USHER

Higher Education PKI Certificate Authority

The U.S. Higher Education Root (USHER) is a Public Key Infrastructure (PKI) for the higher education community. Under the direction of the USHER Policy Authority, USHER supports PKI for applications and services in research, education, and business transactions in higher education that require security, encryption, or true digital signature technologies.

The root certificate authority that offers flexibility for the U.S. higher education community's growing needs

Introducing USHER

The USHER Certificate Authority (CA) is designed to facilitate the inter-institutional use of PKI throughout the higher education community. USHER supports PKI-enabled applications that require the same general level of identity management security and practices that central campus computing groups already use when they issue email accounts, provide access to individual disk storage, personal calendar access, and other similar services. USHER extends the intra-campus PKI-Lite model for use with inter-institutional applications.

Policies and Subscriber Authority CAs

USHER supports a range of lightweight PKIs. USHER identifies eligible higher education institutions and their partners and issues each an authority certificate for its use. The organization itself decides what certification policy, if any, it asserts in the certificates it issues. USHER does not require an audit of the organization's CA and does not make any statement about its practices.

Relying parties base their assurance assumptions either on the USHER community's Expected Practices document or on direct agreements with the issuing organization.

A campus may use the policy OID associated with the existing PKI-Lite policy/practices document in its certificates if it conforms to PKI-Lite.

FAQ

Q. Why should an organization subscribe to USHER ?
By subscribing to USHER, eligible organizations will be able to base PKI applications and services in a common root with peers and collaborative partners. Additionally, USHER charges a single annual fee for an USHER authority certificate. There is no limit on the number or type of certificates a subscriber can use.

Q. Who is eligible to subscribe to USHER?
U.S. Higher Education Institutions and their partners. Institutional subscribers must be listed with one of the U.S. Department of Education's regional accrediting institutions. Partners — organizations, corporate partners, and international institutions — must be sponsored by an USHER institutional subscriber and be approved by the USHER Policy Authority.

Q. Can a campus have multiple CAs under USHER?
Yes, multiple campus groups could apply for USHER authority certificates. Also, an existing campus CA under USHER could issue an authority certificate to another campus identity provider as long as this type of delegation is consistent with the existing general campus practices for identity management.

Q. Is the USHER root preloaded into any browsers?
Not at this time, but one of USHER's goals is to have a root certificate preloaded into as many browser and application root stores as possible.

Q. Does USHER audit subscribing organizations' policies and practices?

USHER does not audit or in any other way validate the policy or practice that a subscriber uses to issue certificate credentials to its users. Instead, USHER has developed a set of Expected Practices for campus CA operators to consider. USHER is designed to support a community of like-minded higher education institutions and partners, and choosing to join this community implies that your organization intends to work within the framework of the Expected Practices.

Q. What about the security and practices of USHER itself?

The USHER CA operates at a relatively high level of assurance. Operations are housed at Internet2, which also runs the PKI for the InCommon Federation.

Q. Is there an USHER CA for organizations that desire a stronger form of assurance?

USHER is designed to be a broadly adoptable PKI. It is designed for easy implementation by leveraging most existing campus identity practices. If there is demand for a stronger level of assurance from the community, USHER will consider operating a CA which enforces a higher level of assurance.

Q. Is the USHER CA a separate CA from any higher assurance USHER CA that may be brought on-line in the future?

Past discussions in HEPKI-TAG regarding the lack of installed PKI software that actually leverages policy OIDs led to the conclusion that these should be separate CAs. The USHER Policy Authority (PA) will need to make a decision in this area at a later date.

Q. Will USHER cross certify with other PKI hierarchies or the HEBCA bridge CA?

USHER's objective is to increase deployment of PKI based on each organization's self-asserted practices and policies. Trust throughout the hierarchy cannot be verified by the PA. Therefore, it is not clear at this time whether USHER will be eligible to cross certify with any other PKI. The USHER PA will continue to listen to the needs of the community.

Q. Who comprises the USHER Policy Authority?

The USHER Policy Authority is composed of individuals representing the broad interests of the U.S. higher education research and education community. A full list of the USHER Policy Authority is available on the USHER website.

www.usherca.org