

**Argonne National Laboratory
Windows Domain
Certificate Policy
Version 1.2**

October 26, 2004

Revised February 5, 2008

Table of Contents

1	Introduction	6
1.1	Overview	6
1.2	General Definitions.....	6
1.3	Identification	8
1.4	Community and Applicability	8
1.4.1	Certification Authorities	8
1.4.2	Registration Authorities	9
1.4.3	End Entities	9
1.4.4	Applicability	9
1.5	Contact Details	10
2	General Provisions	11
2.1	Obligations	11
2.1.1	CA and RA Obligations	11
2.1.2	Subscriber Obligations	12
2.1.3	Relying Party Obligations	12
2.1.4	Repository Obligations	13
2.1.5	Liability	13
2.2	Financial Responsibility.....	13
2.3	Interpretation and Enforcement.....	13
2.3.1	Governing Law	13
2.4	Fees	13
2.5	Publication and Repositories.....	13
2.5.1	Publication of CA information	13
2.5.2	Frequency of Publication.....	14
2.5.3	Access Controls	14

2.5.4	Repositories	15
2.6	Compliance Audit	15
2.7	Confidentiality	15
2.8	Intellectual Property Rights	15
2.9	Initial Registration.....	15
2.9.1	Types of names	15
2.9.2	Name Meanings	15
2.9.3	Uniqueness of Names	16
2.9.4	Method to Prove Possession of Private Key	16
2.9.5	Autoenroll Users.....	16
2.9.6	Authentication of Individual Identity.....	16
2.10	Routine Rekey.....	17
2.11	Rekey After Revocation.....	17
2.12	Revocation Request.....	17
2.13	Renewal	17
2.13.1	Smart Card Users.....	17
2.13.2	Autoenroll Users.....	17
3	Operational Requirements.....	18
3.1	Certificate Application.....	18
3.1.1	Smart Card Users.....	18
3.1.2	Autoenroll Users.....	18
3.2	Certificate Issuance.....	18
3.2.1	Smart Card Users.....	18
3.2.2	Autoenroll Users.....	18
3.3	Certificate Acceptance	18
3.4	Certificate Suspension and Revocation	19
3.4.1	Circumstances for Revocation.....	19

3.4.2	Who Can Request Revocation	19
3.4.3	Procedure for Revocation Request	19
3.4.4	Circumstances for Suspension.....	19
3.4.5	CRL Issuance Frequency	19
3.4.6	Online Revocation/status checking availability.....	19
3.4.7	Online Revocation checking requirements.....	20
3.4.8	Other forms of revocation advertisement available	20
3.5	Security Audit Procedures.....	20
3.6	Records Archival	20
3.6.1	Types of Event Recorded.....	20
3.6.2	Retention Period for Archives.....	20
3.7	Key Changeover.....	20
3.8	Compromise and Disaster Recovery.....	20
3.9	CA Termination	21
4	Technical Security Controls	22
4.1	Key Pair Generation and Installation.....	22
4.1.1	Key Pair Generation	22
4.1.2	Private Key Delivery to Entity	22
4.1.3	Public Key Delivery to Certificate Issuer.....	22
4.1.4	CA Public Key Delivery to Users	22
4.1.5	Key Sizes	22
4.1.6	Public Key Parameters Generation	22
4.1.7	Parameter Quality Checking	22
4.1.8	Hardware/Software Key Generation.....	22
4.1.9	Key usage Purposes	22
4.2	Private Key Protection.....	23
4.2.1	Private Key (n out of m) Multi person control	23

4.2.2	Private Key Escrow	23
4.2.3	Private Key Archival and Backup	23
4.3	Other Aspects of Key Pair Management	23
4.4	Computer Security Rating	23
4.5	Life-Cycle Security Controls	23
4.6	Cryptographic Module Engineering Controls.....	23
5	Certificate and CRL Profiles	24
5.1	Certificate Profile	24
5.1.1	Version number	24
5.1.2	Certificate Extensions.....	24
5.1.3	Algorithm Object identifiers	24
5.1.4	Name Forms.....	24
5.1.5	Name Constraints.....	25
5.1.6	Certificate Policy Object Identifier.....	25
5.1.7	Usage of Policy Constraints Extensions.....	25
5.1.8	Policy qualifier syntax and semantics.....	25
5.2	CRL Profile	25
5.2.1	Version	25
5.2.2	CRL and CRL Entry Extensions	25
6	Specification Administration.....	26
6.1	Specification Change Procedures	26
6.2	Publication and Notification Procedures.....	26
6.3	CP Approval Procedures.....	26
7	Bibliography	27
8	List of Changes.....	28

1 Introduction

1.1 Overview

Argonne National Laboratory is a major multiprogram laboratory managed and operated for the U.S. Department of Energy (DOE) by the University of Chicago under a performance-based contract.

Argonne's mission is to serve DOE by advancing the frontiers of knowledge, by creating and operating forefront scientific user facilities, and by providing innovative and effective tools and solutions for energy and environmental challenges to national and global well-being, in the near and long term, as a contributing member of the DOE Laboratory system.

Argonne supports DOE's missions in science, energy resources, environmental stewardship, and national security, with lead roles in science, operation of scientific facilities, and energy. In accomplishing its mission, Argonne partners with DOE, other federal laboratories, the academic community, and the private sector.

The Argonne National Laboratory (ANL) Windows Domain Public Key Infrastructure is intended to serve the staff and collaborators of the Laboratory. The Laboratory is defined at <http://www.anl.gov>.

This document describes the set of rules and procedures established by Argonne National Laboratory, Computing and Information Systems (CIS) Division for the operations of the Argonne National Laboratory Windows Domain Public Key Infrastructure. This document is organized according to RFC 2527 [RFC2527].

It is the intent of the Windows Domain PKI to issue identity certificates for authenticating to the ANL Windows Domain and its internal administrative application portal. The Windows Domain PKI generally issues two types of certificates: certificates for smart cards and Autoenroll certificates. These certificates are for Argonne employees, contractors, and their colleagues.

The Argonne Windows Domain PKI will be based on the Microsoft Certificate Server. This configuration directly influences the architecture supported.

Not all sections of RFC 2527 are used. Sections that are not included have a default value of "No stipulation".

1.2 General Definitions

Activation Data

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass phrase, or a manually-held key share).

Autoenroll Certificate

A certificate automatically issued to Microsoft Windows users upon logon to Argonne National Laboratory Windows Domain.

Certification Authority (CA)

The entity / system that issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA)

Certificate Policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification Practice Statement (CPS)

A statement of the practices, which a certification authority employs in issuing certificates.

End Entity

Or sometimes called a Subscriber is the individual who applied for and was issued a certificate.

Person Certificate

A certificate used for authentication of an individual. The certificate represents a person.

Policy Qualifier

The Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Point of Contact

The member of a site/VO RA that has been chosen to handle all communications about policy matters with the DOE GRIDS PMA.

Registration Authority (RA)

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Registration Agent (RAg) or "Agent"

RAg is the entity that interacts with the RM in order to cause the CA to issue certificates.

Relying Party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Set of provisions

A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS and employing the approach described in this framework.

Subscriber

Or sometimes called End Entity is the individual who applied for and was issued a certificate.

1.3 Identification

Document title: **Argonne National Laboratory Windows Domain Certificate Policy**

Document version: **1.2**

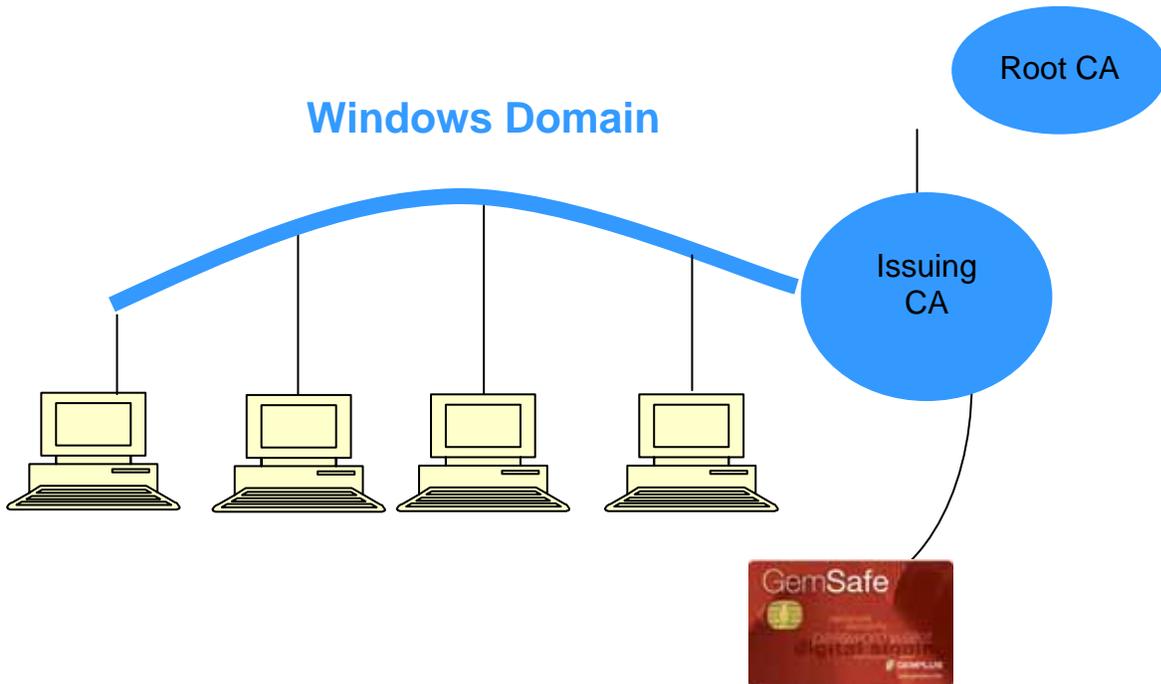
Document date: February 5, 2008

OID: 1.3.6.1.4.1.751.75.10.11

1.4 Community and Applicability

1.4.1 Certification Authorities

The Computing and Information Systems Division will manage and operate the Argonne National Laboratory Windows Domain PKI. This is to include the Off-line Root CA, the On-line Issuing CA, and the Enrollment Station.



The following is a list of the PKI components:

Component	Location	Function
Root Certificate Authority	Building 201 Room 167 Data Center	Signs subordinate CAs certificate requests
Issuing Certificate Authority	Building 221 Room D-130 Data Center	Signs Subscriber and Service Certificates
Enrollment Station	Mobile	Creates token generated Certificate Requests. Agents use this station to submit token generated certificate requests for immediate approval.

The issuing certificate authority (CA) is a subordinate of the Argonne National Laboratory Windows Domain root CA.

1.4.2 Registration Authorities

The Account Services group of Computing and Information Systems will serve as the Registration Agent for the ANL Windows Domain Public Key Infrastructure. The Windows Domain Certificate Authority maintains a browser accessible Registration Manager for use by subscribers to the Windows Domain Public Key Infrastructure. This interface is used to submit certificate requests.

1.4.3 End Entities

The ANL Windows Domain PKI issues certificates to individuals conducting official business for Argonne National Laboratory. This includes scientists, engineers, staff, graduate students, contractors, collaborators and others.

To be issued a certificate by the ANL Windows Domain Public Key Infrastructure, the end entity must be either a staff member or an affiliate of Argonne National Laboratory.

- Staff is defined as employees of the Laboratory.
- Affiliates are those individuals that are affirmed as collaborators by Argonne staff.

All end entities must hold accounts in the ANL Windows domain (required for Microsoft smart card enablement or autoenroll participation).

1.4.4 Applicability

Authentication: Person certificates can be used to authenticate a person to hosts and services that have agreed to accept certificates from the ANL Windows Domain PKI. These hosts and services, managed by relying parties, will typically be computers and applications within Argonne National Laboratory.

While Person certificates may be used for other activities such as e-mail signing and encryption, these are not supported activities. These certificates are not suitable for legally binding digital signatures on documents.

1.5 Contact Details

Argonne National Laboratory Windows Domain PKI is operated by the Computing and Information Systems Division.

The point of contact for questions related to this document is:

Name: John Volmer
Address: Computing and Information Systems Division
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439
phone: +1 630 252 5449
fax: +1 630 252 9689
e-mail: volmer@anl.gov

2 General Provisions

2.1 Obligations

2.1.1 CA and RA Obligations

ANL Windows Domain CA will:

Accept certification requests from entitled entities;

Notify the RA of certification request and accept authentication results from the RA.

Issue certificates upon the approval of the registration authority agents;

Notify the subscriber of the issuing of the certificate;

Publish the issued certificates;

Accept revocation requests according to the procedures outlined in this document;

Revoke certificates upon the approval of the registration authority agents

Issue a Certificate Revocation List (CRL);

Publish the CRL issued.

Keep audit logs of the certificate issuance process

An ANL Windows Domain RA

Argonne National Laboratory's Account Services staff will serve as the Registration Authority staff for the ANL Windows Domain PKI. These persons are members of Argonne's Registration Staff.

ANL RA staff is responsible for implementing and ensuring the ANL RA complies with existing Argonne authentication and authorization mechanisms. Additional persons may be appointed to the ANL Windows Domain PKI RA staff by the Laboratory.

Responsibilities:

Authenticate the entity requesting a smart card according to procedures outlined in this document;

Obtain a smart card for issuance to the user;

Using the smart card, submit the certificate issuance request on behalf of the user;

Upon completion of the smart card, enable the user to change the user personal identification number (PIN)

Accept revocation requests according to the procedures outlined in this document;

Authenticate the entity making the certification revocation request according to procedures outlined in this document

Notify the Windows Domain CA when authentication is completed for a certification revocation request and whether the revocation is approved or rejected.

2.1.2 Subscriber Obligations

Subscribers must:

Read and adhere to the procedures published in this document;

Read and adhere to the Argonne National Laboratory Computer Use Policy, Appendix CC of the Cyber Security Program Plan;

Generate a key pair using a hardware token;

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 personal identification number (PIN) with a minimum length of 8 characters
- Protecting the PIN from others
- Never sharing the PIN with other users.
- Never sharing their Windows Domain userid/password with other individuals.

Provide correct personal information and authorize the publication of the certificate

Notify Account Services immediately in case of private key loss or compromise.

Use the certificates for the permitted uses only.

2.1.3 Relying Party Obligations

Relying parties must:

- Read the procedures published in this document;
- Use the certificates for the permitted uses only.
- Do not assume any authorization attributes based solely on an entity's possession of a Windows Domain certificate.

Relying parties may:

- Verify that the certificate is not on the CRL before accepting the certificate;

2.1.4 Repository Obligations

ANL Windows Domain Public Key Infrastructure will provide access to ANL Windows Domain CA information, as outlined in section 2.6.1, on its web site.

2.1.5 Liability

ANL Windows Domain PKI and its agents issue certificates according to the practices described in this document to validate individual identity. No liability, implicit or explicit, for erroneous or incorrect certificates is accepted. ANL Windows Domain denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

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.

2.2 Financial Responsibility

No financial responsibility is accepted.

2.3 Interpretation and Enforcement

2.3.1 Governing Law

This policy is subordinate to all applicable U.S. government laws, as well as Department of Energy (DOE) orders.

2.4 Fees

No fees are charged for ANL Windows Domain PKI Certificates. All costs for operation are covered directly or indirectly by Argonne National Laboratory.

2.5 Publication and Repositories

2.5.1 Publication of CA information

ANL Windows Domain PKI will operate a secure online repository that contains:

ANL Windows Domain CA's certificate;

A Certificate Revocation List;

A copy of this policy

Other information deemed relevant to the ANL Windows Domain PKI.

2.5.2 Frequency of Publication

Certificates will be published to the ANL Windows Domain PKI repository as issued.

CRLs will be published as soon as issued or refreshed once every month if there are no changes.

Component	Location	Frequency
Root Certificate Authority	<p>URI:ldap:///CN=ArgonneNationalLaboratoryRootCA,CN=ANLROOTCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=anl,DC=gov?certificateRevocationList?base?objectClass=cRLDistributionPoint</p> <p>URI:https://credentials.anl.gov/CertData/ArgonneNationalLaboratoryRootCA.crl</p>	26 weeks
Issuing Certificate Authority	<p>URI:ldap:///CN=ArgonneNationalLaboratoryIssuingCA,CN=mouse222,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=anl,DC=gov?certificateRevocationList?base?objectClass=cRLDistributionPoint</p> <p>URI:http://mouse222.anl.gov/CertEnroll/ArgonneNationalLaboratoryIssuingCA.crl</p>	4 weeks

2.5.3 Access Controls

The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.

ANL Windows Domain PKI does not impose any access control on its Policy, its signing Certificate and issued certificates, and its CRLs.

In the future, ANL Windows Domain PKI may impose access controls on issued certificates, their status information and CRLs at its discretion, subject to agreement between the CA, relying parties and subscribers.

2.5.4 Repositories

CA certificate:

CRLs:

CP/CPS:

<https://credentials.anl.gov/CertificatePolicy/rootcp.pdf>

2.6 Compliance Audit

The ANL Windows Domain PKI may be audited by an outside party. The CA operation may be reviewed by any cross certifying organization or potential relying organization if approved by the PMA.

2.7 Confidentiality

ANL Windows Domain PKI collects no new information from subscribers. The ANL Windows Domain PKI relies entirely on information already contained within Argonne National Laboratory's Windows Domain (active directory).

Information included in issued certificates and CRLs is **not** considered confidential.

ANL Windows Domain PKI does not have access to or generate the private keys of a digital signature key pair of subscribers. These key pairs are generated and managed by the client and are the sole responsibility of the subscriber.

2.8 Intellectual Property Rights

Parts of this document are inspired by [INFN CP], [GridCP], [EuroPKI], [TrustID], [NCSA], [PAG] and [FBCA].

Identification and Authentication

2.9 Initial Registration

2.9.1 Types of names

Name components vary depending on the type of certificate. Names will be consistent with the name requirements specified in RFC2459. See section 7.1.4 for more details.

2.9.2 Name Meanings

For individuals, the value of the Common Name (CN) component of the Distinguished Name (DN) will be the userid of the subscriber as determined by the users Active Directory entry.

2.9.3 Uniqueness of Names

The Distinguished Name is unique for each subscriber certified by the ANL Windows Domain PKI.

Certificates must apply to unique individuals or resources.

2.9.4 Method to Prove Possession of Private Key

2.9.4.1 Smart Card Users

Users will create their private key during the smart card issuance process. The key will be generated on the smart card and cannot be transmitted off of the card.

Key generation, certificate request generation, certificate request submission, and certificate issuance are performed during a single session,

At the close of the issuance process, the user will retain possession of the smart card.

2.9.5 Autoenroll Users

Management of the private key for certificates issued under the autoenroll process is left to Microsoft Windows. The user is not directly involved in the creation of the public/private key pair. Windows stores the encrypted private key in the user's profile and is responsible for providing it to applications when needed.

2.9.6 Authentication of Individual Identity

2.9.6.1 Smart Card Users

The ANL Windows Domain PKI relies in person vetting of users prior to approving smart card certificate requests. The vetting is performed by Computing and Information Systems Division Account Services personnel (Registration Authority)

Argonne National Laboratory staff member will be identified by inspection of their badge. Inspection may take place in person by RA staff members or be conducted by a third party intermediary known and trusted by the RA staff. Trust is based on prior operational interaction with the RA staff.

Affiliates will be identified based on an affirmation by an ANL staff member. The staff member will be identified as detailed above.

2.9.6.2 Autoenroll Users

Autoenroll users are vetted by the Windows login process; that is providing their Argonne National Laboratory Windows domain userid and password.

2.10 *Routine Rekey*

No Stipulation

2.11 *Rekey After Revocation*

Rekey after revocation follows the same rules as an initial registration.

2.12 *Revocation Request*

See section 4.4.2 for details on who can request a certificate revocation.

2.13 *Renewal*

2.13.1 *Smart Card Users*

Smart cards are renewed manually when certificates expire. See 3.1.4 and 3.1.5.

2.13.2 *Autoenroll Users*

Autoenroll users are automatically renewed by the Windows login process. Windows detects that a users certificate has expired or will shortly expire and it automatically replaces the certificate. See 3.1.4 and 3.1.5.

3 Operational Requirements

3.1 Certificate Application

Procedures are different if the subject is a person or a host. **In every case the subject has to generate its own key pair.** A key pair must have a minimum key length of 1024 bits.

3.1.1 Smart Card Users

Access to the Registration Manager is by a web browser from the Enrollment Station.

Certificate signing requests (CSRs) are submitted by an online procedure, using Internet Explorer on the smart card enrollment station. The user's smart card will generate the public/private key pair. The registration interface creates the certificate request, and submits the certificate request to the ANL Windows Domain CA.

The certificate is then automatically signed and a copy returned to the user.

The enrollment station software then writes the certificate to the smart card.

3.1.2 Autoenroll Users

Autoenroll users have certificate requests generated for themselves automatically during the logon process. This includes generating the public/private key pair. The certificate request is automatically submitted to the Issuing Certificate Authority.

The resulting certificate is stored in the user's certificate store.

3.2 Certificate Issuance

3.2.1 Smart Card Users

ANL Windows Domain PKI issues the certificate if, and only if, the certificate request is signed by an enrollment agent.

3.2.2 Autoenroll Users

The certificate request is automatically approved by the Issuing Certificate Authority. A certificate is returned to the user's logon process.

3.3 Certificate Acceptance

No Stipulation.

3.4 Certificate Suspension and Revocation

3.4.1 Circumstances for Revocation

A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

The subscriber's smart card is lost or the password protecting the smart card is suspected of being compromised;

The information in the subscriber's certificate is suspected to be inaccurate;

The subscriber no longer needs the certificate to access Relaying Parties' resources;

The subscriber violated his/her obligations.

3.4.2 Who Can Request Revocation

A request to revoke an End Entity Certificate (Person, Host or Service) can be done by the following entities if they can present reasonable evidence that the private key has been compromised or that the subscriber's data is in error:

- A registration agent
- The ANL Windows Domain PKI managers.
- Argonne National Laboratory Management.

The subscriber may revoke (or request revocation of) the subscriber's own certificate for any reason at any time.

3.4.3 Procedure for Revocation Request

The entity requesting the revocation must authenticate itself to the ANL Windows Domain PKI Registration Authority staff. The RA staff will vet the identity of a person making the revocation request.

3.4.4 Circumstances for Suspension

The ANL Windows Domain PKI does not support Certificate Suspension.

3.4.5 CRL Issuance Frequency

CRLs are issued monthly.

3.4.6 Online Revocation/status checking availability

An online status checking facility will not be provided.

3.4.7 Online Revocation checking requirements

No stipulation.

3.4.8 Other forms of revocation advertisement available

No stipulation.

3.5 Security Audit Procedures

Security Audits of the Windows Domain PKI are conducted periodically by third party reviewers. Because the Windows Domain PKI is closely tied to Argonne's Active Directory infrastructure, and review of active directory includes a review of the Windows Domain PKI.

The third party reviewers include

- Department of Energy Inspector General
- Department of Energy Office of Science
- Department of Energy Office of Health, Safety and Security
- Argonne National Laboratory Internal Audit Department

3.6 Records Archival

3.6.1 Types of Event Recorded

The following events are recorded and archived

- Issued certificates;
- Revoked certificates
- Issued CRLs;

3.6.2 Retention Period for Archives

Minimum retention period is three years.

3.7 Key Changeover

No stipulation.

3.8 Compromise and Disaster Recovery

If the ANL Windows Domain CA's private key is — or suspected to be - compromised, the CA will:

1. Inform subscribers and subordinate RAs;

2. Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

3.9 CA Termination

Before ANL Windows Domain PKI terminates its services, it will:

1. Inform subscribers and subordinate RAs;
2. Make widely available information of its termination;
3. Stop issuing certificates and CRLs.
4. Destroy its private key's and all copies.

4 Technical Security Controls

4.1 Key Pair Generation and Installation

4.1.1 Key Pair Generation

Each End Entity must generate its own key pair.

In the case of smart cards users, the public/private key pair is generated on the smart card.

4.1.2 Private Key Delivery to Entity

The ANL Windows Domain PKI never has access to the End Entity private key.

Private keys associated with Person certificates may not be shared between people.

4.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to the issuing CA in a secure and trustworthy manner (e.g. SSL/TLS).

4.1.4 CA Public Key Delivery to Users

CA certificates are delivered by a secure web server.

4.1.5 Key Sizes

Keys of length less than 1024 bits will not be signed.

4.1.6 Public Key Parameters Generation

No stipulation.

4.1.7 Parameter Quality Checking

No stipulation.

4.1.8 Hardware/Software Key Generation

Subscriber public and private keys will be generated by hardware tokens.

4.1.9 Key usage Purposes

ANL Windows Domain PKI certificates are intended for authentication.

The ANL Windows Domain PKI root CA private key will only be used to sign subordinate CAs.

The ANL Windows Domain PKI issuing CA signing key is the only key that will be used for signing end user certificates and CRLs.

The Certificate Key Usage field must be used in accordance with [RFC2459]

4.2 Private Key Protection

4.2.1 Private Key (n out of m) Multi person control

Not supported.

4.2.2 Private Key Escrow

Not supported.

4.2.3 Private Key Archival and Backup

There is no support for Private Key Archival and Backup for End Entity Certificates.

4.3 Other Aspects of Key Pair Management

Component	Key Length (bits)	Validity
Root Certificate Authority	4096	20 years
Issuing Certificate Authority	2048	10 years
Enrollment Agent		1 year
Smart Card Subscriber	1024	2 years
Autoenroll Subscriber	1024	30 days

4.4 Computer Security Rating

The Argonne National Laboratory Windows Domain PKI has a FIPS-199 rating of Moderate.

4.5 Life-Cycle Security Controls

No stipulations.

4.6 Cryptographic Module Engineering Controls

No stipulations.

5 Certificate and CRL Profiles

5.1 Certificate Profile

5.1.1 Version number

X.509 v3.

5.1.2 Certificate Extensions

Basic Constraints (CRITICAL)

not a CA.

Key Usage (CRITICAL)

Digital Signature,

Key Encipherment

1.3.6.1.4.1.311.21.10:

X509v3 Extended Key Usage:

Microsoft Smartcardlogin,

TLS Web Client Authentication

Subject Key Identifier

Authority Key Identifier

CRL Distribution Points

Certificate Policies

1.3.6.1.4.1.311.21.8.7688835.836473.11357352.16714875.15938187.151.1.402

5.1.3 Algorithm Object identifiers

No stipulations.

5.1.4 Name Forms

Issuer: DC=gov, DC=anl, CN=ArgonneNationalLaboratoryIssuingCA;

Smart Card User: DC=gov, DC=anl, CN=Users, CN=windows-userid

Autoenroll User: DC=gov, DC=anl, CN=Users, CN=*windows-userid*

5.1.5 Name Constraints

Not supported

5.1.6 Certificate Policy Object Identifier

OID: 1.3.6.1.4.1.751.75.10.11

5.1.7 Usage of Policy Constraints Extensions

No stipulated.

5.1.8 Policy qualifier syntax and semantics

No stipulated.

5.2 CRL Profile

5.2.1 Version

X.509 v1.

Version 1 is required for compatibility with Netscape Communicator.

5.2.2 CRL and CRL Entry Extensions

No stipulation.

6 Specification Administration

6.1 *Specification Change Procedures*

Users will not be warned in advance of changes to ANL Windows Domain PKI CP.

6.2 *Publication and Notification Procedures*

The policy is available at:

<https://credentials.anl.gov/CertificatePolicy/rootcp.pdf>

6.3 *CP Approval Procedures*

The Computing and Instrumentation Solutions Division is responsible for the ANL Windows Domain PKI CP.

7 Bibliography

[INFN CP] <http://security.fi.infn.it/CA/CPS/> INFN CA Policy and CPS.

[GridCP] <http://gridcp.es.net/> Global Grid Forum CP

[EuroPKI] - EuroPKI Certificate Policy, Version 1.1 (Draft 4), October 2000

[FBCA] - X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999

[NCSA] - National Computational Science Alliance, Certificate Policy, Version 0.9.1, June 30, 1999

[OpenSSL] - <http://www.openssl.org/>

[PAG] American Bar Associations PKI Assessment Guidelines ("PAG")
<http://www.abanet.org/scitech/ec/isc/pag/pag.html>

[RFC2459] - R. Housley, W. Ford, W. Polk and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999

[RFC2527] - S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999

[TrustID] - TrustID Certificate Policy <http://www.digistrust.com/certificates/policy/tsindex.html>

8 List of Changes

VERSION	DATE	CHANGES
1.0	February 1, 2005	Initial Release based on DOE Science GRID CP.
1.1	June 22, 2006	Revised to match the evolution of the service.
1.2	February 5, 2008	Document Autoenroll certificates