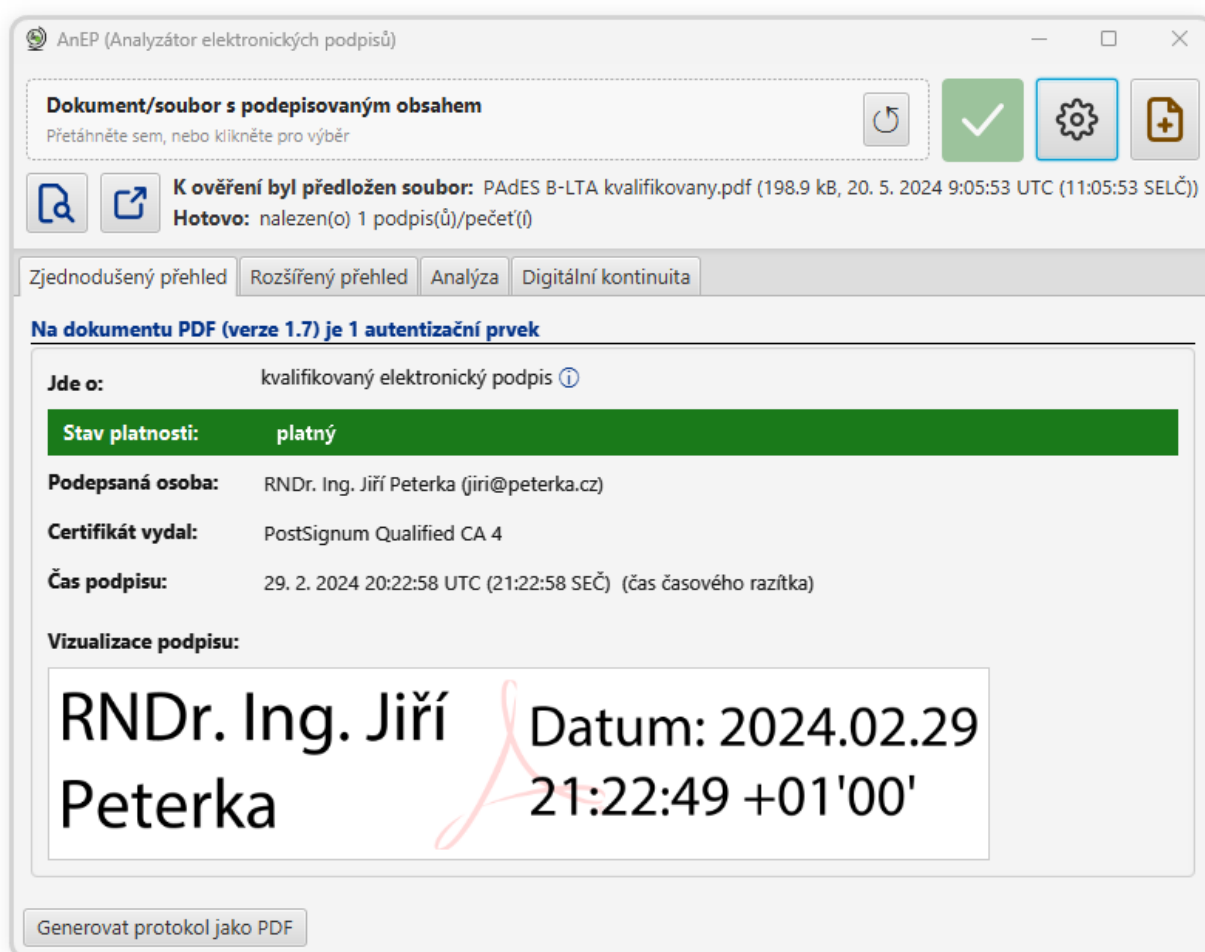


AnEP

Analýzátor elektronických podpisů

Nástroj pro ověřování elektronických podpisů a pečeti, pro analýzu a vysvětlení výsledků ověření, i pro udržování digitální kontinuity

Windows · desktopová aplikace · jádro ověřování DSS (Evropská komise) · rozhraní česky · licence EUPL-1.2



Obrázek 1 Hlavní okno aplikace s kladným výsledkem ověření

Z pohledu standardů ETSI je aplikace AnEP tzv. Driving Application (DA), zatímco vlastní ověřování provádí knihovna DSS (Digital Signature Service) jako tzv. Signature Validation Application (DVA).

Obsah

1 K čemu je AnEP

Tři možné výsledky · Pro koho je určen

2 Co aplikace přečte

Nosiče a formáty · Zvláštní případy při čtení

3 Práce s aplikací

Hlavní okno · Co se děje při ověření

4 Šest záložek

Zjednodušený přehled · Rozšířený přehled · Analýza · Digitální kontinuita · Detailní rozbor · Protokoly DSS

5 Důvody: popis problému a jeho řešení

Z čeho se důvod skládá · Ukázka · Proč se důvody navzájem potlačují

6 Vlastní prohlížeče

Rychlý náhled · Prohlížeč kontejnerů · Prohlížeč certifikátů · Prohlížeč seznamů CRL · Prohlížeč odpovědí OCSP · Přílohy dokumentu · Kudy se k prohlížečům dostat

7 Důvěra a revokační

Odkud pochází důvěra · Revokační údaje · Vlastní zásoby

8 Přísnost a ústupky

Čtyři ústupky · Dvě samostatná nastavení · Jednorázová politika · Rozhodující ústupek

9 Není digitální kontinuita jako digitální kontinuita

Možné přístupy k ověřování · Co určuje datum · Když lhůtu stanovit nelze · O čem informuje záložka

10 Co aplikace může udělat s dokumentem a jeho podpisy

Možnosti prodloužení digitální kontinuity · Souběh více podpisů · Forenzní balíček · Kdy se úkon nenabídne

11 Protokoly

Tři protokoly · Dvě volby

12 Zvláštní obsahy

Datové zprávy ISDS · Evidenční záznamy · Výstupy z eLegalizace · Vizualizace podpisu · Prázdná podpisová pole · Protipodpis · Podpisy v OOXML

13 Nastavení a úložiště

Základní nastavení · Pokročilé nastavení · Zdroje časových razítek · Kde aplikace ukládá svá data

14 Dostupnost a licence

Distribuce a spuštění · Licence

15 Kde jsou hranice

A Dodatek: pojmy, které dokument používá

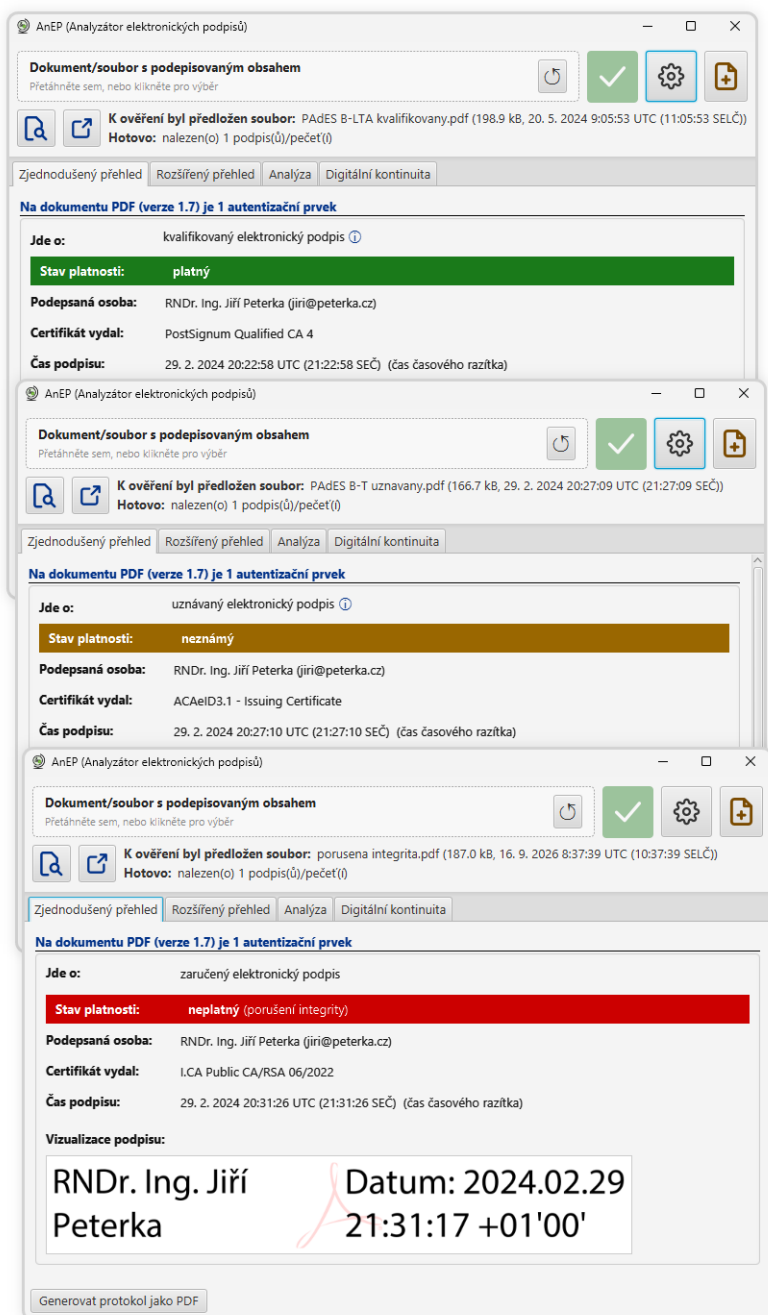
1 K čemu je AnEP

AnEP ověřuje elektronické podpisy, pečeti a časová razítka podle nařízení **eIDAS** a norem **ETSI** — a hlavně vysvětlí výsledek srozumitelně někomu, kdo není odborník na elektronické podpisy a PKI.

Vlastní ověřování obstarává otevřená knihovna **DSS** Evropské komise, tedy referenční implementace ETSI EN 319 102-1. Aplikace AnEP nad ní staví to, co DSS záměrně nedělá: mění strohé INDETERMINATE/REVOKED_NO_POE ve větu, která říká, co se stalo, proč, a co se s tím dá dělat.

1.1 Tři možné výsledky

Výsledek ověření má tři podoby a každá nese svou barvu, kterou pak drží celá aplikace i protokol:



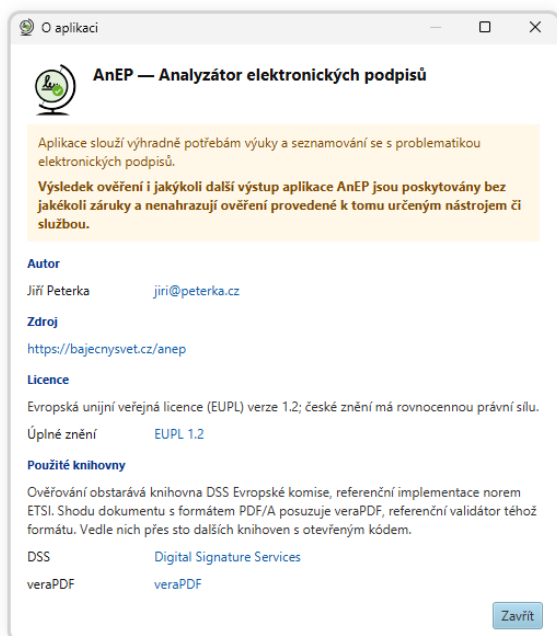
Obrázek 2 Tři barvy výsledku, jak je aplikace ukazuje ve Zjednodušeném přehledu

Výsledek	Co znamená
platný (zelená)	Platnost se podařilo prokázat za pravidel, za kterých se ověřovalo. Pokud se o to zasloužil povolený ústupek, je to u výsledku napsáno.
stav platnosti neznámý (žlutá)	Není to závěr o neplatnosti. Platnost se nepodařilo prokázat — a aplikace vždy řekne, co konkrétně chybělo a jestli to jde ještě opatřit.
neplatný (červená)	Podpis prokazatelně neobstál: porušená integrita, nesprávná dvojice souboru a podpisu, revokace prokázána k rozhodnému okamžiku.

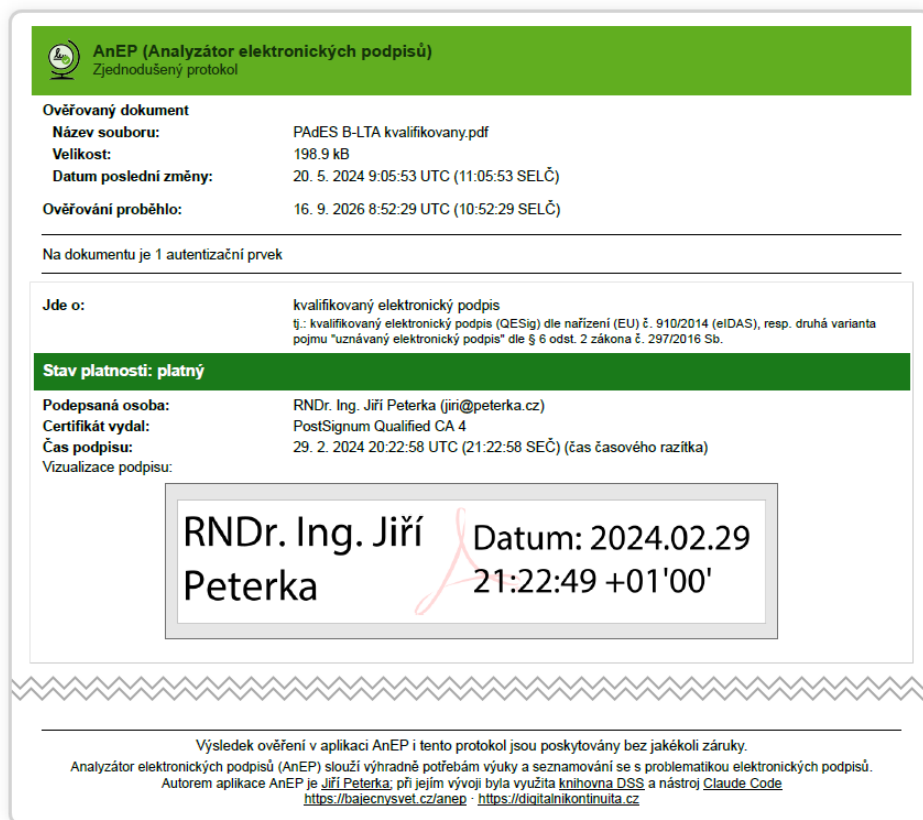
Prostřední případ je ten podstatný. Většina nesází s elektronickými podpisy nekončí slovem „neplatný“, ale tím, že chybí důkaz — a rozdíl mezi „neplatné“ a „neprokázané“ je přesně to, co běžné nástroje zamlčují.

1.2 Pro koho je určen

Pro toho, kdo dostal podepsaný dokument a potřebuje vědět, na čem je: pro úředníka, archiváře, právníka i pro zvědavého uživatele. Aplikace přitom slouží také k seznámení s problematikou elektronických podpisů — proto u každého pojmu, který použije, řekne, co znamená. Své výstupy vydává **bez záruky**; říká to okno „O aplikaci“ i každý protokol.



Obrázek 3 Okno „O aplikaci“



Obrázek 4 Příklad protokolu o výsledku ověření (v PDF)

2 Co aplikace přečte

Formát se pozná podle **obsahu souboru, ne podle přípony**. Přejmenovaný soubor tedy aplikaci nezmate a kontejner uvnitř kontejneru se otevře také.

2.1 Nosiče a formáty

Nosič	Co v něm aplikace ověří
PDF s interními podpisy	PAdES všech úrovní (B-B až B-LTA), včetně podpisů PDF-NOT-ETSI z doby před eIDAS, podpisů PKCS #7 a časových razítek
ASiC-S / ASiC-E kontejnery	.asice, .asics, .sce, .scs i prosté kontejnery .zip
Externí i obalující podpisy	CAdES (.p7s, .p7m, .cms), XAdES (.xml), JAdES (.json, .jose, .jws)
Datové zprávy	.zfo — zprávy ISDS i doručanky
ODF dokumenty	ODT, ODS, ODP — podpisy XAdES v META-INF/document-signatures.xml
Kancelářské OOXML	DOCX, XLSX, PPTX — podpis se neověřuje , ale aplikace nahlédne dovnitř (viz kapitola 12)
Evidenční záznamy	RFC 4998 (.ers, .er) a XMLERS, samostatné i vložené v dokumentu
Holý certifikát, CRL, OCSP	nejsou to podepsané dokumenty, a tak se neověřují — otevřou se rovnou ve vlastním prohlížeči (kapitola 6)

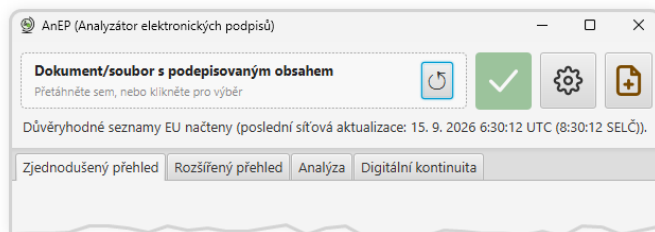
2.2 Zvláštní případy při čtení

- **Externí podpis či evidenční záznam** — přiloží se jako druhý soubor; aplikace pro něj má tlačítko, fungující jako druhé vstupní pole.
- **Heslem chráněné PDF** — aplikace si o heslo řekne, ale až tehdy, když bez něj dokument opravdu neotevře. Na heslo, které čtení nebrání, se neptá.
- **Dokumenty s přílohami** — aplikace upozorní na existenci příloh, otevře prohlížeč a nabídne možnost pracovat s jednotlivými přílohami.
- **Prázdné podpisové pole** — pole připravené k podpisu, ve kterém zatím podpis není, se vypíše také, včetně toho, jestli by bylo vidět a co by po podpisu uzamklo.
- **Detekce a kontrola formátu PDF/A** – aplikace detekuje a ověřuje dílčí formát PDF/A i jeho varianty
- **Vizualizace případných změn po podepsání** – aplikace detekuje a uživateli ukáže případně vizuální změny po podepsání obsahu (např. anotace)

3 Práce s aplikací

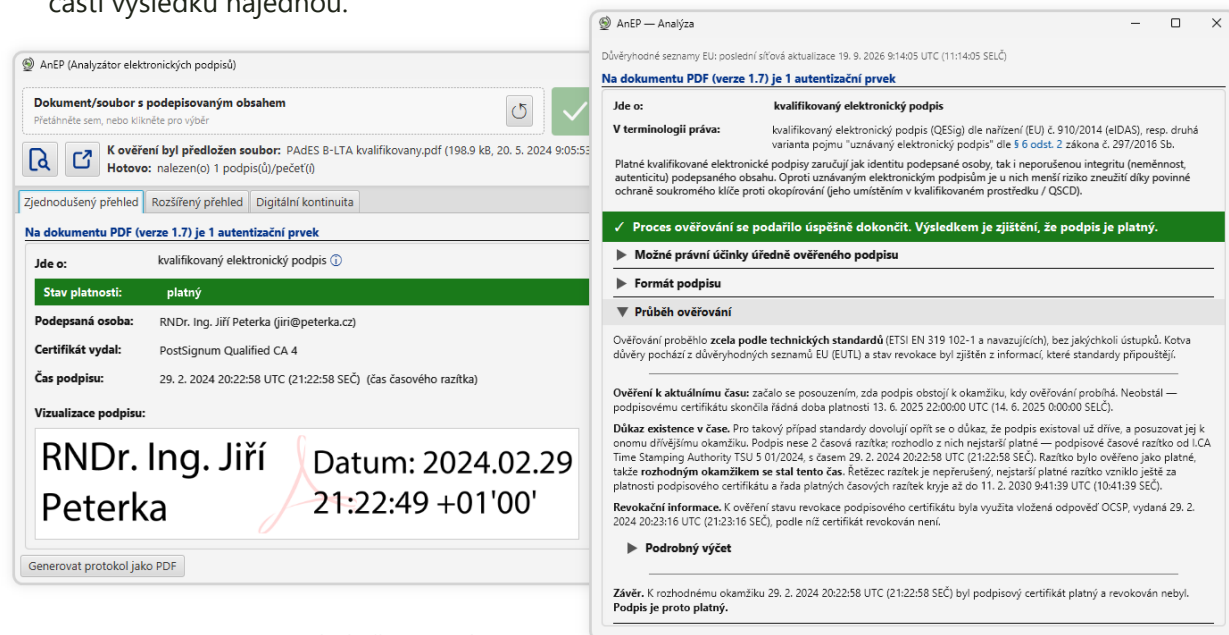
3.1 Hlavní okno

Okno má vlevo nahoře hlavní vstupní pole pro soubor s ověřovaným dokumentem a vedle něj tři tlačítka, pod nimi stavový řádek a pod ním záložky s výsledkem.



Obrázek 5 Záhloví aplikace, před zadáním vstupu

- **Vstupní pole pro dokument** — soubor s dokumentem se do něj přetáhne, nebo se klepnutím vybere.
- **↻ Obnovit naposledy zadaný obsah** — tlačítko v pravém rohu hlavního vstupního pole; vrátí poslední dvojici souborů, aby se ověření dalo zopakovat po změně nastavení bez opětovného zadávání vstupů.
- **Ověřit** — pokud je tlačítko sytě zelené, lze jím spustit ověření. Pokud je bledě zelené, je nutné nejprve zadat vstupy.
- **Nastavení** — otevře nabídku nastavení.
- **Externí obsah** — tlačítko pro externí podpis nebo pro evidenční záznam k předloženému dokumentu. Dokud je prázdné, je tiché; s načteným souborem se rozsvítí.
- **Stavový řádek** jmenuje ověřený soubor, jeho velikost a počet nalezených prvků a nabízí, co k němu patří: otevřít jej v přidružené aplikaci, otevřít jako kontejner a podívat se dovnitř, ukázat přílohy dokumentu i s jejich počtem.
- **Záložku lze odpojit** do vlastního okna (pravé tlačítko na jejím oušku) a mít tak vedle sebe více částí výsledků najednou.



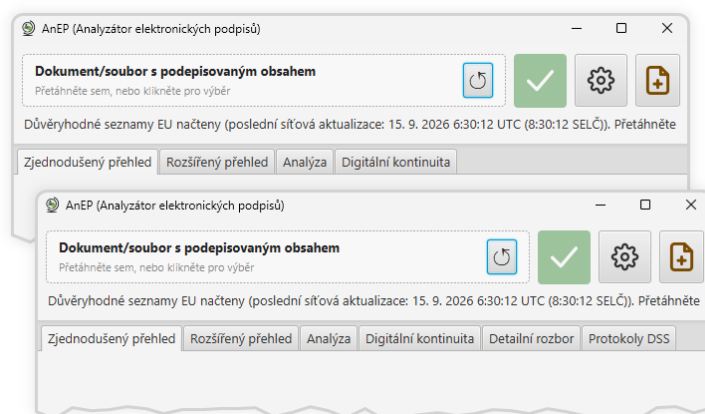
Obrázek 6 Odpojená záložka „Analýza“

3.2 Co se děje při ověření

Ověření běží na pozadí, okno zůstává ovladatelné a průběh je vidět. Start aplikace nečeká na síť: důvěryhodné seznamy se drží v místní mezipaměti a jejich čerstvost se dokontroluje až za běhu. Chybí-li důvěryhodné seznamy některé země nebo jsou-li uložené seznamy staré, řekne to aplikace sama.

4 Šest záložek

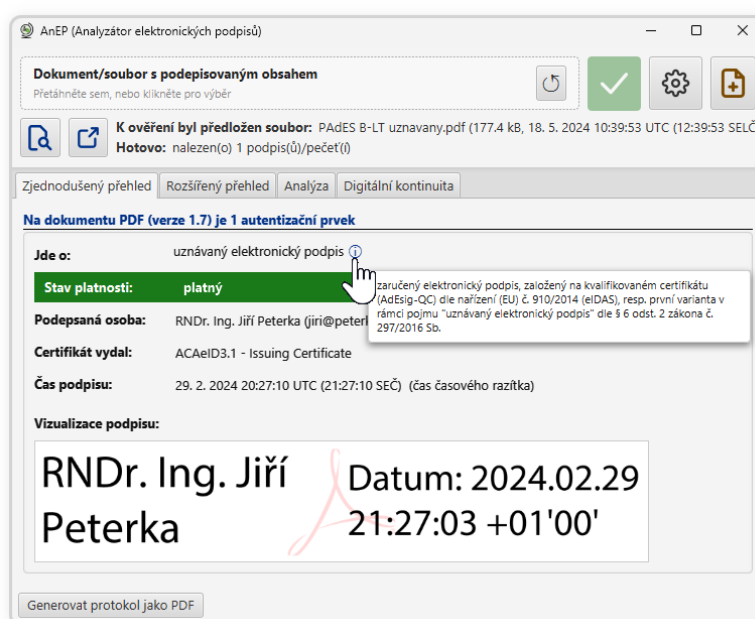
Řazeno podle hloubky. První čtyři vidí každý, poslední dvě se ukazují jen v **expertním módu**.



Obrázek 7 Záložky v základním módu (nahore) a v expertním módu (dole)

4.1 Zjednodušený přehled

Verdikt, druh prvku i s výkladem pojmu (zaručený, uznávaný, kvalifikovaný), podepsaná osoba, vydavatel certifikátu, čas podpisu a vizualizace podpisu tak, jak ji nese PDF. Kdo chce jen odpověď, dál už jít nemusí.

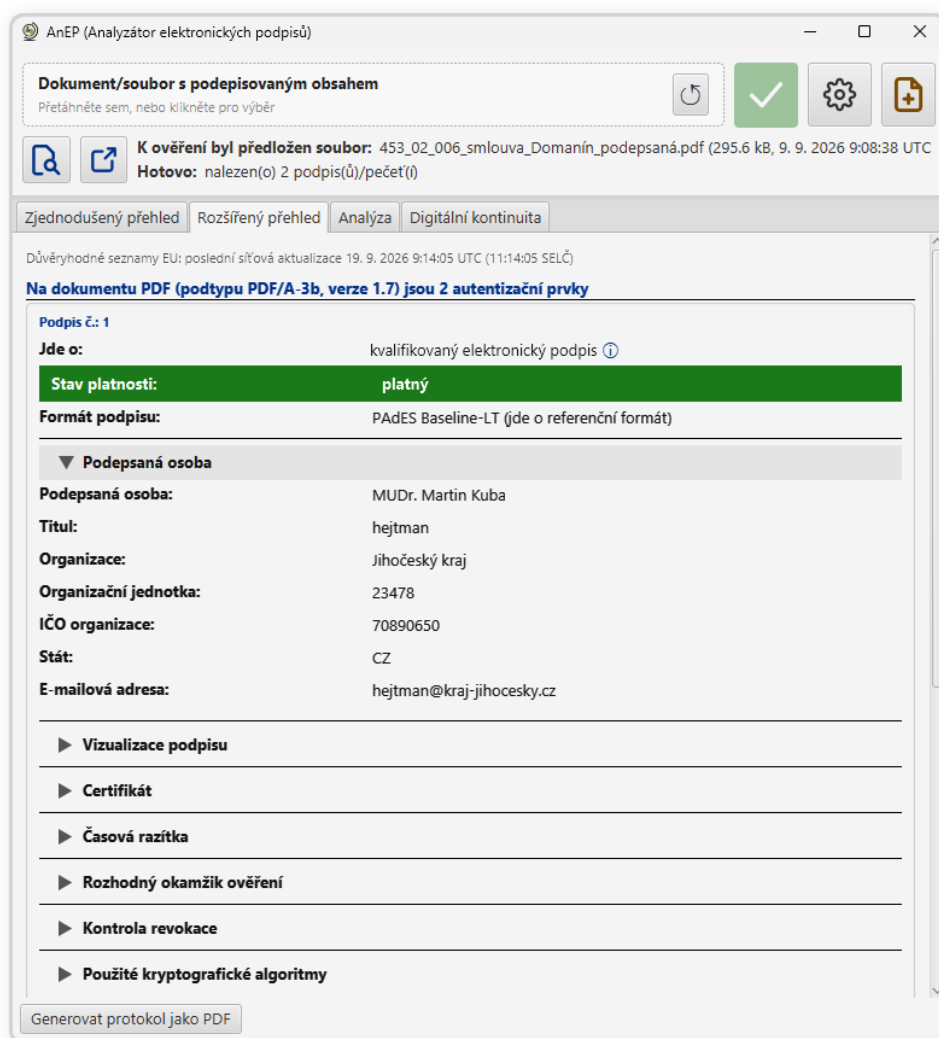


Obrázek 8 Záložka „Zjednodušený přehled“

4.2 Rozšířený přehled

Totéž v devíti pojmenovaných rozbalovacích blocích:

- podepsaná osoba (u pečeti pečetící osoba, u razítka vydavatel razítka),
- vizualizace podpisu,
- důvody podpisu — tedy to, co podepsaná osoba uvedla jako důvod, místo a kontakt,
- certifikát,
- časová razítka — u každého i to, kdo je vydal a do kdy platí jeho certifikát
- evidenční záznamy,
- rozhodný okamžik ověření,
- kontrola revokace,
- použité kryptografické algoritmy.



Obrázek 9 Záložka „Rozšířený přehled“

Pokud je právě ověřován dokument, který se odkazuje na jiné dokumenty v rámci eLegalizace (dle § 6 odst. 1 písm. a) zákona č. 12/2020 Sb.), přibývá ještě desátý blok pro odkazované dokumenty.

4.3 Analýza

Proč to dopadlo takhle. Pro každý podpis, pečeť či samostatné razítko: podle toho, jak ověření dopadlo a o čem je u konkrétního dokumentu co říct, se v ní objeví tyto bloky:

Blok	Co v něm stojí
Formát podpisu	Druh formátu, zapouzdření, úroveň a odpověď na otázku, jestli jde o referenční formát podle prováděcího rozhodnutí Komise (EU) 2015/1506.
Zjištěné důvody a doporučení	Očíslované důvody — co se stalo a co s tím. Celá kapitola 5.
Průběh ověřování	Za jakých pravidel se ověřovalo, jak aplikace postupovala a čím to skončilo; uvnitř složený Podrobný výčet revokačních informací, které měla po ruce, s odkazy „Ukaž“ a „Ulož“ u každé z nich.
Poznámky k výsledku	Co na výsledku stojí za zmínku, i když to verdikt nezměnilo. Uvnitř podblok s připomínkami, které měla sama knihovna DSS.
Možné právní účinky	Jen tam, kde připadají v úvahu — u platného kvalifikovaného či uznávaného elektronického podpisu odkaz na čl. 25 eIDAS a na § 6 zákona č. 12/2020 Sb.
Certifikační podpis	Že podpis certifikuje dokument a jaké změny po sobě povolil.
Zámek dokumentu	Co podpis uzamkl a v jakém rozsahu, je-li dokument uzamčen.
Protipodpis (kontrasignatura)	U podpisu, který podepisuje jiný podpis, se řekne čím a co z toho plyne.
Kde je šance na úspěšné ověření	Kterým dalším nástrojům a službám se ověření může podařit a kterým ne — jde o odhad (možnost), ne o jistotu.

Na dokumentu je 1 autentizační prvek

Jde o: kvalifikovaný elektronický podpis

V terminologii práva: kvalifikovaný elektronický podpis (QESig) dle nařízení (EU) č. 910/2014 (eIDAS), resp. druhá varianta pojmu "uznávaný elektronický podpis" dle § 6 odst. 2 zákona č. 297/2016 Sb.

Platné kvalifikované elektronické podpisy zaručují jak identitu podepsané osoby, tak i neporušenou integritu (neměnnost, autenticitu) podepsaného obsahu. Oproti uznávaným elektronickým podpisům je u nich menší riziko zneužití díky povinné ochraně soukromého klíče proti okopírování (jeho umístěním v kvalifikovaném prostředku / QSCD).

✓ **Proces ověřování se podařilo úspěšně dokončit. Výsledkem je zjištění, že podpis je platný.**

► **Možné právní účinky úředně ověřeného podpisu**

► **Formát podpisu**

▼ **Průběh ověřování**

Ověřování proběhlo **zcela podle technických standardů** (ETSI EN 319 102-1 a navazujících), bez jakýchkoli ústupků. Kotva důvěry pochází z důvěryhodných seznamů EU (EUTL) a stav revokace byl zjištěn z informací, které standardy připouštějí.

Ověření k aktuálnímu času: začalo se posouzením, zda podpis obstojí k okamžiku, kdy ověřování probíhá. Neobstál — podpisovému certifikátu skončila řádná doba platnosti 10. 9. 2024 15:35:18 UTC (17:35:18 SELČ) a k dnešnímu dni je navíc revokován.

Důkaz existence v čase. Pro takový případ standardy dovolují opřít se o důkaz, že podpis existoval už dříve, a posuzovat jej k onomu dřívějšímu okamžiku. Podpis nese jedno časové razítko — podpisové časové razítko od I.CA Time Stamping Authority TSU 3 01/2024, s časem 29. 2. 2024 20:30:05 UTC (21:30:05 SELČ). Razítko bylo ověřeno jako platné, takže **rozhodným okamžikem se stal tento čas**. Řetězec razítek je neporušený, razítko vzniklo ještě za platnosti podpisového certifikátu a certifikát časového razítka sám platí až do 11. 2. 2030 9:41:18 UTC (10:41:18 SELČ).

Revokační informace. K ověření stavu revokace podpisového certifikátu byla využita odpověď OCSP získaná on-line, vydaná 16. 9. 2026 13:18:00 UTC (15:18:00 SELČ), podle níž byl certifikát revokován 10. 9. 2024 5:07:36 UTC (7:07:36 SELČ).

► **Podrobný výčet**

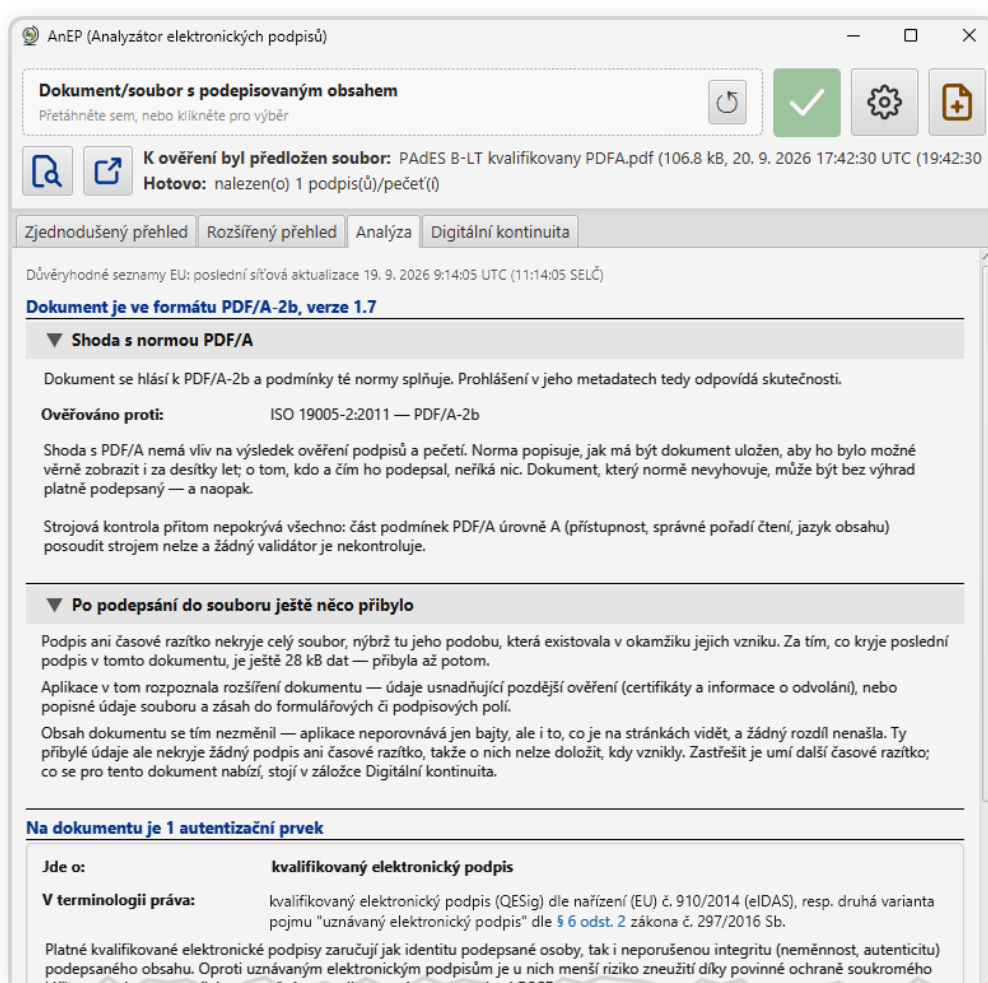
Závěr. K rozhodnému okamžiku 29. 2. 2024 20:30:05 UTC (21:30:05 SELČ) byl podpisový certifikát platný a revokován nebyl — revokace přišla až 10. 9. 2024 5:07:36 UTC (7:07:36 SELČ), tedy o šest a půl měsíce později. **Podpis je proto platný.**

► **Poznámky k výsledku**

Obrázek 10 Analýza — blok Průběh ověřování

Pokud má dokument PDF jako celek archivní formát PDF/A, či pokud k němu bylo po podepsání či připojení pečeti něco připojeno, objeví se nejprve jeden či dva bloky (pro dokument jako takový).

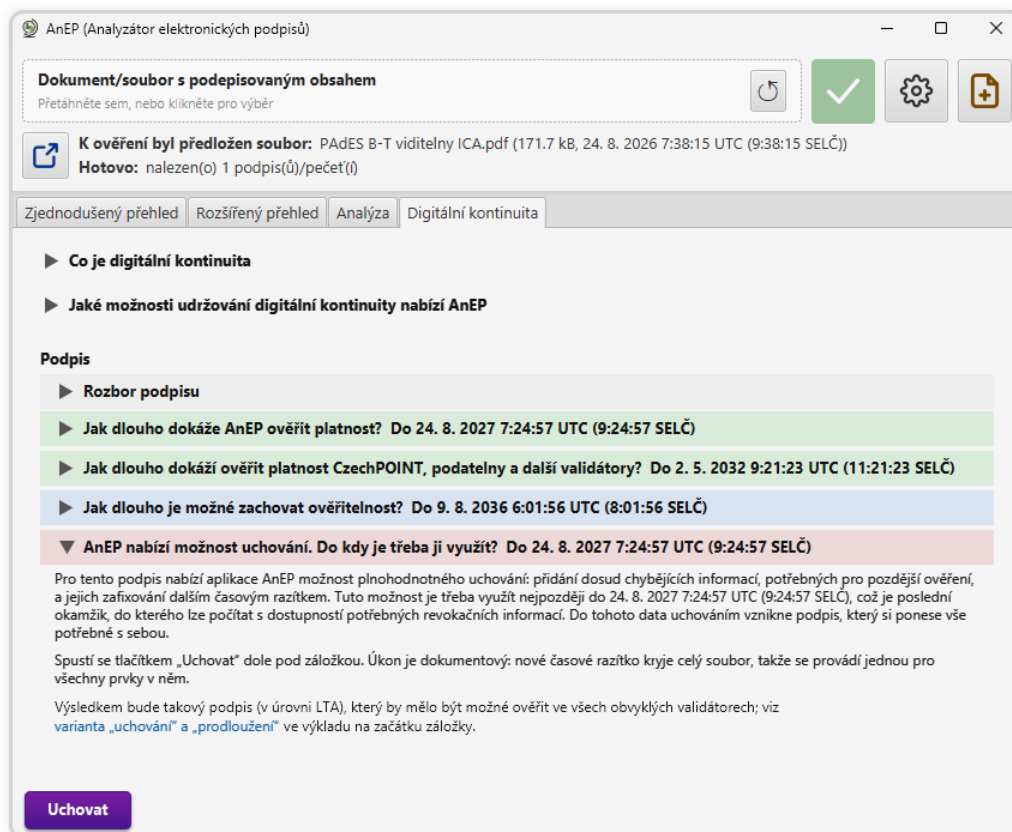
Blok	Co v něm stojí
Shoda s normou PDF/A	Varianta formátu PDF/A, verze PDF.
Po podepsání ještě něco přibýlo	I po podepsání dokumentu PDF je možné k němu přidávat inkrementální přírůstky, které nezpůsobují porušení digitální kontinuity. Nejčastěji jde o dodatečně vkládané revokační informace pro potřeby pozdějšího ověření.



Obrázek 11 Analýza dokumentu jako takového

4.4 Digitální kontinuita

Jak dlouho dokument zůstane ověřitelný, kdo ho ještě ověří, a co a do kdy je proto potřeba udělat. Podrobněji v kapitolách 9 a 10.



Obrázek 12 Digitální kontinuita — Ihůty a úkon, který je posune.

4.5 Detailní rozbor

Vše, co o dokumentu vydá diagnostika DSS, po oddílech: výsledek ověření, certifikát podepisující osoby, certifikační cesta, důvěryhodná služba a její stav v seznámech, časová razítka i s jejich cestou, algoritmy, časy, rozsah podpisu, podpisový slovník PDF, detekce změn po podpisu, záznamy VRI a globální validační data, struktura podpisů CMS a kryté objekty. U certifikátů, seznamů CRL i odpovědí OCSP jsou odkazy „Ukaž“ a „Ulož“ a u nedůvěryhodného kořene i „Přidat do důvěryhodných“. **Jen v expertním módu.**

4.6 Protokoly DSS

Surové zprávy knihovny DSS, jednoduchá i podrobná, ke stažení jako XML nebo PDF. **Jen v expertním módu.**

5 Důvody: popis problému a jeho řešení

Když ověření nedopadne kladně, nestačí to oznámit. **Důvod** je výklad pro uživatele: co se stalo, co to znamená a co se s tím dá dělat. Důvody jsou očíslované a jeden důvod může shrnovat i několik různých zjištění pod jedno vysvětlení a jedno doporučení, protože uživatele nezajímá výčet nálezů, ale odpověď.

Pozor na jmennou shodu Blok „Důvody podpisu“ v Rozšířeném přehledu je něco jiného: tam jde o důvod, který uvedla podepsaná osoba (pole Reason v PDF). Očíslované důvody ve zde popisovaném smyslu jsou jen v Analýze, v bloku „Zjištěné důvody a doporučení“.



Obrázek 13 Důvody podpisu v Rozšířeném přehledu

5.1 Z čeho se důvod skládá

Každý důvod má stejnou stavbu a **stejně pořadí částí: nejprve popis problému, pak jeho řešení**. Uživatel se tedy nejdřív dozví, na čem je, a teprve potom, co s tím.

Část	Co obsahuje	Uvádí se
Popis problému	Co se stalo, běžnou řečí a bez zkratk. Stojí vždy první.	vždy
Technicky	Totéž jazykem standardů — jména polí, mezní hodnoty, důvod, proč to standard zakazuje. Ukáže se pod odkazem „Podrobněji ...“, pro toho, kdo se zajímá o podrobnosti, nebo si chce nález ověřit sám.	jen tam, kde je to vhodné
Co může pomoci	Co může udělat běžný uživatel: které nastavení přepnout, co doplnit, kdy to zkusit znovu.	vždy
Pro zkušenější	Rada, která předpokládá pokročilé nastavení — typicky doplnit vlastní CRL seznam nebo vlastní kotvu důvěry. Je-li na kartě víc důvodů s touto radou, stojí jednou, pod spodním z nich.	jen tam, kde je co doporučit

Tam, kde žádné řešení není, se žádné nepředstírá: například u ztracené digitální kontinuity se místo rady řekne, že vadu už napravit nelze.

Některé důvody mají **náhradní znění** a aplikace vybírá podle toho, co o prvku ví — jinak zní věta o razítku, jehož autorita mezitím expirovala, a jinak o razítku, které neobstálo z jiné příčiny. Údaje z dokumentu (jméno autority, datum konce platnosti) se do vět doplňují.

5.2 Ukázka

Takhle vypadá důvod 2 — revokační informace vydaná po expiraci podpisového certifikátu:

Popis problému Aplikaci se podařilo získat (on-line) revokační informace, prokazující stav revokace certifikátu k rozhodnému okamžiku. Tyto ale byly vydány až po expiraci (skončení řádné doby platnosti) certifikátu, ke kterému se vztahují. Technické standardy však zakazují využití takovýchto revokačních informací.

Co může pomoci Zvolit tolerantní režim ověřování: v Nastavení zrušit zaškrtnutí volby „Ověřování podpisů a pečeti dle standardů“, případně v rámci pokročilého nastavení zapnout jen volbu „Využij i revokační informace, vydané po expiraci certifikátu“, a opakovat ověření.

Pro zkušenější Pokud je možné získat použitelný CRL seznam z vhodné doby, lze jej (v Pokročilém nastavení) vložit do úložiště vlastních CRL seznamů.

Na dokumentu je 1 autentizační prvek

Jde o:	kvalifikovaný elektronický podpis
V terminologii práva:	kvalifikovaný elektronický podpis (QESig) dle nařízení (EU) č. 910/2014 (eIDAS), resp. druhá varianta pojmu "uznávaný elektronický podpis" dle § 6 odst. 2 zákona č. 297/2016 Sb.

Proces ověřování se nepodařilo dokončit, stav platnosti podpisu tak zůstává neznámý.

▼ Zjištěné důvody a doporučení

Aplikace detekovala následující důvod(y) neúspěšného ověření:

V čem je problém:	2. Aplikaci se podařilo získat (on-line) čerstvé revokační informace, prokazující stav revokace certifikátu k rozhodnému okamžiku. Tyto ale byly vydány až po expiraci (skončení řádné doby platnosti) certifikátu, ke kterému se vztahují. Technické standardy však zakazují využití takovýchto revokačních informací (vydaných až po expiraci). Podrobněji ...
Co může pomoci:	Zvolit tolerantní režim ověřování: v Nastavení zrušit zaškrtnutí volby "Ověřování podpisů a pečeti dle standardů", případně v rámci pokročilého nastavení zapnout jen volbu "Využij i revokační informace, vydané po expiraci certifikátu", a opakovat ověření.
Pro zkušenější uživatele:	Pokud je možné získat použitelný CRL seznam z vhodné doby, lze jej (v Pokročilém nastavení) vložit do úložiště vlastních CRL seznamů. Podrobněji ...

► Průběh ověřování

► Kde je šance na úspěšné ověření

► Formát podpisu

Obrázek 14 Příklad důvodu neúspěšného ověření (důvod č. 2)

5.3 Proč se důvody navzájem potlačují

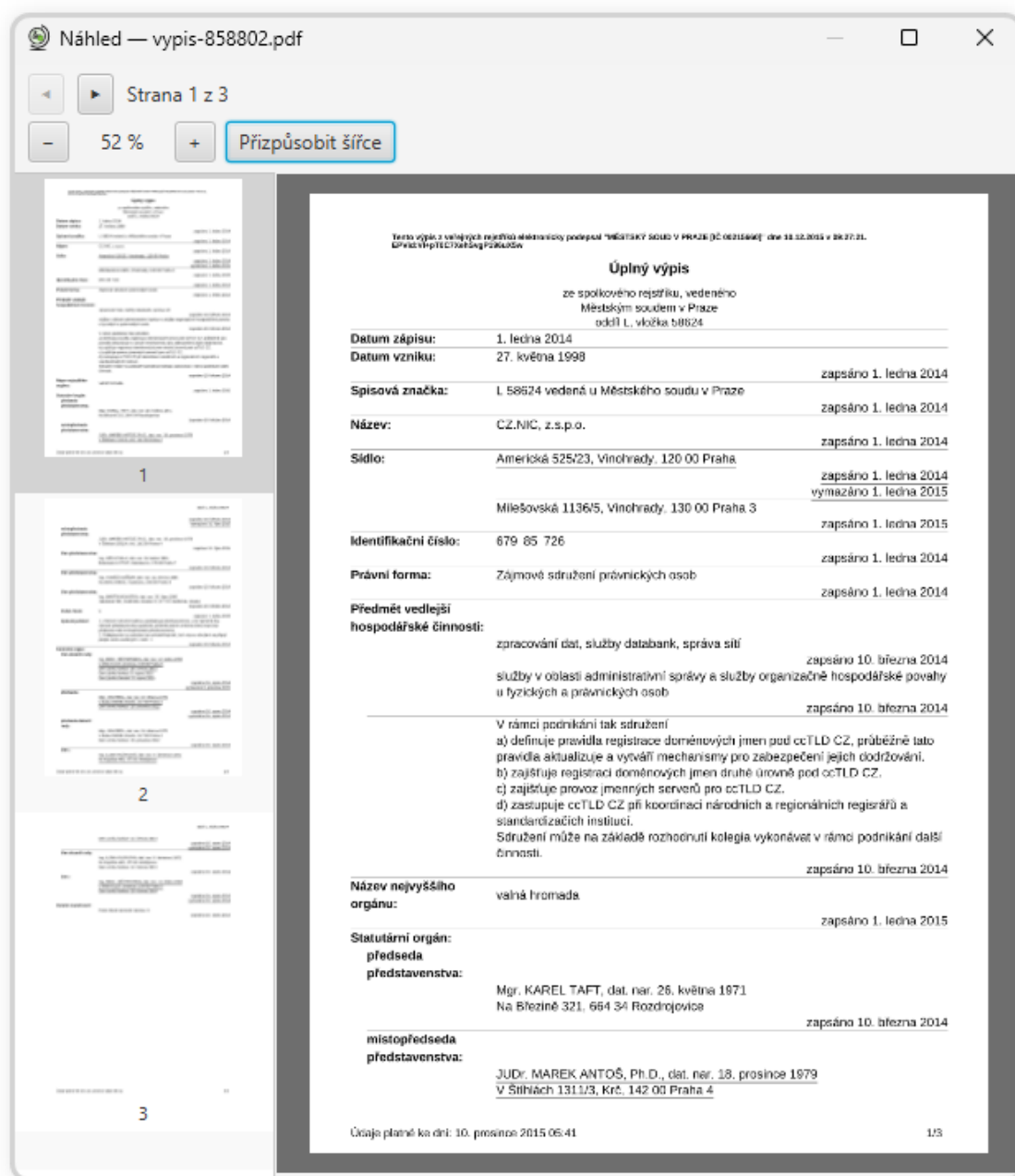
Vypsat všechno naráz by uživatele poslalo hledat příčinu tam, kde žádná není. Silnější nález proto ten slabší umlčí: u podpisu s **porušenou integritou** nemá smysl radit, ať se povolí tolerance k revokačním údajům — dokument je změněný a žádné nastavení s tím nehne. Aplikace tedy vypisuje jen ty důvody, které za daného stavu ještě něco znamenají. A nemá-li čím naplnit výčet, nenabídne ani jeho nadpis.

6 Vlastní prohlížeče

Aplikace AnEP má vlastní nástroje pro prohlížení a další manipulaci s různými objekty, které souvisí s elektronickými dokumenty a jejich podepisováním. Jde např. o prohlížeče datových zpráv z datových schránek (ve formátu ZFO), ASiC kontejnerů, příloh PDF dokumentů, tzv. obalujících elektronických podpisů, ale také o prohlížeče certifikátů, CRL seznamů či OCSP odpovědí. Ale také o možnost rychlého náhledu na samotný ověřovaný dokument, pokud je v datovém formátu PDF.

6.1 Rychlý náhled obsahu dokumentu

Pokud je právě vložený soubor dokumentem v datovém formátu PDF, je možné spustit rychlý náhled jeho obsahu. Pokud má dokument více revizí, je možné mezi nimi přecházet.



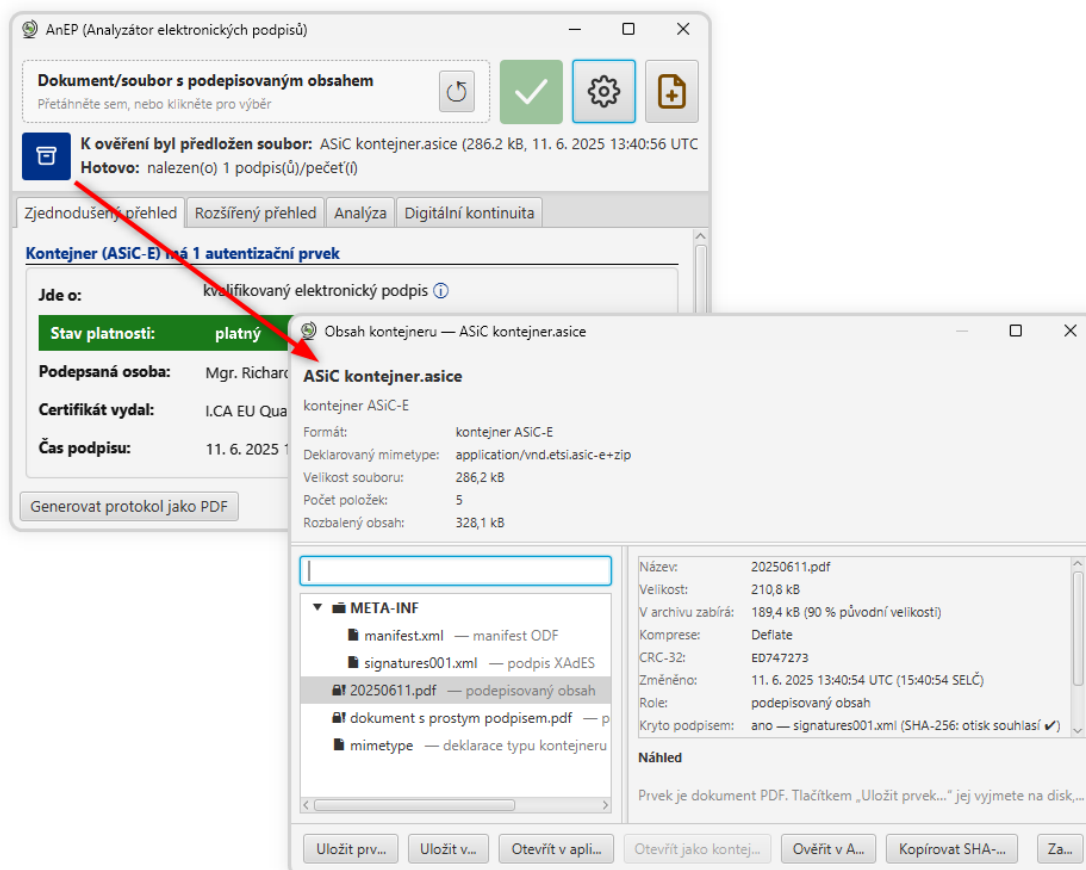
Obrázek 15 Rychlý náhled obsahu dokumentu PDF

6.2 Prohlížeč kontejnerů

Pokud má právě vložený soubor (dokument) charakter kontejneru, lze jej otevřít modrým tlačítkem „Otevřít jako kontejner“ ve stavovém řádku a pracovat s jednotlivými prvky, které tvoří obsah kontejneru.

Tato možnost funguje pro následující formáty, schopné fungovat jako kontejner:

- **ASiC kontejnery**
- **obalující (enveloping) podpisy CAdES, XAdES, JAdES**
- **datové zprávy ISDS (.ZFO)**



Obrázek 16 Prohlížeč ASiC kontejnerů

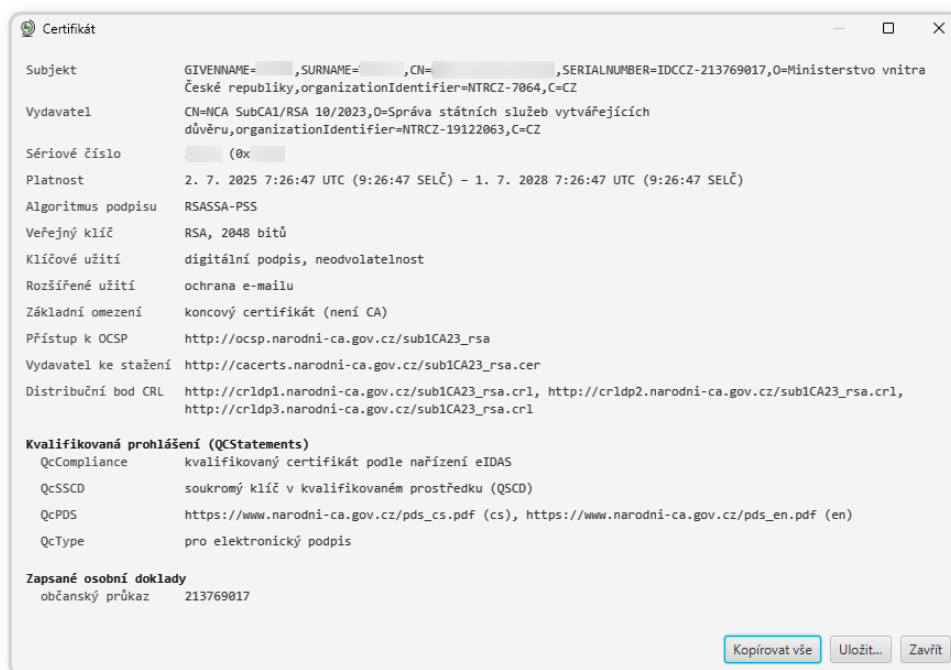
U právě vybraného prvku z obsahu kontejneru se vypíše jeho údaje — velikost uložená i původní, způsob komprese, kontrolní součet, čas změny — a vedle nich náhled: text, obrázek, nebo šestnáctkový výpis u toho, co není ani jedno. XML se pro čtení zformátuje. S prvkem pak jde:

- **Uložit prvek...** — vytáhnout jej ven jako soubor;
- **Uložit vše...** — rozbalit celý kontejner do adresáře se zachováním struktury;
- **Uložit písemnosti...** — u datové zprávy jen to, co odesílatel poslal, pod jeho jmény;
- **Otevřít v aplikaci** — předat prvek programu přiřazenému jeho typu;
- **Otevřít jako kontejner** — vnořený kontejner ve vlastním okně vedle rodičovského;
- **Ověřit v AnEP** — poslat prvek zpět k plnému ověření, jako by jej uživatel vložil sám;
- **Kopírovat SHA-256** — otisk prvku do schránky.

6.3 Prohlížeč certifikátů

Vypisuje obsah certifikátu v lidsky čitelné podobě, ne v šestnáctkové soustavě. Kromě držitele, vydavatele, sériového čísla, doby platnosti a algoritmů řekne i to, co bývá schované v rozšířeních:

- **klíčová užití** česky (digitální podpis, neodvolatelnost, podepisování certifikátů i CRL, časová razítka, podepisování odpovědí OCSP a další) — a rozšíření zvlášť;
- **základní omezení** — jde o koncový certifikát, nebo o certifikační autoritu, a do jaké hloubky;
- **kde se hledá vydavatel a odkud se stahuje revokační údaj** — přístupový bod OCSP i distribuční body CRL;
- **prohlášení podle QcStatements** — je-li certifikát kvalifikovaný podle eIDAS, k čemu slouží (podpis, pečeť, autentizace webu), leží-li klíč v prostředku QSCD, jaký je limit transakce, jak dlouho se uchovávají údaje, podle práva kterých zemí byl vydán a jaké role podle PSD2 nese;
- **zapsané osobní doklady** — nese-li kvalifikovaný certifikát číslo občanského průkazu nebo pasu podle doporučení agentury DIA (kvůli účinkům úředně ověřeného podpisu), vypíše se druh dokladu a jeho číslo samostatně, aby je uživatel nemusel hledat mezi atributy jména.
-

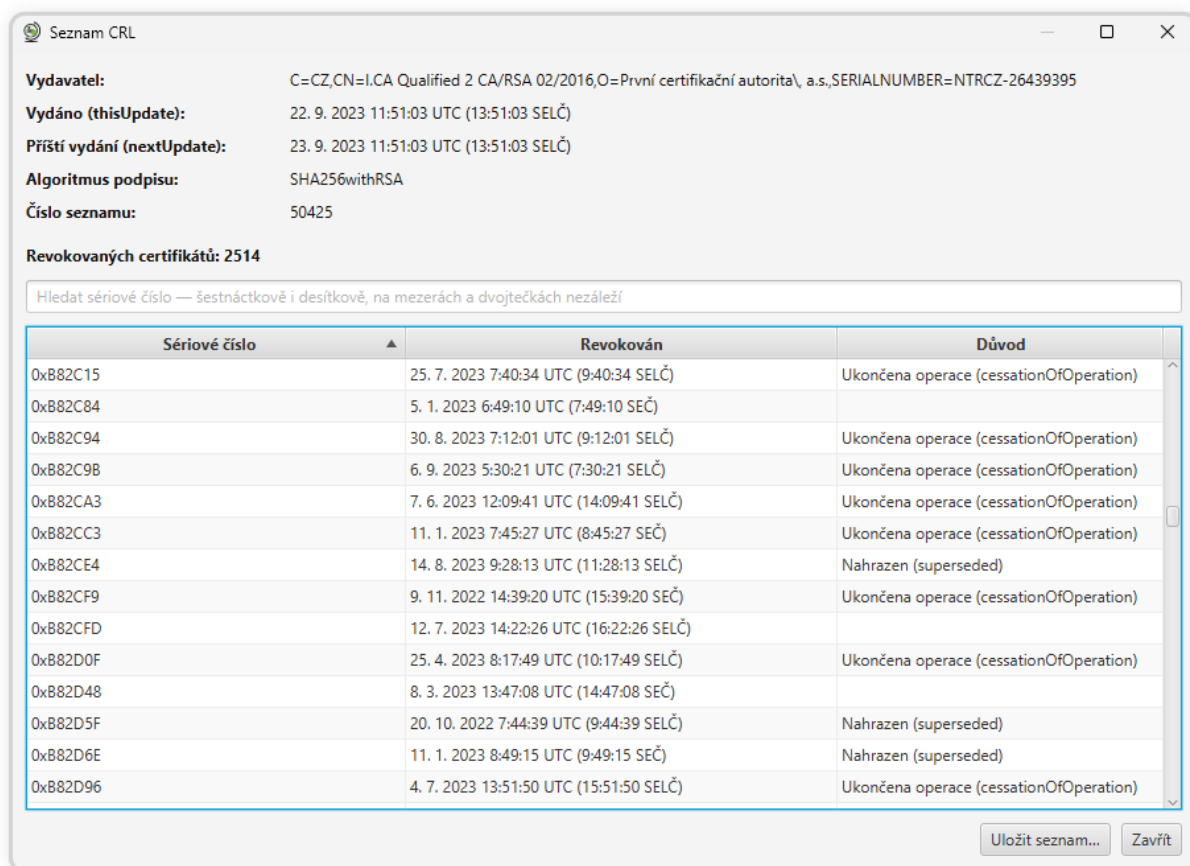


Obrázek 17 Prohlížeč certifikátů

6.4 Prohlížeč seznamů CRL

Reálný seznam CRL může mít tisíce záznamů a otázka se přitom týká jediného. Prohlížeč proto nad tabulkou vypíše hlavičku seznamu — vydavatele (s odkazem na jeho certifikát), kdy byl vydán a kdy má vyjít další, číslo seznamu, i kolik certifikátů uvádí — a **otevře se rovnou na záznamu toho certifikátu, o který jde**. Není-li na seznamu, řekne to nad tabulkou.

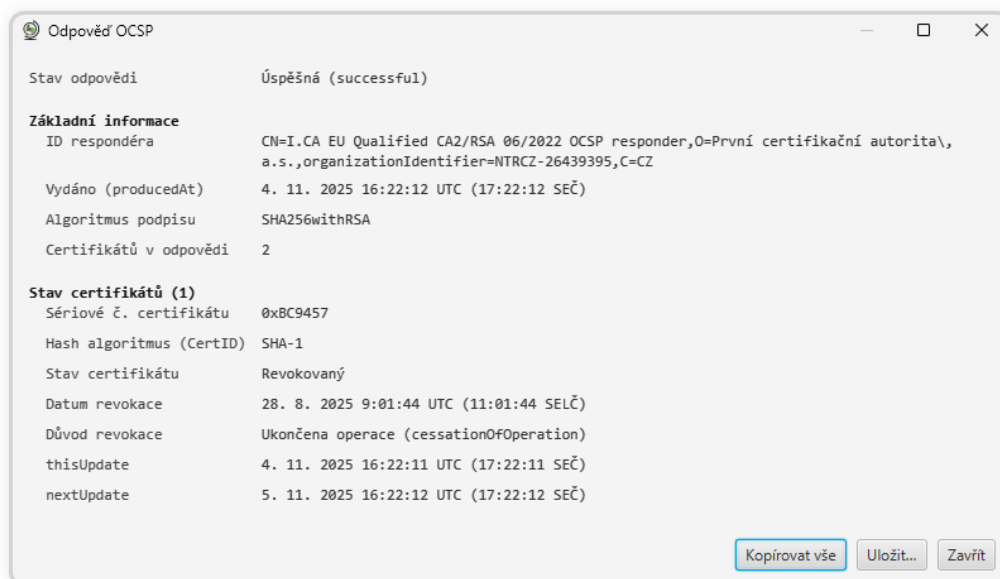
Tabulka uvádí sériové číslo, datum odvolání a jeho důvod, dá se **řadit podle sloupců** a nad ní je **hledání sériového čísla, které bere šestnáctkový i desítkový zápis**.



Obrázek 18 Prohlížeč CRL seznamů

6.5 Prohlížeč odpovědí OCSP

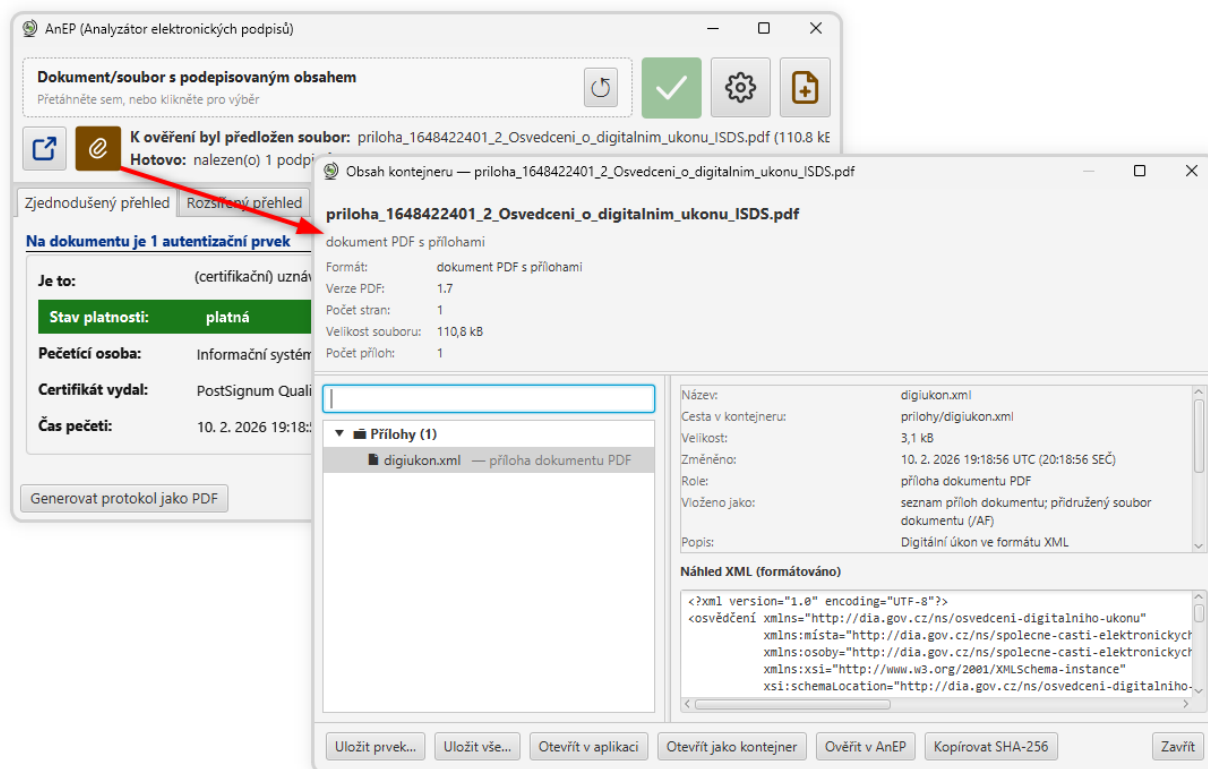
Odpověď OCSP vypsána ve slovech: stav odpovědi jako takové, kdo odpověděl, kdy ji vydal, jaké certifikáty v sobě nese — a pro každý dotázaný certifikát jeho sériové číslo, použitou hashovací funkci, stav (dobrý, revokovaný, neznámý), datum a **důvod odvolání pojmenovaný slovem**, doby platnosti odpovědi.



Obrázek 19 Prohlížeč CRL seznamů

6.6 Přílohy dokumentu PDF

Přílohy PDF se sbírají ze **tří různých míst** — ze jmenného stromu vložených souborů (to je ta „sponka“), z anotací umístěných na stránce a z polí přidružených souborů, kterými nosí data dokumenty typu PDF/A-3. Ukazují se v témže prohlížeči jako kontejner, se všemi jeho možnostmi; příloha bývá sama podepsaným dokumentem, takže „Ověřit v AnEP“ je u ní ta nejužitečnější.



Obrázek 20 Prohlížeč příloh

6.7 Kudy se k prohlížečům dostat

Odkud	Co se otevře
Stavový řádek → Otevřít jako kontejner	prohlížeč kontejnerů nad právě ověřeným souborem
Stavový řádek → sponka	přílohy dokumentu; v závorce je jejich počet
Analýza → Podrobný výčet → Ukaž	seznam CRL otevřený na dotčeném certifikátu, nebo odpověď OCSP
Detailní rozbor → Ukaž	certifikát, seznam CRL nebo odpověď OCSP z kterékoli cesty či slovníku
Prohlížeč kontejnerů	kterýkoli prvek uvnitř — i vnořený kontejner ve vlastním okně
Vložení holého souboru do aplikace	certifikát, seznam CRL nebo odpověď OCSP se rovnou otevře v prohlížeči; poznají se podle obsahu, ne podle přípony

7 Důvěra a revokační informace

7.1 Odkud pochází důvěra

Kotvy důvěry pocházejí z **evropských důvěryhodných seznamů (LOTL/EUTL)** — kolem třiceti národních seznamů a několika tisíc certifikátů. Uloží se do místní mezipaměti, takže start aplikace nečeká na síť; čerstvost se dokontroluje na pozadí a seznam jde kdykoli načíst znovu ručně.

Aplikace si přitom pamatuje, **co ze seznamu plyne**: nejen že je certifikát důvěryhodný, ale i jakou službu poskytuje, pod jakým poskytovatelem a do kdy byla služba v seznamu vedena. Bez toho by se nedalo posoudit časové razítko od služby, která mezitím ze seznamu zmizela.

Pro navazování zabezpečeného (TLS) spojení (např. pro stahování revokačních informací on-line) čerpá aplikace důvěru i od operačního systému Windows.

7.2 Revokační informace

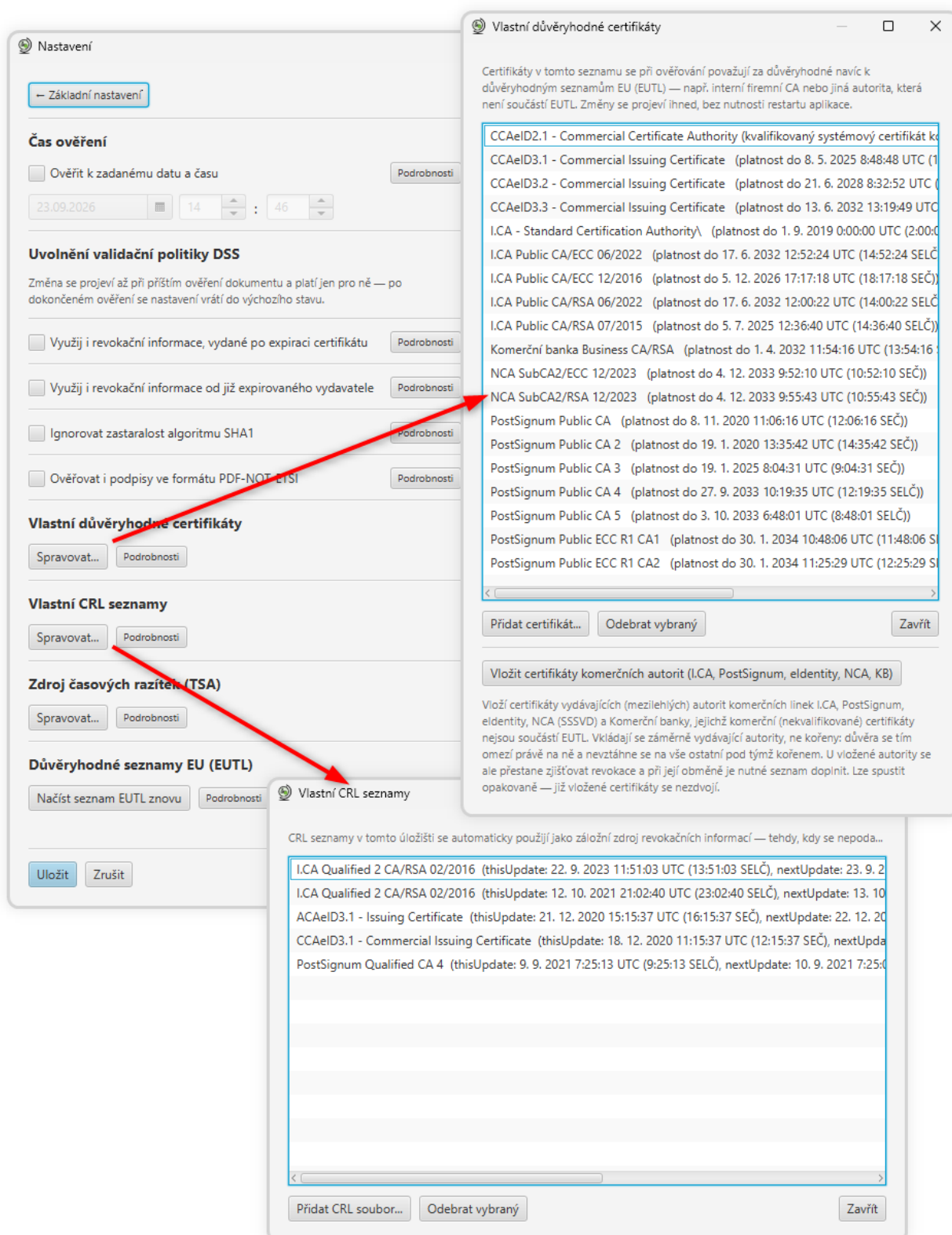
Stav certifikátu se zjišťuje živě — **napřed OCSP, pak CRL** jako záloha — a doplňuje se o to, co dokument nese sám. U každého údaje aplikace sleduje, **odkud pochází**: z dokumentu, z vlastního úložiště, nebo ze sítě. Právě to rozhoduje, jestli půjde závěr zopakovat i jinde a později, a proto se to v Průběhu ověřování uvádí u každého využitého údaje zvlášť.

Údaje se rozdělují do tří skupin, protože „přípustný“ a „využitý“ není totéž: o které se závěr opřel, které standardy připouštějí, ale závěr na nich nestojí, a které použít nešlo — u každého z nich i proč. Tam, kde se na stav revokace správně vůbec nikdo neptal (certifikát je sám kotvou důvěry), řekne se i to; jinak by poctivě „nic se nezjišťovalo, a správně“ vypadalo jako chyba.

7.3 Vlastní zásoby

- **Vlastní úložiště CRL** — seznamy, které si uživatel nashromáždil. Hodí se u starých podpisů, kde už vydavatel nic nezveřejňuje. Je to **záložní zdroj**: sáhne se po něm tehdy, když se použitelný údaj nepodařilo získat obvyklou cestou. Ze seznamů od téhož vydavatele si aplikace vybere ten, který o certifikátu skutečně může vypovídat — seznam vydaný dřív, než certifikát vznikl, nebo dřív než rozhodný okamžik, vypovídají (resp. mlčí) o něčem jiném, než co se právě zjišťuje.
- **Vlastní kotvy důvěry** — certifikáty, které evropské seznamy neuvádějí, například interní firemní autorita. Jedním tlačítkem se vloží vydávající autority tuzemských komerčních linek (I.CA, PostSignum, eldentity, NCA, KB); doplnit se dá libovolná další. Aplikace vždy přizná, že závěr stojí na kotvě, kterou jiný nástroj nemá odkud vzít.

Co ověření z vlastních zásob opravdu použilo, se při uchování **zapíše do dokumentu** — jinak by uchovaný soubor postrádal právě ten důkaz, na kterém jeho verdikt stál, a nikdo jiný by si ho už neopatřil.



Obrázek 21 Pokročilé nastavení — správa vlastních důvěryhodných certifikátů a CRL seznamů

8 Přísnost a ústupky

Ve výchozím stavu se ověřuje **striktně podle standardů**; v základním nastavení to drží jediná volba „Ověřování podpisů a pečeti dle standardů“. Kdo ji zruší, povolí všechny ústupky naráz; v pokročilém nastavení se dají povolit jednotlivě.

8.1 Čtyři ústupky

Ústupek	Co povolí využít
Po expiraci	revokační informaci vydanou až po skončení platnosti certifikátu, o kterém vypovídá
Expirovaný vydavatel	revokační informaci od vydavatele, jemuž mezitím vypršel vlastní certifikát
SHA-1	ignorovat zastaralost algoritmu SHA-1
PDF-NOT-ETSI	ověřovat i podpisy v nereferenčním formátu z doby před eIDAS

8.2 Dvě samostatná nastavení

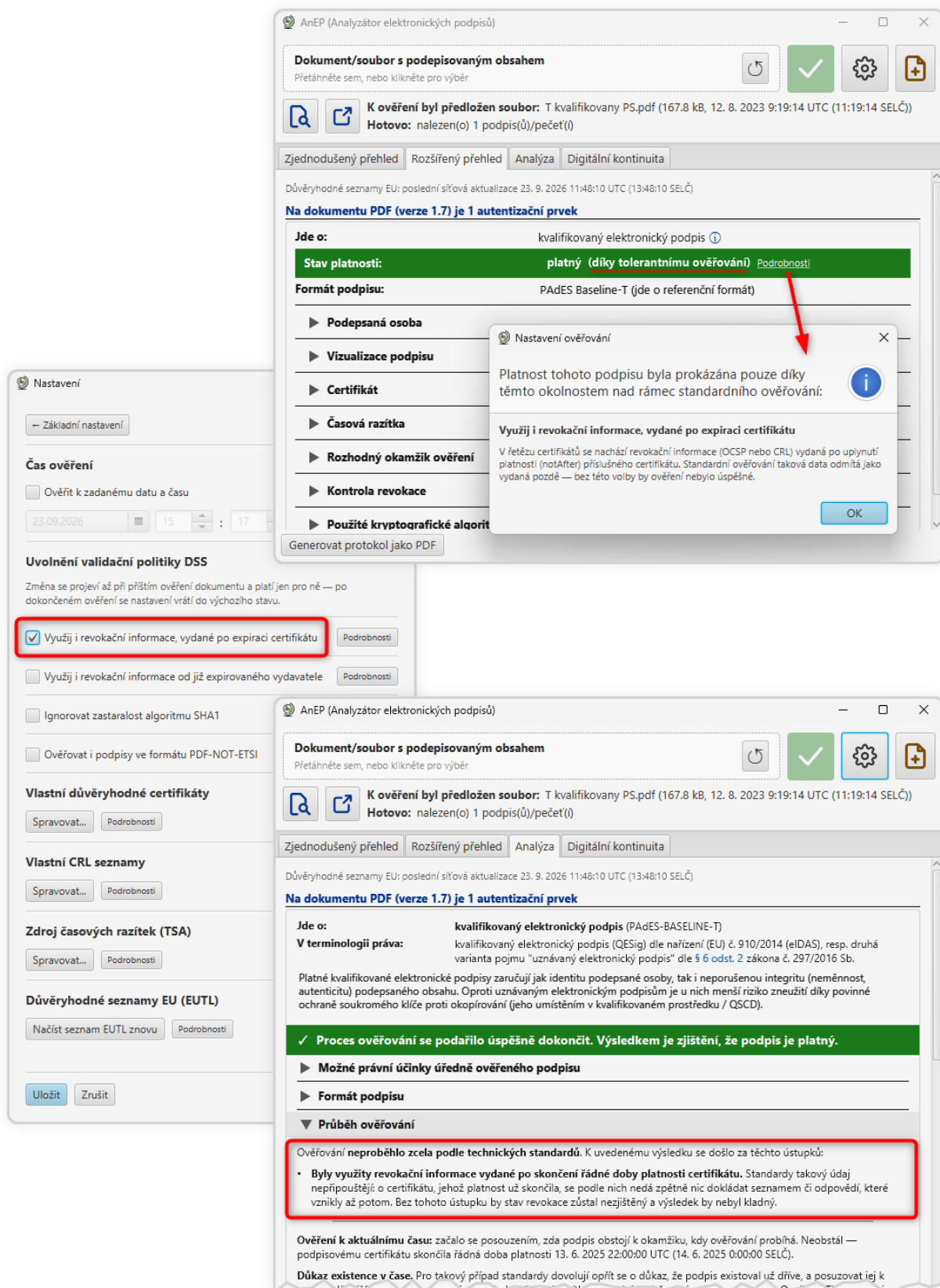
- **Ověřit k zadanému datu a času** — celé ověření se posune do minulosti, což je jediný způsob, jak se dozvědět, jak by dokument dopadl tehdy.
- **Ověřování časových razítek podle standardů** — pokud je tato volba aktivní, razítka se posuzují podle řádné platnosti certifikátů razítkovacích autorit namísto podle data, kdy byla služba vyražena z důvěryhodných seznamů. **Je to zpřísnění**, ne ústupek.

8.3 Jednorázová politika

Každý ústupek platí jen na jedno ověření Po něm se nastavení vrací do výchozího stavu. Kladný verdikt se tedy nemůže tiše opřít o volbu, kterou uživatel zapnul někdy dříve a již na ni zapomněl. Vlastních zásob se to netýká — ty platí, dokud je uživatel neodebere.

8.4 Rozhodující ústupek

Aplikace měří, jestli se ústupek na výsledku opravdu **podílel**: ověření proběhne znovu bez něj a porovná se. U kladného verdiktu se proto vypíší jen ty ústupky, bez kterých by závěr nevznikl — ne ty, které byly jen zapnuté. Totéž platí pro vlastní zásoby a pro zadaný čas ověření, a do protokolu jde též výčet.



Obrázek 22 Pokročilé nastavení — příklad ústupku a jeho indikace ve výsledcích

9 Není digitální kontinuita jako digitální kontinuita

Otázka „do kdy lze ověřit platnost“ nemá jednu odpověď, protože to nezávisí pouze na samotném dokumentu a jeho podpisech či pečetích, ale i na tom, kdo a jak platnost ověřuje (jaký validátor, případně s jakým nastavením).

9.1 Možné přístupy k ověřování

Kdo ověřuje	Za jakých podmínek
AnEP	defaultně podle technických standardů — ale dle volby uživatele i se zapnutými ústupky, s uživateli dodanými CRL seznamy a důvěryhodnými certifikáty, i s explicitně zadaným časem
validátory fungující dle standardů	bez jakýchkoli ústupků
CzechPOINT a podatelny OVM	nástroje a služby s vlastní zásobou revokačních informací, shovívavostí k některým zastaralým kryptografickým algoritmům a formátům (např. SHA-1), ale naopak striktnější v hodnocení časových razítek (podle platnosti jejich certifikátů, bez ohledu na kvalifikovaný status vydavatele v důvěryhodných sezonech).

O třetím variantě mluví aplikace vždy podmíněně („mohly by“): nezná jejich verzi, nastavení ani obsah jejich zásob. Kde jde odhadnout, že se dokument ověřit **podaří**, i do kdy, řekne to.

9.2 Co určuje datum, do kdy lze ověřit platnost

Autentizační prvek (podpis či pečeť) visí v čase na posledním článku, který ho drží, a lhůtu určuje ten, který povolí nejdřív:

- **Důkaz existence** — s platným časovým razítkem smí být podpisový certifikát dávno po expiraci; bez něj končí všechno s jeho expirací.
- **Dostupnost revokačních informací** — údaj v dokumentu ani ve vlastním úložišti se neztratí, ten stahovaný ze sítě je dostupný jen dokud ho vydavatel zveřejňuje. To je povinen dělat jen po dobu řádné platnosti toho certifikátu, ke kterému se revokační informace vztahují. Později může, ale nemusí.
- **Uznatelnost stažených revokačních informací** — i když je vydavatel stále zveřejňuje, pokud jsou revokační informace vydány až po expiraci certifikátu, podle standardů se dají využít jen v některých specifických případech, ne vždy.
- **Uznatelnost vložených revokačních informací** — že informace v souboru zůstanou, ještě neznamená, že půjdou využít: po expiraci certifikátu svého vydavatele se podle standardů již využít nedají.
- **Uznání razítka** — podle standardů lze považovat kvalifikované časové razítko do vyřazení vydavatele z důvěryhodných seznamů, což je datum, které nikdo předem nezná; jinak jeho platnost končí s expirací certifikátu vydavatele razítka.

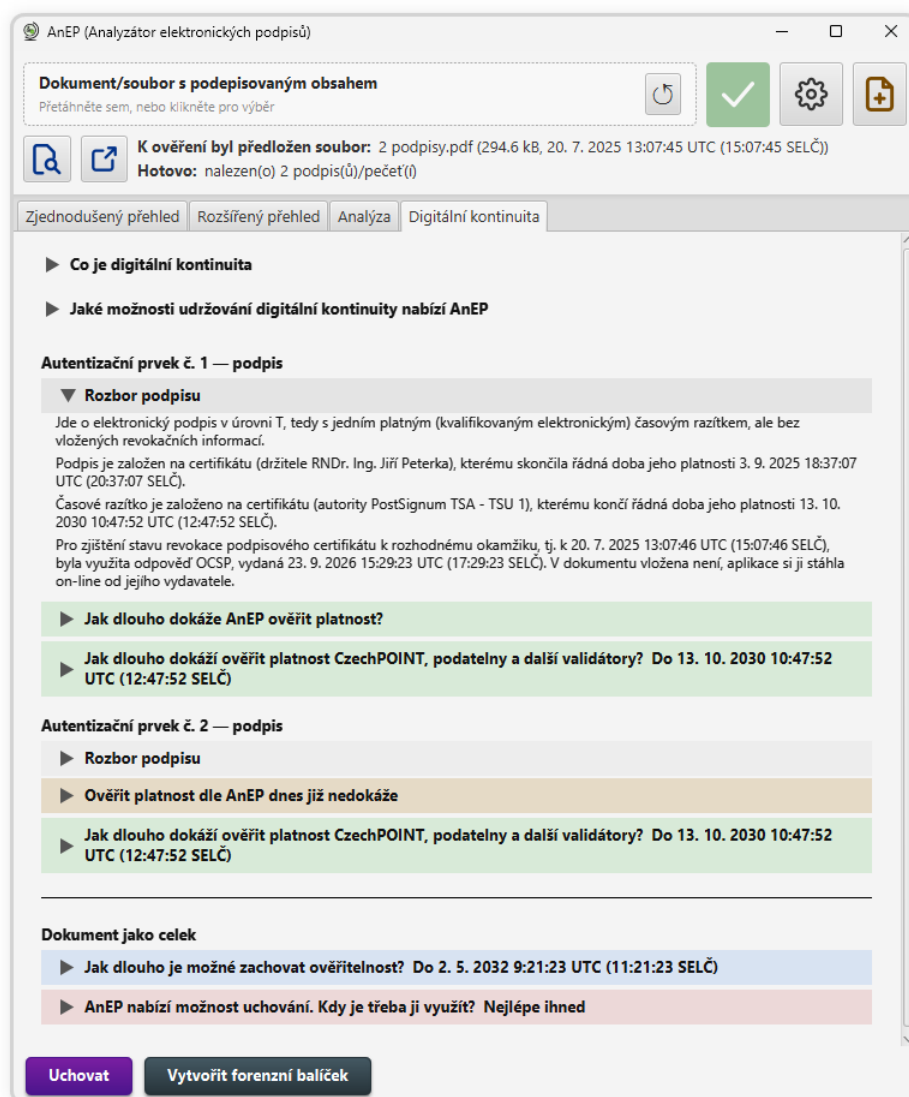
9.3 Když lhůtu stanovit nelze

Zvláštní a poměrně častý případ: dnešní kladný závěr stojí na revokačním údaji staženém právě teď ze sítě a doba, po kterou se na jeho dostupnost dalo spoléhat, už uplynula. Aplikace pak **žádné datum neuvede** — v nadpisu zůstane holá otázka a u úkonu stojí „Nejlépe ihned“. Uvnitř bloku je vysvětlení a s ním i datum, kam by ověřitelnost sahala, kdyby údaj dostupný zůstal. Datum se tím neztrácí, jen přestává být slibem.

9.4 O čem informuje záložka

Záložka „Digitální kontinuita“ má čtyři části: výklad pojmu, přehled možností, které aplikace nabízí, pak bloky po jednotlivých autentizačních prvcích (podpisech či pečetích) a nakonec — má-li dokument prvků víc — pohled na soubor jako celek.

U každého prvku jsou čtyři odpovědi: dokdy platnost ověří AnEP, dokdy ji ověří validátor podle standardů, dokdy CzechPOINT a podatelny, a **co a do kdy je třeba udělat**. Kde lhůta neexistuje, řekne se i to, a kde je pozdě, řekne se to rovnou.



Obrázek 23 Pokročilé nastavení — příklad ústupku a jeho indikace ve výsledcích

10 Co aplikace může udělat s dokumentem a jeho podpisy

Žádný z dostupných úkonů nesahá na podepsané bajty. Každý vytváří **nový soubor** a původní nechává být. Tlačítka jsou v záložce „Digitální kontinuita“, hned pod textem, který říká, co udělají a co z toho uživatel bude mít.

10.1 Možnosti prodloužení digitální kontinuity

Podle toho, v jakém stavu je dokument a jeho podpisy či pečeti, připadají v úvahu tři různé varianty prodloužení digitální kontinuity, resp. zachování ověřitelnosti po další období.

Toto období je určeno dobou platnosti aktuálně používaného zdroje časových razítek, a je vyjádřeno doplňkem jména nově vytvářeného souboru. Například je-li původním souborem *dokument.pdf*, bude výstupem po uchování soubor *dokument_Uchovano_do_02_05_2023.pdf*.

Varianta	Kdy se nabídne
Uchovat	je možné provést plnohodnotné prodloužení digitální kontinuity, neboli tzv. uchování — výsledkem budou podpisy (či pečeti) v úrovni LTA, které si ponесou v sobě vše potřebné pro jejich budoucí ověření. Jejich platnost by mělo být možné ověřit ve všech validátorech.
Přerazítkovat	výsledkem budou takové podpisy (či pečeti), jejichž platnost bude možné ověřit jen ve validátorech typu CzechPOINTu či podatelen OVM. Obecně ve validátorech, které mají vlastní zásobu revokačních informací, které mohou využít při budoucím ověřování. Samotný dokument a jeho podpisy (pečeti) tyto nezbytné informace v sobě nemají (takže v jiných validátorech zůstane stav jejich platnosti neznámý).
Prodloužit	výsledkem budou takové podpisy (či pečeti), jejichž platnost bude možné ověřit jen ve validátorech, které ověřují časová razítka podle standardů. Tedy volněji než validátory typu CzechPOINTů či podatelen OVM, které hodnotí platnost časových razítek striktně podle doby platnosti jejich certifikátů. Naproti tomu podle standardů je možné považovat časové razítko za platné i po expiraci jeho certifikátu, dokud má jeho vydavatel v důvěryhodných seznamech status kvalifikované služby.

Tlačítko pro prodloužení digitální kontinuity (resp. zachování ověřitelnosti) je vždy jen jedno — tři výše uvedené varianty se vzájemně vylučují a uživatel mezi nimi nevybírá; aplikace sama nabídne nejsilnější, na kterou dokument se svými podpisy a pečeti dosáhne. Tuto svou volbu také vysvětlí na rozboru každého jednotlivého podpisu či pečeti, včetně popisu toho, zda a jak dlouho je ještě možné ověření stávající podoby na různých validátorech (typu CzechPOINTu či podatelen, vs. ověřujících podle standardů).

Úkon je přitom opakovatelný: dokument, který už jednou uchován byl, se dá uchovat znovu, až bude po čase potřeba.

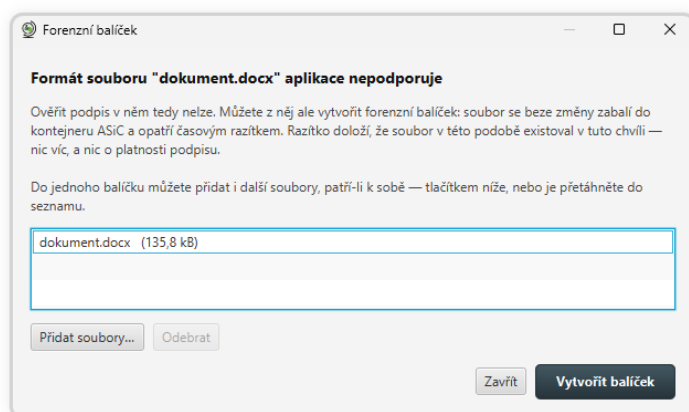
10.2 Souběh více podpisů

Nové razítko, přidávané v rámci prodlužování digitální kontinuity, kryje vždy **celý soubor**, takže se nedá přidat pro jeden podpis a pro druhý ne. U dokumentu s více podpisy je proto úkon jeden a jeho účinek se vypíše po prvcích: kterému podpisu pomůže, kterému ne a proč. Prvku, na který úkon nedosáhne, přitom neuškodí — co je na něm dnes sporné či jen neurčité, zůstane sporné či neurčité i potom.

10.3 Forezní balíček

Pro dokumenty, které již ztratily svou digitální kontinuitu a zachování ověřitelnosti pro ně již není dostupné, nabízí aplikace AnEP jiné řešení: vytvoření tzv. **forezního balíčku**. Cílem je vyjít vstříc případným budoucím sporům o vlastnosti elektronického dokumentu, které již nebude možné řešit běžným způsobem (ověřením ve validátorech), ale budou předmětem expertního posuzování (typicky soudním znalcem): aplikace zabalí **nedotčený** originál do kontejneru ASiC-E spolu se vším ověřovacím materiálem, který se jí podařilo sehnat, a se soupisem toho, odkud co pochází — a opatří to časovým razítkem. Znalec pak má jistotu, že v okamžiku zafixování všechny podklady existovaly.

Stejné řešení se nabízí také pro soubory, jejichž formát aplikace nepodporuje: do balíčku se dá přidat i další soubor či soubory: smlouva se svými přílohami, zpráva s tím, co k ní bylo připojeno atd. Orazítkovat je zvlášť by každý zafixovalo v jiném okamžiku a neřeklo by to nic o tom, že patří k sobě.



Obrázek 24 Forezní balíček lze vytvořit i se souborem nepodporovaného formátu

10.4 Kdy se úkon nenabídne

Úkon se nabídne jen tam, kde je možný **a zároveň poctivý**. Dokument, jehož certifikát byl odvolán dřív, než se dá prokázat existence podpisu, uchovat nelze — a aplikace to řekne, místo aby nabídla tlačítko, které nic nespraví. Řekne také, když vybraný zdroj razítek ověřitelnost prakticky neposune, protože jeho vlastní certifikát končí sotva později než dokument sám.

11 Protokoly

11.1 Tři protokoly

Protokol se generuje ze Zjednodušeného přehledu, z Rozšířeného přehledu i z Detailního rozboru — každý o té hloubce, ve které vznikl — a vždy jako **PDF/A-2b**, tedy v archivním formátu, který přijímají Formátová pravidla Národního archivu. Nese záhlaví s údaji o souboru a s okamžikem ověření, Protokol se jmenuje vždy podle souboru, o kterém vypovídá, rozliší se přidanou předponou.

Do protokolu jde i to, co má uživatel na obrazovce sbalené — rozbalovací blok se exportuje celý.

AnEP (Analýzátor elektronických podpisů)
Rozšířený přehled

Ověřovaný dokument

Název souboru: PAdES B-LTA kvalifikovany.pdf
Velikost: 198.9 kB
Datum poslední změny: 20. 5. 2024 9:05:53 UTC (11:05:53 SELČ)
Ověřování proběhlo: 23. 9. 2026 18:03:00 UTC (20:03:00 SELČ)

Důvěryhodné seznamy EU: poslední síťová aktualizace 23. 9. 2026 11:48:10 UTC (13:48:10 SELČ)
Na dokumentu PDF (verze 1.7) je 1 autentizační prvek

Jde o: kvalifikovaný elektronický podpis
tj.: kvalifikovaný elektronický podpis (QESig) dle nařízení (EU) č. 910/2014 (eIDAS), resp. druhá varianta pojmu "uznávaný elektronický podpis" dle § 6 odst. 2 zákona č. 297/2016 Sb.

Stav platnosti: platný

Formát podpisu: PAdES Baseline-LTA (jde o referenční formát)

Podpsaná osoba: RNDr. Ing. Jiří Peterka
Stát: CZ
E-mailová adresa: jiri@peterka.cz

Kvalifikované, uznávané i zaručené elektronické podpisy, stejně jako pečeti, nemají žádnou vizuální podobu. Jsou to jen data (posloupnost 1 a 0), a pracuje se s nimi jen prostřednictvím programových nástrojů. Pro uživatele, kteří jsou zvyklí vidět něco jako podpis přímo v těle dokumentu, se jako určitá „berlička“ přidává na vhodné místo v dokumentu konkrétní vizuální ztvárnění (vizualizace) těchto elektronických podpisů či pečeti, v podobě obrázku (obdélníkového tvaru). Toto vizuální ztvárnění může být libovolné, a volba jeho provedení je zcela na podepisující, resp. pečeti osobě. Někdy, nejčastěji u pečeti, je obrázek, představující vizualizaci, prezentovaný jako prostý elektronický podpis jiné osoby, než té které patří samotná elektronická pečeť.

RNDr. Ing. Jiří Peterka Datum: 2024.02.29 21:22:49 +01'00'

Druh certifikátu: kvalifikovaný certifikát pro elektronický podpis
S příznakem QSCD: ano
Vydavatel: PostSignum Qualified CA 4
Vydavatel — organizace: Česká pošta, s.p.
Vydavatel — stát: CZ
Sériové číslo certifikátu: 22663569 (0x0159D191)
Rádná doba platnosti: 1. 7. 2022 6:30:42 UTC (8:30:42 SELČ) – 13. 6. 2025 22:00:00 UTC (14. 6. 2025 0:00:00 SELČ)
Aktuální stav: prošlý
Identifikátor držitele (serialNumber): P135491
IK MPSV: 1680937599

Razítko č. 1 (v podpisu): kvalifikované, platné, přidáno: 29. 2. 2024 20:22:58 UTC (21:22:58 SEČ) — vydavatel: I.CA Time Stamping Authority TSU 5 01/2024 — platnost certifikátu TSA do: 11. 2. 2030 9:41:39 UTC (10:41:39 SEČ)
Razítko č. 2 (dokumentové): kvalifikované, platné, přidáno: 20. 5. 2024 9:05:27 UTC (11:05:27 SELČ) — vydavatel: PostSignum TSA - TSU 2 — platnost certifikátu TSA do: 13. 10. 2029 11:20:49 UTC (13:20:49 SELČ)

Výsledek ověření v aplikaci AnEP i tento protokol jsou poskytovány bez jakékoli záruky.
Analýzátor elektronických podpisů (AnEP) slouží výhradně potřebám výuky a seznámení se s problematikou elektronických podpisů.
Autorem aplikace AnEP je **Jiří Peterka**; při jejím vývoji byla využita knihovna DSS a nástroj Claude Code
<https://bajecnysvet.cz/anep> · <https://digitalnikontinuita.cz>

Obrázek 25 Protokol o ověření vysázený jako PDF/A

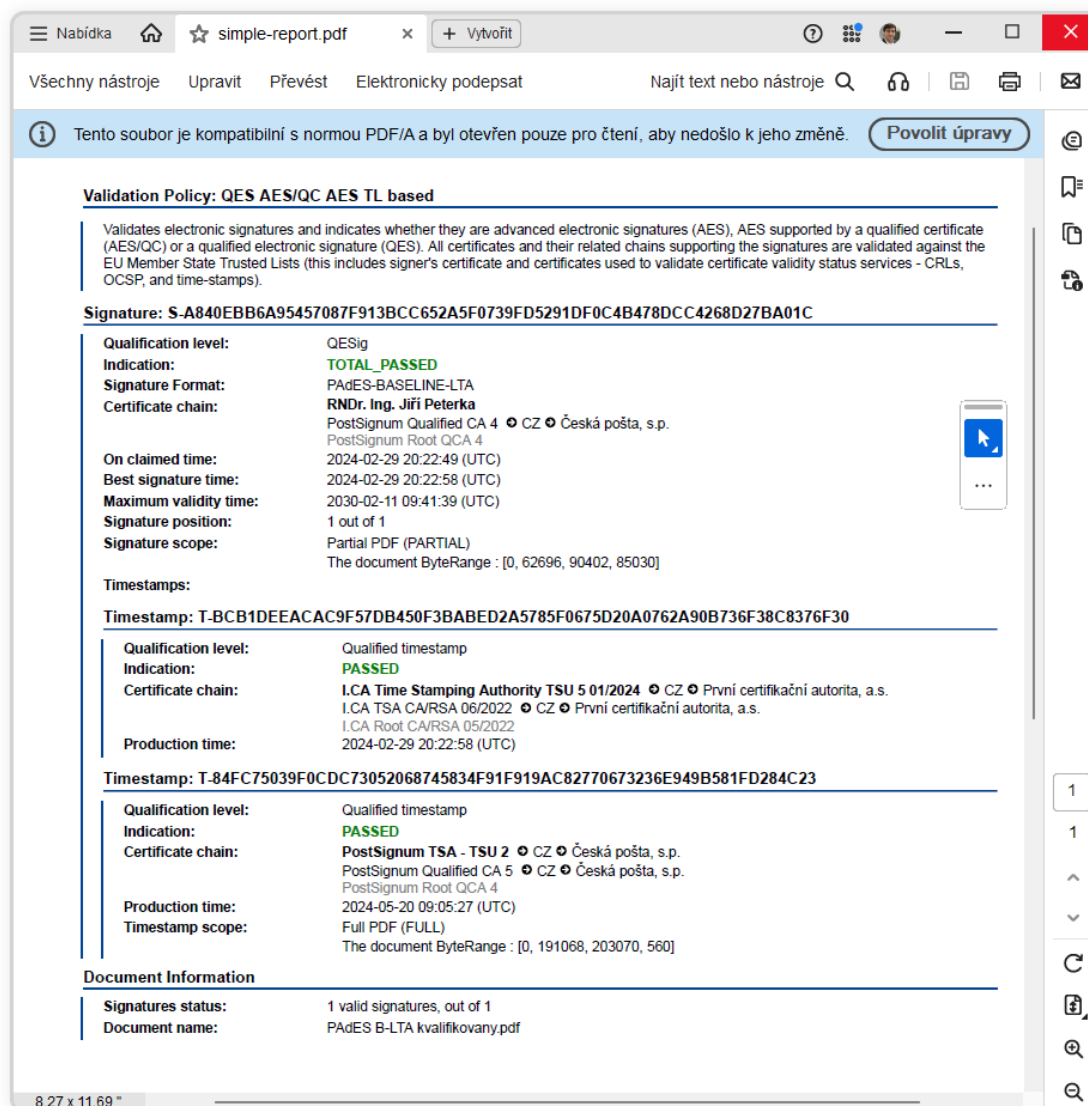
11.2 Dvě volby

Před generováním se aplikace zeptá na dvě věci; obojí je ve výchozím stavu vypnuté:

Volba	Důsledek
Vložit ověřovaný soubor	protokol ponese i soubor, o kterém vypovídá, takže se dá ověřit znovu z jediného souboru — vysází se ale jako PDF/A-3, protože PDF/A-2 přílohu, která sama není PDF/A, nepřipouští
Opatřit protokol časovým razítkem	razítko doloží, kdy protokol vznikl a že se od té doby nezměnil; pořizuje se od zdroje vybraného v nastavení, a nabídne se jen tehdy, když nějaký je

11.3 Protokoly DSS

Vedle toho jdou v expertním módu stáhnout původní protokoly knihovny DSS — jednoduchá i podrobná — jako XML nebo PDF. Hodí se, když je třeba ukázat, co přesně řekla samotná knihovna DSS, bez jakéhokoli výkladu.



Obrázek 26 Protokol knihovny DSS.

12 Zvláštní obsahy

Věci, které se v českém prostředí potkávají a běžný validátor je nezná.

Datové zprávy ISDS (.zfo)

Aplikace podporuje datové zprávy z Informačního systému datových schránek (ISDS), rozumí jejich formátu (ZFO), dokáže ověřovat platnost jejich pečeti i udržovat jejich digitální kontinuitu. Nabízí také prohlížeč obsahu datové zprávy, umožňující pracovat s jejími přílohami.



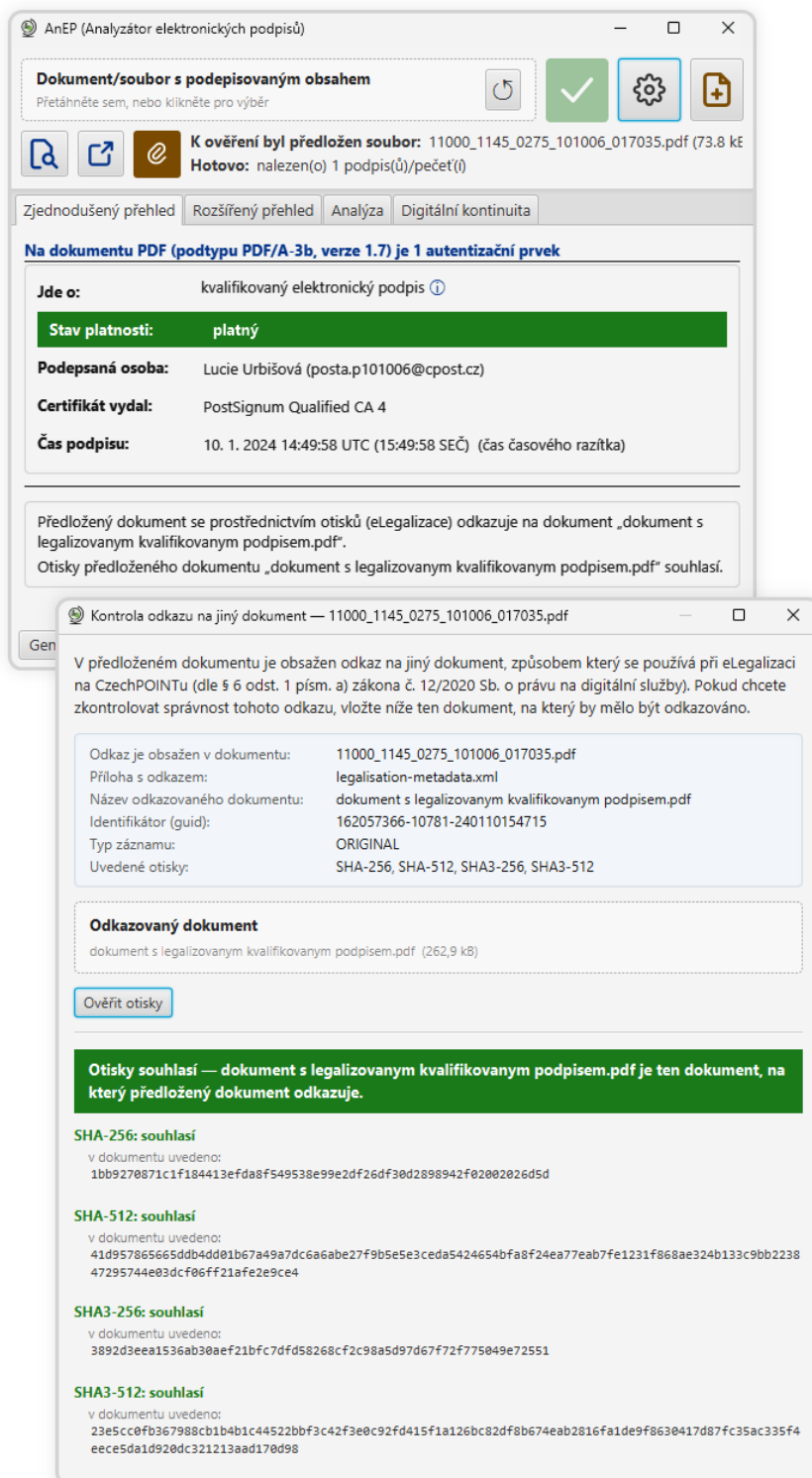
Obrázek 27 Prohlížeč datové zprávy

Evidenční záznamy (ERS, XMLERS)

Aplikace ověří evidenční záznam a řekne, jestli a k jakému okamžiku dokládá existenci předloženého souboru. Kryje-li záznam víc souborů než ten předložený, otevře se okno, kde se ostatní přiloží a zkontrolují proti otiskům záznamu; kterýkoli z nich jde odtud poslat k plnému ověření s tímž záznamem.

Výstupy z eLegalizace

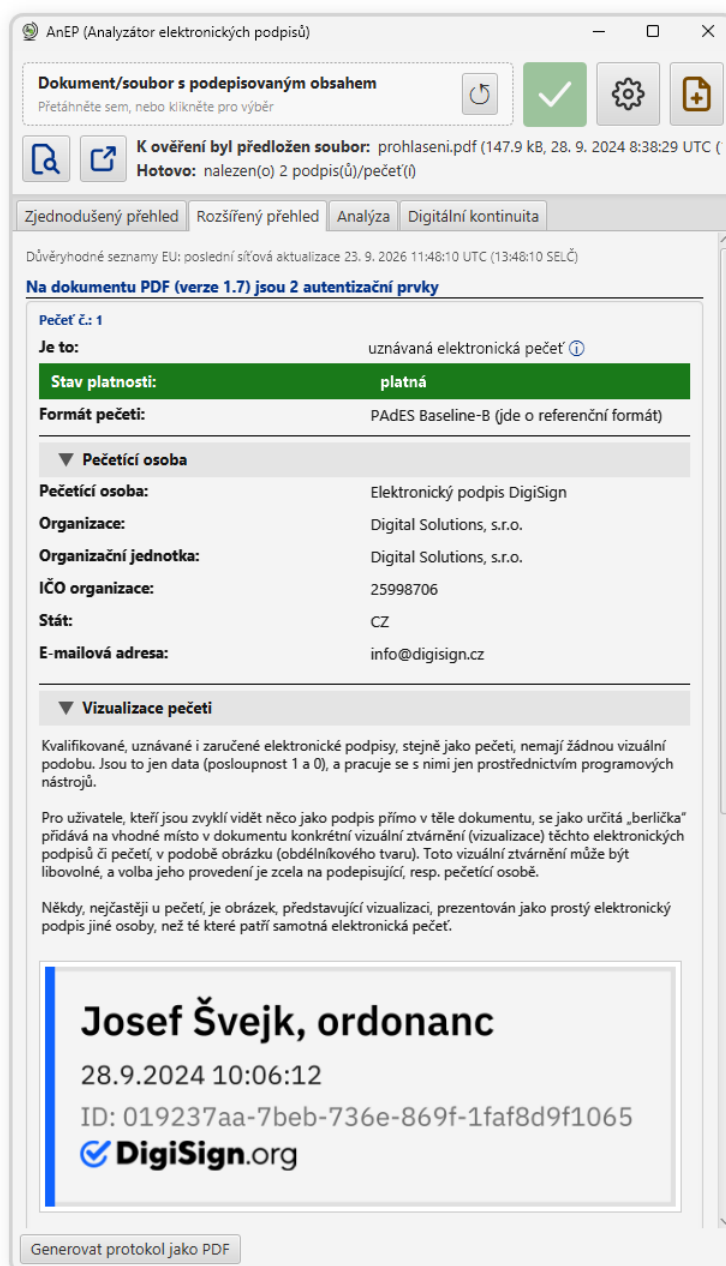
Aplikace dokáže rozpoznat, že se právě ověřovaný dokument odkazuje na jiný dokument (který v souboru není a nikdy nebude), a to skrze jeho otisky, způsobem který používá proces eLegalizace dle § 6 odst. 1 písm. a) zákona č. 12/2020 Sb. o právu na digitální služby, prováděný na CzechPOINTech. Aplikace tuto vazbu na jiný dokument rozpozná, po ověření sama otevře okno, nechá uživatele druhý dokument přiložit — a **ověří všechny otisky**. Nese-li odkázaný dokument odkaz na další, pokračuje se stejně.



Obrázek 28 Kontrola vazby na odkazovaný soubor

Vizualizace podpisu či pečeti

Aplikace detekuje vizualizaci podpisů či pečeti, včetně takových, které jsou netisknutelné či neviditelné. Upozorňuje na to, že vizualizace svým vzhledem nemusí odpovídat identitě podepsané či pečeti osoby, a dokonce může být prezentována jako prostý elektronický podpis někoho jiného.



Obrázek 29 Příklad vizualizace, považované za prostý elektronický podpis jiné osoby

Prázdná podpisová pole

Pole připravené k podpisu se vypíše i tehdy, když v něm podpis není — včetně toho, jestli by byl podpis v něm vůbec vidět a co by se jím uzamklo.

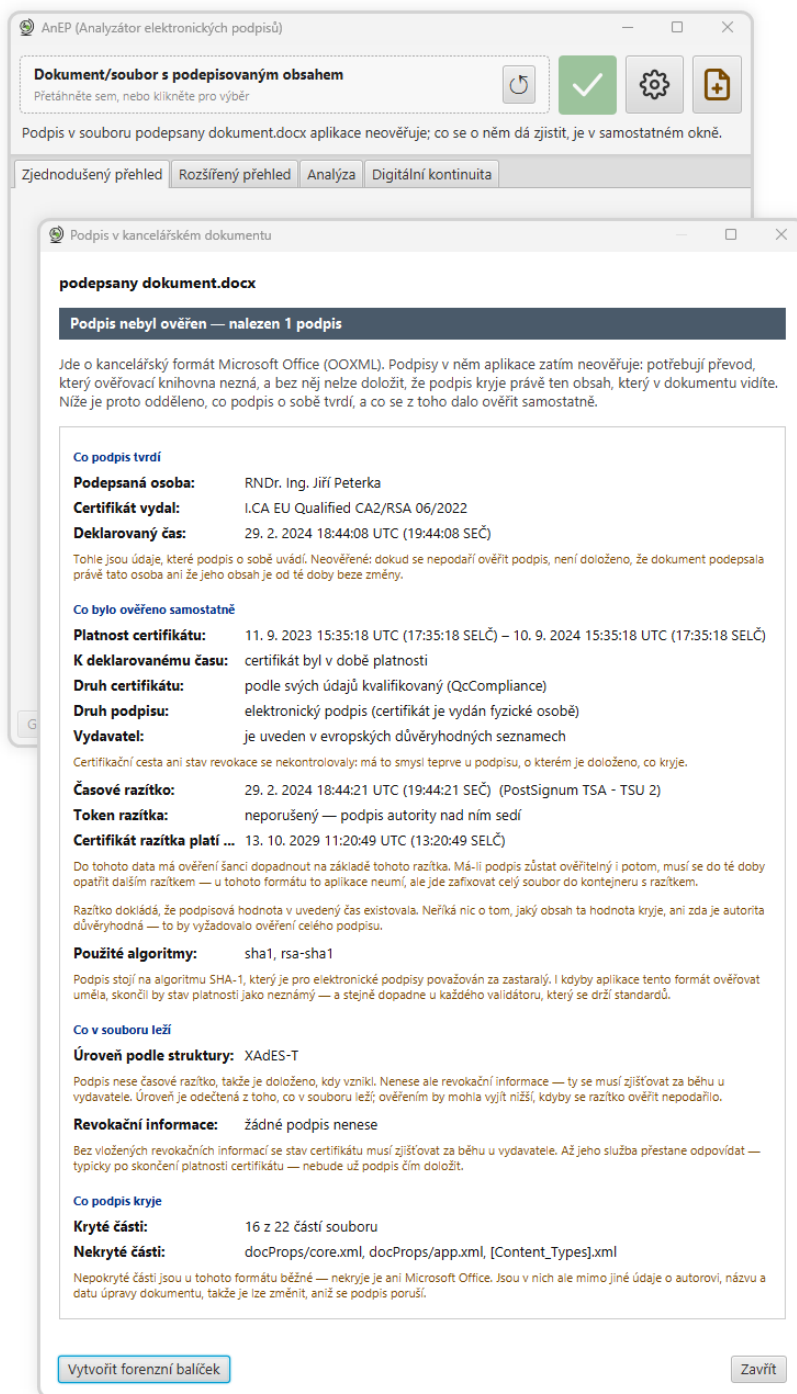
Protipodpis

Podpis, který nepodepisuje dokument, nýbrž jiný podpis, se na kartě pozná a řekne se, či podpis to podepisuje. Je to jiný vztah než dva podpisy vedle sebe a uživateli, který to nerozliší, se změní smysl celého dokumentu.

Podpisy v OOXML

DOCX, XLSX a PPTX aplikace **neověřuje** — jejich formát knihovna DSS nepodporuje. Aplikace proto podpisy (ani pečeti) na dokumentech těchto formátů neověřuje.

Pokud ale v dokumentu detekuje elektronický podpis, aplikace vypíše alespoň všechny informace, které je schopna získat: co podpis o sobě tvrdí (úroveň podle struktury B / T / LT / LTA, vložené revokační informace) a odděleně to, co se ověřit **dá i tak**: samotný token časového razítka a vlastnosti certifikátu — doba platnosti, kvalifikovanost podle QcStatements a to, zda je jeho vydavatel v evropských důvěryhodných seznamech. Nabídne se i vytvoření forenzního balíčku.



Obrázek 30 Informace o podpisu na dokumentu ve formátu DOCX

13 Nastavení a úložiště

13.1 Základní nastavení

- **Ověřování podpisů a pečeti dle standardů** — jediný přepínač přísnosti pro běžného uživatele.
- **Ověřování časových razítek podle standardů** — přísnější posuzování razítek.
- **Expertní mód** — zpřístupní Detailní rozbor a Protokoly DSS.
- **O aplikaci** — k čemu aplikace slouží, že její výstupy jsou bez záruky, dále verze, autor, licence a složka s licencemi použitých knihoven.

Změny se projeví ihned, bez restartu.



Obrázek 31 Základní nastavení

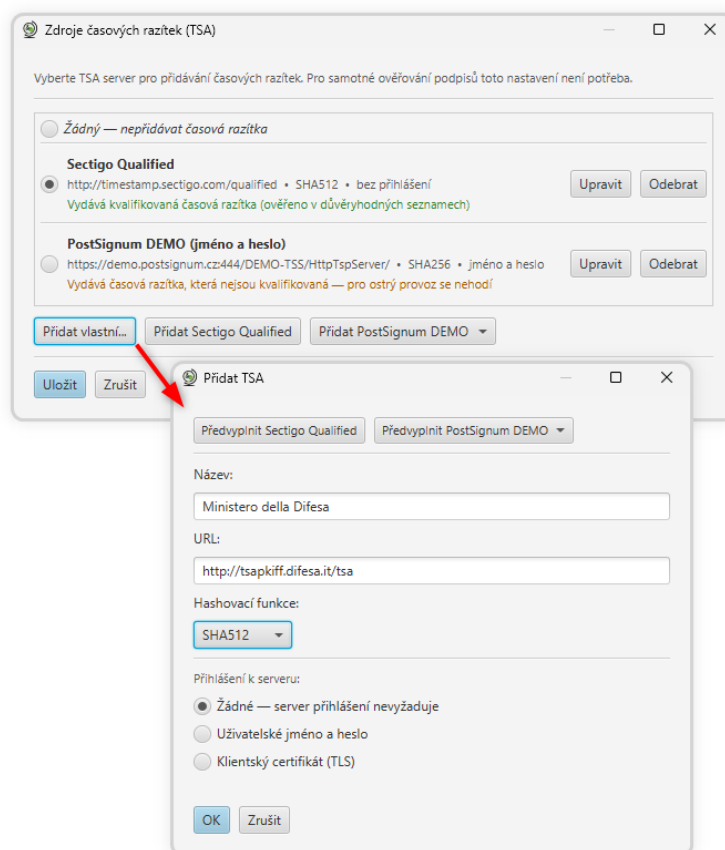
13.2 Pokročilé nastavení

Umožňuje jednorázově povolit jednotlivé ústupky, zadat ověření k zadanému datu a času, správu vlastních důvěryhodných certifikátů a vlastních CRL seznamů, nastavování zdroje časových razítek a ruční obnovu důvěryhodných seznamů EU.

13.3 Zdroje časových razítek

Zdroje se spravují jako pojmenované profily s adresou, možnostmi přihlášení (bez identifikace, jménem a heslem, pomocí certifikátu) a algoritmem otisku. Aplikace umí předvyplnit zdroj testovacích časových razítek od autority PostSignum, a veřejný zdroj kvalifikovaných časových razítek Sectigo Qualified (které jsou v malém množství poskytovány zdarma).

Při zadání se zdroj otestuje: zjistí se konec platnosti jeho certifikátu — právě podle něj se pak počítá, kam až se může posunout ověřitelnost. Kontroluje se i výčet otisků (hashovacích funkcí), které autorita skutečně podporuje, aby se pak nevybíral algoritmus, který odmítne. Nedostupnost zdroje se přitom nezamění za odmítnutí: profil jde uložit i tak, jen se dopředu neví, kam dosáhne.



Obrázek 32 Správa zdrojů časových razítek s výsledkem sondy

13.4 Kde aplikace ukládá svá data

Vše uživatelské leží v %APPDATA%\SignatureAnalyzer: nastavení a profily zdrojů razítek, vlastní úložiště CRL, vlastní důvěryhodné certifikáty a mezipaměť důvěryhodných seznamů. Do systému aplikace jinak nezasahuje.

14 Dostupnost a licence

14.1 Distribuce a spuštění

Aplikace je dostupná zdarma z adresy <https://bajecnysvet.cz/anep>, a to jako instalátor .msi i jako přenosná verze (pro Windows), obojí s vlastním běhovým prostředím — uživatel nemusí nic doinstalovávat. Start je zrychlený předpřípravením ověřovací cesty a mezipamětí důvěryhodných seznamů.

14.2 Licence

AnEP se šíří pod **Evropskou unijní veřejnou licenci (EUPL) verze 1.2**, která má závazné české znění. Licence použitých knihoven a oznámení jejich autorů se dodávají s každou distribucí.

15 Kde jsou hranice

Co aplikace **nedělá**, a je to záměr:

- **Nepodepisuje.** Umí přidat časové razítko a doplnit ověřovací materiál, ale podpis ani pečeť nevytváří.
- **Nevydává právní stanoviska.** Právní účinky uvádí jen tam, kde plynou přímo z výsledku ověření a z textu předpisu.
- **Nepředvídá cizí validátory.** O jiných nástrojích mluví v možnosti, ne v jistotě — nezná jejich verzi, nastavení ani obsah jejich zásob.
- **Nevytváří evidenční záznamy.** Ověřit je umí, vydat ne.
- **Neověřuje podpisy v kancelářských formátech OOXML.** Nahlédne do nich a řekne, co o sobě tvrdí, ale verdikt nevydává.
- **Nezakrývá ústupky.** Kladný verdikt, který stojí na povoleném ústupku, to má u sebe napsáno.
- **Nedává záruku.** Výstupy slouží k seznámení s problematikou a k vlastnímu posouzení, ne jako závazný posudek.

A Dodatek: pojmy, které dokument používá

Pojem	Co znamená
Rozhodný okamžik	Čas, ke kterému se platnost posuzuje. Určuje ho časové razítko, jinak je to přítomnost.
Důkaz existence	Doklad o tom, že podpis existoval už v určitou dobu — typicky časové razítko.
Revokační informace	Údaj o tom, zda byl certifikát odvolán: odpověď OCSP nebo seznam CRL.
Kotva důvěry	Certifikát, kterému se věří bez dalšího dokazování. Pochází z evropských důvěryhodných seznamů nebo je dodán uživatelem do vlastního úložiště aplikace.
Úroveň podpisu (B, T, LT, LTA)	Jak je podpis vybaven: B je holý podpis, T má časové razítko, LT nese i revokační údaje, LTA navíc archivní razítko.
Referenční formát	Formát, který jako referenční stanoví prováděcí rozhodnutí Komise (EU) 2015/1506; orgány veřejné moci s ním musí umět pracovat.
Digitální kontinuita	Schopnost podpisů a pečeti na dokumentu zůstat ověřitelné i po letech — a to, co je pro to třeba udělat, dokud je čas.
Zachování ověřitelnosti	Doplnění revokačních údajů a archivního časového razítka, kterým se dokument dostane na úroveň LTA. Do dokumentu se přidává, nic se v něm nepřepisuje.
Vyřazení služby	Okamžik, od kterého už služba není vedena v důvěryhodných seznamech. Razítka vydaná předtím zůstávají uznatelná, pozdější ne.
Ústupek	Povolená odchylka od standardů, kterou uživatel zapne vědomě a která platí jen na jedno ověření.
Protipodpis	Podpis, jehož předmětem není dokument, nýbrž jiný podpis na něm.
Evidenční záznam	Doklad podle RFC 4998 nebo XMLERS o tom, že soubor existoval už v určitou dobu; s podpisem nemá nic společného. Jde o určitou dobu externího časového razítka.

Aplikace sama vykládá pojmy na místě, kde je použije — v protokolu uvozením „tj.:“, na obrazovce v textu karty. Tento dodatek je jen shrnutí pro čtenáře dokumentu.