Agency Best Practices for Device Certificates

Federal agencies are increasingly reliant on X.509 device certificates to provision security services over agency networks. Several agencies have requested guidance from the Federal PKI Policy Authority with respect to Federal PKI requirements, especially regarding certificate policies. This memorandum is intended to clarify the FPKIPA's position regarding issuance of device certificates by agency CAs.

Does the FPKIPA need to approve the certificate policy for my agency device certificates?

This depends on the intended use of these certificates.

The FPKIPA reviews certificate policies to establish mappings with the Federal Bridge CA (FBCA) certificate policies. This is required if the certificates will be validated by other parties using the FBCA. If the device certificates will only be used internally, validation need not involve the bridge. If the device certificates are intended for use only within your agency, the FPKIPA need not review your certificate policy.

What certificate policy does the FPKIPA recommend for agency use when issuing device certificates?

Where device certificates are intended for internal use, the FPKIPA does not recommend any particular certificate policy. However, several member agencies, including HHS and NASA, have developed certificate policies for such device certificates and have made these certificate policies available for use as a template. Agencies issuing device certificates for internal use are encouraged to use one or more of these device certificate policies as a template, rather than developing their own certificate policy from scratch.

The FPKIPA maintains a certificate policy for device certificates, *id-fpki-common-devices*, as part of the Common Policy Framework. If the device certificates will be validated by other entities, the FPKIPA recommends issuing certificates under *id-fpki-common-devices*. As with all certificate policies in the Common Policy Framework, the FPKIPA reviews and approves operations of all CAs issuing certificates under this policy; this process is time-consuming and relatively complex. Agencies that wish to obtain device certificates issued under *id-fpki-common-devices* should consider procuring certificates from an approved Shared Service Providers.

Alternatively, an Agency may choose to issue device certificates under an agency-specific policy that can be validated through the FBCA. In this case, the FPKIPA will map the device certificate policy to one of the levels of assurance defined in the FBCA CP. As above, this process can be challenging; for details regarding the mapping process see the FPKIPA website. Where agencies choose to develop their own device certificate policy, they are strongly encouraged to select one of the FBCA assurance levels as a target and use the FBCA CP as development tool.

Why is a separate certificate policy for device certificates necessary?

Agencies are not required to maintain a separate policy for device certificates. Both the FBCA CP and the FCPF provide for issuing certificates to devices, in the latter case to include a specific policy OID. Therefore, agencies do not necessarily need to develop and/or cross-certify a separate policy specifically for device certificates.

When should device certificates expire?

The FPKIPA recommends a device certificate lifetime of one year, where permitted by operational considerations. Agencies should set a certificate lifetime of 1 to 3 years, depending upon the level of human interaction required to renew their device certificates. In many cases, device certificates can be automatically renewed by the CA without human involvement. In such cases, a relatively short certificate lifetime, such as one year, will help control the size of certificate revocation lists. Where device certificates cannot be automatically renewed, a longer certificate lifetime may be appropriate. Regardless, the certificate lifetime must not exceed three years.

Which cryptographic algorithms and key sizes should I use to sign my device certificates?

Agencies are required to use Approved cryptographic algorithms, as specified in Federal Information Processing Standards, when signing digital certificates. Digital signature algorithms and hash algorithms are specified in FIPS 186-2 and FIPS 180-2, respectively. Guidance on key sizes may be found in NIST SP 800-57 Part 1.

Where agencies issue one-year device certificates, the FPKIPA recommends generation of digital signatures using RSA (1024 or 2048 bits) and the SHA-1 hash algorithm through December 31, 2009. The FPKIPA recommends generation of digital signatures using RSA (2048 bits) and the SHA-256 hash algorithm on one-year device certificates issued on or after January 1, 2010.

Where agencies issue three-year device certificates, the FPKIPA recommends generation of digital signatures using RSA (1024 or 2048 bits) and the SHA-1 hash algorithm through December 31, 2007. The FPKIPA recommends generation of digital signatures using RSA (2048 bits) and the SHA-256 hash algorithm on three-year device certificates issued on or after January 1, 2008.