Identity Provider Key Rollover

The term key rollover refers to a process whereby one key is systematically replaced by another key in SAML metadata. Since SAML entities (and therefore SAML metadata) are distributed, key rollover must be deliberate, so as not to break the key operations of a relying party.

The general process of rolling over a metadata key in an IdP without causing unnecessary downtime is as follows. The following describes the process in detail for Shibboleth IdPs. The information can be used as inspiration for other IdP implementations.

1. Create a new key pair for signing metadata
2. Add the new KeyDescriptor to your metadata
3. Send the new metadata to Operations and wait for the newly updated metadata to propagate throughout the Federation
4. Reconfigure the IdP software to use the new key (instead of the old key) as the signing key
5. Remove the old KeyDescriptor from your metadata and send the new metadata to Operations

If you need to replace the SSL/TLS key, you do not need to send anything to Operations. If you have a Apache front-end then you need to create the key, CSR and import the signed certificate into Apache's configuration. If you use Tomcat or another Java container, use keytool and update the server.xml. Restart Apache/Tomcat.

Further information:

- Shibboleth.net wiki: Identity Provider Key Rollover
- SWITCH: Shibboleth Identity Provider Certificate Rollover