

Postup ako prepojiť aplikáciu QES s ľubovoľným systémom na správu dokumentov

V prílohe "testQes.zip" sú testovacie údaje: napríklad na podpísanie „testSignPdfCreateAsic.qcfg“

Súbor je identifikovaný cez postupnosť „FILE, HASH a NOTICE“.

Konfiguračný súbor pozostáva z postupnosti dvojíc: súbor na podpísanie – súbor podpisu.

Prvá postupnosť „FILE, HASH a NOTICE“ identifikuje súbor, ktorý sa má podpísať (Žlto).

Druhá postupnosť „FILE, HASH a NOTICE“ identifikuje súbor, do ktorého sa má podpis uložiť.

Text v NOTICE napr. „=Content-Type: application/vnd.etsi.asic-e+zip“ identifikuje typ podpisu a musí sa presne zhodovať s možnosťami:

- ASiC-S - „=Content-Type: application/vnd.etsi.asic-s+zip“
- ASiC-E - „=Content-Type: application/vnd.etsi.asic-e+zip“
- CMS AdES externý - „=Content-Type: application/pkcs7-signature“
- CMS AdES interný - „=Content-Type: application/pkcs7-mime“
- PDF AdES - „=Content-Type: application/pdf“
- XML AdES enveloped - „=Content-Type: application/xml“
- The format of the document timestamp is selected according to the "Content-Type: application/vnd.etsi.timestamp-token" specified in "NOTICE=x" of the signature file "FILE=x", where:
 - The timestamp is ASiC if the signature file extension is one of the ASiC extensions.
 - The timestamp is PDF document timestamp if the signature file extension is ".pdf" extensions.
 - In the other cases the timestamp is the document timestamp "*.tst".

Ak v „*.qcfg“ už existuje súbor s podpisom, tak sa do neho pridá ďalší podpis a ak neexistuje, tak sa vyhotoví nový súbor.

ASiC sa vyhotovuje ako posledný.

V príklade sa najprv vyhotovia podpisy:

- Test.docx.p7s
- Test.docx.p7m
- PdfTest.pdf

A na záver sa vyhotoví ATest.asice, ktorý podpíše Test.pdf a PdfTest.pdf.

„testSignPdfCreateAsic.qcfg“ obsahuje v „META-INF\dms.cfg“ s obsahom:

```
FILE=Test.pdf
HASH=
NOTICE=Content-Type: application/pdf
FILE=ATest.asice
HASH=
NOTICE=Content-Type: application/vnd.etsi.asic-e+zip
FILE=PdfTest.pdf
HASH=
NOTICE=Content-Type: application/pdf
FILE=ATest.asice
HASH=
NOTICE=Content-Type: application/vnd.etsi.asic-e+zip
```

FILE=Test.docx
HASH=
NOTICE=Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
FILE=Test.docx.p7s
HASH=
NOTICE=Content-Type: application/pkcs7-signature
FILE=Test.docx
HASH=
NOTICE=Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
FILE=Test.docx.p7m
HASH=
NOTICE=Content-Type: application/pkcs7-mime
FILE=PdfTest.pdf
HASH=
NOTICE=Content-Type: application/pdf
FILE=PdfTest.pdf
HASH=
NOTICE=Content-Type: application/pdf

Možnosť predávať všetky údaje v jednom balíku zo systému na správu dokumentov do QES aplikácie a následne to z QES aplikácie aj v jednom balíku zaslať späť, pričom pre koncovku balíku bude asociácia na spustenie QES aplikácie v systéme a podporujú sa 3 režimy:

1. podpísanie,
2. zobrazenie podpísaných dokumentov a
3. validácie vybraného podpisu.

Použije sa ZIP premenovaný na "*.QCFG".

Koreňový adresár v ZIP bude obsahovať súbory na podpis a teda aj podpisy buď externé, interné a aj prípadne ASiC-E/S súbory a identifikácia podpisu v súbore "*.DSId".

Adresár META-INF obsahuje txt konfiguračný súbor s koncovkou "*.CFG" zhodný ako pri volaní s parametrom -c pre vyhotovenie podpisu a FILE= obsahuje len meno súboru v hlavnom adresári bez cesty.

Po podpise sa vždy uloží aj identifikátor podpisu "*.DSId" do koreňového adresára.

Pre zobrazenie sa v ZIP nebude nachádzať "*.CFG" a zobrazia sa dokumenty zabezpečené podpisom identifikovaným jedným "*.DSId".

Validáciu si zobrazí užívateľ po zobrazení podpisu identifikovaného "*.DSId".

Aplikácia zatiaľ nemá validáciu úplne implementovanú a aj tak je potrebné volať kvalifikovanú validačnú službu, ktorá sa nachádza v dôveryhodnom zozname.

Zip QCFG bude otvorený exclusive celú dobu.

Ak by nastala chyba, výsledná veľkosť QCFG súboru bude 0, inak aktualizovaná veľkosť. K súborom podpisu pribudnú v QCFG aj súbory s identifikáciou podpisu *.DSId pre správny výber podpisu v ASiC a PDF, keďže oba kontajnery môžu obsahovať rôzne dokumenty a podpisy. Teda pre každý nový podpis sa vyhotoví *.DSId na identifikáciu pre zobrazenie zabezpečených dokumentov.