X.509 Certification Authority Policy & Practices

Higher Education PKI-Lite

Version: 1.0
Last Updated: 2007-11-26
OID: 1.3.6.1.4.1.5923.1.4.1.1

Introduction

The InCommon CA uses the HE-PKI-Lite CP/CPS Template Version 4.7. A URI pointing to this CP/CPS is included in all certificates. In the spirit of PKI-Lite, the CP/CPS is a brief document but one that conveys information sufficient for a PKI-knowledgeable person at a Relying Party institution to determine whether he or she is willing to rely on the CA to meet the needs of a particular application.

1. InCommon Certificate Policy

InCommon will make reasonable efforts to adhere to this policy but assumes only limited liability for policy violations as stated in the InCommon Participation Agreement, available on the InCommon Federation website (www.incommon.org). Parties relying on certificates issued by the InCommon Certification Authority (CA) should study this policy and the associated Certification Practices Statement (CPS) to determine if the assurance level and operational practices are sufficient for the needs of their application. The Higher Education PKI-Lite framework was used in drafting this document.

1.1. Identity

A) Subjects identified in InCommon CA certificates are authenticated using public directories and other reasonable means of establishing a binding between a certificate signing request's subject fields and the requesting entity.

B) Subject names in certificates will uniquely map to InCommon CA participating organizations for the validity period of the certificate. A Relying Party must examine the

associated CPS before making any assumptions about the persistent binding of a certificate Subject name.

1.2. Certificate Revocation

The InCommon CA will revoke certificates. Certificate Revocation Lists (CRLs) will be distributed via HTTP and will be updated one (1) Internet2 business day after certificate revocation requests or every 30 days, whichever is sooner.

1.3. CA Private Key Protection

The InCommon CA has taken reasonable precautions to protect its private keys and has published an outline of these measures in its CPS.

1.4. Subject Key-pair Generation and Private Key Protection

The InCommon CA suggests that the certificate Subject's key-pair be generated by the end-entity. Typically this will be accomplished with software by the end-entity. The key-pair should be generated in a secure environment using best security practices protecting the private key of the Subject. The private key should be securely managed on all media and locations so that the security of the key is not compromised.

1.5. Certificate Profile

The InCommon CA shall issue certificates that conform to the InCommon Certification Authority Server Certificate Profile found in the CPS. This Certificate Policy has been assigned an OID of 1.3.6.1.4.1.5923.1.4.1.1 and certificates will include this OID.

1.6. Certificate Usage

InCommon CA certificates may be used for digital signatures, key encipherment, TLS Web Server and TLS Web Client authentication to support participation in the InCommon Federation.

1.7. Institutional Certification Authority Hierarchy

No stipulation. The InCommon CA will only issue end-entity certificates.

1.8. Certification Practice Statement (CPS)

The InCommon CA uses the HE-PKI-Lite CP/CPS Template Version 4.7. A URI pointing to this CP/CPS is included in the certificate. In the spirit of PKI-Lite, the CPS is a brief document but one that conveys information sufficient for a PKI-knowledgeable person at a Relying Party institution to determine whether he or she is willing to rely on the CA to meet the needs of a particular application.

2.0 InCommon Certification Practices Statement

2.1 CPS Introduction

This statement defines the policies and procedures followed by InCommon for the operation of the InCommon CA in the issuance of Public Key Certificate credentials.

The InCommon CA issues certificates to participants of its federation. See the InCommon Federation Operating Policies and Procedures (FOPP) for more details, available on the InCommon website.

2.2 NO WARRANTY

Although the InCommon CA makes its best efforts to ensure that correct credentials are issued only to appropriate participants of the community, InCommon has no actual control over how participants of the community protect their own credentials. UNDER NO CIRCUMSTANCES IS INCOMMON RESPONSIBLE FOR THE CONSEQUENCES TO A RELYING PARTY OF MAKING USE OF CREDENTIALS INCOMMON ISSUES. INCOMMON OFFERS NO WARRANTY OF ANY KIND AND DISCLAIMS ANY WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE.

Refer to InCommon Federation legal documents for authoritative information.

2.3 CA Private Key Protection

The private key for the InCommon CA is maintained in software on a non-network-connected computer. The private key and its backups are securely managed on all media and at all locations so that the security of the key is not compromised.

Two-factor access control protects the private key at all times. Two officers, one from each of two distinct roles, control each token needed to gain access to the system.

2.4 Authentication upon Registration

The InCommon CA verifies the identity of participants' Executives and Administrators in a way that is generally considered proper and appropriate for a higher education institution.

The following summarizes the registration processes for verifying the identity of Participant Executives and Administrators:

1.0 Participant Executive is named and designated in the Participant Agreement
2.0 Participant Organization submits initial Administrator(s) information via online registration Web form
3.0 InCommon's Registration Authority (RA) independently verifies Executive's phone number through publicly available means.
4.0 RA makes telephone contact with Executive and confirms identity.
5.0 Executive confirms the delegation and information of submitted Administrator(s).
6.0 RA makes telephone contact with Administrator(s), verifying identity information and activating Administrative account(s) for the secure submission of Certificate Signing Requests.

Each Participant Administrator for the InCommon Federation is issued a username and pass phrase which is communicated with them via telephone exchange after acceptance of the application. This user account is required in order to authenticate to the Participant Administrative Interface to manage an organization's participation in the Federation.

The possession of a certificate issued by the InCommon CA implies that at some point the InCommon CA believed that the possessor was a participant of the Federation. However the mere possession of a certificate should not be construed by relying parties that possessor is a current participant in the InCommon Federation or that possessor may legally bind InCommon in any form of negotiation.

2.5 Lifetime of Issued Credential

Certificates are issued to participants of the InCommon Federation by the InCommon CA and are valid from the date of issuance to two years from the date of issuance. Note however that some applications may require, and the CA may choose to issue, certificates that have arbitrarily shorter validity periods.

2.6 Revocation

The InCommon CA revokes certificates via a Certificate Revocation List (CRL). A participant’s Administrator or Executive may request a certificate be revoked. All revocation requests are validated before taking action. In support of the InCommon Federation’s core SAML (see references) construct, metadata is the authoritative location

for certificates and/or certificate information as of January 2008. This metadata file is also kept current as authoritative certificate status information.

2.7 End-Institution Private Key Protection

The InCommon CA does not establish standards for how Participants' private keys are maintained. Keys stored on the hard drives of individually owned or maintained computer systems will likely be as secure (or not) as other information stored on such systems.

Some Institutions may have their preferences files stored in the institutions distributed file system. The security of such stored files will depend on the security of the distributed file system and the strength of the password/key chosen by the Institution to protect the stored file.

3.0 Certificate Profile(s)

3.1 InCommon Certification Authority *Server* Certificate Profile

InCommon Server Cert Profile v20071116				
Field Name	**Value**	**Example**	**Specified**	**Explanation**
Version	0x2	0x2	Yes	A version 3 certificate is specified
Serial Number	a unique integer	334	Yes	An integer that is unique to all certificates issued by the InCommon CA.
Signature Algorithm	SHA1/RSA		Yes	
Issuer	DN	cn=InCommon Certification Authority, o=InCommon Federation, c=US	Yes	
Validity	Time	Not valid before: date Not valid after: date plus two years	Yes	A two year validity period is used by default. A shorter period may be selected in special cases.
Subject	DN	cn=shib.school.edu	Yes	The CN= is the full domain name of the InCommon Shibboleth server at the organization.
Public Key		1024	No	At least a 1024 bit key will be used.
Certificate Extensions				
Key Usage	Digital Signatures and Key Encipherment	Digital signatures and Key encipherment authentication will be asserted	Yes	The extension will be marked critical.
Basic Constraints	CA=false	CA=false	Yes	This extension will be marked critical.

CRL Distribution Points	URI	http://incommoncrl1.incommonfederation.org/crl/eecrls.crl http://incommoncrl2.incommonfederation.org/crl/eecrls.crl	Yes	NonCritical; The InCommon CA will issue CRLs and make them available via http.
Certification Policy	InCommon Policy OID	1.3.6.1.4.1.5923.1.4.1.1	Yes	
CPS Pointer	URI	http://incommonca.incommonfederation.org/practices.pdf	Yes	This certificate practices document will be available on-line in PDF form. PDF was selected to make accidental modification less likely.
Authority Information Access	URI id-ad-caIssuers	http://incommonca1.incommonfederation.org/bridge/certs/ca-certs.p7b http://incommonca2.incommonfederation.org/bridge/certs/ca-certs.p7b	Yes	Two AIA URLs located at different points on the Internet will be specified. The HTTP URL in the AIA field will be a pointer to a PKCS-7 object. When the link is accessed, the web server returns the PKCS-7 file using the MIME type application/x-x509-ca-cert.
Extended Key Usage	Server Authentication Client Authentication	TLS Web Server Authentication and TLS Web Client Authentication will be asserted	Yes	This extension will be marked non-critical
SubjectAlt Name	DNSName	shib.school.edu	Yes	The value for this field is the hostname of the server and must be the same as the CN in the Subject Name.
Subject Key Identifier	KeyID	See RFC-3280 for details	Yes	
Authority Key Identifier	KeyID	See RFC-3280 for details	Yes	

Notes:
Specified column
Yes: The profile specifies the use of this field as documented.
No: The profile does not specify the usage but may recommend a way to use the field.

3.2 InCommon *Root* Certification Authority Profile

InCommon Server Cert Profile v20071116				
Field Name	**Value**	**Example**	**Specified**	**Explanation**
Version	0x2	0x2	Yes	A version 3 certificates is specified
Serial Number	a unique integer	1	Yes	
Signature Algorithm	SHA1/RSA		Yes	
Issuer	DN	Same as Subject - see below	Yes	
Validity	Time	10 Years	Yes	We may re-key every five years.
Subject	DN	cn=InCommon Certification Authority, o=InCommon Federation, c=US	Yes	
Public Key		2048 bit key	Yes	A 2048 or higher bit key will be used
Certificate Extensions				
Key Usage		Certificate Signing , CRL Signing(06)	Yes	The extension will be marked Critical
Basic Constraints	CA=true	Subject Type = CA	Yes	Critical; No Path Length will be specified.
CRL Distribution Points		http://incommoncrl1.incommonfederation.org/crl/eecrls.crl http://incommoncrl2.incommonfederation.org/crl/eecrls.crl	Yes	NonCritical; Two CRL distribution points using servers located at different points on the Internet are specified.
Certificate Policy	InCommon CA Policy OID	1.3.6.1.4.1.5923.1.4.1.1	Yes	Internet2 has allocated a Policy OID for the InCommon CA and will place this OID in all certificates that it issues
CPS Pointer	URI	http://incommonca.incommon	Yes	This certification practices statement will be made

		federation.org/practices.pdf		available on-line in PDF format
Authority Information Access	URI id-ad-caIssuers	http://incommonca1.incommonfederation.org/bridge/certs/ca-certs.p7b http://incommonca2.incommonfederation.org/bridge/certs/ca-certs.p7b	Yes	Two AIA URLs located at different points on the Internet will be specified. The HTTP URL in the AIA field will be a pointer to a PKCS-7 object. When the link is accessed, the web server returns the PKCS-7 file using the MIME type application/x-x509-ca-cert.
Subject Key Identifier	KeyID	See RFC-3280 for details	Yes	
Authority Key Identifier	KeyID	See RFC-3280 for details	Yes	
Notes: Specified column Yes: The profile specifies the use of this field as documented. No: The profile does not specify the usage but may recommend a way to use the field.				

4.0 Acknowledgements

Questions about this Certificate Policy or Certification Practices Statement should be directed to the InCommon Federation at incommon-admin@incommonfederation.org.

Version 1.0 of this CP/CPS was edited by John Krienke, IJ Kim, Nick Lewis, and the InCommon Technical Advisory Committee: RL "Bob" Morgan, University of Washington – Co-Chair; Renee Shuey, Penn State – Co-Chair; Tom Barton, University of Chicago; Scott Cantor, The Ohio State University; Steven Carmody, Brown University; Keith Hazelton, University of Wisconsin – Madison; Ken Klingenstein, InCommon Steering Committee; Mike LaHaye, Internet2; and David Wasley, University of California, Office of the President (ret.).

Nick Lewis drafted the original document with considerable help from IJ Kim, Mike LaHaye, John Krienke, Jim Jokl, Jeff Schiller, RL "Bob" Morgan, Scott Cantor, and HEPKI-TAG.

The original framework for this "PKI Lite" CP and CPS was developed by James Jokl (Virginia), Jeffrey Schiller (MIT), and other members of the HEPKI TAG under the aegis of the Internet2 Middleware activities group. David Wasley (UCOP) created this merged CP/CPS document, adding many enhancements and incorporating changes suggested by

the members of HEPKI-TAG. Eric Norman (Wisconsin), Neal McBurnett (Internet2), and Shelley Henderson (USC) were especially helpful during the creation and review of this document offering many thoughtful suggestions and helping to resolve issues as they were discovered.

5.0 References

HEPKI-TAG PKI Lite CP/CPS:
http://middleware.internet2.edu/hepki-tag/pki-lite/pki-lite-policy-practices-current.html

Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0
http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf