SAML SSO - Self-Signed Certificates to replace CA-Signed Certificates

A few years ago we added an option in Alma's SAML integration profile to choose between a self-signed certificate and a certificate signed by DigiCert.

Before doing so, the only available certificate was a self-signed one, with an expiry period of 7 years. Later, we added the option for the DigiCert one, and we can see that some customers selected to use it.

Because of recent industry changes, we will deprecate the use of DigiCert certificates in Alma's SAML. Instead, starting November 2025 Release, the self-signed certificate will be enhanced with a shorter expiry date (3 years) and longer key (4k).

SAML certificates differ from SSL (TLS) certificates, which are used for browser applications and managed by the server. Cryptographically, there is no difference between self-signed and certificate authority (CA)-signed certificates if they use the same algorithm and key length. From a SAML perspective, they are equivalent as outlined in the SAML V2.0 Metadata Interoperability Profile (**https://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop-os.pdf**):

"In the case of an X.509 certificate, there are no requirements as to the content of the certificate apart from the requirement that it contain the appropriate public key. Specifically, the certificate may be expired, not yet valid, carry critical or non-critical extensions or usage flags, and contain any subject or issuer. The use of the certificate structure is merely a matter of notational convenience to communicate a key and has no semantics in this profile apart from that."

The InCommon Federation, a pioneering and one of the largest SAML federations, encompassing around 550 SAML identity providers and 6200 SAML service providers (https://incommon.org/community-organizations/), advocates for long-lived, self-signed certificates (https://spaces.at.internet2.edu/display/federation/saml-metadata-cryptographic-keys):

"The use of long-lived, self-signed certificates in Federation metadata is strongly RECOMMENDED. Certificates with lifetimes of at least 10 years are RECOMMENDED to avoid unnecessary technically-imposed deadlines on key rollover."

Using long-term certificates offers several advantages:

- **Stability and Reliability**: Long-term certificates ensure a stable and reliable authentication mechanism. By reducing the frequency of renewals, you minimize disruptions and maintain continuous service.
- **Operational Efficiency**: Long-term certificates lessen the administrative burden of frequent renewals, allowing IT teams to focus on other critical tasks, thereby enhancing productivity and efficiency.
- **Cost-Effectiveness**: Extending the validity period of certificates can lead to cost savings in certificate management and renewal processes, which is beneficial for organizations with limited resources.

Many prominent technology corporations and academic institutions recommend or default to long-term certificates.

For more information, see SAML-Based Single Sign-On/Sign-Off.