Fannie Mae
Enterprise Certificate Services
Frequently Asked Questions (FAQ)

July 1, 2017

1. What is the Enterprise Certificate Service?

The Fannie Mae Enterprise Certificate Service provides certificates and certificate management, based on X.509 Version 3 certificates, through a formal Fannie Mae service line, and is provided and maintained under a Fannie Mae Certificate Policy (CP).

2. Can you provide samples of where certificates are used?

The following are sample types of digital certificates:

a. SSL/TLS certificates for securing communication within Fannie Mae and between Fannie Mae and external partners
b. Code signing certificates
c. Certificates for securing email communications
d. Document/email signing certificates
e. Certificates for the encryption of data and documents
f. Authentication Certificates (client identity certificates)
g. Secure Shell (SSH)

3. What is required from digital certificate users?

Users who have received or would like to receive certificates from our Enterprise Certificate Service are responsible for:

a. Ensuring their certificates are currently valid (not expired)
b. Staying aware of where their certificates are implemented
c. Protecting private keys of issued digital certificates

4. What are Fannie Mae's requirements regarding its digital certificates?

Fannie Mae requires digital certificates to adhere to the following requirements:

a. All digital certificates must comply with the X.509 standard
b. All digital certificates must be issued by a reputable certificate authority (CA); wildcard and self-signed certificates are NOT approved for use with Fannie Mae Data and Fannie Mae IT Services
c. Certificates are issued with an expiration of no longer than three years

5. What is required by Fannie Mae regarding encryption algorithms?

Fannie Mae's digital certificate encryption algorithms adhere to the following requirements:

- Symmetric encryption algorithms
  a. AES with 128- or 256-bit keys (preferred)
  b. Triple-DES with 168-bit keys
- Asymmetric encryption algorithms
  a. RSA2 with 2048-bit keys
- Hashing algorithms
  a. SHA-256

6. Why should certificates be upgraded from SHA-1 to SHA-2?

In 2002, SHA-2 became the new recommended hashing standard. SHA-1 hash has been shown to suffer cryptographic weaknesses and was officially deprecated by NIST in 2011. Digital-certificate-consuming devices and applications will begin to display warnings/errors or operationally fail if a digital certificate containing the SHA-1 (or earlier) hash is presented.

7. Who can I contact for questions?

Questions regarding the Fannie Mae Enterprise Certificate Service, please email us. We will respond within 48 hours.

Appendix

1. What are self-signed certificates?

In cryptography and computer security, a self-signed certificate is an identity certificate that is signed by the same entity whose identity it certifies. This term has nothing to do with the identity of the person or organization that actually performed the signing procedure. In technical terms a self-signed certificate is one signed with its own private key. While self-signed SSL Certificates also encrypt customers' log in and other personal account credentials, they prompt most web servers to display a security alert because the certificate was not verified by a trusted Certificate Authority.

2. What is SHA-1?

SHA-1 is a secure hash algorithm first published in 1995, which produces a 160-bit hash value. In 2005, it was found vulnerable to collision attacks and has been deemed as an insecure algorithm.

3. What is SHA-2?

SHA-2 algorithm was introduced in 2001 which includes hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256). It carries major changes from the forerunner SHA-1 algorithm. The encryption hash used in SHA-2 is significantly stronger and not subject to the same vulnerabilities as SHA-1.

4. What are “wild card” certificates?

A wildcard SSL certificate allows you to secure your main domain and all first level sub-domains of that domain. Wildcard certificates can easily be identified by the asterisk which precedes the domain name in the certificate subject field (for example, *.domain).

5. What is OpenSSH ?

OpenSSH is the connectivity tool for remote login with the SSH protocol. It encrypts all traffic to eliminate eavesdropping, connection hijacking, and other attacks. In addition, OpenSSH provides a large suite of secure tunneling capabilities, several authentication methods, and sophisticated configuration options.