https://www.lupa.cz/clanky/zranitelnost-roca-co-se-deje-se-slovenskymi-a-estonskymi-e-obcankami/

Zranitelnost ROCA: co se děje se slovenskými a estonskými e-občankami?

Jiří Peterka 6. 11. 2017

Objev česko-slovenského vědeckého týmu z Masarykovy univerzity v Brně má nepříjemné důsledky pro elektronické občanské průkazy na Slovensku, ale i v Estonsku.

155 názorů

Zatímco u nás doma se kolem občanských průkazů s čipem, elektronického podpisu a služeb eGovernmentu aktuálně nic moc neděje, na Slovensku se naopak „dějí věci“: v nedávných dnech zde orgány veřejné moci přestaly přijímat elektronická podání, podepsaná s pomocí tamních elektronických občanských průkazů, a 31. 10. 2017 (k času 18:23) pak byly zrevokovány všechny kvalifikované certifikáty vystavené k soukromým klíčům na těchto e-občankách. Jejich držitelé si nyní musí pořídit certifikáty nové.

Svým způsobem je to docela bomba, která ale nevybuchla jen na Slovensku. Postihla i další země, konkrétně také Estonsko. I zde nakonec museli revokovat všechny certifikáty na tamních e-občankách (k 3. 11. 2017) a vyzvat jejich držitele k získání nových certifikátů.

Ale proč? Co bylo příčinou? A co je ohroženo?

Zranitelnost ROCA

Za vším je výsledek bádání česko-slovenského týmu vědců z centra CRoCS (Centre for Research on Cryptography and Security) při Fakultě informatiky na Masarykově univerzitě v Brně, ve spolupráci se společností Enigma Bridge a italskou Ca' Foscari University.

Svůj objev prezentovali minulý týden na konferenci ACM CCS 2017, kde za něj dostali jedno ze dvou hlavních ocenění (Real-World Impact Award).

Zdroj: DSL.SK

Podstatou je nalezení chyby v jedné konkrétní softwarové knihovně (RSA Library version v1.02.013 od německé společnosti Infineon), která se využívá v některých krypto-čipech (a to již od roku 2012) pro generování klíčových párů (soukromého a veřejného klíče) pro podpisové schéma RSA. Konkrétně chybuje v generování velkých prvočísel, které jsou u RSA základem pro výpočet obou klíčů. Používá k tomu „urychlovací algoritmus“ Fast Prime, který ale v daném případě negeneruje ona prvočísla tak, jak by správně měl.

Nalezená chyba pak v konkrétních případech (při použití klíčů generovaných touto knihovnou) nabourává základní předpoklad pro praktickou použitelnost elektronického podpisu: že z veřejného klíče není možné odvodit (vypočítat) klíč soukromý. Přesněji: že to nejde rychleji než za dobu tak dlouhou a s takovými náklady, že už by to pro nikoho nemělo cenu. Bohužel z veřejného klíče, který byl vygenerován onou chybující knihovnou, lze soukromý klíč odvodit mnohem rychleji – tak rychle (a s relativně nízkými náklady), že už by se to někomu mohlo vyplatit.

Za jak dlouho by se to podařilo, uvádí autoři v popisu svého objevu: pro dnes nejčastěji používané klíče o velikosti 2048 bitů je to (v nejhorším případě) cca 140 roků běhu jednoho vlákna běžně dostupného CPU. S tím, že výpočet (proces hledání) lze dobře paralelizovat a využít tak více vláken a celých procesorů současně, a tím násobně zkrátit reálný čas výpočtu, klidně i na dny, či dokonce hodiny. Odhad max. nákladů, které autoři uvádí pro prolomení klíče o velikosti 2048 bitů (nalezení soukromého klíče ke konkrétnímu veřejnému klíči), při použití cloudových služeb Amazon AWS c4, je asi 40 000 USD. Pro klíče o velikosti 1024 bitů by to pak bylo jen nějakých (maximálních) 80 USD.

Následně, již po zveřejnění na konferenci ACM, se v odborné komunitě objevily zprávy o možnosti ještě rychlejšího a levnějšího prolomení.

Takovéto prolomení, pro jehož vlastní verzi autoři použili označení ROCA (The Return of Coppersmith's Attack), už by pro někoho (se zlými úmysly) mohlo být reálně využitelné. S nedozírnými následky pro toho, jehož soukromý klíč by byl touto cestou odvozen (vypočítán).

Co je ve hře?

To, že z veřejného klíče není možné odvodit klíč soukromý, resp. že to nejde rychleji, než za nějakou opravdu extrémně dlouhou dobu, je alfou a omegou naší důvěry v elektronické podpisy i základním předpokladem pro možnosti jejich praktického využití. Tedy alespoň u „skutečných“ elektronických podpisů, které jsou založeny na algoritmech a metodách kryptografie a které bychom správně měli označovat spíše jako digitální. Neformálně si je můžeme představovat také jako „počítané“ (ve smyslu: vznikající výpočtem).

Zdůrazňuji to proto, že naše legislativa používá pojem „elektronický podpis“ i pro takové úkony v elektronickém světě, které s kryptografií nemají nic společného, s žádnými klíči vůbec nepracují a u kterých ani není co počítat, co ověřovat, natož pak prolamovat. Ani na co se spoléhat – ale to by bylo na jiné povídání (které už jsem jednou zde na Lupě publikoval).

Pokud tedy zůstaneme u těch elektronických podpisů, které vychází z algoritmů a metod kryptografie a které se soukromými a veřejnými klíči pracují – pak si musíme uvědomit, jak fungují: při podepisování (vytváření elektronického podpisu) podepisující osoba používá svůj soukromý klíč, zatímco platnost již vytvořeného podpisu si protistrana (příjemce, resp. tzv. spoléhající se osoba) ověřuje pomocí veřejného klíče. To znamená, že podepisující osoba si musí pečlivě hlídat svůj soukromý klíč, aby s ním nemohl vládnout nikdo jiný (protože jinak by se mohl podepisovat místo ní). A naopak: veřejný klíč potřebuje mít k dispozici každý, kdo nějaký podepsaný dokument přijímá a má mít možnost si ověřit jeho platnost.

Proto je nutné, aby oprávněný držitel soukromého klíče mohl bez obav dát odpovídající veřejný klíč skutečně komukoli: musí mít jistotu, že ten, kdo jeho veřejný klíč získá, z něj nebude moci odvodit (vypočítat) odpovídající soukromý klíč. Přesněji: že to nedokáže tak rychle, aby ho mohl jakkoli zneužít.

V praxi se veřejné klíče rozdávají nikoli samostatně, ale jako součást certifikátů vystavovaných certifikačními autoritami. Certifikát je vlastně jakési dobrozdání či osvědčení od třetí důvěryhodné strany (certifikační autority), určené širší veřejnosti. Říká, kdo prohlašuje za svůj ten soukromý klíč, kterému odpovídá veřejný klíč obsažený v certifikátu. Podle toho se pak, při ověřování elektronického podpisu (pomocí veřejného klíče), tento podpis přisuzuje konkrétnímu původci. Tj. za podepsanou osobu se považuje ta osoba, jejíž identita je uvedena v certifikátu.

Nicméně samotný soukromý klíč v certifikátu obsažen není a být ani nemůže, a to již z principu (protože certifikáty jsou v zásadě veřejné).

Bývá dobrým zvykem přikládat takovýto certifikát přímo ke konkrétnímu elektronickému podpisu, aby jej příjemce měl k dispozici a nemusel jej sám někde hledat. Třeba na webu té certifikační autority, která certifikát vydala – protože standardním postupem (pokud držitel certifikátu neřekne jinak) je to, že jej autorita zveřejní sama.

V praxi to reálně znamená, že držitel soukromého klíče nemá žádnou kontrolu nad tím, jak se dále šíří jeho veřejný klíč, obsažený v příslušném certifikátu. Kdokoli si ho mohl stáhnout (z webu vydavatele), nebo ho získal z kteréhokoli podepsaného dokumentu, ke kterému se mohl dostat jakkoli. Ostatně, i tomu vděčí veřejný klíč za svůj přívlastek („veřejný“).

Proto je jakékoli narušení základního principu – že z veřejného klíče nejde reálně odvodit klíč soukromý – tak nebezpečné. Protože ten, kdo by si soukromý klíč přeci jen dokázal (v nějakém „ještě únosném“ čase) z veřejného klíče odvodit, by se mohl podepisovat místo

oprávněného držitele soukromého klíče. A nikdo by už nedokázal rozlišit, kdo je skutečným autorem konkrétního podpisu.

Se znalostí soukromého klíče by pak mohl ten, kdo zná jeho hodnotu, elektronicky podepsat třeba smlouvu o prodeji domu, který patří oprávněnému držiteli soukromého klíče. A to bez jeho vědomí, ale vlastně jeho jménem. Pokud by se jednalo o soukromý klíč, ke kterému byl vystaven kvalifikovaný certifikát, šlo by (zde v ČR) o tzv. uznávaný elektronický podpis a jím podepsanou smlouvu by Katastr měl akceptovat jako součást žádosti o vklad. Obdobně pro všechny právní úkony (právní jednání), které lze realizovat elektronickou cestou za použití uznávaných elektronických podpisů. Raději nedomýšlet…

Nedivme se proto, že na Slovensku dočasně přestali přijímat takovéto elektronické podpisy (u kterých prolomení hrozí) a že dochází k revokaci již vystavených certifikátů a vydávání nových. Je spíše otázkou, zda jsou tato opatření dostatečná a zda nepřichází pozdě.

Kde nebezpečí hrozí a jak bylo zveřejněno?

Zdůrazněme si, že právě popsaná zranitelnost (ROCA) se netýká samotného principu fungování (digitálních, kryptografických, resp. „počítaných“) elektronických podpisů. Nejde o žádnou chybu či problém celého jejich konceptu, ani podpisového schématu RSA jako takového. Jde o důsledek chyby jednoho konkrétního softwaru (knihovny), kterou je třeba opravit a napravit přímé důsledky této chyby.

Výzkumný tým podle svého vyjádření odhalil popisovanou zranitelnost (chybu) koncem ledna tohoto roku. Zjistil, že německá společnost Infineon Technologies AG svou chybující knihovnu využívá ve svých čipech, které jsou základem různých kryptografických modulů (TPM, Trusted Platform Module), stejně jako čipových karet a USB tokenů.

Proto tým z MU v Brně ihned informoval společnost Infineon o svém zjištění a v duchu principu tzv. zodpovědného odhalení (Responsible disclosure) počkal plných 8 měsíců se zveřejněním svého zjištění. A i toto zveřejnění „rozfázoval“ do dvou hlavních etap: nejprve (v polovině října) zveřejnil obecnější popis celého zjištění (např. zde) a teprve na konci října a přelomu listopadu pak na již zmiňované konferenci ACM (CCS 2017) představil detaily.

Ona prodleva 8 měsíců umožnila, aby výrobce vadných čipů stihl zareagovat a aby se mohlo zjistit, kam všude se chyba rozšířila – koho a co zasáhla. Prohlášení samotné společnosti Infineon je ale jen dosti obecné, když hovoří jen o „informování zákazníků“ a nabídce cest ke „zmírnění dopadů“.

Dlužno dodat, že německá společnost Infineon není zdaleka jediným výrobcem kryptografických čipů a také ne všechny její produkty mají v sobě „zadrátovánu“ onu chybující knihovnu. A navíc, podle jejího prohlášení, se nalezená zranitelnost (chyba) projevuje jen tam, kde je u oné knihovny zapnuta akcelerace při hledání prvočísel pro potřeby generování klíčového páru.

Jinými slovy: nalézt konkrétní produkty či služby, které nalezenou zranitelností trpí, je poněkud složitější.

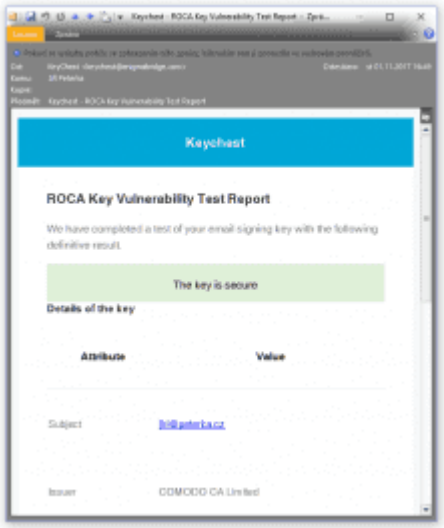
Dnes již víme, že zranitelnost se týká například čipů řady SLE78CFX3000P v nových elektronických občankách na Slovensku (ale stejně tak e-občanek v Estonsku a zřejmě i v Rakousku). Ale díky kryptomodulům TPM (Trusted Platform Module) je dosah celého problému nejspíše mnohem širší a „mapování“ jeho dosahů stále probíhá.

Různých seznamů toho, na co (a na koho) nově objevená zranitelnost dopadá, je samozřejmě více. Asi nejsystematičtější a nejrozsáhlejší přehled, který jsem zatím našel, publikoval a dále aktualizuje britský National Cyber Security Centre: podle něj se zranitelnost týká například platformy ChromeOS, zařízení Yubikey či autentizační karty Gemalto IDPrime.Net, ale také platformy Windows. Zde, na platformě Windows, jde například o použití služby BitLocker s TPM 1.2. Zmíněný seznam britské NCSC pak obsahuje i odkazy na weby příslušných výrobců, kde oni sami informují o postupech řešení a nápravy.

Jak zjistit, zda jste ohroženi?

Možná nejjednodušší cestou, jak zjistit, zda se nově objevená zranitelnost týká i vás, je využít „detekčních“ prostředků, které zpřístupnili sami autoři objevu. Podařilo se jim totiž najít způsob, jak přímo (a pouze) z veřejného klíče snadno a rychle poznat, zda je, či není ohrožen zranitelností ROCA.

Odkazy na tyto prostředky najdete v popisu celé zranitelnosti a jsou dostupné jak pro off-line použití, tak i pro využití on-line. Existuje i jejich emailová verze: pokud na adresu roca@keychest.net pošlete elektronicky podepsaný email, jako odpověď dostanete zprávu o tom, zda váš veřejný klíč (obsažený v podpisovém certifikátu) je v bezpečí.



Nejjednodušší je asi využít on-line verze nástrojů a nechat si zkontrolovat přímo své certifikáty: sám jsem si takto ověřil všechny své kvalifikované i nekvalifikované certifikáty od tuzemských (i zahraničních) vydavatelů a žádný z nich nebyl zranitelností postižen.

Ověřil jsem si takto i starší a dnes již neplatný certifikát, vystavený k soukromému klíči generovanému na mém (českém) občanském průkazu s čipem, a i zde bylo vše v pořádku.

K čemu jsou elektronické občanky?

Naše stávající občanské průkazy s čipem, vydávané od 1. 1. 2012, tedy zřejmě nejsou zranitelností ROCA ohroženy. Už i proto, že jsou vlastně starší a používají technologie dostupné ještě před rokem 2012 (zatímco ona chybující knihovna od společnosti Infineon pochází právě z roku 2012).

Navíc je dobré si připomenout, že naše stávající občanské průkazy, a to i ve verzi s čipem, vlastně vůbec nejsou elektronické. Jejich základní funkcí je prokazování totožnosti, resp. identifikace a autentizace – a z tohoto pohledu jsou jen prostým kusem plastu, na kterém jsou natištěny potřebné údaje (včetně fotografie držitele). Však také tyto své funkce plní úplně stejně i ve verzi bez čipu.

Varianta s čipem, kterou si za příplatek 500 Kč pořídilo jen úplné minimum lidí, podle původních představ možná měla nějak umožňovat a podporovat elektronickou identifikaci a autentizaci, ale zákonodárci to bohužel „nedomysleli“ – když cestou práva umožnili využít onen čip pouze jako úložiště soukromých klíčů (a certifikátů) pro elektronický podpis. Navíc bez toho, že by tento čip, resp. celý občanský průkaz, prošel certifikací na bezpečný (dnes: kvalifikovaný) prostředek pro vytváření elektronických podpisů (SSCD, resp. QSCD).

Takže ve finále je to vlastně jen taková dvojkombinace: čistě plastová občanka, plus (necertifikovaná) čipová karta, kterou je možné využít pro elektronické podepisování. Ale nikoli formou nejspolehlivějšího kvalifikovaného elektronického podpisu, protože k tomu by byla nutná právě ona certifikace na bezpečný/kvalifikovaný prostředek (SSCD/QSCD).

Zdůrazněme si, že zranitelnost ROCA se týká jen funkce čipové karty. A to ještě jenom tam, kde je klíčový pár (soukromý a veřejný klíč) generován přímo uvnitř čipu.

Je to důležité pro správné pochopení toho, co se nyní děje se slovenskými občanskými průkazy (eID) a také s tamními elektronickými doklady o pobytu (eDoPP): stejně jako

v našem případě to jsou „dvojkombinace“, zahrnující jak „průkaz totožnosti“ (eID funkci), tak i čipovou kartu pro potřeby elektronického podpisu.

Na rozdíl od našich průkazů ale jsou ty slovenské skutečně elektronické, a to v obou svých částech, resp. funkcích. Tedy i pokud jde o funkci elektronické identifikace a autentizace, která ale není zranitelností ROCA nijak ohrožena – a svou roli „skutečně elektronického průkazu totožnosti“ tak slovenské průkazy mohou plnit i nadále a beze změny.

Zranitelností ROCA je ohrožena pouze ta část slovenských průkazů, která je fakticky čipovou kartou pro uchovávání soukromých klíčů a k nim vystavených kvalifikovaných certifikátů. Podstatným rozdílem oproti našim občanským průkazům s čipem, resp. jejich funkce čipové karty, je skutečnost, že na Slovensku tato část průkazu prošla potřebnou certifikací a je bezpečným prostředkem pro vytváření elektronických podpisů (SSCD, dnes „kvalifikovaným prostředkem“, zkratkou QSCD).

Na Slovensku totiž od začátku dodržují ducha unijní legislativy k elektronickým podpisům, která počítá s používáním bezpečných (dnes: kvalifikovaných) prostředků pro vytváření elektronických podpisů – zatímco u nás jsme se již v roce 2000 vydali cestou národních výjimek („přeci nebudeme lidi nutit kupovat si nějakou drahou čipovou kartu“) a zavedli si uznávané elektronické podpisy (které nevyžadují ony bezpečné/kvalifikované prostředky). Nicméně skutečné využití občanského průkazu jako bezpečného prostředku pro vytváření el. podpisů je i na Slovensku dobrovolné, a nikoli povinné. Čip sice mají všechny průkazy (kterých bylo vydáno již cca 2,5 milionu), ale klíče a certifikáty si na nich nechávají generovat jen ti, co o tuto možnost mají zájem (těch bylo cca 300 000, zdroj).

Paradoxně jsou ale dnes na Slovensku biti za to, že se vydali předepsanou cestou bezpečných/kvalifikovaných prostředků – a doplatili na to, že ani předepsaná certifikace bezpečných prostředků v akreditovaných laboratořích (zde konkrétně provedená v Německu) nedokázala odhalit dnes popisovanou zranitelnost. Což je docela smutné zjištění.

Jak postupovali na Slovensku a jak v Estonsku

Jak jsme si již řekli v úvodu článku, na Slovensku nakonec – po určitém počátečním váhání, nepochopení a popírání celého problému a jeho zlehčování – nakonec přistoupili k revokaci podpisových certifikátů, umístěných na čipu tamních občanských průkazů a dokladů o pobytu. Přesněji: všech tří certifikátů, které jsou zde umístěny a které byly vydány k soukromým klíčům, vygenerovaným v příslušném páru přímo na kartě a jejím čipu (s využitím chybující knihovny): jde o kvalifikovaný certifikát pro elektronický podpis (certifikát ACA, dle bodu 15 článku 3 nařízení eIDAS), dále o (ne-kvalifikovaný) certifikát pro elektronický podpis (certifikát PCA, dle bodu 14 článku 3 nařízení eIDAS) a dále o šifrovací certifikát (certifikát SCA). Podle tohoto zdroje mělo být revokováno celkem 296 037 kvalifikovaných certifikátů.

Současně na Slovensku vyzvali ty držitele, kteří nadále chtějí využívat své průkazy i pro elektronické podepisování, aby si pořídili certifikáty nové. Původní představa byla taková, že to půjde zařídit na dálku, ale nakonec to přeci jen vyžaduje osobní účast (dostavit se na „kterékoli oddělení dokladů“). Mělo by se jednat o nové certifikáty ke klíčům o velikosti 3072 bitů. U těch je ale, alespoň podle tohoto zdroje, otázkou, zda také nejsou ohroženy zranitelností ROCA.

Nicméně i toto by mělo být jen krátkodobým řešením před přechodem na řešení zásadnější. Tím by měl být (prý již v lednu 2018) přechod na podpisové schéma DSA, resp. jeho variantu s eliptickými křivkami ECDSA. Zde už se totiž s prvočísly vůbec nepracuje, a tak zde nalezená zranitelnost ROCA nehrozí. Také další vlastnosti tohoto podpisového schématu jsou příznivější (např. pro praktické nasazení vyžadují menší výpočetní kapacitu). Nevýhodou je ale to, že u nich již nejde jednoduše „obrátit“ využití soukromého a veřejného klíče a místo k podepisování je využít pro šifrování. To jde dělat jen u schématu RSA, kde se dá šifrovat veřejným klíčem a dešifrovat klíčem soukromým.

Celkově je ale možné konstatovat, že na Slovensku se „začaly dít věci“ až po první fázi zveřejnění celé zranitelnosti, tedy až ve druhé půlce října. I když (podle tohoto zdroje) se slovenská autorita Disig, vydávající certifikáty pro tamní e-občanky, o problému dozvěděla již 20. června 2017. A nedovedu si představit, že by si to nechala jen pro sebe a neinformovala o tom kompetentní orgány státu.

To Estonsko veřejně zareagovalo prakticky okamžitě poté, co bylo (30. srpna) o nalezené zranitelnosti informováno přímo jejími objeviteli – s tím, že nebezpečí nebere na lehkou váhu a dále jej zkoumá. K tomu je vhodné dodat, že v Estonsku bylo před volbami, které tam mohou probíhat i elektronicky, právě s využitím tamních elektronických občanek. O to více si Estonci nemohli dovolit problém jakkoli ignorovat či jen bagatelizovat.

Podle tohoto zdroje estonský předseda vlády, jakmile se o zranitelnosti dozvěděl, odvolal plánovanou státní návštěvu Polska a jal se věci řešit. Asi i včetně hodnocení toho, co a jak hrozí a zda nebude nutné odvolat nadcházející volby. To na Slovensku tamní ministr vnitra Kaliňák zareagoval „trochu jinak“ (výzvou, ať mu hacknou jeho e-občanku).

Jedním z prvních opatření, které v Estonsku přijali (počátkem září, a tedy jen několik málo dnů, co se o problému dozvěděli), bylo znepřístupnění (uzavření) veřejné databáze certifikátů na e-občankách. Museli tedy již znát podstatu zranitelnosti a vědět, že hrozí právě odvození soukromého klíče z klíče veřejného. Současně doporučili svým občanům, aby místo „čipových“ e-občanek raději používali mobilní eID, které nalezenou zranitelností netrpí. Informovali i své e-rezidenty, kterých se celý problém týká také.

Nakonec i v Estonsku, po zveřejnění detailů celé zranitelnosti a s pravděpodobnou brzkou dostupností různých nástrojů na reálné prolamování soukromých klíčů, přistoupili také k revokaci všech certifikátů ze svých e-občanek (viz úvod článku). Současně vyzvali jejich držitele k získání nových.

V souvislosti se zranitelností ROCA se hodně mluvilo i o Rakousku, které by mělo být také „zasaženo“. Tamní e-občanky ale již delší dobu používají podpisové schéma ECDSA (tedy to, na které na Slovensku i v Estonsku teprve chtějí přejít), a tudíž zranitelností ROCA nejsou ohroženi.

Co způsobila revokace?

Za zmínku určitě stojí i dopady hromadné revokace certifikátů, ke které došlo na Slovensku i v Estonsku – k datu 31. 10. 2017, resp. 3. 11. 2017. Jak to tedy je s platností podpisů vytvořených ještě před tímto datem?

Obecně je možné konstatovat, že platnost takovýchto podpisů ovlivněna není, protože se s časem nemění. Co se ale v čase mění a co je revokací zásadně ovlivněno, je naše schopnost ověřit a prokázat stav platnosti nějakého konkrétního podpisu.

U takových dokumentů, které byly řádně podepsány ještě před revokací podpisového certifikátu, a stejně tak byly ještě před revokací opatřeny (kvalifikovaným) časovým razítkem, se na možnosti ověřit jejich platnost nic nemění. Díky časovému razítku je totiž možné prokázat, že podpis existoval již před okamžikem přidání razítka. Zde tedy problém nevzniká, resp. možnost ověření se kvůli revokaci nemění.

Ovšem u dokumentů, které sice byly podepsány před revokací, ale ke kterým nebylo včas (rozuměj: ještě před revokací) přidáno časové razítko, už problém je. Kvůli absenci (kvalifikovaného) časového razítka totiž přicházíme o důkaz toho, že podpis existoval již před okamžikem revokace. Obvyklé metody (strojového) ověřování platnosti pak musí ověřovat platnost podpisu k aktuálnímu časovému okamžiku (tedy: už po revokaci), a už tedy nemohou podpis ověřit jako platný.

Možnost ověřit takovýto podpis bez časového razítka však stále existuje, ale už je to spíše na „ruční“ ověřování, případně až na ověřování před soudem cestou soudního znalce: musí se najít nějaký jiný důkaz (než chybějící časové razítko), který bude dosvědčovat, že daný podpis existoval ještě před revokací. A bude na „lidském“ posouzení (případně až před soudem), zda je takovýto důkaz dostatečně spolehlivý (i vzhledem k tomu, co je ve hře).

Příkladem takového důkazu o existenci podpisu v určitém čase může být třeba záznam elektronické podatelny o okamžiku přijetí podepsaného dokumentu. Nebo nějaká „digitální stopa“, případně svědecká výpověď apod.

Takže: ne, že by to nešlo (prokázat platnost podpisu i bez časového razítka). Ale může to být dosti složité, hodně nákladné a nemusí to vždy vést k očekávanému výsledku.

Berme to proto jako ponaučení a argument pro používání (kvalifikovaných) časových razítek i tam, kde to není explicitně předepsáno jako povinnost. V ČR to mají jako povinnost (z §11 zákona č. 297/2016 Sb.) všechny orgány veřejné moci, u všech elektronických dokumentů, které produkují v rámci výkonu své působnosti: musí podepisovat (nebo pečetit) a současně musí opatřovat časovými razítky. Pro právnické a fyzické osoby ale připojování časových razítek povinností není. Nicméně lze to vřele doporučit, i kvůli právě popsanému příkladu ze Slovenska a Estonska.

K tomu lze ještě dodat, že časová razítka nejsou zdarma. Nicméně i „v malém“ stojí srovnatelně či méně než tisk či kopírování jedné strany A4. A rozhodně mnohem méně, než jaké mohou být náklady na řešení případných sporů, když dojde na příslovečné lámání chleba.

Je to vůbec rozumné?

Na samotný závěr možná ještě jeden osobní postřeh a názor: podle mne není úplně ideální kombinovat v sobě (elektronický) průkaz totožnosti a čipovou kartu (bezpečný/kvalifikovaný prostředek pro vytváření elektronických podpisů).

Samozřejmě to má určité výhody, ale i řadu nevýhod, které spíše převažují. Například to, že „režim používání“ bývá odlišný: průkaz totožnosti u sebe obvykle nosíme pořád, zatímco čipovou kartu pro podepisování už pořád u sebe mít nemusíme. Spíše si ji nějak hlídáme a raději uchováváme na nějakém bezpečném místě. Nehledě již na rozdílnou „životnost“ průkazu totožnosti (klidně i 10 let) a podpisových certifikátů (dnes standardně 1 rok).

Nebo, a to se ukazuje právě nyní: když u jedné složky takovéto „dvojkombinace“ dojde k nějakému problému, veze se s ní i druhá složka. A zdaleka ne každý dokáže rozlišit, čeho se problém týká, a čeho naopak nikoli.