

Public Key Infrastructure Certification Practice Statement



Version 1.52a

14. November 2000

Please send all comments and feedback to: pkiadm@sun.com

1. INTRODUCTION

1.....	INTRODUCTION	2
1.1.....	Overview	3
1.2.....	Identification	3
1.3.....	Community and Applicability	3
1.3.1.....	<i>Certification Authorities</i>	3
1.3.2.....	<i>End entities</i>	3
2.....	GENERAL PROVISIONS	4
2.1.....	Obligations	4
2.1.1.....	<i>CA obligations</i>	4
2.1.2.....	<i>Subject obligations</i>	4
2.1.3.....	<i>Relying party obligations</i>	4
2.1.4.....	<i>Repository obligations</i>	5
2.2.....	Liability	5
2.2.1.....	<i>Liability</i>	5
2.2.2.....	<i>Hazardous activities</i>	5
2.2.3.....	<i>Force Majeure</i>	6
2.3.....	Financial Responsibility	6
2.3.1.....	<i>Indemnification by relying parties</i>	6
2.3.2.....	<i>Fiduciary relationships</i>	6
2.3.3.....	<i>Administrative processes</i>	6
2.4.....	Interpretation and Enforcement	6
2.4.1.....	<i>Governing law</i>	6
2.4.2.....	<i>Severability, survival, merger, notice</i>	6
2.4.3.....	<i>Dispute resolution procedures</i>	7
2.5.....	Intellectual Property Rights	7
2.6.....	Amendment	7
2.7.....	Right to Investigate Compromises	7
3.....	IDENTIFICATION AND AUTHENTICATION	7
3.1.....	Initial Registration	7
3.1.1.....	<i>Types of names</i>	7
3.1.2.....	<i>Need for names to be meaningful</i>	8
3.1.3.....	<i>Rules for interpreting various name forms</i>	8
3.1.4.....	<i>Uniqueness of names</i>	8
3.1.5.....	<i>Name claim dispute resolution procedure</i>	8
3.1.6.....	<i>Method to prove possession of private key</i>	8
3.2.....	Routine Re-key	8
3.3.....	Re-key after Revocation	8
3.4.....	Revocation Request	8
4.....	CERTIFICATE AND CRL PROFILES	9
4.1.....	Certificate Profile	9
4.1.1.....	<i>Version number(s)</i>	9
4.1.2.....	<i>Certificate extensions</i>	9
4.1.3.....	<i>Algorithm object identifiers</i>	9
4.1.4.....	<i>Name forms</i>	9
4.1.5.....	<i>Name constraints</i>	9
4.1.6.....	<i>Certificate policy object identifier</i>	9
4.1.7.....	<i>Usage of Policy Constraints extension</i>	9
4.1.8.....	<i>Policy qualifiers syntax and semantics</i>	9
4.1.9.....	<i>Processing semantics for the critical certificate policy extension</i>	9
5.2.....	CRL Profile	10

5.2.1.....	Version number(s)	10
5.2.2.....	CRL and CRL entry extensions	10
6.....	Approval Matrix	10
7.....	Revision History	10

1.1 Overview

This document is the Certification Practice Statement (CPS) for the Sun Microsystems, Inc. (Sun) Public Key Infrastructure (Sun PKI). This CPS provides the general public with information about the practices which Sun follows in creating and using digital certificates issued by Sun-controlled Certification Authorities (CA).

1.2 Identification

Sun Microsystems, Inc. Certification Practice Statement.

Version 1.5 – Last Updated: 14. November 2000

1.3 Community and Applicability

The use of the Sun PKI is for the purpose of conducting business between Sun and other entities, which include (but may not be limited to):

- Systems and network devices – servers, routers, storage, communication;
- Software – system, application, patches, documents.

Certificates are issued and used in accordance with Sun's SecurityIT PKI Policy.

1.3.1 Certification Authorities

There is one top level CA for Sun (referred to as the root level CA in this CPS), whose Distinguished Name (DN) is "C=US, O=Sun Microsystems Inc, CN=Sun Microsystems Inc Root CA". The certificate and its corresponding public key can be found at <http://www.sun.com/pki/rootcacert.html>. Other CAs may be created by Sun for its own use. However, the only CA whose certificate relying parties are required to trust is that of this root level CA.

Sun may choose to contract with any public CA to sign its root level CA public key.

The root level CA certificate will be available in HTML, or as a base64 encoded application/x-x509-ca-cert MIME format.

1.3.2 End entities

The end entities that receive digital certificates from a Sun CA include, but are not limited to:

- Systems and Network devices – servers, routers, storage, communication;
- Software – system, application, patches, documents.

1.4 Contact Details

Michael Borek, PKI Operations Manager
 Sun Microsystems, Inc.
 500 Eldorado Blvd, Bldg 5
 Broomfield, CO 80021
 United States of America

 pkiadm@sun.com

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

Sun CAs issue digital certificates. By issuing a certificate, Sun attests that:

- it has authenticated the identity of the named Subject in the normal course of its business;
- it has issued the certificate to the named Subject;
- the public key in the certificate is paired with a private key that is held by the named Subject;
- the Subject has accepted the obligations detailed in Section 2.1.2, below;
- the Subject has been granted a privilege by Sun to use the certificate for Sun's business purposes only, within the guidelines of Sun's Certificate Policy.

Sun CAs renew certificates, as required, in accordance with Sun's Certificate Policy.

Sun CAs may revoke or suspend digital certificates that they have issued. By revoking or suspending a certificate, the privilege to use the corresponding private key is withdrawn and subsequent use will be in violation of Sun's Certificate Policy. Sun CAs may, or may not, issue another certificate to the named Subject. Sun CAs publish information on the validity of Sun issued certificates. By publishing a certificate and/or a Certificate Revocation List (CRL), Sun attests to the validity of a specific certificate to all relying parties. Sun does not assume any responsibility for the actions of a relying party based on their reliance on a certificate that has been revoked and published as such, or for which a Certification Path cannot be established in the normal course.

2.1.2 Subject obligations

In all cases, the Subject is a non-human Subject in Sun's current PKI Operations implementation. For this reason, the designated administrator (or other person with administrative or business responsibility for that Subject) is responsible for all obligations incumbent on that Subject.

By applying for a certificate under this certificate policy, the designated administrator certifies and agrees that, at the time of certificate application and throughout the operational period of the certificate, until notified otherwise by the designated administrator:

- no unauthorised person has ever had or will have access to the Subject's private key;
- the designated administrator will make all reasonable efforts to protect the private key from unauthorised access;
- the designated administrator will return the private key token they have been issued, if any, to a designated Sun employee or destroy the private key as, and when, directed to do so by Sun;
- all representations made by the designated administrator to Sun's CAs or RAs regarding the information in the certificate are true;
- the certificate and associated keys are being used for authorised and legal purposes, consistent with this CPS and the policies of Sun;
- the designated administrator has read, understood, and agrees to be bound by the terms and conditions of this CPS and the policies of Sun.

2.1.3 Relying party obligations

Responsibility for ensuring that a certificate is used appropriately is the responsibility of the relying party. The certificate user shall use the certificate only in accordance with the certification path

validation procedure specified in ISO/IEC 9594–8 (ITU–T CCITT X.509).

2.1.4 Repository obligations

The Sun PKI maintains repositories of information pertinent to certificate life–cycle operations, as are appropriate for its implementation. Sun represents that these repositories are:

- accessible only to authorised personnel in the PKI Operations Group;
- maintained with the same level of security as the CA infrastructure;
- operated with appropriate controls and procedures to maintain the integrity of the information within them.

The Sun PKI also employs information repositories such as LDAP Directory Services and Web sites. The PKI Operations Group will make reasonable efforts to ensure that these repositories are operated in such a way that changes to PKI related information in such repository are performed by authorised personnel.

2.2 Liability

2.2.1 Liability

SUN MICROSYSTEMS, INC. DISCLAIMS ALL WARRANTIES AND OBLIGATIONS, EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY, AND WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED, AND FURTHER DISCLAIMS ANY AND ALL LIABILITY FOR NEGLIGENCE AND LACK OF REASONABLE CARE.

IN ADDITION, SUN MICROSYSTEMS, INC. DOES NOT WARRANT THE ACCURACY, AUTHENTICITY, RELIABILITY, COMPLETENESS, CURRENCY, MERCHANTABILITY, OR FITNESS OF ANY INFORMATION CONTAINED IN CERTIFICATES ISSUED BY SUN MICROSYSTEMS, INC. OR OTHERWISE COMPILED, PUBLISHED, OR DISSEMINATED BY OR ON BEHALF OF SUN MICROSYSTEMS, INC. SUN MICROSYSTEMS, INC. SHALL NOT INCUR LIABILITY FOR REPRESENTATIONS OF INFORMATION CONTAINED IN A CERTIFICATE ISSUED BY SUN MICROSYSTEMS, INC.

IN NO EVENT SHALL SUN MICROSYSTEMS, INC. BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING FROM, OR IN CONNECTION WITH, THE USE, DELIVERY, LICENSE, PERFORMANCE, OR NON–PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, REVOCATION LISTS, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS, EVEN IF SUN MICROSYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO EVENT SHALL SUN MICROSYSTEMS INC. BE LIABLE FOR THE NON–PERFORMANCE, LOSS, MISUSE, OR ANY OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING FROM THE USE OR MISUSE OF ANY OTHER COMPONENTS USED IN PROVISION OF PKI SERVICES.

2.2.2 Hazardous activities

Sun’s CA services and products are not designed, intended, or authorised for use or resale as control equipment in hazardous circumstances or for uses requiring fail–safe performance such as the operation of nuclear facilities, aircraft navigation, communication, or control systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

2.2.3 Force Majeure

Sun shall not be responsible for any breach of warranty, delay, failure or inability to perform, hereunder, due to acts of God, war or national emergency, epidemic, fire, flood, earthquake, power outages, strikes, riots, and other natural disasters, as well as circumstances and occurrences that are beyond the control of Sun.

2.3 Financial Responsibility

2.3.1 Indemnification by relying parties

All relying parties agree to indemnify and hold harmless Sun Microsystems, Inc. together with its employees, officers, agents, and contractors, from any loss, damage, claim, and any suit of any kind or nature, together with any expenses related to the foregoing, including reasonable attorneys fees and costs, associated with any loss, damage, claim, or suit that arises by the use or publication of a certificate or certificate revocation list, and that arises from:

- any false and misleading information or misrepresentation of fact by the Subject;
- a failure by the Subject to disclose a material fact;
- the failure of the Subject to adequately protect the private key, to use a trustworthy system, or otherwise take reasonable and necessary precautions to prevent the loss, compromise, disclosure, or unauthorised use of the Subject's private key.

2.3.2 Fiduciary relationships

Issuance of certificates in accordance with this CPS does not make Sun an agent, fiduciary, or representative of any Subject or relying parties.

2.3.3 Administrative processes

No administrative processes are applicable since no finances are involved.

2.4 Interpretation and Enforcement

2.4.1 Governing law

Unless otherwise stated, this CPS shall be interpreted and governed by the laws of the State of California, United States of America, excluding its conflict of laws provision.

Various laws and regulations may apply based on the jurisdiction in which a certificate is issued or used. It is the responsibility of the certificate holder to ensure that all applicable laws and regulations are adhered to.

2.4.2 Severability, survival, merger, notice

In the event that any of the terms, conditions, or provisions contained in this CPS are determined invalid, unlawful, or unenforceable to any extent, such term, condition, or provision shall be severed from the remaining terms and conditions which shall continue to be valid and enforceable to the fullest extent permitted by law.

No terms or provision of this CPS directly affecting the rights and obligations of Sun may be orally amended, waived, supplemented, modified, or terminated. Modifications to this CPS will only be issued by an authenticated message or document from Sun.

All the terms and provisions of this CPS shall be binding upon, and inure to the benefit of, the Subject and shall not be assigned by the Subject, whether voluntarily or involuntarily, or by operation of law, in

whole or in part, to any party.

Any notice or document required to be served on Sun or the Subject in relation to the provisions of this CPS may be served at the address contained within this CPS. Any such notice shall be sent by prepaid registered post and, if sent by post, shall conclusively be deemed to have been received 72 hours from the time of posting.

The obligations contained within this CPS shall survive the termination of this CPS.

2.4.3 Dispute resolution procedures

Any dispute relating to this Agreement shall be submitted by the parties for binding arbitration which shall conform to the Commercial Arbitration Rules of the American Arbitration Association and any judgement or award entered therein may be entered in any court of competent jurisdiction. The arbitrator's authority in granting relief is expressly limited by the principles of substantive law and the terms and conditions of this Agreement, including any documents incorporated herein by reference.

2.5 Intellectual Property Rights

Private and public keys that are generated and used within the context of the Sun PKI are the property of Sun.

The certificates may contain copyrighted material, trademarks, and other proprietary information. No copying, reverse engineering, automated browsing or downloading, distribution, publication, or commercial exploitation of the material or information available in or via the certificates is permitted, except as otherwise explicitly permitted under the terms and conditions of this CPS. In the event of any permitted use of copyrighted material, no changes in, or deletion of, author attribution or copyright notice shall be made without written authorisation from the publisher or the copyright owner.

All certificates, software, and/or hardware provided to the Subject for purposes of this CPS are proprietary to Sun and the use of any certificates, software, and/or hardware shall be subject to the provisions of this clause.

2.6 Amendment

Sun may amend this CPS at any time (prospectively and retroactively) and from time to time.

2.7 Right to Investigate Compromises

Sun has, at its discretion, the right to investigate any and all alleged compromises. By applying for certificates issued by Sun CAs, all Subjects authorise the undertaking and scope of such investigations and agree to assist in determining all facts, circumstances, and other pertinent information that Sun deems appropriate, provided that such investigations comply with all applicable privacy and data protection laws. Investigations may include, but are not limited to, interviews, examination of records and other data, and examination of premises and other physical locations.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

Name types and formats may be referenced at <http://www.sun.com/pki/>.

3.1.2 Need for names to be meaningful

All Relative Distinguished Names shall be semantically meaningful within the naming domain of the given level of the Distinguished Name. They shall be easily understood by the relying party, and shall be unambiguous.

3.1.3 Rules for interpreting various name forms

Rules for interpreting the name forms may be referenced at <http://www.sun.com/pki/>.

3.1.4 Uniqueness of names

All Relative Distinguished Names shall be unique at any given level of the Distinguished Name.

3.1.5 Name claim dispute resolution procedure

Name claim disputes for individual Sun employees shall be resolved by Human Resources.

All other name disputes shall be resolved by the PKI Operations Group, and if unsuccessful, by Sun Legal.

3.1.6 Method to prove possession of private key

For Sun personnel and contractors, smart cards will be issued in person by Corporate Security. Access to the PKI to cause keys to be generated and signed requires possession of the smart card and an assigned PIN.

In other cases, the keys will be generated by the key user. The public key being presented for signing shall be signed by the corresponding private key.

3.2 Routine Re-key

The root level CA shall be re-keyed at least every 20 years from the date of adoption of Version 1.0 of this CPS. All copies of the private key for the root level CA shall be irretrievably destroyed at the time of re-key.

Subordinate CAs shall be re-keyed at least every 10 years from the date of adoption of Version 1.0 of this CPS. All copies of the private key for these CAs shall be irretrievably destroyed at the time of re-key.

3.3 Re-key after Revocation

Any public key corresponding to a certificate that is revoked prior to normal expiration shall not be reused again. Consequently, the private key shall be destroyed irretrievably, and a new key pair issued. Sun reserves the right to reuse the token that stores the private key database.

3.4 Revocation Request

The following requests shall be considered sufficient authorisation to revoke a certificate:

- A digitally signed request from the designated administrator of the Subject to revoke a certificate;
- A digitally signed request from a product group to revoke an object signing certificate for one of its products;
- A digitally signed request from a business unit to revoke an SSL certificate for one of its web sites;
- A business requirement from the PKI Operations Group to revoke PKI operations certificates.

4. CERTIFICATE AND CRL PROFILES

4.1 Certificate Profile

4.1.1 Version number(s)

Certificates shall be issued with version numbers that conform to X.509v3.

4.1.2 Certificate extensions

The specific certificate extensions used by the Sun PKI may be referenced at <http://www.sun.com/pki/>.

Wherever possible, only certificate extensions defined in ISO/IEC 9594–8 and ITU–T CCITT X.509 shall be used. Version X.509v3 shall be the reference version.

4.1.3 Algorithm object identifiers

Algorithm object identifiers are defined by the Netscape CMS software.

4.1.4 Name forms

Name forms may be found at <http://www.sun.com/pki/>.

4.1.5 Name constraints

Certificates will be issued with the first components of the Distinguished Name being constrained to O=Sun Microsystems Inc.

The only exception to this is the root level CA certificate in which the first components of the Distinguished Name are constrained to be C=US, O=Sun Microsystems Inc.

4.1.6 Certificate policy object identifier

2.16.840.1.113536.509.2527

Joint–ISO–ITU–t:	2
Country:	16
USA:	840
Organization:	1
Sun Microsystems:	113536
PKI:	509
CPS:	2527

4.1.7 Usage of Policy Constraints extension

The use of the Policy Constraints extension field are located at <http://www.sun.com/pki/>.

4.1.8 Policy qualifiers syntax and semantics

The Policy Qualifiers syntax and semantics are located at <http://www.sun.com/pki/>.

4.1.9 Processing semantics for the critical certificate policy extension

Only critical policy extensions that are defined in the ISO/IEC 9594–8 and ITU–T CCITT X.509 standards shall be used.

If a critical certificate policy extension is encountered that is not understood, then that certificate shall be rejected as not valid.

5.2 CRL Profile

5.2.1 Version number(s)

The CRL version number shall be CRLv2.

5.2.2 CRL and CRL entry extensions

The CRL entry extensions used by the Sun PKI may be found at <http://www.sun.com/pki/>.

6. Approval Matrix

<i>Date</i>	<i>Who</i>	<i>Title</i>	<i>Action</i>
Mar 31, 2000	Mike Borek	PKI Operations Manager	Recommended for Approval
Mar 31, 2000	Chuck Dolci	Legal Counsel	Recommended for Approval
Nov 9, 2000	Tim Townsend	SecurityIT Director	Approve
	Jim Evans	SecurityIT Director	Approve
	H. William Howard	Chief Information Officer	Approve

7. Revision History

<i>Date</i>	<i>Version</i>	<i>Who</i>	<i>Reason</i>
Nov. 7, 2000	Version 1.5	TJTownsend	Policy consistency; scope to first release only.