DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

eLegalizace

Texty jsou převzaty z článku https://www.lupa.cz/clanky/elektronicky-uredne-overeny-podpis-jak-funguje-elegalizace-na-czech-pointech/

Možnost legalizace elektronických podpisů (eLegalizace) na Czech POINTech, díky které takového podpisy mají účinky úředně ověřených podpisů, se otevřela v polovině roku 2022. To když nabyly účinnosti příslušné pasáže (§ 6 odst. 1 písm. a) zákona č. 12/2020 Sb., o právu na digitální služby, a také zákona č. 21/2006 Sb., o ověřování.

Legalizace jednoho podpisu, a to jak toho elektronického v rámci eLegalizace, tak i toho vlastnoručního při klasickém ověřování, stála do 31. 12. 2023 30 Kč, od 1. 1. 2024 (díky novelizaci zákona o správních poplatcích) přijde již na 50 Kč.

K uvedené možnosti eLegalizace na Czech POINT existují (a u příjemců začínají být reálně akceptovány) i další možnosti, jak u elektronických podpisů dosáhnout účinků úředně ověřených podpisů. Jde například o jednorázové vložení kvalifikovaného certifikátu do základního registru obyvatel (dle § 6 odst. 2 zákona č. 12/2020 Sb., o právu na digitální služby).

Varianta zapsání kvalifikovaného certifikátu do základního registru obyvatel má smysl, pokud uživatel potřebuje dosáhnout požadovaného efektu opakovaně. U uživatelů, kteří by službu potřebovali jen jednorázově, bude k dispozici eLegalizace na Czech POINT.

K čemu je eLegalizace?

eLegalizace slouží k tomu, aby se to, co vyžaduje úředně ověřený podpis, dalo dělat elektronicky. Jde například o návrhy vkladu do katastru, souhlasy se zápisem do veřejného rejstříku, hlasovací lístky v insolvencích, některé plné moci atd.

Kromě toho právní úprava eLegalizace (v § 6 odst 1 zákona č. 12/2020 Sb. o právu na digitální služby) přichází i s tím, že legalizovaný elektronický podpis může nahradit také uznávaný elektronický podpis. Tedy „slabší“ podpis, který nemá účinky úředně ověřeného podpisu. Jsou to jakási zadní vrátka pro toho, kdo by chtěl dělat elektronicky něco, co ani nevyžaduje úředně ověřený podpis, ale současně se nechtěl sám řádně elektronicky podepsat, a to pomocí uznávaného elektronického podpisu. Třeba proto, aby si nemusel pořizovat kvalifikovaný certifikát. A tak využije toho, že legalizovaným elektronickým podpisem může být úplně cokoli elektronického. Třeba (pouze) zaručený elektronický podpis (např. založený na certifikátu, který si někdo vystavil sám sobě), nebo dokonce i tzv. prostý elektronický podpis (třeba smajlík, viz dále). Takovýto podpis si nechá (jednorázově, za oněch 50 Kč) legalizovat a pak jej může použít i tam, kde by jinak musel použít svůj uznávaný (či kvalifikovaný) elektronický podpis.

Primární účel eLegalizace spočívá v dosažení účinků úředně ověřeného podpisu. Úředně ověřený podpis neměl donedávna žádnou elektronickou variantu, ale mohl se například využít proces, kdy potřebné písemnosti se připravily v listinné podobě, podepsaly vlastnoručními podpisy, ty se nechaly úředně ověřit a pak se celé dokumenty nechaly autorizovaně konvertovat do elektronické podoby.

Kvalifikované (či jen uznávané) elektronické podpisy nemají účinky úředně ověřených podpisů proto, že neidentifikují podepsanou osobu dostatečně jednoznačně. I podle nařízení eIDAS musí stačit, aby tato osoba byla určena jen (křestním) jménem a příjmením (tj. aby příslušný kvalifikovaný certifikát obsahoval jen tyto údaje). Ovšem osob stejného jména a příjmení může být (a je) více. Proto aby mohl mít elektronický podpis účinky úředně ověřeného podpisu, musí k němu být doplněna vhodná upřesňující informace o podepsané osobě. U vlastnoručních podpisů takovouto informaci obsahuje ověřovací doložka, nedílně spojená se samotným listinným dokumentem a jeho podpisem.

V případě elektronických podpisů lze postupovat více různými způsoby. Jedním z nich je již zmiňované jednorázové vložení kvalifikovaného certifikátu do účtu konkrétního držitele v základním registru obyvatel (ROBu). Tím vzniká ona „upřesňující informace“, která je ale dostupná jen pro toho příjemce podepsaného dokumentu, který má možnost si ji v registru obyvatel ověřit. Tomu, kdo ji nemá, ale může podepisující osoba vyjít vstříc tím, že k podepsanému dokumentu přiloží svůj vlastní výpis z ROBu, kde jsou údaje o vložených kvalifikovaných certifikátech uvedeny (mezi nereferenčními údaji).

V současné době je to asi nejjednodušší řešení, navíc zcela zdarma pro libovolný počet vytvořených podpisů. Vlastně pro všechny platné elektronické podpisy založené na příslušném kvalifikovaném certifikátu a vytvořené v době, kdy byl tento certifikát vložen do základního registru. Funguje ale jen pro uznávané a kvalifikované elektronické podpisy, což jsou právě ty, které jsou založené na kvalifikovaném certifikátu. Nefunguje pro zaručené elektronické podpisy ani pro tzv. prosté elektronické podpisy.

Jak připojit ověřovací doložku?

Další možností, jak dosáhnout toho, aby jednotlivý elektronický podpis konkrétní osoby mohl mít účinky úředně ověřeného podpisu, je přidat potřebné „upřesňující informace“ přímo k podepsanému dokumentu a jeho podpisu. Je to vlastně stejný princip jako u klasického ověřování vlastnoručních podpisů, kdy se k listinnému dokumentu a jeho podpisu připojuje ověřovací doložka. Ta obsahuje křestní jméno, příjmení, datum a místo narození i místo pobytu podepsané osoby, které zjistila a v doložce uvedla ověřující osoba.

Tvorba doložek v elektronické podobě funguje například u autorizovaných konverzí. U nich není problémem ani připojení takovéto doložky ke konvertovanému dokumentu, při jeho konverzi z listinné do elektronické podoby: výstupem je nový dokument v datovém formátu PDF, jehož jednou (poslední) stránkou je právě ona doložka v elektronické podobě. No a ověřující osoba pak celý dokument opatří svým kvalifikovaným elektronickým podpisem (a také kvalifikovaným elektronickým časovým razítkem). Je to první a jediný elektronický podpis na výstupu z konverze, který současně vytváří nedělitelné pouto mezi samotným konvertovaným obsahem a doložkou a chrání je proti změně.

Co je problémem, je připojení obdobné doložky k takovému elektronickému dokumentu, který již může být elektronicky podepsán. Nejde totiž měnit obsah již dříve podepsaného dokumentu ani jej nějak „prodlužovat“ (něco přidávat), protože to by způsobilo zneplatnění již připojených podpisů. Jinými slovy, obsah ověřovací doložky, o který nám zde jde (tj. onu „upřesňující informaci“), nelze přidat přímo do již elektronicky podepsaného dokumentu (jehož elektronický podpis má být ověřen neboli legalizován).

Co se udělat dá, je vytvořit doložku jako samostatný elektronický dokument, řádně elektronicky podepsaný ověřující osobou (či opatřený její pečetí) a také časovým razítkem. Jenže jak tuto samostatnou doložku spojit s původním dokumentem, ke kterému se doložka vztahuje, do vhodného celku? Navíc tak, aby to bylo korektní – aby se nedalo fixlovat a různě zaměňovat buď dokument s legalizovaným podpisem, či naopak doložku. Tedy aby se dosáhlo toho, co právní úprava požaduje a označuje jako „nedílné spojení“.

Notáři používají ASiC kontejnery

Notáři, kteří legalizaci elektronických podpisů mohou provádět od září 2021 „zabalí“ doložku i s legalizovaným dokumentem do ASiC kontejneru, který „uzavře“ tím, že jej opatří svým (kvalifikovaným) elektronickým

podpisem. Postupuje přitom podle § 3 nařízení vlády č. 317/2021 Sb., o postupu notáře při legalizaci elektronického podpisu, kde je tento postup zakotven.

Samotné ASiC kontejnery, formálně „kontejnery s přidruženým podpisem“, jsou standardizovaným řešením, se kterým počítají i prováděcí předpisy k nařízení eIDAS. Zejména Prováděcí rozhodnutí Komise 2015/1506, „kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru“ a které veřejnoprávním subjektům mj. ukládá povinnost akceptovat ASiC kontejnery.

Podpora ASiC kontejnerů se může opírat o detailní technické standardy od organizace ETSI. Díky tomu mohou existovat – a skutečně existují – běžně dostupné nástroje a služby pro práci s ASiC kontejnery, stejně jako programové knihovny pro využití při tvorbě nových programů a služeb.

ASiC kontejnery podporují například všechny tuzemské kvalifikované služby pro ověřování platnosti elektronických podpisů.

Místo nedílného celku samostatné dokumenty

Výstupem eLegalizace na Czech POINTu není jeden celek zahrnující jak originální dokument s legalizovaným podpisem, tak i ověřovací (legalizační) doložku, jako je tomu u ASiC či u klasické legalizace [1)]

To u eLegalizace na Czech POINTu je ověřovací (legalizační) doložka zcela samostatným elektronickým dokumentem. Právě takováto samostatná doložka je to, co dostanete od Czech POINTu, když si u něj necháte provést nějakou eLegalizaci. To, co vám (po ověření na přepážce Czech POINTu) buď pošlou do datové schránky, nebo co si na základě vydaného „šatního lístku“ můžete sami vyzvednou v úschovně Czech POINTu.

Jde o samostatné PDFko, opatřené kvalifikovaným elektronickým podpisem ověřující osoby a kvalifikovaným elektronickým časovým razítkem. Kromě identifikace konkrétní fyzické osoby obsahuje doložka ještě údaje o samotném legalizovaném elektronickém podpisu. Dále v doložce najdete údaje o certifikátu, na kterém je podpis založen.

Elektronickým podpisem, který chcete legalizovat, může být i prostý elektronický podpis, což může být úplně cokoli.

Podstatné je, že tyto „doplňující údaje“ nepostačují k jednoznačnému určení dokumentu, na kterém se legalizovaný podpis má nacházet. Tedy ke kterému (elektronickému) dokumentu se doložka vztahuje. A ještě přesněji, ke které jeho instanci, protože tento dokument může procházet změnami. Smysl těchto „doplňujících údajů“ je jiný: určit, o který konkrétní podpis na originálním dokumentu se jedná, protože jich tam může být více. V případě zaručených (a vyšších) elektronických podpisů k tomu slouží údaje o certifikátu, na kterém je podpis založen.

V případě prostých elektronických podpisů jde už i o to, co vlastně je oním podpisem, když to může být úplně cokoli. Třeba některé slovo v textu, nějaké interpunkční znaménko, ikona a podobně. Proto zde ověřující osoba uvádí určité své hodnocení.

Nedílné spojení skrze otisky (hashe)

Čím je tedy dáno to, ke kterému konkrétnímu dokumentu se doložka vztahuje? Doložka je zcela samostatným dokumentem, který tak existuje „vedle“ originálního dokumentu s legalizovaným podpisem. Jak a čím je mezi oběma samostatnými dokumenty tvořena vazba, o které právní úprava hovoří jako o nedílném spojení?

Odpověď je taková, že doložka se odkazuje na originální dokument prostřednictvím jeho kryptografického otisku neboli tzv. hashe. Což je stejný princip, jaký používají třeba externí elektronické podpisy, které jsou také samostatnými objekty (dokumenty) a na podepsaný obsah (dokument) se odkazují přes jeho otisk.

Zásadní rozdíl je ale v tom, že externí podpisy jsou standardizovaným řešením. Existují pro ně platné standardy, které určují, jak má vše vypadat a fungovat. Díky tomu může být (a dávno je) jejich podpora zabudována všude tam, kde je o ni zájem. Pro programátory jsou k dispozici různé knihovny a další potřebné nástroje usnadňující další zavádění této podpory.

Vazbu vytváří hned 4 různé otisky

Zpětnou analýzou výstupu z eLegalizace lze vysledovat, že doložka se na dokument s legalizovaným podpisem odkazuje nikoli jedním, ale hned čtyřmi různými kryptografickými otisky. Tedy otisky, vytvořenými pomocí různých hashovacích funkcí. Což posiluje odolnost vůči postupnému zastarávání těchto funkcí, a lépe chrání před nebezpečím existence tzv. kolizních dokumentů. To jsou takové, které mají jiný obsah, ale stejný otisk.

Tyto otisky lze nalézt v textové podobě přímo v doložce.

Je to ale spíše „pro úplnost“, protože těžko někdo bude ručně kontrolovat shodu otisků mezi doložkou a dokumentem, ke kterému se doložka vztahuje. Strojovému zpracování vychází vstříc to, že otisky jsou dostupné i ve strojově čitelné podobě – jako XML dokument, obsažený v PDFku s ověřovací doložkou jako jeho přílohou.

[1)]
jeden ASiC kontejner v případě eLegalizace u notáře, či několik „sešitých“ a přelepkou opatřených listů papíru u klasické legalizace vlastnoručních podpisů na listinných dokumentech (případně jen jeden list s nalepenou doložkou či doložkami).

From:
https://archi.gov.cz/ - **Architektura eGovernmentu ČR**

Permanent link:
https://archi.gov.cz/nap:elegalizace

Last update: **2024/08/14 09:53**