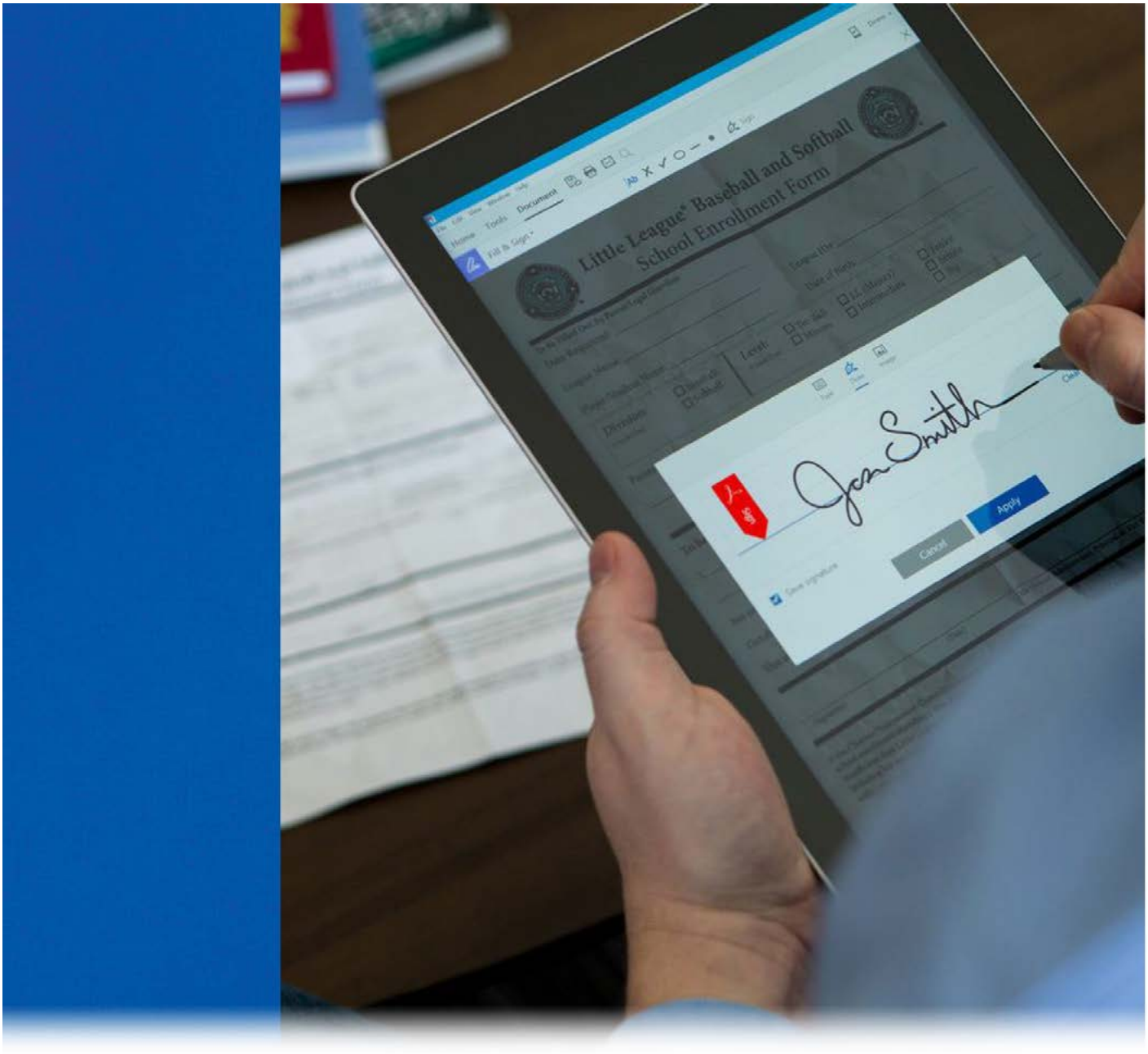

ADOBE SIGN

Soulad s evropskými právními předpisy o elektronických podpisech

DLA PIPER

Adobe

OBSAH

1 ÚVOD

Tento dokument hodnotí právní účinnost řešení Adobe Sign ve vztahu k evropským požadavkům platným pro elektronické podpisy. V první části tohoto dokumentu uvádíme přehled příslušného právního rámce. Stručně popisujeme oblast působnosti, hlavní pojmy a právní důsledky nařízení 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (dále jen „**nařízení eIDAS**" nebo „**nařízení**"), které je základním nástrojem upravujícím platnost elektronických podpisů v EU. Dále budeme analyzovat klíčové otázky týkající se platnosti a vymahatelnosti elektronicky podepsaných dohod.

Ve druhé části tento dokument popisuje klíčové funkce služby Adobe Sign a posuzuje tyto klíčové funkce s ohledem na příslušné právní požadavky, s cílem analyzovat povahu právní závaznosti elektronických podpisů realizovaných pomocí služby Adobe Sign.

Dospěli jsme k závěru, že je-li vybráno odpovídající uživatelské nastavení, z právního hlediska je Adobe Sign důvěryhodným a bezpečným nástrojem, který umožňuje vytvářet elektronické podpisy, jež splňují nebo dokonce překračují požadavky na elektronický podpis, definované v čl. 3 odst. 10 nařízení eIDAS.

Navíc se domníváme, že lze doložit, že Adobe Sign, i bez použití technologie digitálního podpisu, může umožnit vytváření zaručených elektronických podpisů, jak je definováno v článku 3 (11) nařízení eIDAS.

Dále sledujeme, že Adobe Sign rovněž zahrnuje možnost podpory použití technologie digitálního podpisu, zejména zaručených elektronických podpisů založených na digitálních certifikátech a kvalifikovaných elektronických podpisů, jak jsou definovány v čl. 3 odst. 12 nařízení eIDAS. Pokud tedy uživatel uvedenou možnost aktivuje, lze Adobe Sign považovat za nástroj vhodný pro obchodní a podnikové využití, který podporuje a usnadňuje proces vytváření zaručených a kvalifikovaných elektronických podpisů.

S ohledem na výše uvedené úvahy lze Adobe Sign, je-li odpovídajícím způsobem nakonfigurován, považovat za spolehlivé řešení elektronického podpisu, jež umožňuje spravovat proces podepisování typu end-to-end v souladu se všemi typy elektronických podpisů dostupných podle nařízení eIDAS. Uživatelé služby Adobe Sign s její pomocí mohou konfigurovat a vytvářet pracovní postupy pro podepisování, a to v souladu s příslušnými předpisy, odvětvím a svojí bezpečnostní politikou.

2 REGULAČNÍ RÁMEC

2.1 Nařízení eIDAS

Směrnice o eSignu – Ještě poměrně nedávno se používání elektronických podpisů v EU řídilo směrnicí 1999/93/ES o zásadách Společenství pro elektronické podpisy (směrnice o eSignu). Harmonizace, kterou tato směrnice přinesla, byla nedokonalá a vedla k nedostatečné interoperabilitě mezi řešeními pro elektronický podpis v různých členských státech EU a následně vedla k roztříštěnosti trhu. Ačkolivsměrnice specifikovala právní účinky elektronických podpisů, nezajistila, aby uznání elektronického podpisu v jednom členském státě EU znamenalo také přijetí stejného elektronického podpisu v jiném členském státě EU. Přijetí elektronických podpisů používaných při mezinárodních elektronických transakcích bylo tedy velmi nejisté. Směrnice navíc již nebyla uzpůsobena inovativním řešením, která rovněž umožňují ukázat, že podepisující osoba přijímá obsah elektronického dokumentu nebo dohody.

Za účelem podpoření využívání elektronických podpisů a dalších služeb vytvářejících důvěru, a aby se přispělo k vytvoření jednotného digitálního trhu v celé EU, přijal evropský zákonodárce v červenci 2014 nařízení eIDAS. Nařízení eIDAS, jehož většina ustanovení platí od 1. července 2016, ruší výše uvedenou směrnici o elektronických podpisech, přičemž na ni navazuje a vyjasňuje a rozšiřuje v ní obsažené principy.

Nařízení eIDAS – Jelikož evropský zákonodárce namísto revize směrnice (již by bylo třeba aplikovat do vnitrostátních právních předpisů členských států) šel cestou nařízení (které je přímo použitelné ve všech členských státech EU), podniky již nemusí čelit požadavkům národních zákonů o elektronických podpisech, ale musí se řídit pouze jednou sadou pravidel, což významně snižuje riziko problémů při jejich interpretaci. Nařízení eIDAS, i když si klade za cíl zajistit právní účinnost elektronických podpisů a jejich přípustnost jako důkazů v soudních řízeních, stejně jako jeho předchůdce neupravuje žádné aspekty uzavírání a platností (elektronických) dohod (viz oddíl 2.2 níže).

Nařízení eIDAS rozlišuje mezi elektronickými podpisy, zaručenými elektronickými podpisy a kvalifikovanými elektronickými podpisy.

2.1.1 Standardní elektronické podpisy

Širší definice – Nařízení eIDAS stanoví širší definici standardního „elektronického podpisu" bez jakéhokoli odkazu na konkrétní technologii. Takový standardní „elektronický podpis" je definován jako data v elektronické formě, jež jsou připojena nebo logicky spojena s jinými daty v elektronické formě, a která podepisující osoba používá k podpisu.

V bodě 26 odůvodnění nařízení eIDAS uvádí, že vzhledem k tempu technologických změn by měl být přijat přístup otevřený inovacím. Bod 27 odůvodnění dále stanoví, že nařízení eIDAS by mělo být technologicky neutrální, a že právní účinky, které poskytuje, by měly být dosažitelné jakýmikoliv technickými prostředky (za předpokladu, že jsou splněny požadavky nařízení). Tři kritéria pro kvalifikaci jako standardní elektronický podpis jsou: (i) existence „dat v elektronické podobě", (ii) „připojených k jiným datům v elektronické podobě nebo s nimi logicky spojených" a (iii) „používaných podepisující osobou k podpisu". Tato kritéria nejsou v nařízení eIDAS dále definována ani vysvětlena, a ponechávají tak prostor pro interpretaci a technologické inovace. V praxi to znamená, že mnoho elektronických nástrojů, zachycujících záměr podepisující osoby schválit obsah dokumentu, lze považovat za elektronický podpis. Může to být mimo jiné PIN kód, heslo, naskenovaný podpis, kryptografický podpis symetrického nebo veřejného klíče a biometrický podpis.

Právní účinek – Podle čl. 25 odst. 1 nařízení eIDAS nelze standardnímu elektronickému podpisu upřít právní účinek a přípustnost jako důkaz v soudním řízení pouze z toho důvodu, že je v elektronické podobě, nebo že nesplňuje požadavky na kvalifikovaný elektronický podpis. Přestože členské státy EU mohou volně definovat právní účinky standardních elektronických podpisů, z článku 25.1 plyne, je, že jim není dovoleno připravovat nebo udržovat právní předpisy ani schvalovat nebo povolovat národní pravidla s cílem odmítnutí používání nástrojů elektronického podepisování jen z důvodu jejich elektronického formátu či „nekvalifikovanosti".

Skutečnost, že nelze popřít právní účinek a přípustnost standardního elektronického podpisu jako důkazu založeného na určitých technických vlastnostech, ale neznamená, že by se mu dostalo stejného právního zacházení jako vlastnoručnímu podpisu. Tak tomu bude, pouze pokud to stanoví zvláštní zákony. Ani to nemá vliv na národní pravidla týkající se svobodného posuzování důkazů soudy.

> Nelze popřít právní účinek a přípustnost standardního elektronického podpisu jako důkazu v soudním řízení pouze z toho důvodu, že je v elektronické podobě a nesplňuje požadavky na kvalifikovaný elektronický podpis.

2.1.2 Zaručené elektronické podpisy

Čtyři kritéria – „Zaručený elektronický podpis" je definován v čl. 3 odst. 10 nařízení eIDAS jako standardní elektronický podpis, který splňuje požadavky článku 26 nařízení eIDAS, zejména: (a) je jednoznačně spojen s podepisující osobou; (b) umožňuje identifikaci podepisující osoby; (c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a (d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Ačkolivbyla právní definice zaručeného elektronického podpisu formulována technologicky neutrálním způsobem, dodnes se obecně uznává výklad, že koncept se týká hlavně elektronických podpisů, které jsou založeny na technologii digitálního podpisu, nebo jinými slovy, s použitím kryptografie veřejného klíče. V rámci této interpretace musí být zaručený elektronický podpis považován za digitální soubor obsahující otisk (hash) dokumentu získaný šifrováním pomocí soukromého klíče podepisující osoby. Zaručený elektronický podpis lze následně ověřit pomocí příslušného veřejného klíče podepsané osoby. Odpovídající digitální certifikát, zejména elektronické osvědčení, které spojuje údaje pro ověření podpisu s fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby, potvrzuje podepisující osobu jako vlastníka jeho veřejného klíče.

Vzdálené podpisy – Technologicky neutrální definice zaručeného elektronického podpisu však nevylučuje, že by jakékoli jiné technologie mohly umožňovat vytváření zaručených elektronických podpisů, samozřejmě za předpokladu, že jsou splněny čtyři výše uvedené požadavky. Na jedné straně bod 26 a 27 odůvodnění potvrzují, že nařízení eIDAS je, nebo by mělo být, otevřeno inovacím, a že právní účinky, které poskytuje, by měly být dosažitelné jakýmikoliv technickými prostředky. Na druhé straně, bod 52 odůvodnění otevírá cestu používání řešení právně účinných elektronických podpisů založených na cloudu. Tento bod odůvodnění připouští, že se bude rozšiřovat používání vzdálených elektronických podpisů v prostředích pro elektronické podepisování, spravovaných poskytovateli služeb vytvářejících důvěru jménem podepisující osoby. V tomto ohledu dále stanoví, že těmto elektronickým podpisům by se mělo dostávat stejného právního

uznání, jako elektronickým podpisům vytvořeným v prostředí plně spravovaném uživatelem, pokud poskytovatel služeb vzdáleného elektronického podepisování aplikuje určité postupy správy a zabezpečení, a používá důvěryhodné systémy a produkty za účelem zajištění spolehlivosti prostředí pro vytváření elektronického podpisu a jeho používání pod výhradní kontrolou podepisující osoby. Vzhledem k široké formulaci tohoto bodu odůvodnění lze prohlásit, že podepisující osoba může uložit svůj soukromý klíč v cloudu, nebo může dokonce použít cloudové řešení elektronického podpisu, nevyžadující žádné podpisové klíče.

Nařízení eIDAS nepřiznává zaručenému elektronickému podpisu žádné konkrétní právní účinky, lišící se od standardního elektronického podpisu. Pojem se však používá jako stavební kámen pro definování kvalifikovaného elektronického podpisu, což je zaručený elektronický podpis, splňující řadu dalších právních požadavků (viz oddíl 2.1.3 níže).

Zvýšená úroveň důvěry – Hlavní rozdíl mezi standardními elektronickými podpisy a zaručenými elektronickými podpisy je však v tom, že technická bezpečnost zaručeného elektronického podpisu (často elektronického podpisu založeného na digitálním certifikátu) je obecně považována za vyšší, než u některých zákonem uznávaných standardních elektronických podpisů, jako například PIN kód, nebo naskenovaný podpis připojený k dokumentu. Obecně jsou tak zaručené elektronické podpisy považovány za důvěryhodnější a obecně mají u soudu větší důkazní váhu. Z právního hlediska však použitá technická metoda může být pouze jedním z prvků, na které je brán ohled při rozhodování soudů. V jednom konkrétním případě tedy může být zpochybněna důvěryhodnost konkrétního elektronického podpisu založeného na digitálním certifikátu, zatímco v jiném případě může soud za dostatečné důkazy považovat PIN kód.

Ačkoliv zaručenému elektronickému podpisu nejsou připisovány žádné konkrétní právní účinky, obecně se považuje za důvěryhodnější a u soudu má větší důkazní váhu. Navíc se zdá, že nařízení eIDAS ponechává prostor pro to, aby elektronické podpisy, jež nejsou založeny na digitálním certifikátu, byly kvalifikovány jako zaručené elektronické podpisy.

2.1.3 Kvalifikované elektronické podpisy

Rovnocenný vlastnoručnímu podpisu – „Kvalifikovaný elektronický podpis" je definován v čl. 3 odst. 12 nařízení eIDAS jako zaručený elektronický podpis, který je vytvořen kvalifikovaným zařízením pro vytváření elektronického podpisu a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.

Klíčovým principem nařízení eIDAS je, že v souladu s jeho článkem 25.2 je kvalifikovaný elektronický podpis automaticky rovnocenný vlastnoručnímu podpisu a má rovnocenné právní účinky. Článek 25.3 dále stanoví, že kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě EU bude uznáván jako kvalifikovaný elektronický podpis ve všech ostatních členských státech EU. Článek 25.3 jako takový se vypořádává s nedostatečnou interoperabilitou, jíž trpěla směrnice 1999/93/ES o elektronických podpisech, a umožňuje bezpečné a bezproblémové mezinárodní elektronické transakce zvýšením legálního uznávání kvalifikovaných elektronických podpisů ve všech členských státech EU.

Rozsáhlá sada kritérií – Aby elektronický podpis mohl být považován za kvalifikovaný elektronický podpis, musí být založen na kvalifikovaném certifikátu. „Kvalifikovaný certifikát je digitální certifikát, který musí obsahovat konkrétní informace stanovené v příloze I nařízení eIDAS a musí být vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru (po ověření totožnosti a konkrétních atributů, pokud existují, dotčené fyzické osoby). Kvalifikovaný poskytovatel služeb vytvářejících důvěru je takový poskytovatel, který poskytuje kvalifikované služby vytvářející důvěru v souladu s požadavky stanovenými v oddíle 3 nařízení eIDAS. V praxi to pro kvalifikované elektronické podpisy znamená komerční nebo vládní certifikační autoritu, která potvrzuje vlastnictví veřejného klíče jmenované osoby vydáním digitálního certifikátu.

Kvalifikovaný elektronický podpis musí být také vytvořen kvalifikovaným zařízením pro vytváření elektronického podpisu. To znamená, že nakonfigurovaný software nebo hardware (např. čipová karta, USB token nebo cloudový hardwarový bezpečnostní modul) použitý k vytvoření uvedeného podpisu musí splňovat požadavky týkající se důvěryhodnosti dat zpracovávaných zařízením, jak je stanoveno v příloze 11 nařízení eIDAS.

Kvalifikovaný elektronický podpis má automaticky rovnocenný právní účinek s vlastnoručním podpisem a musí být uznán v ostatních členských státech EU.

2.2 Platnost a vymahatelnost elektronických dohod

Při zvažování použití elektronických podpisů v rámci smluvních ujednání je posouzení právní účinnosti elektronického podpisu pouze jednou z otázek. Vyvstávají ještě dvě další, stejně důležité. První se týká platnosti elektronicky podepsané dohody. Druhá se týká důkazní hodnoty a vymahatelnosti elektronicky podepsané dohody.

Platnost – První otázka, na kterou je třeba odpovědět, se týká formálních požadavků, které je třeba splnit, aby bylo možné platně uzavřít dohodu. V evropském smluvním právu je klíčovou zásadou „konsensualismus". To znamená, že k uzavření platné dohody postačuje svobodný a vzájemný souhlas smluvních stran a nejsou vyžadovány žádné formální požadavky, jako je písemný dokument, registrace nebo podpisy.

Dohody lze uzavírat ústně, písemně, elektronicky nebo dokonce „samosebou". Výjimky z této obecné zásady však existují v různých členských státech EU. Dohody o nemovitostech, dohody o veřejných zakázkách, spotřebitelské dohody, dohody o narovnání, dohody o záruce mohou vyžadovat splnění zvláštních náležitostí za účelem uzavření platné dohody. I když skutečně existují výjimky, pro drtivou většinu dohod bude stačit pouhý souhlas smluvních stran a k uzavření platné dohody nebude třeba podpisů.

Vymahatelnost – Druhá otázka, na kterou je třeba odpovědět, se týká způsobu, jakým lze dohody platně vymáhat. Z právního hlediska je tato druhá otázka velmi důležitá, protože existuje významný rozdíl mezi uzavřením platné dohody a schopností vymáhat uvedenou dohodu prokázáním její existence a obsahu.

Právní pravidla upravující důkazní hodnotu a vymahatelnost dohod se liší podle jurisdikce. V zemích s občanským právem, jako je Belgie, Francie a Itálie, které mohou sloužit za příklad nakládání s pravidly o důkazech v kontinentální Evropě, se rozlišuje mezi volnými a regulovanými důkazy. V B2B sporech je přípustná jakákoli forma důkazů (např. jakýkoli typ psaní, svědectví, e-mail nebo faktické údaje). Samozřejmě zůstává na soudu, aby vyhodnotil důkazní hodnotu předložených důkazů. Ve sporech B2C a ve sporech mezi soukromými osobami jsou formy důkazů regulovány, což znamená, že pokud je spor oceněn nad určitou částku, je obvykle vyžadována podepsaná dohoda (jedná se o písemný dokument podepsaný stranami, které přijímají závazky).

Ve většině jurisdikcí je však přijatelné odchýlit se smluvně od pravidel dokazování. To znamená, že smluvní strany se mohou dohodnout, které důkazní prostředky postačují a / nebo která důkazní hodnota se přisuzuje určitým dokumentům. Typický příklad lze nalézt v podmínkách služeb online bankovnictví, které často vyžadují, aby uživatel souhlasil s tím, že potvrzení transakce pomocí čtečky karet bude považováno za elektronický podpis splňující funkční požadavky vlastnoručního podpisu.

Dále je třeba zdůraznit, že i když jsou regulované důkazy vyžadovány zákonem (například podepsaná dohoda), pravidla dokazování obecně připisují určitou právní důkazní hodnotu bezplatným důkazům (např. E-maily popisující obsah dohody), ať už jako právní pravidlo nebo v praxi.

I když mezi členskými státy EU existují rozdíly, je namístě konstatovat (i), že drtivá většina dohod je platná i bez jakýchkoli formalit a (ii) že u většiny smluvních sporů nejsou při prokazování vykonatelnosti dohody dopředu vyloučeny žádné důkazy (např. jakýkoli typ elektronického podpisu).

3 POSOUZENÍ SHODY ADOBE SIGN

3.1 Popis služby Adobe Sign

Cloudové řešení – Adobe Sign je řešení elektronického podepisování založené na SaaS, pomocí kterého uživatelé mohou flexibilně spravovat proces podpisu dokumentu. Adobe Sign se stará o všechny aspekty procesu elektronického podpisu, od zajištění různých možností ověření uživatele až po vložení potvrzení do finálního dokumentu a zapečetění dokumentu certifikací, chránící jej před následnou manipulaci. V každém kroku procesu se Adobe Sign stará o ověření uživatele a propojuje všechny auditní informace od podepisujícího po jeho podpis v dokumentu. Adobe Sign lze používat s využitím počítačové aplikace Adobe Acrobat, webového prohlížeče, mobilního zařízení nebo prostřednictvím API, které se mohou připojovat k dalším aplikacím uživatele.

Proces podepisování – Chce-li uživatel odeslat dokument k podpisu, nahraje dokument do služby Adobe Sign. Pro elektronické podepisování pomocí Adobe Sign jsou podporovány různé formáty zdrojových dokumentů. Uživatelé mohou určit jednoho nebo více účastníků, kteří musí dokument podepsat, posílat účastníkům zprávy, a volitelně použít v dokumentu další prvky zabezpečení. Adobe Sign také umožňuje uživatelům ručně vytvářet formulářová pole a umísťovat přetažením do dokumentu pole pro podpisy pomocí jednoduchého webového rozhraní. V průběhu procesu podepisování je pak po podepisujících požadováno, aby vyplnili tato pole a podepsali se na příslušných místech.

Autentizace – Adobe Sign podporuje celou řadu způsobů ověření identity uživatelů služby Adobe Sign a podepisujících.

Uživatelé služby Adobe Sign se ověřují na základě jedinečného identifikátoru uživatele, který vytvoří buď uživatel sám, nebo který mu (v případě podnikových účtů) přidělí správce. Uživatelé se mohou přihlásit a autentizovat pomocí následujících druhů identifikátorů uživatele:

- Adobe Sign ID – uživatelé k bezpečnému přihlášení ke svému účtu používají ověřenou e-mailovou adresu a heslo. Správci účtů v organizaci mohou stanovit určité požadavky na heslo uživatele (např. minimální složitost a počet znaků).
- Adobe ID – uživatelé se mohou pomocí Adobe ID přihlásit k Adobe Sign. Adobe ID je identifikátor, který používají všechny služby Adobe pro povolení přístupu k těmto službám. Organizace mají volnost v rozhodování, zda jejich uživatelé mohou k přihlášení do Adobe Sign používat Adobe ID.
- Google Gmail a Google Apps – Adobe Sign podporuje také přihlašování uživatelů prostřednictvím účtu Google Gmail nebo Google Apps. Správci účtů mohou určit, zda uživatelé mohou tuto metodu použít.
- Single sign-on (SSO) s využitím Security Assertion Markup Language (SAML) – Podniky, které vyžadují striktnější mechanismus řízení přístupu, mohou pro centrální správu svých uživatelů prostřednictvím systému podnikové identity nasadit SAML SSO. To správcům účtů umožňuje využívat silnou kontrolu přístupu a také zajistit, aby požadavky na heslo byly v souladu s podnikovými zásadami zabezpečení informací.

Adobe Sign navíc podporuje různé způsoby identifikace podepisujícího (který nemusí být nutně uživatelem Adobe Sign a nemusí se nejprve zaregistrovat do Adobe Sign) pro ověření ještě před podepsáním dokumentu.

Pro základní autentizaci se podepisujícímu posílá e-mail s jedinečnou adresou URL. Jelikož většina podepisujících má výlučný přístup k určitému e-mailovému účtu, je to považováno za první úroveň ověřování. K podepsání dokumentu je nutný odkaz URL, sestávající z jedinečných identifikátorů, které jsou specifické pro dotyčnou transakci, a mohou být chráněny uživatelským heslem služby Adobe Sign. Po kliknutí na uvedený URL odkaz mohou podepisující pomocí myši nebo předdefinovaných stylů písma vytvořit „ručně psaný" podpis na obrazovce, nahrát existující soubor (např. naskenovaný podpis), anebo zadat své jméno a podepsat kliknutím na tlačítko (zobrazující *„kliknutím podepsat"*).

Kromě toho Adobe Sign umožňuje i vícefaktorovou autentizaci a nabízí další ověřovací mechanismy pro zjištění identity podepisujícího, včetně jedinečných hesel pro jednotlivé podepisující, ověřování telefonem (hlasem nebo SMS), nebo podle sociální identity s využitím facebookového či Google účtu podepisujícího.

Certifikace dokumentu – Poté, co podepisující osoby dokument podepsaly, opatří Adobe Sign dokument certifikátem, a tím zajistí, aby jakékoliv případné následné změny dokumentu byly patrné. Adobe Sign implementuje vlastní certifikát PKI, který je v souladu s programem *Adobe Approved Trust List (AATL)* pro certifikaci dokumentů. Před distribucí podepsaného dokumentu podepisujícím osobám Adobe Sign automaticky certifikuje finální PDF podepsaného dokumentu. Když si příjemci stáhnou a otevřou podepsaný soubor v Adobe Acrobatu nebo Adobe Acrobat Readeru, zobrazí se v horní části dokumentu modrý banner, který potvrzuje, že s dokumentem během doručování nebo v jakémkoli okamžiku od opatření certifikátem nebylo nijak neoprávněně manipulováno.

Poté, co dokument podepsali všichni podepisující, Adobe Sign také automaticky uloží všechny podepsané dokumenty do centralizovaného zabezpečeného úložiště, kde jsou snadno přístupné. Uživatelé se ale také mohou rozhodnout integrovat služby do svých vlastních existujících řešení správy dokumentů.

Auditní stopa – Adobe Sign umožňuje sledování procesu podepisování v reálném čase. Jakmile je dokument odeslán k podpisu, Adobe Sign se automaticky stará o postup práce, uchovávání, sledování, připomínání a autentizaci, aby byl proces elektronického podepisování jasný a snadný.

Každý klíčový krok v procesu podepisování je protokolován, například kdy byl dokument odeslán, otevřen a podepsán, adresy IP nebo geolokace podepisujících, a konkrétní forma autentizace použitá pro každého podepisujícího nebo schvalovatele. Výsledek je zachycen v zabezpečené auditní stopě, která poskytuje jasné a snadno doložitelné důkazy podpisu každé podepsané osoby. Zpráva o auditní stopě může být načtena uživatelem služby Adobe Sign prostřednictvím řídicího

panelu Adobe Sign, nebo podepisující osobou (která není uživatelem) kliknutím na podpis v podepsaném dokumentu, či zadáním unikátního ID transakce pro získání přístupu k auditní zprávě.

Digitální podpisy – Adobe Sign umožňuje nejen vytváření elektronických podpisů, nezaložených na digitálním certifikátu, ale podporuje též použití digitálních podpisů založených na certifikátech, prostřednictvím aplikace Adobe Sign ve spolupráci s aplikacemi Adobe Acrobat či Adobe Acrobat Reader, které se použijí k vytvoření digitálních podpisů v dokumentech. Během procesu podepisování je certifikát podepisující osoby kryptograficky navázán na dokument pomocí soukromého klíče této osoby. Během procesu ověřování se z podpisu extrahuje veřejný klíč, který se použije k ověření identity podepsaného, a pomůže zajistit, aby v dokumentu nebyly od okamžiku jeho podpisu provedeny žádné změny. Zde auditní stopa navíc dává další hodnotné informace, jako je IP adresa podepisující osoby, nebo geolokace.

Adobe není certifikační autorita. Adobe Sign tudíž nevydává digitální certifikáty sám, ale pracuje prakticky s jakýmkoliv digitálním certifikátem vydaným třetími stranami – poskytovateli služeb vytvářejících důvěru, nebo certifikačními autoritami autorizovanými eIDAS. Téměř všichni tito poskytovatelé jsou v Adobe Sign uznáváni prostřednictvím jejich zařazení do EUTL *European Trustcenter List* a do AATL *Adobe Approved Trust List* (tento seznam zahrnuje služby vytvářející důvěru, jako jsou DigiCert, Global Sign, QuoVadis atd.).

Zabezpečení v cloudu – Společnost Adobe používá řadu technických a organizačních opatření souvisejících s fyzickým zabezpečením datových center, obnovou po problému, kontrolami prostředí, logickým zabezpečením, ochranou dat, detekcí narušení, reakcí a dohlížením, aby byla zajištěna bezpečnost služby Adobe Sign a jakýchkoliv jiných souvisejících procesů. Business procesy Adobe Sign jsou certifikovány v souladu s normami ISO 270001, SSAE SOC 2 Type 2 a PCI DSS.

Předplatné – Adobe Sign lze využívat prostřednictvím tří různých plánů předplatného: „Individual", „Business" a „Enterprise". Podle zvoleného plánu předplatného nabízí Adobe Sign další funkce. Konkrétně například vícefaktorová autentizace je k dispozici pouze pro plány předplatného „Business" a „Enterprise", zatímco používání elektronických podpisů založených na digitálních certifikátech je k dispozici výhradně v rámci plánu předplatného „Enterprise".

3.1 Jak může Adobe Sign podporovat soulad s eIDAS

V této části dokumentu se zaměříme na to, jak si Adobe Sign stojí ve vztahu k právním požadavkům na standardní, zaručené a kvalifikované elektronické podpisy, jak jsou stanoveny výše.

3.1.1 Adobe Sign splňuje evropské požadavky standardních elektronických podpisů

Požadavky – V souladu s definicí standardních „elektronických podpisů" v nařízení eIDAS musí být data v elektronické podobě připojena k jiným datům v elektronické podobě, nebo s nimi být logicky spojena a musí být podepisující osobou použita k podepsání.

Adobe Sign – Pokud jde o výše uvedený popis služby Adobe Sign, docházíme k závěru, že z právního hlediska Adobe Sign splňuje či dokonce překračuje požadavky na standardní elektronické podpisy:

- „Data v elektronické podobě" – Elektronické podpisy vytvořené pomocí služby Adobe Sign skutečně sestávají z řetězce dat v elektronické podobě.
- „Připojeno k jiným elektronickým datům nebo s nimi logicky spojeno" – Elektronický podpis může signatář připojit k různým elektronickým dokumentům, přičemž služba Adobe Sign dovoluje nahrávání více formátů zdrojových dokumentů.
- „používá podepisující osoba k podepsání" – Adobe Sign byl navržen tak, že je jasně určen k zaznamenání záměru podepisující osoby podepsat v procesu podepisování:
  - *Podepisující obdrží e-mail s předmětem „Požádáno o podpis dokumentu [název dokumentu]", ve kterém hypertextový odkaz na Adobe Sign říká: „Proveďte kontrolu a dokončete dokument [název dokumentu]";*
  - *Když podepisující zkontroluje dokument, je požádán, aby podepsal dokument zadáním svého jména, vytvořením „ručně psaného" podpisu na obrazovce nebo nahráním obrázku naskenovaného podpisu. Podepisujícího k tomu vyzve pole formuláře v dokumentu, které uvádí „Klepnutím sem podepíšete".;*
  - *Poté, co to bude provedeno, se zobrazí oznámení, které uvádí „Souhlasím s podmínkami používání a zpřístupněním údajů zákazníka tohoto dokumentu" spolu s tlačítkem „Klepnutím podepište". Až když podepisující osoba klikne na toto tlačítko a tím podruhé potvrdí svůj úmysl podepsat, považuje Adobe Sign dokument za podepsaný a rozešle jej ostatním účastníkům.*

Ačkolivvzhled podpisu na dokumentu lze chápat pouze jako vizuální, estetický prvek bez dopadu na hodnotu elektronického podpisu, tento mnohostranný přístup k zachycení záměru podepsané osoby podepsat dokument umožňuje splnění tohoto třetího kritéria. To není jen požadavek při vytváření standardních elektronických podpisů, ale také důležitý aspekt při uzavírání smluv. Jelikož dohody jsou v zásadě uzavírány na základě vzájemného souhlasu smluvních stran, jasný proces podepisování pomáhá prokázat ochotu podepsaného být vázán zákonnými povinnostmi a vyvodit z toho příslušný souhlas.

To podle článku 25.1 nařízení eIDAS znamená, že u elektronického podpisu vytvořeného pomocí služby Adobe Sign nelze v zásadě zamítnout jeho právní účinek a přípustnost coby důkazu v soudním řízení pouze z důvodu jeho technických vlastností. To však neznamená, že takový elektronický podpis automaticky získá stejnou právní platnost jako vlastnoruční podpis, pokud ovšem nebude použit kvalifikovaný certifikát (viz níže část 3.2.3).

Adobe Sign navíc nabízí řadu funkcí, které by mohly posílit vymahatelnost na bázi elektronického podpisu ve srovnání s jinými běžně přijímanými elektronickými podpisy, například:

- Auditní stopa – Pokud by byla zpochybněna platnost elektronického podpisu, mohla by auditní stopa generovaná službou Adobe Sign sloužit jako relevantní důkaz prokazující souvislost mezi identitou signatáře a podpisem.
- Metody vícefaktorové autentizace – Pokud byla od podepisující osoby výběrem příslušného nastavení vyžadována vícefaktorová autentizace, nepochybně se tím zvyšuje schopnost náležitě autentizovat podepisující osobu a vytvářet elektronické podpisy se zvýšenou důkazní hodnotou.

Z výše uvedeného vyplývá, že Adobe Sign není pouze řešením, které umožňuje vytvářet standardní elektronické podpisy v souladu s nařízením eIDAS: lze usuzovat, že Adobe Sign je důvěryhodný a bezpečný způsob, jak toho dosáhnout.

Adobe Sign umožňuje důvěryhodným a bezpečným způsobem vytvářet standardní elektronické podpisy. Adobe Sign (i) umožňuje identifikovat signatáře pokročilejším způsobem, (ii) zachycuje záměr podepsat jednoznačným způsobem a (iii) spravuje záznam auditní stopy podporující vymahatelnost na základě vytvořeného elektronického podpisu.

3.2.2 Adobe Sign a zaručené elektronické podpisy

Požadavky – V souladu s definicí zaručených elektronických podpisů v nařízení eIDAS musí být takový elektronický podpis jednoznačně spojen s podepisující osobou, musí být schopný identifikovat podepisující osobu, musí být vytvořený pomocí dat pro vytvoření elektronického podpisu, jež podepisující s vysokou úrovní důvěryhodnosti může použít pod svojí výhradní kontrolou, a musí s daty jimi podepsanými být spojen takovým způsobem, aby byla zjistitelná jakákoli následná změna dat.

Adobe Sign – Pokud jde o výše uvedený popis Adobe Sign, vidíme, že z právního hlediska Adobe Sign podporuje vytváření zaručených elektronických podpisů založených na digitálním certifikátu.

Jak je uvedeno výše, požadavky zaručených elektronických podpisů jsou obvykle splněny elektronickými podpisy založenými na digitálních certifikátech, a společnost Adobe nevydává ani nespravuje certifikáty k vytváření těchto podpisů. Adobe Sign však obsahuje nativní integraci s aplikacemi Adobe Acrobat a Adobe Acrobat Reader, jež umožňují vytváření takzvaných „digitálních podpisů". Aby se předešlo nedorozuměním, je třeba zdůraznit, že pojem „digitální podpis", jak jej používá Adobe Sign, není právně definován v nařízení eIDAS, ale musí být interpretován tak, že zahrnuje zaručené elektronické podpisy založené na digitálním certifikátu, kvalifikované elektronické podpisy i elektronické podpisy založené na certifikátech vydaných držitelem.

Pokud je dokument nahrán do aplikace Adobe Sign k podpisu, může uživatel služby Adobe Sign tím, že do dokumentu přidá pole digitálního podpisu, vyžadovat, aby podepisující osoby použily digitální podpis. Podepisující osoby budou poté vyzvány ke stažení dokumentu, který se otevře v aplikaci Adobe Acrobat nebo Adobe Acrobat Reader (v závislosti na tom, co je nainstalováno v počítači podepisující osoby), a poté bude podepisující veden do pole podpisu, bude moci vybrat certifikát ze svého zařízení, a pomocí aplikace Adobe Acrobat nebo Adobe Acrobat Reader na dokument aplikovat zaručený elektronický podpis. Podepsaný dokument se poté automaticky nahraje do služby Adobe Sign (aniž by byla vyžadována jakákoli další podepisovací akce), ostatní signatáři budou upozorněni, a záznam o digitálním podpisu bude zaznamenán v rámci auditní stopy dokumentu. I když auditní stopa uvede pouze to, že dokument byl podepsán digitálně, platnost použitého digitálního certifikátu může být ověřena uživatelem Adobe Sign a podepisujícími osobami, když nahlédnou

do podepsaného dokumentu prostřednictvím služby Adobe Sign nebo otevřou dokument přímo v aplikaci Adobe Acrobat Reader nebo Adobe Acrobat.

Zaručené elektronické podpisy založené na digitálních certifikátech lze integrovat do uceleného (end-to-end) procesu elektronického podpisu, podporovaného a spravovaného prostřednictvím služby Adobe Sign.

Jak je uvedeno výše v oddíle 2.1.2, lze prohlásit, že požadavkům zaručených elektronických podpisů mohou vyhovět i jiné podpisové technologie než kryptografie veřejného klíče, jako například procesně orientovaná cloudová řešení elektronického podepisování. Pokud tedy nebude brána v úvahu funkcionalita „digitálních podpisů" služby Adobe Sign, a řešení bude posouzeno s ohledem na čtyři kritéria zaručeného elektronického podpisu, je třeba dodržet následující:

- „je jednoznačně spojen s podepisující osobou" – Adobe Sign umožňuje propojit každý elektronický podpis, který je vytvořen na platformě, s podepisující osobou. Adobe Sign nabízí vícefaktorové metody autentizace, které jasně autentizují podepisující osobu. Navíc auditní stopa, která sleduje všechny elektronické podpisy v dokumentu, umožňuje propojit konkrétní podpis s konkrétní podepisující osobou.

- „umožňuje identifikaci podepisující osoby" – Aby se zajistilo splnění tohoto požadavku, doporučuje se uživatelům vyžadovat vícefaktorové autentizaci pro přihlášení a podepsání dokumentu, namísto toho, aby pro přístup vyžadovali pouze kliknutí na hypertextový odkaz.

- „je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou" – Typicky se za splnění tohoto kritéria považují pouze zaručené elektronické podpisy založené na digitálním certifikátu, přičemž soukromý klíč podepisující osoby je považován za „data pro vytvoření elektronického podpisu". Koncept „dat pro vytvoření elektronického podpisu" se však nemusí nutně omezovat na soukromé klíče, protože nařízení eIDAS jej definuje v širším smyslu jako „jedinečná data, která podepisující osoba používá k vytvoření elektronického podpisu".

Pokud jde o bod 52 odůvodnění nařízení eIDAS, mohou být schopna splnit toto kritérium také cloudová řešení elektronického podpisu (která nemusí nutně vycházet z digitálních certifikátů), za předpokladu, že budou zavedeny konkrétní postupy řízení a zabezpečení a k zajištění spolehlivosti prostředí pro vytváření elektronického podpisu a pod výlučnou kontrolou signatáře budou používány důvěryhodné systémy a produkty. Pokud se k získání přístupu k personalizovanému podepisovacímu prostředí a k samotnému dokumentu, který má být podepsán, používají silné metody vícefaktorového ověřování, lze tvrdit, že platforma Adobe Sign skutečně umožňuje vytvářet elektronické podpisy prostředky, které jsou s vysokou úrovní důvěry pod kontrolou podepisující osoby. V tomto ohledu je důležité zdůraznit, že správci systémů Adobe nemají přístup k žádným uživatelským účtům nebo profilům podepisujících osob ani k žádným přihlašovacím údajům (včetně hesel), aby mohli získat přístup k těmto účtům nebo profilům

- „je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat" – Jakmile podepisující osoby dokument podepsaly, Adobe Sign automaticky certifikuje podepsaný dokument svým digitálním certifikátem, aby dokument chránil proti jakýmkoli následným změnám. Jakmile je dokument podepsán pomocí služby Adobe Sign, je navíc každá následná změna snadno viditelná, protože auditní stopa zaznamenává všechny aktivity a změny týkající se příslušného dokumentu.

Na základě existujících argumentů lze prohlásit, že Adobe Sign umožňuje vytvářet zaručené elektronické podpisy, které nejsou založeny na digitálním certifikátu.

3.2.3 Adobe Sign a kvalifikované elektronické podpisy

Požadavky – Podle nařízení eIDAS je kvalifikovaný elektronický podpis právně ekvivalentní s vlastnoručním podpisem, a jako takový je uznáván ve všech ostatních členských státech EU. Jak je uvedeno výše, nařízení eIDAS definuje kvalifikovaný elektronický podpis jako zaručený elektronický podpis s dalšími požadavky, který musí být založen na kvalifikovaném certifikátu a musí být vytvořen kvalifikovaným zařízením pro vytváření elektronického podpisu.

Prvním požadavkem je použití kvalifikovaného certifikátu. To znamená digitální certifikát, který vydává kvalifikovaný poskytovatel služeb vytvářejících důvěru a splňuje požadavky přílohy I nařízení eIDAS. Pokud jde o požadavky nařízení eIDAS, definici kvalifikovaného certifikátu splňuje certifikát vydaný kvalifikovanou komerční nebo vládní certifikační autoritou, který obsahuje podpisový klíč a totožnost vlastníka.

Druhým požadavkem je použití kvalifikovaného zařízení pro vytváření elektronického podpisu. Takovým zařízením je nakonfigurovaný hardware nebo software (např. čipová karta, USB token nebo cloudový hardwarový bezpečnostní modul) používaný k vytvoření elektronického podpisu, a splňující požadavky přílohy II nařízení eIDAS.

Adobe Sign – Adobe Sign nespravuje ani nevydává kvalifikované certifikáty a nenabízí kvalifikovaná zařízení pro vytváření elektronických podpisů, ale můžeme zodpovědně konstatovat, že z právního hlediska podporuje Adobe Sign produkci kvalifikovaných elektronických podpisů prostřednictvím své spolupráce s kvalifikovanými poskytovateli certifikátů.

Adobe Sign obsahuje nativní integraci s aplikacemi Adobe Acrobat a Adobe Acrobat Reader, což umožňuje práci s takzvanými „digitálními podpisy". Aby se předešlo pochybnostem, je třeba zdůraznit, že pojem „digitální podpis", jak jej používá Adobe Sign, není právně definován v nařízení eIDAS, ale musí být interpretován tak, že zahrnuje zaručené elektronické podpisy založené na digitálním certifikátu, kvalifikované elektronické podpisy i elektronické podpisy založené na certifikátech vydaných držitelem.

Pokud je dokument nahrán do aplikace Adobe Sign k podpisu, může uživatel služby Adobe Sign tím, že do dokumentu přidá pole digitálního podpisu, vyžadovat, aby podepisující osoby používaly digitální podpis. Podepisující osoby budou poté vyzvány ke stažení dokumentu, který se otevře v aplikaci Adobe Acrobat nebo Adobe Acrobat Reader (v závislosti na tom, co je nainstalováno v počítači podepisující osoby), a poté bude podepisující veden do pole podpisu, bude moci vybrat certifikát ze svého zařízení, a pomocí aplikace Adobe Acrobat nebo Adobe Acrobat Reader na dokument aplikovat kvalifikovaný elektronický podpis. Podepsaný dokument se poté automaticky nahraje do služby Adobe Sign (aniž by byla vyžadována jakákoli další podepisovací akce), ostatní signatáři budou upozorněni, a záznam o digitálním podpisu bude zaznamenán v rámci auditní stopy dokumentu. I když auditní stopa uvede pouze to, že dokument byl podepsán digitálně, platnost použitého digitálního certifikátu může být ověřena uživatelem Adobe Sign a podepisujícími osobami, když nahlédnou do podepsaného dokumentu prostřednictvím služby Adobe Sign nebo otevřou dokument přímo v aplikaci Adobe Acrobat Reader nebo Adobe Acrobat.

Protože v některých případech je k platnému elektronickému podpisu smlouvy vyžadováno použití kvalifikovaných elektronických podpisů, doporučuje se uživatelům služby Adobe Sign a podepisujícím osobám ověřit, zda jsou aktivována příslušná nastavení, aby bylo možné uzavřít platnou dohodu.

Pro úplnost je třeba zmínit, že Adobe Acrobat i Adobe Acrobat Reader obsahují funkce pro identifikaci kvalifikovaných certifikátů pomocí standardních kvalifikovaných potvrzení o certifikátu na základě seznamu důvěryhodných certifikátů EU (EUTL), a pro ověření a důvěru kvalifikovaným certifikátům na základě seznamu EUTL, k identifikaci kvalifikovaných zařízení pro vytváření podpisů pomocí standardních kvalifikovaných potvrzení o certifikátu a k podpoře digitálních podpisů ve formátu PAdES Baseline (ETSI TS 103 172 a nejnovější ETSI EN 319 142-1).

Kvalifikované elektronické podpisy mohou být integrovány do uceleného (end-to-end) procesu elektronického podpisu, podporovaného a spravovaného prostřednictvím služby Adobe Sign.

4 ZÁVĚR

Adobe Sign je řešení elektronického podpisu založené na SaaS, které se stará o všechny aspekty procesu elektronického podpisu, od poskytování možností ověření uživatele až po vložení schválení do finálního dokumentu a zapečetění dokumentu certifikací proti neoprávněné manipulaci.

Adobe Sign podporuje celou řadu možností pro ověřování identity uživatelů a signatářů služby Adobe Sign, tj. pomocí konkrétních identifikátorů – např. Adobe (Sign) ID nebo účet Google Gmail – a (vícefaktorových) metod ověřování – např. jedinečná hesla, ověření telefonem (hlas nebo SMS) nebo sociální identita. Procesy podporované Adobe Sign byly navíc navrženy tak, aby jasně zachytily záměr podepisující osoby. A konečně, aby byl podepsaný dokument chráněn před jakýmikoliv následnými změnami, Adobe Sign udržuje auditní stopu, která registruje všechny změny provedené v podepsaném dokumentu a certifikuje výsledný dokument před jeho odesláním všem účastníkům.

Z právního hlediska můžeme s jistotou uzavřít, že když je zvoleno příslušné uživatelské nastavení, je Adobe Sign důvěryhodným a bezpečným nástrojem, který umožňuje vytvářet standardní elektronické podpisy, splňující nebo dokonce překračující požadavky standardního „elektronického podpisu", jak je definován v čl. 3 odst. 1 nařízení eIDAS. To znamená, že podle článku 25.2 nařízení eIDAS jim nelze upřít právní účinnost pouze na základě jejich technických vlastností. I když standardní elektronický podpis nemá automaticky stejný právní účinek jako vlastnoruční podpis, z hlediska zamýšleného použití elektronických podpisů jako prostředku pro snadnější a pružnější uzavírání platných dohod a z hlediska vymaha-

telnosti, jsou standardní elektronické podpisy často považovány za přiměřené. Když soudy potřebují posoudit hodnotu jim předložených důkazů, obecně přikládají větší důkazní váhu dokumentům, které jsou elektronicky podepsány důvěryhodnější a bezpečnější technologií. V tomto ohledu poskytuje Adobe Sign důležitou důkazní hodnotu tím, že poskytuje vícefaktorové ověřování, registruje každou akci provedenou v Adobe Sign a certifikuje podepsaný dokument.

Navíc se domníváme, že existují argumenty pro tvrzení, že Adobe Sign může i bez použití technologie digitálního podpisu umožnit vytváření „zaručených elektronických podpisů", jak jsou definovány v článku 3 (11) nařízení eIDAS. Jelikož nařízení eIDAS nepřisuzuje zaručeným elektronickým podpisům žádné specifické právní účinky oproti standardním elektronickým podpisům, je nutno vidět, že i kdyby nebyly splněny zákonné požadavky zaručeného elektronického podpisu, je třeba na Adobe Sign pohlížet jako na důvěryhodné a bezpečné řešení elektronického podpisu.

Dále sledujeme, že Adobe Sign rovněž poskytuje možnost použití technologie digitálního podpisu, zejména zaručených elektronických podpisů založených na digitálních certifikátech a „kvalifikovaných elektronických podpisů", jak jsou definovány v čl. 3 odst. 12 nařízení eIDAS. Pokud tedy uživatel uvedenou možnost aktivuje, lze Adobe Sign považovat za nástroj vhodný pro obchodní styk, který podporuje a usnadňuje proces vytváření zaručených a kvalifikovaných elektronických podpisů. V případě kvalifikovaných elektronických podpisů to znamená, že Adobe Sign podporuje vytváření elektronických podpisů, které v souladu s článkem 25 nařízení eIDAS mají rovnocenný právní účinek jako vlastnoruční podpis a jsou uznávány v jiných členských státech EU.

Adobe Sign je spolehlivé řešení pro elektronické podepisování, s jehož pomocí lze spravovat ucelené (end-to-end) procesy podepisování ve shodě se všemi typy elektronických podpisů dostupných podle nařízení eIDAS. S Adobe Sign uživatelé mohou zejména konfigurovat a vytvářet pracovní postupy v souladu s konkrétními předpisy, odvětvím a svým rizikovým profilem.

5 O AUTOROVI

Prof. Dr. Patrick Van Eecke je partnerem skupiny pro právní praxi v IT ve společnosti DLA Piper v Bruselu, členem advokátní komory v Bruselu a přidruženým členem americké advokátní komory.

Prof. Van Eecke poskytuje poradenství orgánům veřejné správy i podnikům při implementaci řešení elektronických podpisů v souladu s právními předpisy.

Patrick Van Eecke se intenzivně podílí na různých výzkumných a poradenských projektech pro Evropskou komisi a několik národních vlád. Například se podílel na první studii Evropské komise o právních aspektech elektronických podpisů (1998), studii EK o politikách elektronického podpisu (2001), studii EK o dlouhodobé archivaci elektronických podpisů (2001) a studii EK o právních a tržních aspektech elektronických podpisů (2003). Byl hlavním konzultantem ve studii EK o budoucnosti politiky normalizace ICT (2006). V poslední době se intenzivně podílel na studii proveditelnosti Evropské komise o politice elektronické identifikace, autentizace a podpisu (IAS) (2010) a také na Studii EK na podporu implementace celoevropského rámce pro elektronickou identifikaci a služby vytvářející důvěru pro elektronické transakce na vnitřním trhu (2014).

Jako národní zástupce byl Patrick Van Eecke zapojen do debat Evropské rady o směrnici o elektronických podpisech a směrnici o elektronickém obchodu. V těchto záležitostech poskytoval rovněž poradenství Hospodářskému a sociálnímu výboru Evropských společenství. Jako právní expert expertního týmu EESSI (European Electronic Signature Standardization Initiative) byl spoluautorem první zprávy EESSI a následujících právních výstupů.

Dr. Van Eecke získal titul PhD na univerzitě v Lovani (včetně hostujícího stipendia na Stanford University) v předmětu „Právní status elektronických podpisů" (2003). Je profesorem na univerzitě v Antverpách a vyučuje evropské informační a komunikační právo. Je také hostujícím přednášejícím na Kings College a Queen Mary University (Londýn). Patrick Van Eecke je autorem několika právních článků a knih o počítačové kriminalitě, elektronických podpisech, elektronických kontraktech a ochraně soukromí a je pravidelným řečníkem na národních a mezinárodních konferencích.

Překlad a redakční úprava pro Amos Software: Tomáš Metlička, říjen 2020