X.509 Certification Authority Policy & Practices Higher Education *PKI-Lite*

Draft 4.3: December 19, 2001

Introduction

Discussions within the Higher Education PKI community and with others working in the field suggest that one of the reasons for the slow rate of deployment of PKI is the relatively high overhead associated with building a Certification Authority (CA). While the technical aspects of a full-featured PKI may be complex, they are usually dwarfed by some of the policy and operational constraints often imposed on a PKI designed to support high assurance financial and legal transactions. PKI-Lite focuses on employing PKI technology for standard assurance applications that already have known and implemented requirements for initial user authentication and overall system security. For example, a use for PKI-Lite may be to improve the security of a password-based application by using PKI for authentication instead of passwords. The application's existing process for system security would be used and its practice for identifying the user before creating their password would be satisfied by an equivalent process in the PKI environment. PKI-Lite can also enable standard assurance implementations of newer services such as S/MIME enhanced email. HE-PKI-Lite is the deployment of PKI technology using existing standard campus mechanisms for identifying individuals affiliated with the institution and for securing systems.

Motivation and Philosophy

Many higher educational institutions that operate a campus-wide IT computing infrastructure have had to face the problem of issuing credentials to members of their constituent community. Traditionally this has been in the form of a user-ID and password. We will refer to these as "password" credentials for the purposes of this document. Institutions that issue password credentials often have some policy regarding who may obtain them, how they are issued, how they are changed, both by the credential owner and "forcibly" by the credential administrators (e.g. to deal with a forgotten password).

There are typically two sets of policies: those that are published and those which are operational within the Information Technology (IT) organization, but are not published. For example the published policy may state how often users are expected to change their password while the unpublished policy may state what happens when someone fails to change their password. A better example may be when the published policy states that to have an end-user's password changed manually requires showing up in person with a picture ID. However the unpublished policy may provide for exceptions to this rule. For example, a traveling faculty member who is out of the country but for whom we can establish that the person requesting the change really is that faculty member.

Interoperability

Published policies are often "internal" in the sense that they are made known to the users of the institution's IT infrastructure, but they are not published for the "world." Specifically the institution is not engaging in a contract with the "rest of the world" that it will in fact follow its policies, published or otherwise. In the case of password credentials this makes sense. In general they are only valid to access facilities belonging to the institution and are not valid otherwise.

As we move from password credentials to something stronger and more portable, to wit public key credentials (PKI), we need to address how we have to change policies to make use of the new features of PKI credentials. PKI credentials may be usable by institutions other than the issuing institution. We refer to any entity that accepts PKI credentials generically as a "Relying Party." We need to address what contract, implied or otherwise is being entered into between the PKI credential issuer and a Relying Party.

When an IT department issues credentials that are primarily for use by the institution itself, the credential is not generally viewed as representing a legal contract with potential liability for the institution. In fact if the institution's counsel believed that the act of issuing credentials might result in liability for the institution, there are likely cases where the counsel would recommend against the deployment of a PKI. Password credentials don't normally have any perceived liability associated with them.

Making the issuance of PKI credentials a "risky" operation means that either an institution will avoid PKI solutions, or will install policies and procedures that significantly increase the cost of the credential management business. Yet many institutions are not in a position to significantly increase the cost of operating their authentication infrastructure (if they even think of it in those terms!).

To address this we need a policy that "fits" higher education. We need a solution which can be deployed within the context of an existing IT management organization (aka, no increase in staffing) and which does not bring undue liability upon the institution.

Thus we are driven toward the creation of "PKI Lite." PKI Lite is an attempt to establish a PKI which is "good enough" for higher education's mission and is therefore cost effective to deploy.

Documentation

When setting up a PKI, an institution is expected to publish a "Certificate Policy (CP)" and a "Certification Practices Statement (CPS)." The CP describes the requirements for operation of the PKI and for granting PKI credentials as well as lifetime management of those credentials. The CPS describes the actual steps that an institution takes in implementing the CP. These two statements taken together are designed so that a Relying Party can look at them and obtain an understanding of the trustworthiness of the certification offered by the credential's issuing Certificate Authority (CA).

1. HE-PKI-Lite Certificate Policy

Institutions issuing HE-PKI-Lite X.509 certificates agree that they will make reasonable efforts to adhere to this policy but assume no liability for policy violations. Parties relying on certificates issued by a HE-PKI-Lite 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

HE-PKI-Lite certification authorities agree to use existing campus practice for identifying the certificate Subject before issuing the certificate.

a) People identified in HE-PKI-Lite certificates are authenticated using standard university practices for identifying people for other applications such as issuing user-IDs and passwords for on-campus systems.

b) Subject names in the certificate must uniquely map to the individual for the validity period of the certificate. Furthermore, it is strongly recommended that Subject names uniquely map to the individual in perpetuity regardless of the certificate's validity period but this is not required. 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

HE-PKI-Lite Certification Authorities (CAs) are not required to be able to revoke certificates. However, if a CA issues certificates containing a Certificate Revocation List (CRL) or OCSP distribution point extension, then the CA is obligated to issue CRLs and must update the CRLs and/or OCSP database as specified in the Next Update field of the CRL.

1.3. CA Private Key Protection

Operators of HE-PKI-Lite certification authorities must understand the significance of the CA's private key(s) and take action to protect the key(s) appropriately. On-line CAs are specifically permitted in the PKI-Lite framework to help make user certificates easy to obtain. The operator of the CA is expected to take reasonable precautions to protect the private key(s) and must publish an outline of these measures in their CPS.

1.4. Subject Key-pair Generation and Private Key Protection

HE-PKI-Lite requires that the certificate Subject's key-pair be generated by the Subject's computer. Typically this will be accomplished with software in a standard browser. 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

HE-PKI-Lite certification authorities shall issue certificates that conform to the basic HE-PKI-Lite Certificate Profile. Additional fields or extensions may be included but must be documented in a Certificate Profile for the Institution in the associated CPS. The certificate policy OID should be the generic HEPKI OID for PKI-Lite certificates if and only if all requirements of the PKI-Lite CP are met. Otherwise the institution should arrange for its own OID and define its meaning in the associated CPS.

1.6. Certificate Usage

PKI-Lite certificates may be used for digital signatures and key encipherment. The institution may also choose to allow their use for data encryption but this might raise key escrow and recovery issues. If decryption keys are escrowed, the method should be described in the associated CPS.

A PKI-Lite CA should not issue an authority certificate for another CA.

1.7. Certification Practice Statement (CPS)

Operators of HE-PKI-Lite certification authorities must either edit the HE-PKI-Lite CPS Template below as needed or develop their own CPS and publish their practices statement. A URI pointing to this statement must be included in the certificate's CPSuri extension. In the spirit of PKI-Lite, the CPS should be 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.

2. HE-PKI-Lite Certification Practices Statement

Remove boxed text after creating the institution's version of this document. The following is intended to be a template for a typical institution's CPS. Basic text defines common suggested practices. Some text is enclosed in brackets [ ] to indicate that it is optional. The institution using this template either should adopt one or more of the options suggested or delete the bracketed section.

{INSTITUTION} should be replaced with the name of the institution adopting this CPS.

{N}, {X}, etc. should be replace with appropriate numbers or text.

2.1. CPS Introduction

This statement defines the policies and procedures followed by {INSTITUTION} in the issuance of Public Key Certificate credentials.

{INSTITUTION} issues certificates to members of its community. This includes Faculty, Staff and Students [and Alumni]. [In addition {INSTITUTION} may issue a modest number of certificates to others who maintain a loose affiliation with the institution but who are not officially listed as Faculty, Staff or Students [or Alumni]].

2.2. NO WARRANTY

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

2.3. CA Private Key Protection

The private key for {INSTITUTION}'s CA is maintained

Choose the text below describing the institution's method.

in tamperproof hardware.

in non-tamperproof hardware.

in software on a non-network connected computer.

in software on a network connected computer.

[X] employees have access to this key and [Y] employees are in a position to issue certificates signed by this key. [In cases where the key is stored in hardware, {INSTITUTION} can make no representation of the strength of that hardware protection, it is a user of technology provided by [vendor] and cannot provide assurances beyond what [vendor] has provided]

2.4. Authentication upon Registration

In general {INSTITUTION} verifies the identity of people it issues certificates to in a way that is generally considered proper and appropriate for a higher education institution. Specifically:

Describe the steps that are required by an end-entity to obtain a certificate.

Example:

Each member of the community is issued a pass phrase which is printed and mailed to them via a postal mail. This pass phrase is required in order to authenticate to a certificate issuing website. Exactly how and when this mailing is performed depends on the class of end-user.

Students receive their pass phrases at their home address prior to arriving on campus. In addition the Student Services organization can issue a new pass phrase to students who appear personally at the Student Services Center with appropriate ID.

Faculty and Staff generally receive their pass phrase from personnel in their home department as part of the orientation provided a new employee. Students who transition to Faculty or Staff keep their existing credentials.

[The following is optional (but probably important):

The possession of a certificate issued by {INSTITUTION} implies that at some point {INSTITUTION} believed that the possessor was a member of its community. However the mere possession of a certificate should not be construed by relying parties that possessor has a current association with {INSTITUTION} or that possessor my legally bind {INSTITUTION} in any form of negotiation.]

2.5. Lifetime of Issued Credential

The renewal period of “June-July” and the maximun validity period of 14 months can be adjusted to meet specific campus needs. Validity periods longer than 15 months are strongly discouraged.

Normally certificates issued to individuals by {INSTITUTION}'s CA are valid from the date of one day prior to the date of issuance (to avoid time zone problems) until the next July 31st that is more than 2 months and less than 14 months from the date of issuance. This means that in June of each year the fixed expiration date of new certificates issued is updated to be July 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. Certificates issued to individuals will not have validity periods longer than 14 months.

[The following is an optional, simpler version:

Certificates issued by {INSTITUTION}'s CA are valid for no more than {N} months from the date of issuance.]

2.6. Revocation

Choose whichever one of the following applies:

{INSTITUTION} does not revoke certificates.

[{INSTITUTION} does revoke certificates.

If revocation supported:

{INSTITUTION} revokes certificates via a Certificate Revocation List [and/or the use of the On-line Certificate Status Protocol (OCSP)]. {INSTITUTION} will revoke a certificate when informed by the certificate owner that the key associated with the certificate may have been compromised. As a general rule, {INSTITUTION} does not revoke certificates for people who leave the employment of {INSTITUTION} or who are no longer students. Certificates for such people will eventually expire. Under some unusual circumstances the certificate of a departing individual may be revoked.

In general certificates for people who have lost their private key will not be revoked as such certificates are useless already and revoking them adds no overall value to the community at large.

2.7. End-User Private Key Protection

{INSTITUTION} does not establish standards for how individual private keys are maintained. It is expected that many keys will be stored in browser preferences files as many end-users obtain their credentials via a web browser. 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 users may have their preferences files stored in the campus 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 user to protect the stored file.

3. Certificate Profile(s) for the Institution

[Insert the PKI-Lite profile here]

4. Acknowledgements

Questions about this Certificate Policy or Certification Practices Statement should be directed to {the responsible office} at {INSTITUTION}.

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.