be a federation-wide announcement, prior to closure.

The ESGF CA Root CA shall issue no certificate whose lifetime will exceed the date of termination and is obligated to maintain its CRL until its termination.

9.11 Individual notices and communications with participants

All agreements between the ESGF CA Root CA and any organization must be documented and signed by the appropriate authorities. A mailing list shall be maintained for announcements pertaining to the ESGF CA Root CA, or announcements affecting all Subject CAs.

9.12 Amendments

The ESGF CA Root CA shall communicate amendments to Subject CAs and to the ESGF.

9.13 Dispute resolution provisions

ESGF CA Security Officers shall resolve any disputes arising out of the CP/CPS.

9.14 Miscellaneous provisions

No stipulation.

9.15 Other provisions

No stipulation.

10 Change log