

Version: 0.84

Last Updated: 08-18-2004

2.0 HE-PKI-Lite Certification Practices Statement

2.1. CPS Introduction

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

InCommon Federation issues certificates to participants of its community. This includes participants of the InCommon Federation.

2.2. NO WARRANTY

Although InCommon Federation makes its best efforts to ensure that correct credentials are issued only to appropriate participants of the community, InCommon Federation has no actual control over how participants of the community protect their own credentials. UNDER NO CIRCUMSTANCES IS INCOMMON FEDERATION RESPONSIBLE FOR THE CONSEQUENCES TO A RELYING PARTY OF MAKING USE OF CREDENTIALS INCOMMON FEDERATION ISSUES. INCOMMON FEDERATION OFFERS NO WARRANTY OF ANY KIND AND DISCLAIMS ANY WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE. INCOMMON FEDERATION CANNOT BE HELD LIABLE FOR ANY DAMAGES OF ANY KIND WHETHER DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL EVEN IF INCOMMON FEDERATION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Refer to InCommon Federation legal documents for additional information.

2.3. CA Private Key Protection

The private key for InCommon Federation CA is maintained in software on a non-network connected computer.

[6] employees have access to this key and [2] employees are in a position to issue certificates signed by this key.

2.4. Authentication upon Registration

InCommon Federation verifies the identity of people it issues certificates to in a way that is generally considered proper and appropriate for a higher education institution.

Refer to InCommon Storefront activities documentation for more information about the operation of the storefront.

Each Administrative Contact for the InCommon Federation participant institution will be issued a username and pass phrase which will be communicated with them via a telephone exchange after acceptance of the application. This pass phrase is required in order to authenticate to a certificate signing request, metadata, and revoking service.

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

2.5. Lifetime of Issued Credential

Normally two certificates issued to participants of the InCommon Federation by the InCommon Federation CA and are valid from the date of one day prior to the date of issuance (to avoid time zone problems) until the next December 31st that is more than 2 months and less than 14 months from the date of issuance. This means that in January of each year the fixed expiration date of new certificates issued is updated to be December 31st in the following year. It is therefore possible for some certificates to be valid up to 14 months. Note however that some applications may require, and the CA may choose to issue, certificates that have arbitrarily shorter validity periods.

2.6. Revocation

InCommon Federation does revoke certificates.

InCommon Federation will revoke a certificate when informed by the certificate owner's Administrative Contact that the key associated with the certificate may have been compromised. As a general rule, InCommon Federation does revoke certificates for Institutions who leave InCommon Federation participation.

2.7. End-Institution Private Key Protection

InCommon Federation does not establish standards for how individual institution 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.

2. Certificate Profile(s) for the Institution

InCommon Federation Certificate Profile Server Certificate Profile

From: <http://middleware.internet2.edu/hepki-tag/usher-common/in-common-ee-6.html>

Version: 0.1 with specific branded URI's
Last Update: 03-18-2004

There are changes to the URI's and Issuer DN contained in this profile for branding reasons. It also contains the Certificate Policy OID.

Draft #6: March 16, 2004

InCommon Server (EE) Certificate Profile Summary Table			
Field Name	Value	Example	Explanation
Version	0x2	0x2	A version 3 certificate is specified
Serial Number	a unique integer	334	An integer that is unique to all certificates issued by the InCommon Federation CA.
Signature Algorithm	SHA1/RSA		
Issuer	DN	cn=InCommon Certification Authority, o=InCommon Federation, c=US	
Validity	Time	Not valid before: date Not valid after: date plus one years	A one year validity period is proposed
Subject	DN	cn=shib.school.edu, o=shib.school.edu, c=US	The CN= is the full domain name of the InCommon Shibboleth server at the institution. The O= is the normal name of the university as supplied by the institution when they submit their paperwork for the I&A process. The InCommon RA will ensure that no schools have overlap in the O= field. An

			alternative is to make CN == O to ease the workload on the IN-Common RA.
Public Key		A 1024 bit keypair will be used	
Certificate Extensions			
Key Usage	Digital Signature Key Encipherment	Digital Signature and Key Encipherment will be asserted	The extension will be marked critical.
Basic Constraints	CA=false	CA=false	This extension will be marked critical.
CRL Distribution Points	URI	http://incommoncrl1.incommonfederation.org/crl/eecls.crl http://incommoncrl2.incommonfederation.org/crl/eecls.crl	NonCritical; The InCommon CA will issue CRLs and make them available via http. The CA will issue a new CRL each month and by the end of the next business day after receiving any request to revoke a certificate.
Certificate Policy	InCommon Policy OID	1.3.6.1.4.1.5923.1.4.1.1	
CPS Pointer	URI	http://incommonca.incommonfederation.org/practices.pdf	The redacted public version of the 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-calssuers	http://incommonca1.incommonfederation.org/bridge/certs/ca-certs.p7b http://incommonca2.incommonfederation.org/bridge/certs/ca-certs.p7b	At least two AIA URLs located at different points on the Internet will be specified. See Note 3 below for information on the content of the AIA field.
Extended Key Usage	Server Authentication Client Authentication	TLS Web Server Authentication and TLS Web Client Authentication will be asserted	This extension will be marked non-critical
SubjectAlt Name	DNSName	shib.school.edu	This extension will be marked non-critical. The value for this field is the hostname of the server and must be the same as the CN in the Subject Name.

Notes:

1. The host names in the URLs are simply examples and are likely to change based on branding decisions and available hostnames.
2. Likewise, the email addresses and file names are also just examples and will change as needed.
3. Authority Information Access
The HTTP URL in the Authority Information Access field will be a pointer to a PKCS-7 object. When the link is accessed, the web server will return the PKCS-7 file using the MIME type application/x-x509-ca-cert. The PKCS-7 bundle will contain any appropriate cross-certificates that an application may find useful when in constructing the trust path in a bridged PKI environment.

InCommon Federation Root Certification Authority Certificate Profile

From: <http://middleware.internet2.edu/hepki-tag/usher-common/in-common-root-6.html>

Version: 0.1 with specific branded URI's
Last Update: 03-18-2004

There are changes to the URI's and Issuer DN contained in this profile for branding reasons. It also contains the Certificate Policy OID.

Draft 6: December 17, 2003

InCommon CA Certificate Profile Summary Table			
Field Name	Value	Example	Explanation
Version	0x2	0x2	A version 3 certificates is specified
Serial Number	a unique integer	1	
Signature Algorithm	SHA1/RSA		

Issuer	DN	Same as Subject - see below	
Validity	Time	10 Years	We will rekey every five years.
Subject	DN	cn=InCommon Certification Authority, o=InCommon Federation, c=US	
Public Key			A 2048 bit key will be used
Certificate Extensions			
Key Usage		Certificate Signing , CRL Signing(06)	The extension will be marked Critical
Basic Constraints	CA=true	Subject Type = CA	Critical; No Path Length will be specified.
CRL Distribution Points		http://incommoncr1.incommonfederation.org/crl/eecls.crl http://incommoncr2.incommonfederation.org/crl/eecls.crl	NonCritical; At least two CRL distribution points using servers located at different points on the Internet will be specified.
Certificate Policy	InCommon CA Policy OID	1.3.6.1.4.1.5923.1.4.1.1	Internet2 will allocate a Policy OID for the InCommon CA and place this OID in all certificates that it issues
CPS Pointer	URI	http://incommonca.incommonfederation.org/practices.pdf	A redacted version of the practices document will be made available on-line in PDF format
Authority Information Access	URI id-ad-calssuers	http://incommonca1.incommonfederation.org/bridge/certs/ca-certs.p7b http://incommonca2.incommonfederation.org/bridge/certs/ca-certs.p7b	At least two AIA URLs located at different points on the Internet will be specified. See Note 3 below for information on the content of the AIA field.

Notes:

1. The Issuer may change if the InCommon CA is placed into the USHER hierarchy.
2. The CA will issue a new CRL each month and by the end of the next business day after receiving any request to revoke a certificate.

3. Authority Information Access

The HTTP URL in the Authority Information Access field will be a pointer to a PKCS-7 object. When the link is accessed, the web server will return the PKCS-7 file using the MIME type application/x-x509-ca-cert. The PKCS-7 bundle will contain any appropriate cross-certificates that an application may find useful when in constructing the trust path in a bridged PKI environment.

3. Acknowledgements

Questions about this Certificate Policy or Certification Practices Statement should be directed to INTERNET2 InCommon at incommon-admin@incommon.federation.org.

Nick Lewis drafted this document with considerable help from IJ Kim, Mike LaHaye, Jim Jokl, Jeff Schiller, Bob Morgan, Scott Cantor, and HEPKI-TAG.

The original framework for this CP and CPS was developed by James A. Jokl, Jeffrey I. Schiller, and other members of the HEPKI TAG under the aegis of the Internet2 Middleware activities group.