

Grid PKI Disclosure Statement

Status of This Memo

This memo provides information to the Grid community regarding the publication of Certificate Authority information. It does not define any standards or technical recommendations. Distribution is unlimited.

Copyright Notice

Copyright © Global Grid Forum (2003). All Rights Reserved.

Abstract

The Grid PKI disclosure Statement (PDS) is designed to provide a way for a Grid Certificate Authority to succinctly publish information for subscribers and relying parties. It is a distillation of the information in the Certificate Policy document of the Grid CA. It is not designed to replace the CP but to provide a mechanism that Subscribers/Relying parties can use to quickly review their obligations and the policies of the Grid Certificate Authority.

Contents

Abstract.....	1
1. Introduction	2
1.1 Prior art.....	2
1.2 PDS structure	2
2. Security Considerations.....	3
Author Information	5
Intellectual Property Statement	5
Full Copyright Notice	5
References	5

1. Introduction

Certificate Policies (CP) and Certification Practice Statements (CPS) are very detailed documents that describe what and how a Certificate Authority issues certificates. It also describes the obligations and responsibilities of all parties participating in the Grid Public Key Infrastructure service. These documents tend to be very detailed and reflect legal and instructional rules for the operation of the service. They are a necessity for the proper operation of the PKI. They reflect the contractual relationship between the Subscribers/Relying parties and the CA they trust. This complexity is hard for none PKI experts to understand.

The goal of the Grid PDS is to allow Grid CAs to publish a simplified version of their CP. This will facilitate Subscribers/Relying party's review of the policies implemented by the Grid CA. This is **not** a replacement for a detailed review of the Grid CA CP. The PDS will help Subscribers and Relying parties to quickly determine if the CA is producing certificates that are appropriate for their Certificate requirements.

1.1 Prior art

An internet draft on PDS was submitted to PKIX [PKIX1] that expired November 2000. That work and this work were based on the American Bar Associations PAG appendix B [ABA1].

1.2 PDS structure

The PDS will consist of the following parts:

- TITLE
- Version, Date
- PDS fields

The body of the PDS must contain the following fields [ABA1].

Statement Types	Statement Descriptions
CA contact information	The name, location and relevant contact information for the CA.
Certificate type, validation procedures, and usage:	A descriptions of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage.
Reliance limits:	The reliance limits, if any.
Obligations of subscribers:	The description of, or reference to, the critical subscriber obligations.
Certificate status checking obligations of relying parties:	The extent to which relying parties are obligated to check certificate status, and references to further explanation.
Limited warranty and disclaimer/limitation of liability:	Summary of the warranty, disclaimers, limitations of liability, and any applicable warranty or insurance programs.

Applicable agreement, Certification Practice Statement, Certificate Policy:	Identification and references to applicable agreements, CPS or CP.
Privacy Policy:	A description of and reference to the applicable privacy policy, if any.
Refund Policy:	A description of and reference to the applicable refund policy, if any.
Applicable law and dispute resolution:	Statement of the choice of law and dispute resolution mechanism.
CA and repository licenses, trust marks, and audit:	Summary of any governmental licenses, seal programs, a description of the audit process and, if applicable, the audit firm.

2. PDS publication requirements

The PDS must follow the publication requires for the Grid CA that was specified in their CP

3. Example PDS

VeriSign provides a PDS for its Certificate service. You can find it at:

<http://www.verisign.com/repository/disclosure.html>

The following is an example for the DOEGrids PKI. It is based on their CP/CPS located at:

<http://www.doegrids.org/Docs/CP-CPS.pdf>

DOEGrids PKI Disclosure Statement Version 1 February 13, 2003

1. CA Contact info:

Tony J. Genovese
One Cyclotron Road, B50A 3131
Berkeley, CA 94706
phone: +1 510 486 4003
fax: +1 510 486 4790
e-mail: Tony@es.net

2. Certificate type, validation procedures, and usages: The DOE Grids Certificate Services supports DOE Scientists and Engineers working on the new Computational Grids being deployed around the world. This service issues Identity Certificates to individual subscribers and Service certificates for Grid services.

The DOE Grids PKI uses an architecture where the approval of certificate requests is the responsibility of the Registration Authority for a specific community. The work flow of subscriber certificates request/approval can be found on the service website: <http://www.doegrids.org/pages/workflow.pdf>

Each RA will be responsible for determining the identity used in the subject field of the Certificate. The procedure for determining identity differs depending on the type of certificate and RA policies. Each VO/Site must document their procedures in their individual RA appendix in DOEGrids CP/CPS.

3. Reliance Limits: DOEGrids does not set reliance limits on its certificates.

4. Obligations of subscribers:

- Read and adhere to the procedures published in the DOEGrids CP/CPS;
 - Read and adhere to the ESnet Acceptable Use Policy (<http://es.net/hypertext/esnet-aup.html>)
 - Generate a key pair using a trustworthy method;
 - Take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:
 - For Person Certificates
 - Selecting a pass phrase of at minimum 8 characters
 - Protecting the pass phrase from others
 - Always using the pass phrase to encrypt the stored private key.
 - Never sharing the private key with other users.
 - For Service Certificates
 - Storing them encrypted whenever possible.
 - They may be kept unencrypted on the host that they represent.
 - Provide correct personal information and authorize the publication of the certificate
 - Notify DOE GRIDS PKI immediately in case of private key loss or compromise.
 - Use the certificates for the permitted uses only.
5. **Certificate checking obligations of relying parties:** A relying party should only rely on the validity of the certificate after it has checked that the certificate has not be revoked. CRLs are maintained at: <http://www.doe grids.org/pages/crls.htm>
6. **Limited warranty & disclaimer/Limitation of liability:** DOE GRIDS PKI and its agents issue person certificates according to the practices described in the CP/CPS to validate identity. No liability, implicit or explicit, is accepted.
- DOE GRIDS PKI and its agents make no guarantee about the security or suitability of a service that is identified by a DOE GRIDS certificate. The certification service is run with a reasonable level of security, but it is provided on a *best effort only* basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.
- DOE GRIDS PKI denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.
7. **Applicable agreements, Certification Practice Statement, Certificate Policy:** <http://www.doe grids.org/Docs/CP-CPS.pdf>
8. **Privacy policy:** Only email addresses are collected and are published in the certificate. No other private data is collected.
9. **Refund policy:** DOEGrids does not collect fees for certificates.
10. **Applicable law and dispute resolution:** The DOEGrids CP/CPS is subordinate to all applicable U.S. government laws, as well as Department of Energy (DOE) orders.
11. **CA and repository licenses, trust marks, and audit:** DOEGrids repository is located at: <http://www.doe grids.org/CA/> No audits are done except by the DOEGrids community.

4. Security Considerations

This document describes a community best practice for the publication of information and does not specify or require security. It is expected PDS will be widely available to its community.

Author Information

Tony J. Genovese
One Cyclotron Road
Berkeley, CA USA94706

Michael Helm
One Cyclotron Road
Berkeley, CA USA 94706

Intellectual Property Statement

The GGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the GGF Secretariat.

The GGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the GGF Executive Director.

Full Copyright Notice

Copyright (C) Global Grid Forum (date). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the GGF or other organizations, except as needed for the purpose of developing Grid Recommendations in which case the procedures for copyrights defined in the GGF Document process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the GGF or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE GLOBAL GRID FORUM DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

References

PKIX1: PKIX working Group, May 10, 2000, Internet X.509 Public Key Infrastructure PKI Disclosure Statement: draft-ietf-pkix-pds-00.txt: <http://www.verisign.com/repository/pds.txt>

ABA1: Appendix 6, American Bar Association PKI Assessment Guidelines, PAG v0.30, June 18, 2001 <http://www.abanet.org/scitech/ec/isc/pagv30.pdf>