5.2. Spoločná autorizácia elektronických dokumentov

V tejto súvislosti uvádzame technickejšiu špecifikáciu spoločnej autorizácie dokumentov:

Pri spoločnej autorizácii externe podpísaného dokumentu (napr. rozhodnutie v XAdES_ZEP alebo ASiC) a nepodpísaného dokumentu (napr. XML doložka právoplatnosti) sa obvykle podpisujú iba samotné dokumenty bez ich pôvodných podpisov. Do XAdES_ZEP alebo ASiC obsahujúceho už podpísaný dokument sa len doplní ďalší dokument a ďalší paralelný podpis. Nepodpisuje sa teda podpis pôvodného dokumentu ale len samotný pôvodný dokument bez podpisu.

(Pozn.: eIDAS však umožňuje podpisovať aj podpis pôvodného dokumentu.)

Pri spoločnej autorizácii priamo podpísaného dokumentu (napr. PDF rozhodnutie s PAdES) a nepodpísaného dokumentu (napr. XML doložka právoplatnosti) sa podpisuje aj pôvodný podpis. Obvykle sa vytvorí XAdES_ZEP, ZEPf alebo ASiC obsahujúci spoločne externe podpísané dokumenty, pričom tieto dokumenty môžu byť zároveň priamo podpísané.

Pre informáciu:

XAdES_ZEP je slovenský formát podpisového kontajnera, ktorý je nutné prestať vytvárať lebo je celý v rozpore s eIDAS,

ZEPf je slovenský formát podpisového kontajnera, ktorý je potrebné prestať vytvárať aj keď obsahuje podpis v súlade s eIDAS,

ASiC je eIDAS formát podpisového kontajnera, pričom podpisy môžu byť uložené aj mimo kontajnera.

Zobrazovanie spoločne autorizovaných dokumentov je už dnes podporované v elektronických schránkach na ÚPVS a tiež napríklad v aplikácii D.Viewer (poskytovanej na stiahnutie z ÚPVS a integrovanej do prostredia elektronickej schránky).

Vytváranie spoločne autorizovaných dokumentov je zatiaľ na ÚPVS podporované len cez služby (používané napríklad registratúrami, špecializovanými portálmi alebo rezortami ktoré majú elektronické schránky u seba).

Klikateľné používateľské rozhranie pre vytváranie spoločnej autorizácie na portáli ÚPVS sa momentálne pripravuje. Klikateľné používateľské rozhranie pre spoločnú autorizáciu však už existuje - napríklad ho má SAK pre osvedčovacie doložky zaručenej konverzie.

Pri spoločnej autorizácii sa zjednodušene deje zhruba toto:

1. - Vypočítajú sa jedinečné digitálne odtlačky tých dokumentov, ktoré sa majú spoločne podpísať, pričom digitálny odtlačok je vždy jedinečný pre konkrétny dokument.

Počítajú sa hašovacou funkciou ako je napríklad SHA256.

Pozn. 1: Ak sa dokument zmení, jeho digitálny odtlačok bude iný než bol pred zmenou.

Pozn. 2: Pri niektorých formátoch podpisových kontajnerov (napr. ASiC-S, ZEPf) sa spoločne podpisované dokumenty vkladajú do jedného súboru (napr. do súboru .zip alebo .eml) a až z tohto súboru sa počíta digitálny odtlačok.

2. - Do predpísanej štruktúry (vyplývajúcej z použitého formátu podpisu a podpisového kontajnera) sa zapíšu digitálne odtlačky dokumentov.

3. - Vytvorí sa podpis, ktorý podpíše štruktúru obsahujúcu digitálne odtlačky dokumentov (prípadne jeden digitálny odtlačok ak boli spoločne autorizované dokumenty pred autorizovaním uložené v jednom súbore).

4. - Podpis sa spolu s predpísanou štruktúrou uloží v príslušnom formáte (napr. ZEPf, XAdES_ZEP, ASiC-S, ASiC-E, PAdES, XAdES enveloping/enveloped, CAdES enveloping/enveloped).