

Version: 0.33
Last Updated: 08-18-2004
OID: 1.3.6.1.4.1.5923.1.4.1.1

1. HE-PKI-Lite Certificate Policy

InCommon Federation will make reasonable efforts to adhere to this policy but assume no liability for policy violations. Parties relying on certificates issued by the InCommon Federation CA should study this policy and the CA's Practices Statement to determine if the assurance level and operational practices are sufficient for the needs of their application.

1.1. User Identity

Identification, Authentication, and Authorization of contacts for the InCommon Federation identification is described in the Storefront Activities documentation.

Subject names in the certificate will uniquely map to the InCommon Federation participating end entities 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 Federation CA will revoke certificates. CRLs will be distributed via HTTP and will be updated 1 business day after notice or every 30 days.

1.3. CA Private Key Protection

InCommon Federation has taken reasonable precautions to protect the private key(s) and has published an outline of these measures in the CPS.

1.4. Subject Key-pair Generation and Private Key Protection

InCommon Federation CA requires that the certificate Subject's key-pair be generated by the Subject's computer. Typically this will be accomplished with software on the Subjects computer. It may be accomplished with a hardware device such as a smartcard but this is not required.

Once generated, the private key will be encrypted and protected with a pass-phrase. It may be backed up in this form on portable media as long as it remains completely under the control of the Subject. The private key may not be archived by a third party.

1.5. Certificate Profile

InCommon Federation certification authority shall issue certificates that conform to the basic HE-PKI-Lite Certificate Profile. Additional fields or extensions will be included and will be documented in a Certificate Profile for the Institution in the associated CPS.

1.6. Certificate Usage

InCommon Federation certificates may be used for digital signatures and key encipherment to support participation in the InCommon Federation.

1.7. Certification Practice Statement (CPS)

Operators of InCommon Federation certification authority have edited the HE-PKI-Lite CPS Template as needed and will publish their practices statement. A URI pointing to this statement will be included in the certificate's CPSuri extension. 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 they are willing to rely on the CA to meet the needs of their application.

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