NASAZENÍ ELEKTRONICKÉHO PODPISU V ORGANIZACI

(zkrácená verze pro externí použití)

verze dokumentu ze dne: **9. 4. 2010**

autor: **Vojtěch KMENT**
AXONNET, spol. s r.o.

Právní upozornění

Vytvoření tohoto dokumentu byla věnována odborná péče. Konkrétní nasazení nebo provedení elektronického podpisu v organizaci však může vyžadovat přídavné činnosti nebo postupy nebo jejich změny oproti tomuto dokumentu, nebo podrobnější provedení.

OBSAH

Úvod

Tento dokument poskytuje úvod a orientační seznam činností, které jsou v menší či větší míře potřebné pro organizaci nasazující elektronický podpis.

Dokument mohou především použít organizace, které se elektronický podpis teprve nasadit chystají. Mohou ho ale použít i organizace, u kterých nasazování probíhá nebo proběhlo, aby si své činnosti a postupy v hrubé rovině přiblížení ověřily.

Míra bezpečnosti a jejích záruk

Elektronický podpis lze implementovat v mnoha různých úrovních bezpečnosti. Platné právo ČR nepředepisuje důsledně všechny náležitosti provedení, ale ponechává prostor pro pružné možnosti přizpůsobení se podmínkám.

Přitom právo ale zásadně klade odpovědnost za podpisy na osobu, které byl vystaven certifikát. Důsledkem je, že největším běžným rizikem nasazení elektronického podpisu není popření pravosti podpisu, který osoba skutečně vytvořila, ale riziko opačného skutku. Osoba nebude schopna právně popřít vytvoření podpisu, který skutečně nevytvořila, tj. když její podpis byl zfalšován. Toto riziko se týká i organizace, rovněž její úkony mohou být zfalšovány. V případě úřadů a soudů mohou vznikat i falešné veřejnoprávní akty.

V praxi naštěstí zatím příliš k naplňování popsaného rizika nedochází. Jednorázový podvod by musel být mimořádně výnosný, opakování by podvodné schéma záhy znevěrohodnilo. S prosazováním se elektronizace dokumentů nicméně lze očekávat, že se s technologiemi seznámí širší populace, s tím pak vzroste četnost útoků i sofistikovanost útočných schémat.

Běžně existujícím postupem nasazování je níže popsaný *minimalistický přístup*. Pokrytí rizik nastává až při *systematickém přístupu*, kterému se tento dokument především věnuje.

Organizacím, které si nemohou dovolit plně systematický přístup, lze doporučit, aby se pokusily omezit použitelnost certifikátů, které podepisující osoba používá, na ty aplikace, které organizace chce používat. Toho lze dosáhnout certifikační politikou použité certifikační autority, do jisté míry i obsahem vystaveného certifikátu.

Cíloví čtenáři

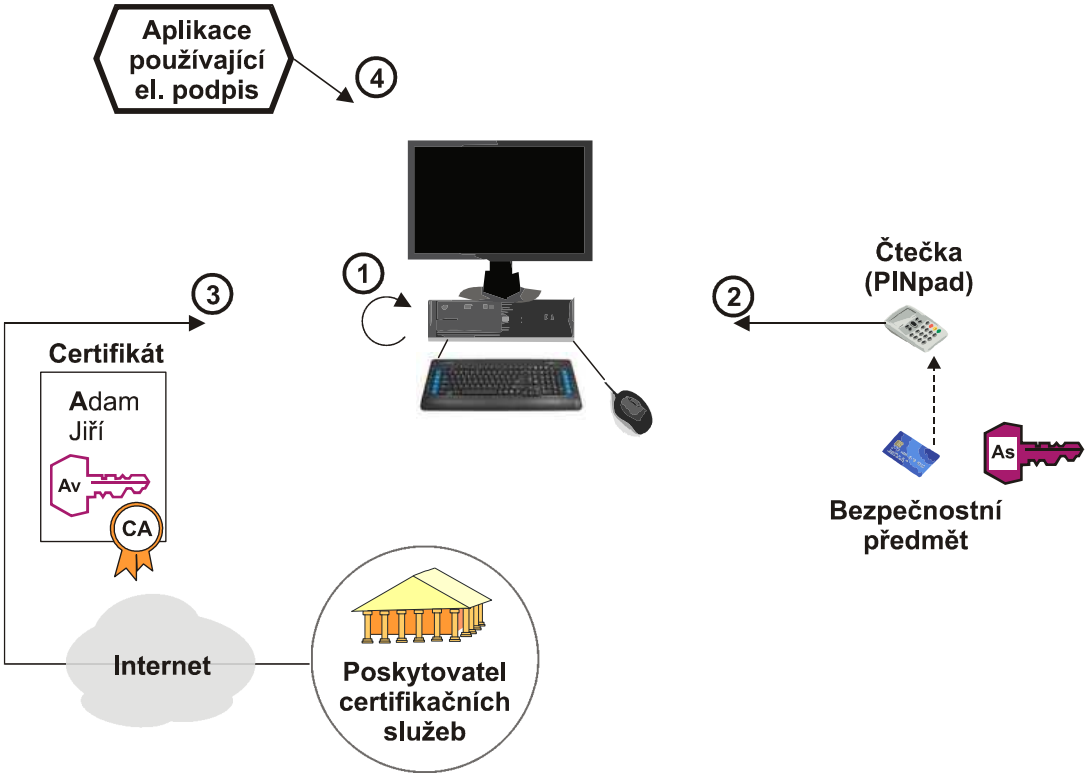
Tento úvod je určen pro všechny druhy čtenářů. Za ním následující seznam činností může být již méně čtenářsky přístupný. V tabulce obsažené v dodatku D lze nalézt rozdělení činností podle odborností zaměstnanců v organizaci.

Dodatek A popisuje vlastnosti elektronického podpisu a srovnává jej s běžným vlastnoručním podpisem. Je obecný a je určen všem čtenářům.

Dodatky B a C popisují význam pojmů a zkratek, v dokumentu používaných.

Minimalistický přístup k nasazení elektronického podpisu

Obrázek 1 dokumentuje minimalistický přístup k nasazení elektronického podpisu.



Obr. 1 – Doplnění pracovní stanice o prostředky

Pro možnost vytváření elektronického podpisu dostačuje v minimalistické verzi ověřit či doplnit existující pracovní stanici o 1) podporu požadovaného podpisového schématu, vytvořit 2) soukromý klíč a zajistit jeho uložení, 3) získat certifikát k veřejnému klíči a instalovat 4) aplikaci používající elektronický podpis.

1) Pracovní stanice podporující podpisové schéma.

Za vyhovující pracovní stanici bývá běžně považován desktop nebo notebook s dobově aktuální verzí operačního systému Windows. Protože řada aplikací používající elektronický podpis běžně využívá kryptografické knihovny operačního systému, je nutné ověřit, zda knihovny dané verze Windows podporují všechny potřebné kryptografické operace a algoritmy, které aplikace potřebuje.

Ministerstva vnitra vydalo akreditovaným PCS pokyn, aby od 1. 1. 2010 začali namísto hašovací funkce SHA-1 používat ve vydávaných certifikátech hašovací funkci SHA-2. Hašovací funkce SHA-1 je nyní považovaná za zastaralou. Přechod na SHA-2 v zásadě vyžaduje migraci na stanice s Windows Vista nebo Windows 7, možnosti funkce na Windows XP SP3 jsou omezené[1]. Vyhnout se migraci na vyšší verzi Windows lze pouze v případě, že aplikace používající elektronický podpis částečně nebo vůbec nevyužívají knihovny operačního systému.

Stanice mívá instalován bezpečnostní software různých funkcí, kvality a možností centrální správy.

2) Soukromý klíč a jeho uložení

Soukromý klíč lze vytvářet a ukládat v samotné pracovní stanici. Toto řešení zásadně nedoporučujeme, neboť v pracovní stanici existuje podstatně nižší úroveň kontroly a ochrany klíče, jak po stránce softwarově-kryptografické, tak po stránce fyzické bezpečnosti, než poskytují vnější bezpečnostní předměty.

Zásadně proto doporučujeme používat bezpečnostní předmět. Bezpečnostní předmět je externí účelové kryptografické zařízení malého rozměru s několika málo možnostmi použití, jednou z nichž je i elektronický podpis. Pro práci bývá nejjednodušší fyzická forma tokenu USB, možná je i podoba čipové karty.

Bezpečnostní předměty mívají různou úroveň záruk bezpečnosti, ale i použití těch levnějších z nich **vede na zásadně lepší bezpečnost**. Soukromý klíč je ve stálém fyzickém držení podepisující osoby a do výpočetního prostředí pracovní stanice se připojuje pouze na nezbytně nutnou dobu vytvoření elektronického podpisu.

---

[1] Hernady, R.: *Zavedení hash algoritmů SHA-2 v prostředí OS Microsoft Windows*, e-zine Lupa.cz, 6. 11. 2009, http://www.lupa.cz/clanky/zavedeni-hash-algoritmu-sha-2-v-prostredi-ms-win/

3) Certifikát

Certifikát je v zásadě elektronický dokument stanoveného formátu (X.509 v3), jehož nejvýznamnějšími obsaženými poli jsou jméno a příjmení osoby a hodnota veřejného klíče. Obsah certifikátu je elektronicky podepsán poskytovatelem certifikačních služeb (PCS), který certifikát vydal. Účelem certifikátu je prokázat třetí osobě, že obsažený veřejný klíč náleží osobě uvedeného jména a příjmení. V certifikátu mohou být i další osobní údaje osoby (např. adresa, název organizace, adresa elektronické pošty), které blíže upřesňují její totožnost. Použití certifikátů umožňuje, aby spolu mohlo komunikovat značné množství osob bez potřeby úvodního navázání komunikace způsobem každý s každým. Místo toho dostačuje, aby podepisující osoba si jednou nechala vydat certifikát od PCS a každá spoléhající osoba si instalovala kořenový certifikát stejného PCS spolehlivým způsobem.

V praxi se vyskytuje značné množství certifikátů různého označení.

Kvalifikovaný certifikát je certifikát, jehož „kvalifikace“ spočívá v tom, že obsah a způsob vydávání jsou upraveny platným právem. Kvalifikovaný certifikát se vydává fyzické osobě a je přípustné používat ho pouze pro účely elektronického podpisu. Důvodem tohoto právního omezení je především prevence případů, kdy fyzická osoba pomocí certifikátu vytvoří elektronický podpis k datům, které mají ryze strojový význam v rámci jiného kryptografického použití, přičemž mu hrozí nebezpečí podsunutí nezamýšleného obsahu k podpisu.

Pro použití v oblasti orgánů veřejné moci předepisuje v ČR platné právo doplňkovou podmínku: kvalifikovaný certifikát musí vydat akreditovaný PCS. Akreditace je formalizovaný kontrolní postup, kterým určené ministerstvo ověřuje kvalitu postupů, technologií a zabezpečení daného PCS, včetně kvality kryptografických algoritmů. V únoru 2010 jsou v ČR akreditováni tři PCS. Jejich akreditované služby lze považovat za vrchol kvality certifikačních služeb od subjektů sídlících v ČR.

Komerční certifikát je certifikát, který vydává třetí subjekt (PCS) fyzické osobě, ale jeho obsah ani vydávání nejsou upraveny právním předpisem. Obsah i postupy se proto řídí výhradně smluvním ujednáním PCS s certifikovanými osobami, vůči ostatním (spoléhajícím osobám) zpravidla jen jednostrannými prohlášeními PCS.

Použití komerčního certifikátu není rovněž právně upraveno a lze si představit, že certifikovaná osoba jej bude používat pro více účelů zároveň, včetně elektronického podpisu. Taková praxe přesto není z výše uvedených důvodů vhodná[2]. Vhodnější je používat pro každou fyzickou osobu dvojici klíčů a certifikátů. Komerční certifikáty používat pro šifrování obsahu a autentizaci, kvalifikovaný certifikát pro elektronický podpis.

Jinou možností je používat komerční certifikát pouze pro elektronický podpis a pro žádné jiné účely.

Komerční certifikáty vydávané PCS, kteří jsou akreditovaní, jsou považovány za důvěryhodné, ačkoli přesně vzato (kromě jednoho PCS) jsou akreditovány služby vydávání kvalifikovaných certifikátů a nikoli vydávání komerčních certifikátů.

Komerční certifikáty vydané jinými PCS z ČR jsou považovány za podstatně méně důvěryhodné.

Kvalifikovaný systémový certifikát je certifikát, který se vydává pro účel vytváření elektronické značky namísto pro vytváření elektronického podpisu. Elektronická značka je právně slabší analogií elektronického podpisu s tím, že entita která značku vytváří, mívá technickou povahu. Elektronické značky se vytváří jménem organizace nebo fyzické osoby, ale nepředpokládá se, že označující osoba se seznámila s obsahem označeného dokumentu, význam obsažené lidské vůle je pouze nepřímý. Určitá osoba nastavila automat, aby zpracovával a označoval elektronické dokumenty určitým způsobem bez toho, že by každé jednotlivé zpracování ověřila skutečná fyzická osoba. Nasazení elektronických značek bývá vždy zvláštní a v tomto dokumentu se jím dále nezabýváme.

Certifikát vnitřní CA je jakýkoliv certifikát, který si organizace vydá svým vlastním informačním systémem. Typicky se takové certifikáty používají pro vnitřní účely, včetně možností elektronického podpisu. Důvěryhodnost takto vydaných certifikátů bývá poměrně malá a spíše by se vůbec neměly používat jakkoli navenek mimo organizaci.

[2] Jistou výjimkou jsou uzavřené aplikační systémy, např. telebankingy některých bank.

Serverový certifikát je certifikát, který se vydává technické entitě, typicky webovému serveru, pro účely on-line autentizace serveru vůči přistupujícím vzdáleným klientům a šifrování probíhající komunikace sezení. Serverový certifikát by se zásadně neměl používat pro vytváření elektronických podpisů. K těmto účelům slouží kvalifikovaný systémový certifikát pro elektronické značky.

4) Aplikace používající (vytvářející / ověřující) elektronický podpis

Pro vytvoření nebo ověření elektronického podpisu je potřeba aplikace. Na trhu v zásadě chybí dostatečně univerzální aplikace, schopná bez omezení vytvářet a ověřovat elektronický podpis, a to postupy, které by byla právně zakotvené. Za jedny z rozšířenějších lze považovat aplikace poštovních klientů, zejména Microsoft Outlook. Jejich použití má však pouze omezenou užitečnost, neboť prostředí příjemců takto podepsaných poštovních zpráv neumí většinou došlé elektronické podpisy ověřit a vyhodnotit.

Elektronické podpisy v minimalistickém přístupu se proto nejvíce používají v rámci zvlášť vytvořených aplikací (telebanking banky, formuláře FÚ, formuláře zdravotní pojišťovny…), spojených vždy s určitou společností, úřadem nebo institucí.

Problémy minimalistické metodiky

Minimalistický empirický model pomíjí řadu náležitostí, které je třeba pro elektronický podpis předem vyřešit v rovině jak funkční, tak v rovině bezpečnostní.

Výsledným nasazením proto chybí univerzálněji použitelná funkcionalita. Jsou u nich opakovaně již téměř dekádu shledávány nedostatky typu „co se stane s platností elektronického podpisu v případě vypršení platnosti jeho certifikátu“?

Často se zjišťuje, že již zakoupené technologie elektronický podpis nepodporují buď vůbec, nebo jen omezeně.

Zcela samostatné problémy způsobuje nasazení elektronického podpisu pracovníků v organizaci. Technické a právní záležitosti elektronického podpisu jsou totiž až na výjimku[3] vyřešeny pro vztah podepisující fyzické osoby vůči spoléhající fyzické

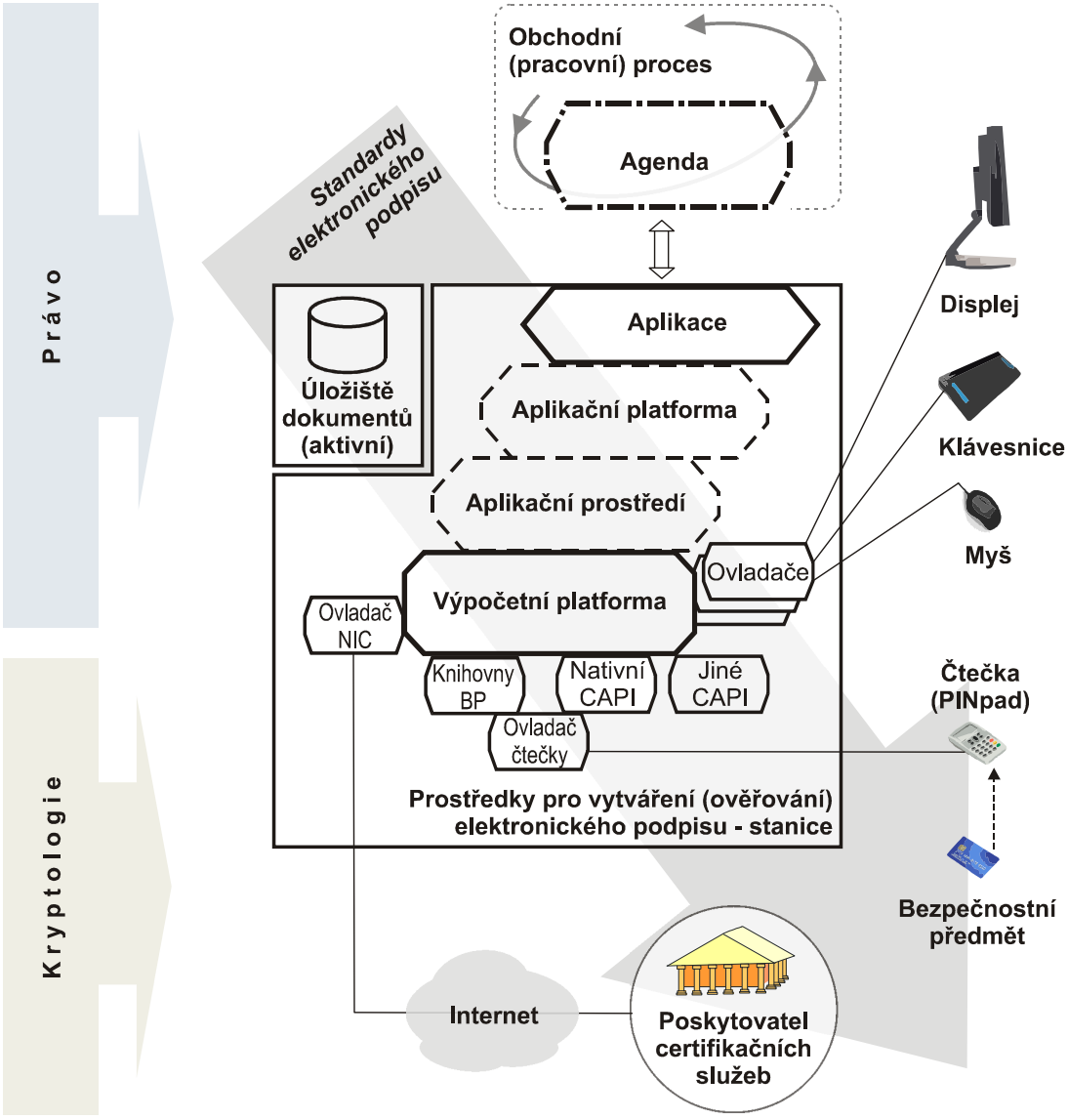
[3] Výjimkou je pojem zákonný pojem „držitel certifikátu”.

osobě, nikoli však pro vztah podepisující/spoléhající fyzické osoby vůči organizaci. V praxi bývají porušovány jak zákonná ustanovení, tak zásady bezpečné správy.

Hrubě podceňovány bývají i požadavky bezpečnosti a záruk bezpečnosti. Jejich nedořešení může mít za následek vznik právní odpovědnosti za škodu.

Systematický přístup k nasazení elektronického podpisu

Systematický přístup bere do úvahy veškeré požadavky právní, teoretické výsledky kryptologie, potřebu podkladové standardizace, rozdělení řešení na produkty a služby včetně nezávislého ověřování, otázky bezpečnosti i funkcionality.



Obr. 2 – Systém pro vytváření (ověřování) elektronického podpisu

Obrázek 2 provádí rozklad systému na množství softwarových a hardwarových prostředků, které se podílí na vytváření (ev. ověřování) elektronického podpisu.

Přitom platí zásadní požadavek § 2 písm. b) bod 2. ZoEP na elektronický podpis, tj. aby *„byl vytvořen a připojen k datové zprávě* ***pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou****“*.

Všechny prostředky z obrázku 2 proto musí přímo nebo nepřímo být pod výhradní kontrolou podepisující osoby, pracovat v souladu s její vůlí určitý dokument (datovou zprávu) podepsat. Obdobně zásada **WIPIWIS**[4] zdůrazňuje potřebu věrného zobrazení: „**Co je prezentováno, to je podepsáno**“. V žádném z prostředků nesmí dojít k záměně nebo změně (obecně podsunutí) jiného obsahu tak, aby výsledný elektronický podpis neodpovídal tomu dokumentu, který podepisující osoba podepsat chtěla. Žádný prostředek rovněž nesmí začít nebo umožnit vytváření elektronického podpisu samočinně, tj. podepisovat takové dokumenty, které podepisující osoba podepsat nikdy vůbec nezamýšlela, nebo který se v jednotlivém případě rozhodla nepodepsat. Elektronický podpis se vytváří bezprostředně poté, co podepisující osoba dala aplikaci jejím uživatelským rozhraním pokyn k vytvoření elektronického podpisu, aplikace požádala kryptografické knihovny o vytvoření elektronického podpisu, který se fyzicky provádí v připojeném (vloženém) bezpečnostním předmětu, přičemž operace podpisu se vůči bezpečnostnímu předmětu samostatně povoluje osobní autentizací podepisující osoby, zpravidla zadáním PIN, u každého podpisu zvlášť. Není-li bezpečnostní předmět připojen nebo PIN zadáno, nelze podpis vytvořit a v případě zájmu je nutné celý postup opakovat. Nelze tedy např. žádost o vytvoření elektronického podpisu uložit do pracovní fronty a vytvořit jej po několika minutách až hodinách později, když se podepisující dostaví ke svému počítači, a podepisovat žádosti bez zobrazení. Za dodržení těchto pravidel odpovídá ve smyslu § 5 odst. 1 písm. a) ZoEP podepisující osoba, která je povinna: *„zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak,* ***aby nemohlo dojít k jejich neoprávněnému použití****“*.

Souhrnně je odpovědností podepisující fyzické osoby, aby veškeré jí používané prostředky byly ve stavu, že 1) je má pod kontrolou a 2) že nemůže dojít k jejich

[4] Akronym z „What Is Presented Is What Is Signed”.

neoprávněnému použití. Pokud k úspěšnému útoku přesto dojde, bude za vzniklou škodu třetích (spoléhajících) osob odpovídat.

Systematický přístup k nasazení elektronického podpisu bere v potaz právní odpovědnost podepisující osoby za zfalšovaný podpis, která je u elektronického podpisu odlišná od případu vlastnoručního podpisu (viz tabulku 1). **Nedostačuje vytvářet platné elektronické podpisy, ale mít prostředí, v němž je dostatečně vyloučeno zfalšování elektronického podpisu kteréhokoli pracovníka organizace.**

Podepisuje-li elektronicky fyzická osoba v rámci činností v pracovním nebo obdobném poměru v organizaci, odpovídá za škodu třetím stranám zaměstnavatel (§ 420 odst. 2 ObčZ) a pracovník jemu zpravidla pouze do určitého limitu daného pracovněprávními předpisy.

Je proto v nejlepším vlastním zájmu zaměstnavatelů i pracovníků, aby veškeré použité prostředky, ale též způsoby jejich používání, skutečně zaručily, že tyto prostředky jsou pod kontrolou a nelze je zneužít.

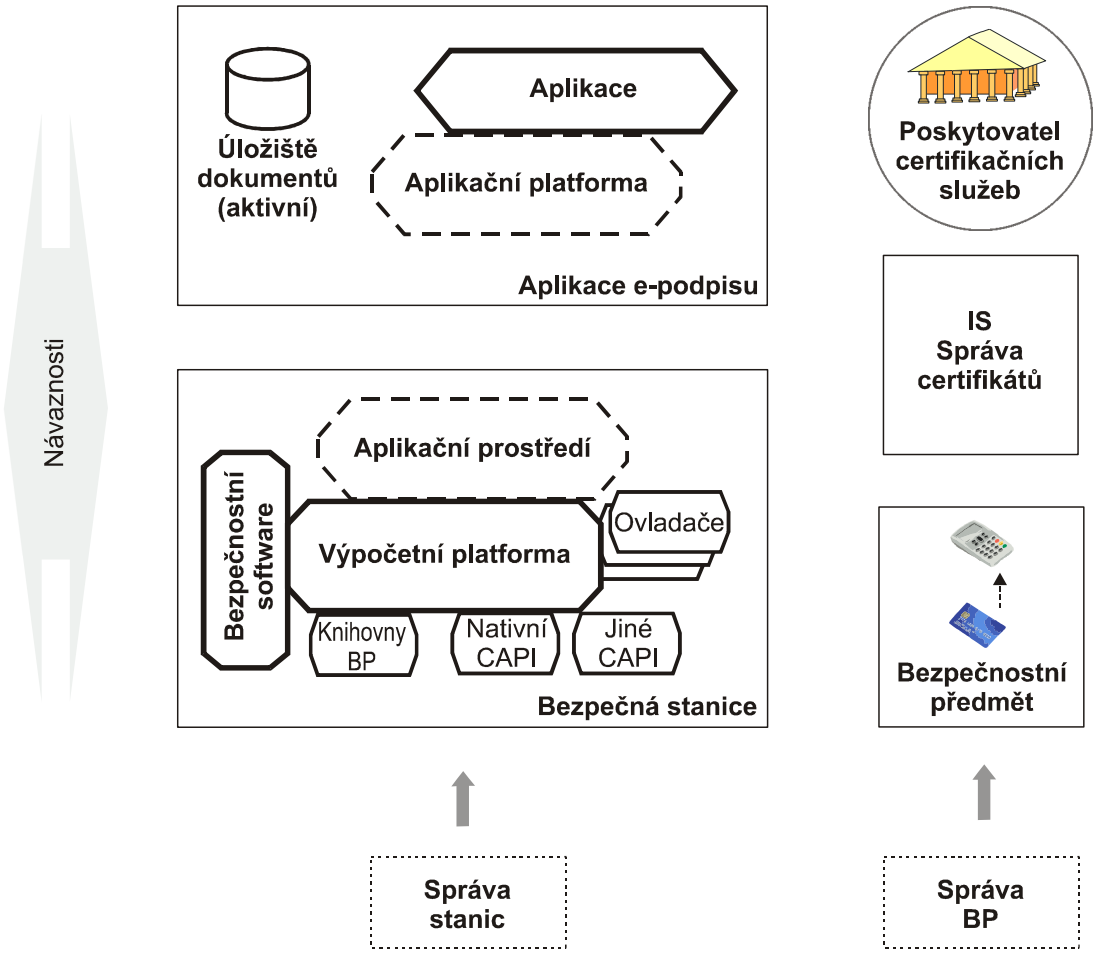
Obdobné požadavky v zásadě platí i v případě ověřování elektronického podpisu. Ověřující osobě musí být předložen (prezentován) dokument v tom zobrazení, jaké je správné (ideálně zcela stejné zobrazení, v jakém jej podepisující podepsal), a právě vůči tomuto zobrazení musí být indikováno, zda je k (v) dokumentu připojený elektronický podpis, nebo více podpisů, aktuálně platný. Právní úprava ověřování je oproti vytváření kusá, ale platí, že jedná-li spoléhající (ověřující) osoba na základě sobě podvrženého elektronického dokumentu nebo neplatného nebo již neplatného elektronického podpisu, kteréžto podvržení nebo neplatnost elektronického podpisu mohly její prostředky pro ověřování elektronického podpisu při řádné funkci odhalit, nese odpovědnost za škodu, kterou tím sobě nebo dalším osobám způsobí. V případě pracovního a podobného poměru se odpovědnost opět rozkládá a nese ji tedy především zaměstnavatel.

Rozdělení na technologické subsystémy

Prostředky pro vytváření a ověřování elektronických podpisů, uvedené na obrázku 2, nevznikají, nepořizují, nepřidělují se a nespravují se zpravidla jako jeden celek.

Pro účel volby, tvorby, návrhu a akvizicí je lze rozdělit až na jednotlivé produkty a služby. Vhodnější však bývá rozdělení na několik technologických subsystémů podle obrázku 3 níže. Každé části se lze věnovat poměrně samostatně a specificky.

Poskytovatel certifikačních služeb je dodavatel služeb souvisejících s vystavováním certifikátů a časových razítek. Typicky se bude jednat o akreditovaného PCS, tedy o vnější subjekt, může však být vytvořen i vnitřní organizační útvar v organizaci.



Obr. 3 – Technologické subsystémy z pohledu organizace

IS správa certifikátů je informační systém, který organizaci umožňuje vykonávat dohled a správu certifikátů vydaných jejím pracovníkům, popř. podporu před jejich vydáním.

Aplikace e-podpisu je souhrn aplikačního softwaru a služeb, které tvoří potřebnou aplikační logiku, provádí zpracování dokumentů a zejména vytvářejí a ověřují elektronický podpis.

Bezpečná stanice je typicky pracovní stanicí s konsolidovanou bezpečností. Stanice musí udržovat integritu svoji i aplikace e-podpisu, popř. dalších aplikací. Stanice má běžně podobu desktopu nebo notebooku. Myslitelná jsou i jiná provedení jako PDA (handheld) nebo mobilní telefon.

Správa stanic je sice nikoli nutný, ale z hlediska ekonomie i bezpečnosti vhodný systém centralizované správy pracovních stanic pracovníků organizace.

Bezpečnostní předmět je přenosný kryptomodul (čipová karta, token), v nepřetržitém držení podepisující osoby. Obsahuje soukromý klíč a provádí vlastní operaci asymetrického kryptoalgoritmu, tedy vytváření elektronického podpisu. Provedení čipové karty vyžaduje čtečku, která však může poskytovat další potřebnou úroveň zabezpečení (zadání PIN na PINpadu, nebo zadání biometrie).

Správa BP (bezpečnostních předmětů) je nikoli nutný, ale vhodný centralizovaný systém správy bezpečnostních předmětů.

Ať již se na systém hledí prizmatem obrázku 2 nebo 3, je potřeba si uvědomit, že z hlediska jiného kriteria dělení se jedná o souhrn: 1) hardware, 2) software, 3) služeb po síti, 4) vlastností prostředí a 5) postupů, podle nichž části byly převzaty, nasazeny a používají se. Bezpečnost záleží na správném provedení každé ze složek, nelze tedy zanedbat ani úpravu a dodržování postupů.

Postupy uvedené ad 5) mají charakter pomocných pracovních postupů, vykonávaných opakovaně, stejně, tedy rutinně, v době provozu.

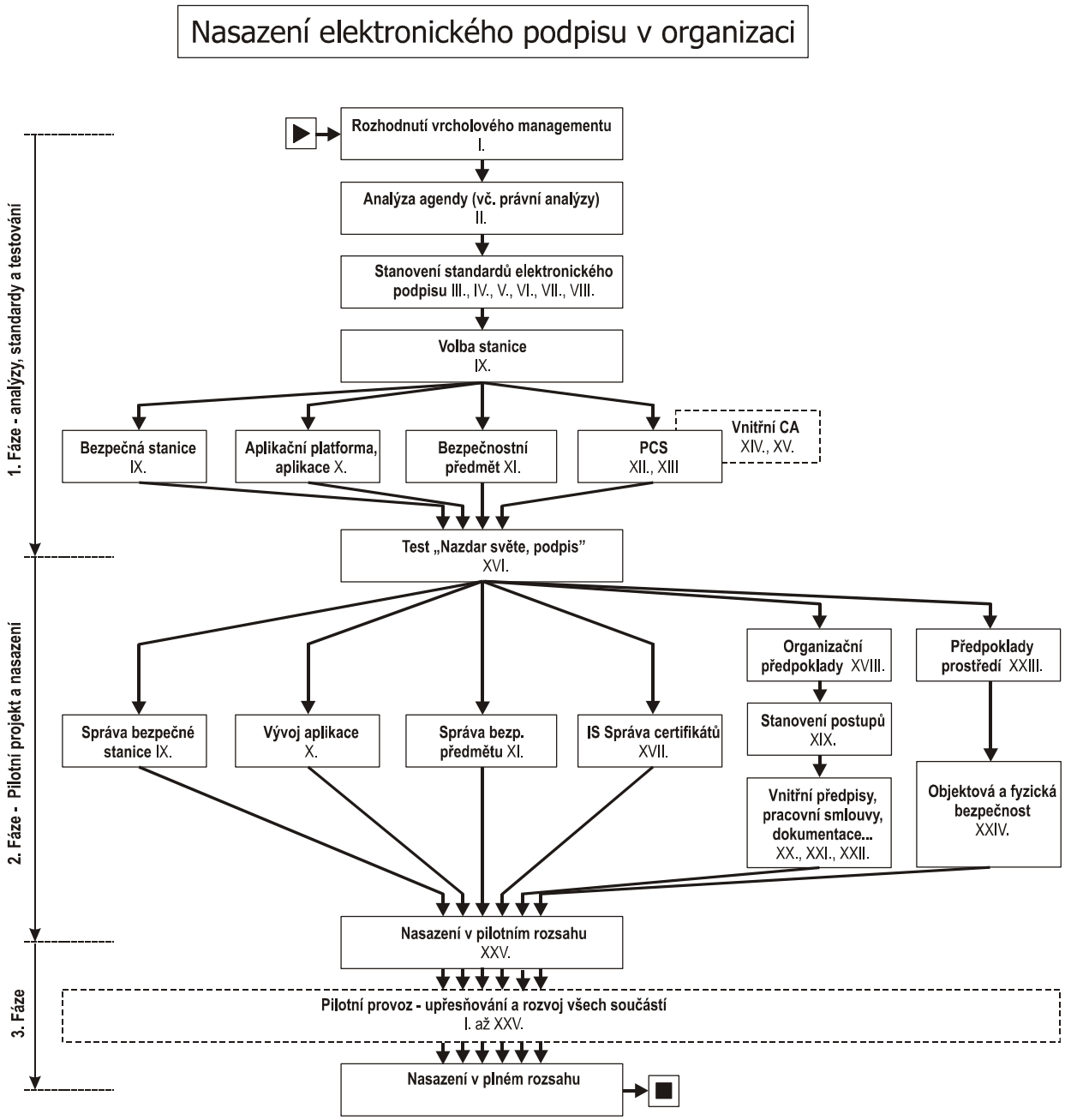
Od těchto postupů je nutné odlišit postupy, kterými části byly určeny, byly zvoleny jejich vlastnosti, vybrány nebo vytvořeny, ověřen jejich vzájemný soulad, vyhovování právním předpisům atd. Tyto postupy mají charakter projektových činností, vykonávaných jednorázově, neopakovaně, ještě před tím, než se běžné rutinní postupy začnou vůbec vykonávat.

Právě pro projektové činnosti má smysl rozdělení podle obrázku 3, neboť jednotlivé technologické subsystémy obrázkem vymezené lze v rámci projektu nasazování elektronického podpisu v organizaci řešit relativně samostatně. Jednotlivé

subsystémy jsou navzájem spojeny standardy, v dlouhodobém horizontu jsou jednotlivé části nahraditelné jiným řešením.

Činnosti projektu „Nasazení elektronického podpisu v organizaci“

Systematický přístup k nasazení elektronického podpisu lze vhodně realizovat jako projekt. Může nést název „Nasazení elektronického podpisu v organizaci“ a jeho typický postupový diagram může mít podobu dle obrázku 4 níže.



Obr. 4 – Postup činností projektu „Nasazení elektronického podpisu v organizaci”

Navržený sled činností je vhodný z několika hledisek. Rozděluje cíl projektu na řadu menších činností, tematicky vymezených a snáze zvládnutelných. Stanoví základ pořadí provádění činností, jakkoli může být nutné se v diagramu vracet zpět (pro přehlednost nejsou zpětné návraty zobrazeny), popř. provádět některé činnosti s výhledem na činnosti teprve později následující, aby se vracení spíše předešlo. Konečně, většina zásadních obtíží se zachytí během testů kapitoly XVI. „Nazdar světe, podpis“, čímž se předejde plýtvání náklady na technologie či postupy, které elektronický podpis implementovat v plné nebo požadované míře neumožní.

V reálné organizaci může být potřebné sled v menší či větší míře změnit. Může existovat potřeba navázat se na již zvolené technologie, nebo využít již existující technologické prostředí elektronického podpisu. I v takovém případě poskytuje uvedený diagram a popis v následujících kapitolách hrubý postup, nebo kontrolní seznam, s jehož pomocí lze zjistit, jak si organizace skutečně stojí – jaké činnosti byly provedeny, v jakém rozsahu a jak správně, jaké zatím byly zcela opomenuty.

Diagram v zásadě zobrazuje činnosti pro nasazení jediné aplikace. V reálné organizaci se zpravidla bude plánovat nasazení celé řady aplikací. Návrh je pak vhodné buď přizpůsobit požadavkům té aplikace, která má nejvyšší požadavky, nebo té úrovně, kterou se v dané etapě (1–2 roků) rozhodnete implementovat.

Reálná organizace potřebuje během činností provádět i akvizice. Okamžiky a provádění akvizic nejsou v diagramy zachyceny. Optimální je neprovádět žádnou velkou akvizici před dokončením testů kap. XVI. „Nazdar světe, podpis“, a finální akvizici provádět až po dokončení 2. fáze, tj. po provedení pilotního nasazení. Pokud organizace musí např. z důvodů zákonných nebo vnitřních požadavků provádět akvizice spíše hromadně pro celý projekt, pak je vhodné, aby podmínky zakázky obsahovaly ověřovací mezníky, které odpovídají fázím projektu a jakákoliv neschopnost dodržení striktně určených podmínek vedla k možnosti výpovědi zbytku projektu.

1. Fáze: analýzy, standardy a testování

Po (I) rozhodnutích vrcholového managementu by měla následovat (II) analýza agendy, která oproti běžné obsahuje i technická a právní hlediska požadavků elektronického podpisu. Na základě těchto analýz lze navrhnout či vybrat standardy

(III) podpisového schématu, (IV) formátu podepsaných dokumentů, (V) formátu podpisu, (VI) formátu certifikátu a profilu jeho obsahu, (VII) pravidel pro vytváření elektronického podpisu aplikací, (VIII) pravidel pro ověřování elektronického podpisu aplikací.

Technologicky klíčovým rozhodnutím je (IX) volba stanice, tj. výpočetní platformy. Je třeba ji volit s ohledem na řadu kritérií, včetně schopnosti vyhovění a podpory výše uvedených zvolených standardů. U zvolené stanice se následně zkoumají vlastnosti a možností její (IX) bezpečnosti – jakými způsoby lze bezpečnost zajistit, popř. vyztužit nebo konsolidovat.

Vyjma případů tvorby jediné aplikace je třeba věnovat pozornost **volbě aplikační platformy** (X) tak, aby umožnila vyvíjet a provozovat pokud možno všechny nebo mnoho druhů zamýšlených aplikací s elektronickým podpisem. Pokud je aplikace vyvíjena bez aplikační platformy, je třeba věnovat obdobnou pozornost vývojovému prostředí a aplikačnímu prostředí. Měly by mj. zajistit dlouhodobou životnost, tj. udržovatelnost vývoje i aplikací.

Bezpečnost podepisujícího z podstatné části zajišťuje (XI) bezpečnostní předmět již jen tím, že je použit. Úroveň bezpečnosti lze dále významně zvýšit volením jeho lepších bezpečnostních vlastností a záruk bezpečnosti, aniž by se podstatně zvyšovaly celkové náklady na pracovníka. Nejvyšší úrovně lze dosáhnout vnější čtečkou s klávesnicí (tzv. PINpad), která brání odchycení PIN škodlivým kódem.

Samostatnou oblastí činnosti je i určení parametrů certifikátu, jímž v současnosti bude(ou) profil(y) X.509. Kontrolou možností (XII) poskytovatele certifikačních služeb a výběrem vhodného obsahu certifikátů pro své pracovníky a dalších služeb jako jsou i (XIII) časová razítka lze opět dále významně zvýšit bezpečnost, věrohodnost a tím i smysluplnost celého řešení. Je možné navrhnout i (XIV) vnitřní certifikační autoritu /příliš se nedoporučuje/ popř. (XV) vnitřní autoritu časových razítek /vhodnější/. Riziku zneužití certifikátu lze čelit volbou certifikační politiky.

Celá první fáze vrcholí extenzivním (XVI) testem aplikací „Nazdar světe, podpis“. Na této aplikaci je nutné pečlivě odtestovat kombinaci všech zvolených technologií, produktů a služeb, včetně podkladových standardů a všech do úvahy přicházejících časově-věcných situací, do nichž se uživatelé aplikace mohou dostat.

2. Fáze: Pilotní projekt a nasazení

Je potřeba vyztužit bezpečnost stanice, instalovat bezpečnostní software a provádět správu bezpečné stanice (IX). Dle analýz a standardů (VII, VIII) musí proběhnout (X) vývoj aplikace vč. jejího závěrečného testování. Zpřesní se bezpečnostní profil a používání bezpečnostního předmětu (XI) včetně případné jeho centrální správy. Obdobně je vhodné zavést určitý (XVII) informační systém správy certifikátů.

Je třeba určit (XVIII) organizační předpoklady činností, tj. organizační jednotky a osoby, které se budou podílet na správě infrastruktury elektronického podpisu. Tyto osoby a pracovníci budou provádět (XIX) hlavní postupy. Postupy musí být reflektovány v řadě dokumentů, jejichž obsah je nutné navrhnout či změnit vč. (XX) změny vnitřních předpisů, (XXI) pracovní smlouvy a (XXII) další dokumentace.

Méně náročnými činnostmi zpravidla by mělo být zjištění dalších (XXIII) předpokladů prostředí a na něj navazující ustavení (XXIV) objektové a fyzické bezpečnosti.

Druhá fáze vrcholí v pilotním nasazení (XXV).

3. Fáze: K plnému nasazení

Ve třetí fázi dochází ke sběru informací z pilotního nasazení a provozu pilotní aplikace za období několika měsíců. Smyslem této fáze je zjistit situace a těžkosti, které nebyly odhaleny analýzou a prováděním žádné předchozí činnosti. Správně dříve provedený krok (XVI) testu aplikací „Nazdar světe, podpis“ by měl zajistit, že všechny nově zjištěné potřeby je možné hladce[5] integrovat do již provedených voleb pouze menší změnou. Běžně by tedy mělo docházet pouze k drobnému upřesňování již zavedených standardů, technologií, služeb, postupů, vlastností prostředí nebo změnám aplikací.

Ve stávajícím prostředí by měl být možný vývoj dalších aplikací a nasazení v plném rozsahu, popř. v postupně se zvyšujícím počtu nebo rozsahu agend a s nimi souvisejících aplikací.

Dodatek A obsahuje kontrolní seznam činností projektu nasazení el. podpisu.

[5] V případě méně zkušených návrhářů ale nelze vyloučit, že i v této fázi dojde ke zjištění zásadních nedostatků a potřebě dalekosáhlých návratů ve sledu činností.

I. Rozhodnutí vrcholového managementu

Vrcholový management organizace musí na počátku provést strategická rozhodnutí o elektronizovaných agendách, v jejichž rámci se budou vytvářet a ověřovat elektronické podpisy. Rozhodnutí by mělo být založeno nebo doprovozeno zjištěním předběžných znalostí a zastřešujících analýz, včetně právních. Součástí rozhodnutí je ustavení projektu, týmu projektu a jeho vedení, přidělení finančních aj. zdrojů.

II. Analýza agendy

Pro každou agendu je vhodné provést analýzu běžnou z hlediska návrhu IT a analýzu z hlediska elektronického podpisu. Analýzu může vykonat obecný analytik IT, ale její úplný výsledek by měl být přehlédnut specialistou na elektronický podpis pro vyvození důsledků. Analýza má dopad na volbu standardů.

Analýzu je částečně možné vytvářet postupně, zpřesňovat ji během rozhodování o implementaci aplikací a v průběhu postupu implementace.

III. Podpisové schéma

Kryptologické algoritmy jsou předmětem vývoje, kryptoanalýzy a zastarávání. Většina organizací bude mít tendenci zabývat se podpisovým schématem pouze jednoho druhu v krátkodobém horizontu. Pro dlouhodobou existenci je třeba se vypořádat s faktem rozvoje kryptologie, technologie a standardy mít vytvořeny pro možnost přechodu mezi schématy.

Základní perspektivní kryptografické schéma je RSA (délka klíče 2048 bitů) s hašovací funkcí SHA-2. Dosavadní prosazené jsou RSA s kratší délkou klíče (1024 bitů) a hašovací funkce SHA-1. Schémata mohou potřebovat určit vyšší podrobnosti o kryptoschématu.

IV. Formát podepisovaných dokumentů

Elektronický podpis má na formát podepisovaných dokumentů tento požadavek: „čím jednodušší, tím lepší”.

Požadavek je v ostrém rozporu s tradičními požadavky na bohatou funkcionalitu produktů IT a běžným způsobem jejich marketingu. Příčinou požadavku je kontrolovatelnost obsahu dokumentu a jednoznačnost při jeho zobrazení.

V. Formát podpisu

Datový formát, v němž se provádí spojení hodnoty elektronického podpisu s dokumentem, který byl podepsán. Formáty dále typicky umožňují připojování podepsaných a nepodepsaných atributů, připojení certifikátů. Formáty zpravidla poskytují jak možnost zaobalení dokumentu, tak možnost odloučeného podpisu.

Nad základním zvoleným formátem podpisu lze dále vytvářet volby formátů pro složitější elektronické podpisy s časovým razítkem, s validačními daty, až po archivní podpisy.

VI. Obsah (kvalifikovaného) certifikátu

Organizace musí stanovit, jaké položky certifikátu se budou vyplňovat, jaké údaje bude certifikát obsahovat. Existují dva přístupy: **minimalistický** (jméno a příjmení, název organizace, vnitřní číslo zaměstnance) vs. **maximalisticky** (co nejvíce podrobností vymezujících zaměstnance). Výhoda minimalistické verze spočívá v ožnosti ponechat certifikát v platnosti i pokud dojde ke změnám, které v širší verzi nutí k vydání nového certifikátu. Další její výhodou je, pokud jeden pracovník vykonává více druhů práce a uvedení pouze jediné pozice by bylo matoucí. Výhoda maximalistické verze je v přesnějším určení pracovníka a jeho pracovní pozice, omezuje riziko zneužití certifikátu při jednání navenek. Doporučení zní spíše ve prospěch maximalistické verze, neboť vede k vyšší bezpečnosti organizace.

VII. Vytváření elektronického podpisu aplikací

Aplikace vytvářející elektronický podpis zahrnuje řadu speciálních funkcí a technik. Aplikace by měla mít určitou vnitřní bezpečnostní architekturu.

VIII. Ověřování elektronického podpisu aplikací

Aplikace ověřující elektronický podpis (tzv. SVA) zahrnuje řadu speciálních funkcí a technik. Ověřování elektronického podpisu může probíhat ve fázích: 1) prvotní, 2) následná, 3) udržování dlouhodobé platnosti podpisu. Ověřování elektronického

podpisu nemusí dokonce provádět aplikace jediná, ale výše uvedené fáze lze rozdělit mezi více aplikací. S problematikou ověřování úzce souvisí tématika formátů elektronického podpisu dle V a technicko-právní rozbor tzv. doby latence

IX. Bezpečná stanice

Zajištění a udržování bezpečnosti stanice před škodlivými kódy je v současnosti **nutné i bez používání elektronického podpisu**. Příprava nasazení elektronického podpisu by však měla vést k reflexi dosavadního stavu v organizaci, k bezpečnostní konsolidaci, k podrobnějšímu pochopení a ovládnutí nástrojů, které bezpečnost stanice zajišťují, k prevenci výskytu situací, které mohou bezpečnost stanice zhoršit.

Obecný cíl je zajistit integritu výpočetní platformy resp. stanice tak, že:

- je vyloučen výkon řádně nautorizovaného nebo dokonce škodlivého kódu a aplikací, a
- výpočetní platforma včetně všech aplikací na ní zůstávají pod kontrolou pracovníka nebo centrálního správce organizace, popř. je kontrola mezi pracovníkem a správcem přesně rozdělena.

Požadavky na centrálně spravovanou stanici řízeného obsahu vyplývají ale i z důvodů právních (licence, omezení činností pracovníka), technických a též ekonomických. Splnění požadavků by proto nemělo být přičítáno pouze na vrub a účet vytváření infrastruktury elektronického podpisu, ale obecných nákladů IT.

X. Aplikační platforma, aplikace, úložiště

Aplikací se rozumí software (programové vybavení). Aplikace se v současnosti typicky vyvíjí v rámci aplikační platformy nebo aplikačního prostředí, na které navazuje. Pouze vzácně se vyvíjí přímo pro výpočetní platformu. Všechny použité knihovní nebo komponentové funkce by měly být vyvinuty s určitou mírou záruky bezpečnosti nebo důvěryhodnosti, jejich integrita být zajištěna i při běhu aplikace. Vývoj aplikace probíhá ve vývojovém prostředí, které umožňuje dosáhnout požadovanou úroveň záruk bezpečnosti a skutečně ji dosáhnout. Po vyhotovení aplikace musí být její vydání konzervováno se zajištěnou integritou, prováděno její šíření a nasazování.

XI. Bezpečnostní předmět

Bezpečnostní předmět je malý externí kryptografický modul, nejčastěji ve formě tokenu USB nebo čipové karty. Tím, že modul obsahuje soukromý klíč podepisujícího, umožňuje mu fyzickou držbu a kontrolu použití, která při uložení na disku není dosažitelná. Bezpečnostní předměty se mohou výrazně lišit v míře záruk bezpečnosti i v užitných vlastnostech.

XII. Poskytovatel certifikačních služeb: certifikáty

Poskytovatel certifikačních služeb (PCS) bude běžně vnější subjekt. V oblastech orgánů veřejné moci lze používat pouze kvalifikované certifikáty vydané PCS s akreditací pro tuto službu. V jiných případech lze použít služby i jiných PCS nebo neakreditované služby.

PCS je třeba zvolit z hlediska vyhovění řadě požadavkům, které vaše organizace na certifikační služby klade nebo by měla klást. Kromě vyhovění obsahu certifikátu (VI) je důležitá schopnost poskytnout nebo navázat IS správy certifikátů (XVII), podporovat vaše aplikace a bezpečnostní předměty. Je zapotřebí, aby PCS podporoval celý životní cyklus certifikátu z pohledu organizace.

XIII. Poskytovatel certifikačních služeb: razítka

Službu časových razítek lze poptávat i smluvně zajistit relativně nezávisle na službách vydávání certifikátů. Může být potřebné získávat časová razítka i od více na sobě nezávislých PCS.

XIV. Vnitřní certifikační autorita

Tento dokument zřízení vnitřní certifikační autority spíše nedoporučuje. V oblasti orgánů veřejné moci její použití není ani právně přípustné.

Konečný význam provozu CA je právní. Má-li být elektronický podpis použitelný jako důkaz, musí i provoz CA být důvěryhodný a tato důvěryhodnost být v případě potřeby prokazatelná třetí straně.

Takové nasazení vyžaduje trvalé angažování nejméně 3-4 na sobě nezávislých osob. Je potřeba použití jednoúčelových důvěryhodných systémů, splnění režimů fyzické

bezpečnosti, nepřetržitosti provozu vč. řešení kritických situací, využití prověřených, proškolených a loajálních pracovníků obsluhy, značného množství rigidních postupů, včetně následného vyhodnocování bezpečnostních záznamů.

Alternativa vnitřní CA – outsourcing s vlastní správou certifikátů

Namísto zřízení vnitřní CA je možné, aby organizace svou potřebu kontroly nad vydáváním certifikátů řešila spíše správou certifikátů ze strany organizace, spojené s outsourcingem jádra certifikačních služeb, některou v ČR akreditovanou CA. Součástí outsourcingu může být i provoz vlastní registrační kanceláře (RA).

Odlehčená vnitřní CA – omezení použití certifikátů

Použití vlastní vnitřní CA je možné, pokud se její použití připustí pouze pro předem omezená použití a s nimi související rizika. Omezení použitelnosti musí vyplývat (pořadí dle míry účinnosti omezení) z: smluvního ujednání, vnitřních předpisů, certifikační politiky, obsahu certifikátu.

XV. Vnitřní autorita časových razítek

Organizace může zřídit i vlastní autoritu časového razítka (TSA). Běžně není dosažitelné vydávání „kvalifikovaných časových razítek“, jejich použití ale zatím není v oblasti elektronického podpisu obecně závaznými právními předpisy uloženo.

Možnost vytvoření vnitřní TSA je řádově realističtější a méně nákladná než vytvoření vnitřní CA stejné úrovně bezpečnosti. Po instalaci a konfiguraci, která může být do značné míry zajištěna i externími pracovníky, vyžaduje vlastní provoz jen minimum správy a dozoru.

XVI. Kontrola „Nazdar světe, podpis“

Klíčová kontrolní fáze, která musí podchytit a) kompatibilitu všech částí, b) správnou funkci vytváření a ověřování elektronického podpisu na úrovni výsledné aplikace a c) záruky bezpečnosti všech použitých částí. Záruky bezpečnosti se prověřují vůči existujícím produktům. V případě teprve budoucí tvorby produktů se prověřuje udržitelnost dosažených záruk bezpečnosti nebo dosažitelnost požadovaných záruk bezpečnosti navrženým způsobem tvorby a podle okolností výrobce.

Teprve po úspěšném provedení kroků z této kapitoly je vhodné provádět akvizice ve větším rozsahu.

XVII. IS správa certifikátů

IS Správa certifikátů musí především umožnit organizaci udržet si přehled o certifikátech, které byly vydány jejím pracovníkům. Měl by organizaci umožnit takovou míru kontroly nad obsahem certifikátu, procesy jeho vydávání, kontrolou akutálnosti a možnosti zneplatňování certifikátů, aby organizaci v zásadě odpadla nutnost vytvářet vlastní vnitřní CA a byl tak umožněn outsourcing služeb některé akreditované CA.

XVIII. Organizační předpoklady postupů a personální bezpečnost

Postupy v organizaci musí provádět nebo podporovat určité osoby. Při provozu může existovat asi desítka rolí v postupech, jejichž provádění musí být přiřazeno konkrétním osobám z organizace. Tyto osoby by měly být vybrány podle vhodných kritérií znalostí, kvalifikace, důvěryhodnosti.

XIX. Hlavní formalizované postupy

Pro vystižení potřebného jednání osob je vhodné za **primární hledisko třídění** považovat **postup** dané osoby. Předměty, s nimiž osoba zachází (hw, sw, služby), i dokumenty, v nichž je postup popsán, mohou zpětně ovlivňovat obsah postupu.

Obecné druhy postupů jsou: nasazení, používání, správa, změny, mimořádné události a vysazení. Postupy se dotýkají mnoha softwarových a hardwarových produktů a služeb a jsou popsány v dokumentech více druhů (např. vnitřní předpisy, dodatky pracovní smlouvy, dokumentace …). Kombinacemi lze dospět až ke zhruba tisícovce potenciálních záznamů, nicméně běžné bude záznamy vhodně spojovat.

XX. Změny vnitřních předpisů

Vnitřní předpisy stanoví práva a povinnosti pracovníků při postupech s elektronickým podpisem, které jsou zvláštní pro danou organizaci. Vnitřní předpisy mohou ukládat povinnosti pouze v mezích zákona popř. jiných platných právních předpisů a jejich ukládání musí mít zákonný nebo smluvní základ.

XXI. Změny pracovní smlouvy

Jedná se o změnu nových textů nebo doplněk stávající pracovní smlouvy, jiné smlouvy zakládající pracovní poměr nebo výkon závislé práce či služeb. V těchto změnách je nutné soustředit úpravu vzájemných práv a povinností v těch oblastech, kde zákon o elektronickém podpisu nepředpokládá vůbec žádné jejich rozdělení mezi dva subjekty (typicky zaměstnavatel – zaměstnanec), ale z povahy věci se jedná o rozdělení nutné. Pracovní smlouva jako dvoustranný právní úkon rovněž může stavět najisto ty právní vztahy, u nichž by se jedna či druhá strana domnívala, že je v její kompetenci je upravovat sama, např. vydáním vnitřního předpisu.

XXII. Tvorba a změny dokumentace

Dokumentací se míní návod k použití nebo k postupu. Dokumentace napomáhá pracovníkovi nebo jiné osobě dodržovat stanovené postupy, nemůže však ukládat povinnosti (vyhrazeno vnitřním předpisům, právním předpisům a smlouvám).

Dokumentace lze řadit do dvou skupin: 1) Produktově orientované dokumentace (vytvářené výrobci nebo úpravou dokumentace výrobců), 2) Dokumentace postupů.

XXIII. Předpoklady prostředí

V tomto dokumentu řadíme do předpokladů prostředí dva rozdílné druhy předpokladů:

- Předpokládané bezpečnostním profilem ochrany, bezpečnostním cílem nebo bezpečnostní dokumentací některého produktu, pokud nejsou podchyceny nebo splněny v jiném bodu tohoto textu.

- Ty předpoklady prostředí, které jsou nutné nebo vhodné pro spolehlivou nebo bezpečnou činnost systémů a zařízení a nejsou uvedeny v části XXIV (fyzická bezpečnost).

XXIV. Fyzická bezpečnost

V tomto dokumentu je fyzická bezpečnost pojata v metodice, která se používá pro fyzickou bezpečnost při ochraně utajovaných skutečností dle právních předpisů ČR. Důvodem při podpoře elektronického podpisu není vyhovění právním předpisů, ale

získání výhody, která spočívá v lepší tržní podpoře takto rozdělených a systematizovaných opatření. Volby konkrétního opatření a jeho úrovně je nutné provést přiměřeně zjištěným rizikům, existujícímu stavu jejich uplatňování apod.

Při běžném nasazování dostačuje pro pracovní stanice fyzická bezpečnost stávajících kanceláří. Vyšší fyzickou bezpečnost mohou vyžadovat serverovny a pracoviště technické správy.

XXV. Nasazení v pilotním rozsahu

Pilotní nasazení se provádí vůči omezenému počtu pracovníků s vybranou aplikací. Při pilotním nasazování by valná většina postupů měla probíhat tak, jak jsou navrženy a předpokládány pro plný ostrý provoz. Přitom probíhá pečlivé sledování s cílem podchytit chyby, nejasnosti, neefektivity.

XXVI. Návaznosti a návazné systémy

Během průběhu projektu nasazování elektronického podpisu v organizaci se **nedoporučuje** jakkoli podmiňovat kroky projektu provedením integrace s takovými systémy, neboť to může oddálit úspěšné dokončení projektu, popř. vytvářet rizika pro provoz elektronického podpisu v organizaci.

Je však vhodné, aby vedoucí projektu byli v přiměřené míře informováni o takovýchto již existujících nebo připravovaných systémech a při návrhu a provádění projektu dbali na to, aby existovala možnost budoucí integrace.

Dodatek A – Vlastnosti a srovnání elektronického a vlastnoručního podpisu

Obecné vlastnosti a znaky podpisu

Podpis je ověřitelné trvalé zachycení v čase jedinečného projevu vůle podepisující osoby, kterým stvrdila určité informace v písemnosti obsažené, a zpravidla i završila své složitější právní jednání v písemnosti vyjádřené.

Podle povahy písemnosti a konkrétního obsahu může mít podpis mnoho významů (tzv. komitmentů), např.: autogram; podpis na prezenční listině; předběžné schválení písemnosti pro další postup; podpis objednávajícího na objednávce; podpis přijímacího na akceptaci objednávky; podpis na smlouvě; potvrzení průchodu písemnosti podatelnou; potvrzení osoby odesilatele (osoba písemnost vypravuje); potvrzení osoby příjemce (osoba písemnost přijala); podpis na podání vůči úřadu; podpis na úředním rozhodnutí osoby, která jej vydala; podpis na stejnopisu úředního rozhodnutí osoby, která odpovídá za vyhotovení; podpis na účetním dokladu; podpis na kvitanci; podpis na směnce atd.

Podpis tedy nevyjadřuje vždy určení autora (původce) dokumentu a nemusí ve všech ohledech nebo částech nutně vyjadřovat vůli podepsané osoby, nemusí být ani právně závazný nebo relevantní.

Nicméně typicky podpis znamená těsný vztah k původu dokumentu, dokument určuje vůli podepsané osoby (proč podpis připojila) a zakládá její povinnosti minimálně v úrovni právní odpovědnosti za stvrzené informace.

Platné právo může v některých případech stanovit určité náležitosti nebo okolnosti podpisu, bez nichž celá písemnost nebude platná i když podpis projevem vůle byl. Např. může být přikázán podpis na stejné listině (u některých vícestranných právních úkonů nebo jednání); provedení podpisu za přítomnosti svědků, kteří se rovněž podepíší; provedení podpisu před úředníkem úřadu nebo pracovníkem notáře, který pravost podpisu a totožnost podepisujícího potvrzuje doložkou. Právní předpis může předepisovat nebo implikovat formu dokumentu (listinná, elektronická, zcela zvláštní technická provedení – průkazy, bankovky apod.) a tím předurčit i možnou formu podpisu, nebo může stanovit formu podpisu přímo (např. vlastnoruční podpis) a tím naopak implikovat formu dokumentu.

Vlastnoruční podpis

Vlastnoruční podpis je vytvářen inkoustovým nebo kuličkovým perem na listinu, zásadně vlastní psací rukou podepisujícího. Má podobu tzv. holografní značky, která ve více či méně čitelné podobě představuje především jméno a příjmení podepisujícího. Vzhled značky daného podepisujícího je ustálený a podepisující běžně záměrně nemění její vzhled (podpis provedený v dobré víře).

Při podrobnějším zkoumání vlastnoručního podpisu na listině (papírové) lze zjistit, že podpis není pouze dvojrozměrným obrazem, jako by byl např. otisk razítka, ale že byl vytvářen tahem pera, které během vytváření mělo proměnlivou rychlost pohybu po papíře, tlak a sklon. Výsledný záznam v papíře je proto výsledkem činnosti s volností v nejméně čtyřech prostorových dimenzích a v čase. Udává se, že na tvorbě vlastnoručního podpisu se kromě vypěstované psychomotorické dovednosti podílí až 500 svalů.

Ověřování vlastnoručního podpisu se běžně provádí některou z metod:

- Kontrola přítomnosti podpisu bez ověřování pravosti vůbec.
- Laické ověřování zpaměti nebo srovnáním vůči podpisům v jiných dokumentech.
- Ověřování vyškolenými zaměstnanci proti jednomu záznamu podpisového vzoru, zejména srovnávací metodou.
- Přítomnost při vytváření podpisu podepisující osobou.
- Písmoznalecký posudek opřený o metody: grafologická, grafometrická, analytická, patografická, srovnávací a syntezující metoda systematická.

Ověření se tedy provádí se značně různou kvalitou, náklady a stráveným časem.

Elektronický podpis

Elektronickým podpisem se běžně rozumí[6] **právně upravená** podoba tzv. digitálního podpisu, který spočívá na kryptografických asymetrických algoritmech

[6] Pojem *elektronický podpis* dle českého práva nevyžaduje nutně použití asymetrické kryptografie. Použití asymetrické kryptografie vyplývá až v případě tzv. „zaručeného elektronického podpisu".

veřejného klíče a dalších matematických funkcí, které společně vytváří rodinu tzv. podpisového schématu. Kryptologicky je založen na existenci vzájemně související dvojice klíčů: soukromého klíče a veřejného klíče, které jsou jedinečné pro každého podepisujícího. S pomocí soukromého klíče, který je pod výhradní kontrolou podepisujícího, se vytváří jeho elektronický podpis určitého dokumentu. S pomocí veřejného klíče, který může být volně šířen, může jiná osoba ověřit, že se jedná o platný podpis dokumentu danou podepsanou osobou.

Mezi podepisující a ověřující osobu bývá běžně včleňován poskytovatel certifikačních služeb (PCS), který zejména vydává certifikáty. Certifikáty především osvědčují, že určitý veřejný klíč náleží určitému podepisujícímu. To umožňuje, aby ověřující osoba spoléhala na identifikační údaje v certifikátu. Odpadá nutnost předem vytvořit komunikaci každého s každým, důvěryhodně si vyměnit veřejné klíče a učinit o tom i vzájemně průkazné záznamy. Místo toho dostačuje, aby si podepisující nechal vystavit certifikát a ověřující si jednorázově instaloval a provedl kontrolu kořenového certifikátu PCS.

Jedině tyto poměrně složité metody zajišťují, že i v prostředí číslicových údajů může existovat mechanismus, který má všechny podstatné vlastnosti podpisu.

Elektronický podpis se **vytváří** nebo **ověřuje** pomocí výpočetních prostředků, zejména pomocí aplikace vytvářející nebo ověřující elektronický podpis. Bezpečné provedení vyžaduje technické (viz obr. 1) a organizačně postupové zabezpečení.

Elektronický podpis může vyžadovat **udržování platnosti** včasným připojováním časových razítek a validačních dat.

Srovnání vlastnoručního a elektronického podpisu

I když záměrem tvůrců elektronického podpisu bylo vytvořit nápodobu mechanismu vlastnoručního podpisu, z číslicové povahy dokumentů i elektronických podpisů určité rozdíly vznikají a vyplývají. Shrnuje je následující tabulka.

Protože podrobnosti právní terminologie jsou vůči čtenáři matoucí (příliš mnoho pojmů, nejasné pojmy, např. za *zaručený* elektronický podpis bez dalšího žádná třetí osoba ani stát neručí), v tomto textu až na zřetelně označené výjimky používáme pojem „elektronický podpis" zhruba ve významu „zaručeného elektronického podpisu" (v anglickém originálu "advanced electronic signature").

Vlastnost	Vlastnoruční podpis	Elektronický podpis
Projev vůle	Ano.	Ano.
Tajnost	V centrálním nervovém systému.	Jedinečný soukromý klíč v BP.
Kopírovatelnost tajnosti	Zásadně ne.	Velmi obtížné až nemožné[7].
Oddělitelnost tajnosti od podepisujícího a jeho vůle.	Ne.	Ano, ale mělo by být pohotově zjistitelné postrádáním BP.
Zneplatnění	Zásadně ne.	Ano, certifikátu a pozdějších podpisů.
Integrita písemnosti	Ne, pouze úpravou listiny.	Ano. I velmi rozsáhlé dokumenty s přílohami, příp. i zvukové nebo obrazové záznamy.
Totožnost podepisujícího	Sám o sobě podpis o totožnosti příliš neinformuje, k dispozici mohou být tvrzené informace v listině.	Ověřené údaje v certifikátu s menší až vyšší úrovní určení totožnosti (může se blížit úředně ověřenému podpisu). Soudem je zásadně zjistitelná totožnost od PCS.
Stárnutí podpisu	Není potřeba zvláštní činnosti pro úchovu platnosti podpisu.	Potřeba aktualizace časovými razítky a validačními daty, není-li řešeno jinak.
Kopírovatelnost dokumentu a podpisu	Reprodukční technika podpis nekopíruje zcela věrně a originál nelze zcela rovnocenně nahradit. Právně často vzniká potřeba úřední vidimace, ale ani ta neprostředkuje kopii podpisu pro účely dokazování jeho pravosti znaleckými posudky v té míře jako originál podpisu.	Je možné vytvořit libovolný počet kopií dokumentu i s vytvořenými podpisy, nerozlišitelných od originálu. Potřebné kopie lze vytvářet bez znatelných nákladů.
Falšování podpisu[8]	Snadné při běžné úrovni ověřování, obtížné až velmi obtížné s vyšší úrovní ověřování pravosti.	Velmi obtížné při vedení útoku na konkrétní osobu, snazší při vedení plošného útoku na mnoho osob.
Podvržení písemnosti	Obtížné při pozornosti podepisujícího. Při velkém počtu podpisů nutné přípravné kontrolní postupy.	Hrozba technického podsunutí oproti vlastnoručnímu podpisu existuje navíc. Přípravné kontrolní postupy mohou být elektronizovány a být efektivní.
Zkreslení vlastního podpisu[9]	Snadno možné. Prevence přítomností a srovnáním. Prokazování znaleckým posudkem.	Není běžně možné. Platný podpis by musel náležet jiné osobě shodného jména a příjmení.
Odpovědnost za zfalšovaný podpis	Spoléhající osoba.	Osoba, které náležel úspěšně zfalšovaný podpis, pokud včas neprovedla zneplatnění certifikátu.
Odpovědnost za podvrženou písemnost	Podepsaná osoba.	Podepsaná osoba.

Tabulka 1 – Srovnání vlastností vlastnoručního a elektronického podpisu

[7] Je-li soukromý klíč uložen v bezpečnostním předmětu (BP) a dodrženy postupy práce s BP.

[8] Při **podvržení** písemnosti nebo jeho části je podpis pravý, ale jeho vytvoření nebylo zamýšleno vůči podvrženým částem. Při **falšování** podpisu osoba vydávaná za podepisujícího tento podpis sama vůbec nevytvořila, falešná pak bývá i celá písemnost.

[9] **Zkreslení podpisu** je vytvoření vlastního podpisu ve špatné víře, s účelem jeho budoucího popření.

Tabulka 1 provádí nezaujaté srovnání vlastnoručního a elektronického podpisu[10]. Všechny potíže elektronického podpisu plynou z toho, že tajnost, na které spočívá, není inherentní součástí podepisující osoby. Z této vlastnosti plyne potřeba možnosti zneplatnit elektronické podpisy pro budoucnost, pokud přeci jen dojde k úniku tajnosti mimo kontrolu podepisujícího. Následně plyne potřeba ověřující osoby ověřovat stav platnosti certifikátu a většina dalších obtíží se stárnutím, které tvoří asi nejvýznamnější negativa současného elektronického podpisu. Na druhé straně má elektronický podpis řadu vlastností, které vlastnoruční podpis nemá a mít nebude.

Především správně provedený elektronický podpis je obtížnější zevně napadnout než podpis vlastnoruční. Jedná se o důsledek toho, že elektronický podpis nelze napodobit, je možné ho zfalšovat buď jen zcela přesně nebo vůbec.

Elektronický podpis může obsahovat mnohem více ověřených údajů o totožnosti než poskytuje vlastnoruční podpis.

Elektronický podpis kryje integritu (nenarušenost) dokumentu, umožňuje podepisovat i zvukové a obrazové záznamy, popř. data jiného druhu, včetně software.

Praktický význam mohou mít i právní rozdíly. Za škodu vzniklou úspěšně zfalšovaným elektronickým podpisem odpovídá bez dalšího ta osoba, jejíž podpis byl zfalšován. Spoléhající (ověřující) osobě proto mohou odpadnout náklady na potřebu velmi pečlivého ověřování pravosti vlastnoručního podpisu.

Kladem ale i záporem může být možnost neomezeného kopírování dokumentů s elekronickými podpisy.

Elektronický podpis poskytuje i další výhody, které plynou z možností použití elektronických dokumentů v agendách, z použití a hladké integrace agendy s informačními technologiemi.

[10] Nezabýváme se zde případem podpisu vytvořeného nesvobodně, pod fyzickým nebo psychickým donucením, tj. zejména v důsledku vydírání. Podle okolností násilí nebo nátlaku tyto podpisy budou nebo mohou být právně neplatné i když jsou formálně bez vady. Právní následky včetně neplatnosti jsou však v zásadě stejné bez ohledu na formu, v níž byl podpis proveden.

Dodatek B – Slovník pojmů

V tomto dokumentu se následující pojmy používají s přesným a opakovaně stejným významem. Pro účel stručnosti a pochopitelnosti čtenářem je definice některých pojmů oproti přesnému právnímu významu zjednodušena, snaží se jej však vystihnout co nejpřesněji.

Aplikace – programové vybavení nejvyšší úrovně, které řídí logiku a obsah interakce s uživatelem. Aplikace implementuje potřeby *agendy*.

Aplikační platforma – softwarový produkt, který umožňuje používání rapidně vyvinutých *aplikací* s *dokumenty* nebo *formuláři* (typicky 602 Form Server, systémy pro správu a oběh dokumentů apod.). Obecně nemusí být použita.

Aplikační prostředí – softwarové běhové prostředí poskytující služby vyšší úrovně (typicky Microsoft .Net, JavaEE, Java JRE …). Obecně nemusí být použito.

Agenda – dokumentově nebo formulářově orientovaná součást *obchodního procesu*.

Bezpečnostní předmět – hardwarový kryptografický modul sloužící pro bezpečné uložení soukromého klíče podepisující osoby a pro vytváření *elektronického podpisu* (typicky ve formě čipové karty nebo kryptografického tokenu).

CAPI – knihovny kryptografie s rozhraním pro *aplikace* (API).

Certifikát – formulář v elektronické podobě vydaný *poskytovatelem certifikačních služeb*, osvědčující vzájemnou souvislost a význam údajů v certifikátu.

Časové razítko – údaj v elektronické podobě, vztažený k určitému *dokumentu* nebo k jeho části (včetně možného zahrnutého elektronického podpisu(ů)), vyjadřující datum a čas svého vytvoření a tím i existenci *dokumentu* nebo jeho části před tímto okamžikem. Časové razítko vydává *poskytovatel certifikačních služeb*.

Činnost – činností se v tomto textu, neplyne-li z kontextu jinak, míní jednorázové aktivity fyzických osob provádějící nasazení elektronického podpisu v organizaci. Mají charakter složek projektu. Výsledkem činností je i ustavení *postupů*.

Čtečka (PINpad) – zpravidla externí hardwarová jednotka, do níž se zasouvá *bezpečnostní předmět* (čipová karta) na dobu vytvoření *elektronického podpisu*. Varianta PINpad obsahuje vlastní klávesnici pro oddělené zadávání PIN.

Datová zpráva – pojem, který ZoEP používá namísto pojmu *dokument*.

Dokument – posloupnost formátovaných znaků popř. i obrázků, se zjistitelným grafickým zobrazením (příklady: dopis, poštovní zpráva, objednávka, prospekt, nabídka, smlouva, časopis, webová stránka, katalogový lístek, výpis z veřejného registru, formulář…). V případech zvláštních potřeb dokument může obsahovat i zvukový, obrazově zvukový nebo jiný záznam, smysly zjistitelného vyjádření.

Elektronický podpis – údaj v elektronické podobě významu podpisu, vztažený k určitému *dokumentu* nebo k jeho části, umožňující zjistit platné provedení podpisu a některé údaje o podepsané fyzické osobě, které částečně nebo plně určují její totožnost.

Elektronická značka – obdoba elektronického podpisu. Elektronickou značku vytváří předem nastavený automat, může ji vytvářet i jménem právnické osoby nebo organizační složky (státu, společnosti apod.).

Formulář – druh *dokumentu* nebo *listiny* sestávající téměř výhradně z graficky a významově formátovaných polí pro zvláštní vyplňování.

Holografní podpis – je běžný vlastnoruční podpis v originále na papírové listině. Vzniklý záznam reflektuje několik dimenzí volnosti v prostoru a čase.

Jiné CAPI – *CAPI*, které není *nativním CAPI*, ale vyžaduje zvláštní instalaci a správu (na OS Windows typicky Cryptoki, ale i jiné knihovny).

Kvalifikovaný certifikát – *certifikát* jehož obsah a postup vydávání jsou upraveny právním řádem ČR a který slouží pro *elektronický podpis*.

Listina – zásadně papírový nosič pokrytý trvalým znakovým, obrazovým nebo kódovým záznamem, včetně možnosti nést jeden nebo více holografních podpisů.

Nativní CAPI – *CAPI*, které je vždy přítomnou součástí nebo doplňkem *výpočetní platformy* (na OS Windows typicky Microsoft CryptoAPI, CAPICOM).

Obchodní (pracovní) proces – pravidelný nebo opakovaný postup jednoho nebo více *pracovníků organizace*, včetně interakce s pracovníky partnerů a s klienty, který uspokojuje dílčí cíl činnosti *organizace*.

Organizace – subjekt veřejného práva (typicky úřad) nebo soukromého práva (typicky obchodní společnost) nebo jejich organizační složka, která zavádí *elektronický podpis* pro své *pracovníky* a *obchodní (pracovní) procesy*.

Ovladač – programový modul nízké úrovně obsluhující určitou hardwarovou jednotku rozhraní *výpočetní platformy* nebo hardwarovou jednotku vnější vůči *výpočetní platformě*.

Písemnost – *listina* nebo *dokument*.

Poskytovatel certifikačních služeb – subjekt, který poskytuje certifikační služby jimiž jsou zejména: provoz certifikační autority, provoz registrační autority, vydávání *certifikátů*, zneplatňování *certifikátů*, vedení seznamů vydaných certifikátů, vedení seznamu zneplatněných certifikátů, vydávání časových razítek.

Postup – postupem se v tomto textu, neplyne-li z kontextu jinak, míní opakované aktivity fyzické osoby během využívání elektronického podpisu v organizaci. Tyto postupy jsou formalizovány, dokumentovány a jsou výsledkem nasazení elektronického podpisu v organizace. Srovnej použití pojmu *činnost*.

Pracovní proces – viz *obchodní proces*.

Pracovník – fyzická osoba v pracovním nebo obdobném poměru vůči *organizaci*.

Úložiště dokumentů (aktivní) – trvalá paměť (disk, diskové pole), které umožňuje dlouhodobou úchovu *dokumentů* pro *aplikace*. Aktivita úložiště spočívá v údržbě platnosti elektronicky podepsaných dokumentů aktualizovanými *časovými razítky*. Může ale nemusí být součástí *výpočetní platformy*. Může ale nemusí být spoluvyužíváno více *aplikacemi*.

Uznávaný elektronický podpis – *elektronický podpis*, který vyhovuje určitým právně technickým požadavkům stanoveným právními předpisy ČR. V oblasti orgánů veřejné moci (úřady, soudy, policie…) zákon povoluje používat pouze

uznávané elektronické podpisy nebo podpisy vyšší úrovně, které pokrývají znaky uznávaného elektronického podpisu.

Virtuální privátní síť – je systém softwarové podpory na stanici pracovníka, který začleňuje provoz stanice do vnitřní sítě organizace při vzdáleném připojení, zpravidla prostřednictvím šifrovaného tunelu v internetu, vedoucího ze stanice do brány VPN, jako by stanice byla připojena přímo ve vnitřní síti organizace.

Výpočetní platforma – základní běhové prostředí programového vybavení, typicky operační systém a služby jeho podkladového hardware.

Dodatek C – Seznam zkratek

BES – Basic electronic signature.

BP – Bezpečnostní předmět.

CA - Certification Authority, tj. certifikační autorita popř. certifikační úřad.

DTBS – Data To Be Signed, tj. data určená k podepsání. Složení podepisovaného dokumentu a podepisovaných atributů.

EKS – Elektronická kontrola vstupu, opatření fyzické bezpečnosti.

EZS – Elektronický zabezpečovací systém, opatření fyzické bezpečnosti.

IDS – Intrusion Detection System, tj. systém detekce narušení prostředí, zejména provozu sítě (intranetu), provozu serverů. Moderní systémy přecházejí na IPS.

IPS – Intrusion Prevention System, tj. systém předcházení narušení. Může být na úrovni sítě, serverů i stanice.

IT – Information technology, tj. informační technologie.

ObčZ – Občanský zákoník.

PCS – Poskytovatel certifikačních služeb, viz slovník pojmů.

SCA – Signature-creation Application, tj. aplikace vytvářející podpis.

SCDev – Signature-creation device, tj. *prostředek pro vytváření elektronických podpisů* (pojem ZoEP).

SSCD – Secure signature-creation device, tj. *prostředek pro bezpečné vytváření elektronických podpisů* (pojem ZoEP).

SSO – Single Sign On, systém jednotného přihlašování do systému a aplikací.

SVA – Signature-verification Application, tj. aplikace ověřující podpis.

TSA – Time Stamping Authority, tj. autorita časového razítka.

TWS – Trustworthy system, důvěryhodný systém.

VPN – Virtual Private Network, tj. virtuální privátní síť.

WIPIWIS – akronym z „What Is Presented Is What Is Signed“, tj. „Co je prezentováno, to je podepsáno“.

ZoEP – zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů.

Dodatek D – Osoby a útvary účastnící se projektu

Nasazení elektronického podpisu by v organizaci mělo probíhat jako projekt. Tento dokument sice není popisem určitého projektu, nicméně je vystavěn jako částečně volitelná osnova činností projektu, který se upraví na míru organizaci.

Hegemonem projektu musí být projektový tým (zejména jeho vedení), který je vedením organizace pověřen provedením projektu, jsou mu poskytnuty zdroje a pravomoce k jeho provedení. Projektový tým může být složen z interních i externích pracovníků, přičemž interní odpovídají především za vynakládání zdrojů, informační a systémovou provázanost a komunikaci v organizací, externí vnášejí specifické technologické, právní apod. know-how. Projektový tým nebo jeho klíčoví členové se z rozvoje projektu odpovídají stanoveným dozorující osobě, zpravidla z vedení organizace.

S projektový týmem se musí povinně koordinovat další útvary a osoby z organizace. Níže uvedená tabulka obsahuje přehled typicky se účastnících útvarů a osob a určení činností, jimiž se typicky v projektu zabývají.

Druhy útvarů a osob

Útvar, osoba	**Provádí činnosti v projektu**
I. Pravidelné útvary účastné na projektu (ev. pozdějším provozu)	
1) Vedení organizace (vrcholový management)	Provedení strategických rozhodnutí o nasazení aplikací a elektronických podpisů, provedení pověření projektu a alokace zdrojů dle I. Kontrola milníků projektu a výsledků projektu.
2) Obchodní oddělení, ev. výroba, nákup aj. klíčová oddělení organizace vč. řízení vnitřní administrativy a postupů	Prosazování agend (II), které mají být elektronizovány. Zjišťování agend, jejichž elektronizace přináší organizaci nejvyšší užitek nebo prospěch.
3) Oddělení IT - vedoucí IT - bezpečnost IT - správa stanic - správa serverů - správa sítí a telekomunikací, - podpora IT a helpdesk	Obecně: vyjadřování se k vhodnosti technologií a standardů, nápomoc s testy, následně správa a podpora postupů. Těžiště: Vyjadřování se k vhodnosti II, III, IV, V. Správa bezpečné stanice (IX). Správa aplikačního prostředí a aplikace (X). Správa sítě a síťové bezpečnosti (IX). Správa bezp. předmětů (XI). Správa IS certifikátů (XVII). Podpora systému dokumentace + tvorba dokumentace postupů se systémy IT (XXII). Správa části předpokladů prostředí (XXIII). Podpora nasazení v pilotním rozsahu (XXV).

	Integrace s návaznými systémy (XXVI).
4) Oddělení personální - personální vedoucí, - osoba potvrzující žádosti vůči PCS	Obecné úlohy: Výběr osob na pozice provádění postupů, úprava pracovní náplně osob, zajišťování školení. Příprava podílu personálního oddělení na postupech. Vydávání potvrzení během pilotní fáze i během provozu vůči PCS pro osoby, které se mají nechat certifikovat. Ovládání IS správa certifikátů (XVII). Návrhy osob na pozice a zajišťování personální bezpečnosti (XVIII). Vyjadřování se k návrhům postupů (XIX). Vyjadřování se k návrhům vnitřních předpisů (XX) a změn pracovní smlouvy (XXI). Marginální účast na dokumentaci postupů, které se týkají personální problematiky (XXII). Integrace správy certifikátů s personálním IS (XXVI).
5) Oddělení právní - právník (vlastní nebo externí).	Přehled hlavních právních úprav, které regulují činnost organizace. Posouzení návrhů smluv a vytvářených vnitřních předpisů. Vyjadřování se nebo změny návrhů vnitřních předpisů (XX) a změn pracovní smlouvy (XXI).
6) Správa budov	Fyzická bezpečnost (XXIV), část předpokladů prostředí (XXIII).
II. Nepravidelné útvary účastné na projektu nebo pozdějším provozu	
A) Projektový tým: - vedoucí projektu, dále dle povahy: - IT bezpečnost, - kryptolog, - vývojář, - právník. (složení týmu může být částečně interní a částečně externí).	Prosazování, řízení nebo koordinace provádění veškerých činností (I – XXVI). Návrhy, prezentace, sběr vyjádření, projednávání, rozhodování nebo vydávání doporučení pro rozhodnutí, akvizice, dohled nad prováděním. Osoby týmu jsou určené dle I, musí být vybaveny pravomocemi vůči ostatním osobám organizace, vybaveny zdroji a odpovědností za projekt.
B) Vývoj (software): - vedoucí vývoje, - analytik, - vývojáři, - dokumentace.	Vývoj zvláštních aplikací (X, VII, VIII) na klíč, nebo úprava vlastního software organizace.
C) Správa CA - bezpečnostní vedoucí, - registrační úředník, - systémový správce, - systémový operátor, - systémový auditor.	Instalace, konfigurace, správa, provoz vnitřní CA a TSA (XIV, XV).
D) Vedoucí zaměstnanci (vedoucí odborů, oddělení apod.)	Udílení pokynů k pořízení si certifikátu, k používání určité aplikace s elektronickým podpisem. Dohled nad využíváním aplikací.

Tabulka 2 – Druhy útvarů, skupin, týmů a osob účastnících se projektu