Memo

Working Group: Document Management System Working Group

Date of Resolution: September 15, 2020

Members involved: Astellas (Devry Spreitzer), GSK (Tosin Sule), Trans Sped (Cezar Ignat), McDougall Scientific (Daniel McKenna), Carillon (Patrick Patterson), IdenTrust (Jeff Hutchison), AstraZeneca (Aaron Fier)

Memorandum ID: DMSWG002

Problem statement/challenge to be addressed:
The problem of usability in the context of signing PDF documents relates to the case when the user has multiple credentials that are present inside the key store and the signing software does not provide any guidance to the user about which certificate(s) he should be using to sign the document.

Proposed Options and/or Discussions:
This problem can be solved in multiple ways:
- The signing software would allow the user to define criteria for the selection of the default signing credential that could be based on a specific issuer, key usage, certificate assurance level, and other criteria. The criteria could also allow defining priorities for listing the credentials. When no criteria are present, the signing software would process the available credentials in the key store and order the credentials in a standard way across all certified signing software.
- Conversely, the credential issuer could adjust the subject names for end entity issued certificates to include a description (e.g. [SAFE or EXTERAL or SIG]) that indicates to the users that a particular certificate is SAFE's compliant or suffices for external use. The user is more likely to choose the correct certificate when multiple certificates are present for signing if the name of the certificate helps users choose the correct certificate.

Resolution/Decision:
SAFE has adopted both of the above proposed solution options by:

1. Including test cases in the PDF Signature Test Specification under the usability track where the signing software is tested for its ability to order signing certificates in a way that helps end users select the most appropriate certificate. Preference is given to a default signing credential above all other criteria. Secondary criteria includes key usage, extended key usage and cryptographic strength. This criteria can be found in section 13 of the PDF digital signature specification.

2. SAFE recommends that its certified issuers offer the ability to add extra information in the subject name field in their human issued certificates to guide end users to easily select the most appropriate certificate for document signing.

Links to Artifacts associated with the Resolution:
- [PDF Digital Signature Specification](#).