Certificate Migration in Metadata

Certificate Migration in Metadata

In the last few months, InCommon Operations has encountered two significant interoperability “incidents” (but it is likely there were others we didn’t hear about) that were subsequently traced to improper migration of certificates in metadata. When migrating certificates in metadata, site administrators are advised to carefully follow the detailed processes documented in the wiki. These processes have been shown to maintain interoperability in the face of certificate migration, which tends to be error prone.

Of particular importance is the migration of certificates in SP metadata since a mistake here can affect users across a broad range of IdPs (whereas a mistake in the migration of a certificate in IdP metadata affects only that IdP’s users). When migrating a certificate in SP metadata, the most common mistake is to add a new certificate to metadata *before* the SP software has been properly configured. This causes IdPs to unknowingly encrypt assertions with public keys that have no corresponding decryption keys configured at the SP. A major outage at the SP will occur as a result.

Another issue we’re starting to see is due to increased usage of Microsoft AD FS at the IdP. As it turns out, AD FS will not consume an entity descriptor in SP metadata that contains two encryption keys. To avoid this situation, the old certificate being migrated out of SP metadata should be marked as a signing certificate only, which avoids any issues with AD FS IdPs. See the Certificate Migration wiki page for details.

Please share this information with your delegated administrators. By the way, if you’re not using delegated administration to manage SP metadata, please consider doing so since this puts certificate migration in the hands of individuals closest to the SP.