Vlastnoruční digitální podpis a jeho implementace v O_2

část II.

Jak vypadá celková architektura řešení? Jaké poznatky přinesl pilotní provoz? Jaké hlavní závěry, poučení a doporučení z projektu vzešly?

V předcházející části byla popsána výchozí situace, z níž jen připomeneme, že veškerá zákaznická dokumentace vznikala primárně v papírové podobě, což komplikovalo další zpracování, zdržovalo a přinášelo zbytečné náklady. Proto telekomunikační operátor hledal řešení, které nebude mít negativní dopad na zákazníky a nezhorší důkazní pozici O2 ani zákazníka v případě sporu. Dále jsme v prvním díle popsali provedení analýzy dopadů, kroky potřebné pro získání podpory klíčových skupin, výběr technologického řešení a dodavatele i vlastní vývoj řešení. Pozornost jsme věnovali také právní přípravě projektu.

Principy zabezpečení / bezpečnostní mechanismy

Za účelem definice bezpečnosti řešení byla provedena Analýza rizik, hrozeb a zranitelností. Na tomto základě byl vytvořen Bezpečnostní koncept popisující konkrétní opatření implementovaná v jednotlivých krocích procesu od vzniku dokumentu až po jeho finální uložení.

Opatření jsou aplikována na mnoha úrovních (architektura, systémy, procesy, metodika, uživatelé):

- Certifikované podpisové podložky a tablety
- Certifikovaná podepisovací komponenta SignDoc od německé společnosti SOFTPRO
- Vlastnoruční digitální podpis spojený s daným dokumentem (neuchovává se samostatně)
- Otisk dokumentu (hash)
- Asymetrická kryptografie
- Přístupová oprávnění a autentizace uživatelů
- Security Gateway zajišťující příjem dokumentů, validaci a předání na další systémy
- Kvalifikovaná elektronická značka a časové razítko
- O2 Důvěryhodný archiv zajišťující dlouhodobou archivaci
- Smlouva zasílaná zákazníkům je chráněna heslem (OTP)
- Zásada „čtyř očí“ – dokument je vždy zpracován a podepsán za účasti zákazníka i uživatele
- Podepsanou smlouvu nelze uložit lokálně v čitelné podobě
- Dohledovaná a autorizovaná instalace aplikace SignoSoft a aktivace profilu uživatele (unikátní link, login, OTP)

Tak vysoký počet opatření jsme zavedli proto, abychom eliminovali všechna rizika a zároveň zajistili platnost a důvěryhodnost smlouvy po celou dobu zpracování včetně následné archivace.

Pro nezávislé potvrzení realizovaných bezpečnostních opatření jsme si nechali po nasazení celého řešení do produkce vypracovat znalecký posudek v oblasti bezpečnosti informačního

systému, jehož autorem je Ing. Jindřich Kodl, CSc., znalec v oboru kybernetika, odvětví výpočetní technika se specializací kryptologie, bezpečnost informačních systémů a informatika. Jeho závěry potvrdily, že implementace odpovídá požadavkům a že zvolená bezpečnostní opatření pokrývají identifikovaná rizika. Řešení tedy prokazatelným způsobem zajišťuje vložení podpisu pouze do podepisovaného dokumentu a jeho platnost – nezměněná integrita a autenticita – může být prokázána i v budoucnu.

Technické řešení / architektura

Technické řešení zahrnuje produkty SignoSoft a jejich integraci na stávající systémy. Součástí dodávky je také zpracování zákaznické dokumentace.

Klientská a serverová aplikace

Řešení SignoSoft je postavené na robustní klient / server architektuře. Klientská aplikace je natolik multiplatformní, aby mohla být nasazena na všech prodejních kanálech. Navíc může plnohodnotně fungovat i v off-line režimu. To je důležité pro nasazení u mobilních prodejců, kteří nemusí být vždy v lokalitách s dostupným připojením k internetu (uvnitř budov atd.). V tom případě mohou smlouvu vytvořit a se zákazníkem podepsat, ale k jejímu odeslání na server dojde později automaticky, jakmile se obnoví připojení. Smlouva je již v momentě podpisu v klientské aplikaci zašifrována a bezpečně uložena, takže nemůže dojít ke zneužití. Na server se odesílá dávka obsahující podepsaný dokument včetně metadat nezbytných pro další zpracování a kopie ID dokladů.

S ohledem na technické vybavení prodejních kanálů a způsob přístupu k systémům O2 se liší použitá klientská aplikace a způsob její komunikace se serverem:

- Značkové prodejny a franšízy – osobní počítač s podpisovou podložkou Wacom, platforma Windows XP/7 + Citrix, odesílání dávek přes interní síť O2
- Mobilní prodejci – tablety Samsung Galaxy Note 10.1, platforma Android, odesílání dávek přes internet
- Externí obchodní zástupci – notebook s podpisovou podložkou Wacom, platforma Windows XP/7/8, odesílání dávek přes internet

Serverovou část tvoří tzv. Security Gateway a jak název napovídá, plní roli elektronické podatelny spojené s navazujícími systémy. Přijímá dávky z klientské aplikace a ověřuje jejich integritu, platnost elektronických podpisů, validitu metadat a oprávnění uživatelů. Pokud je ověření v pořádku, předává je dalším systémům, zejména do DMS a O2 Důvěryhodného archivu. Kromě toho zajišťuje správu uživatelských účtů a profilů (včetně možností blokace nebo resetu), distribuci a správu certifikátů pro šifrování podpisových dat a certifikátů pro šifrování dávek, zpracování metadat, auditování procesů a další činnosti.

Integrace

Integrace řešení SignoSoft na okolní systémy je obousměrná – na vstupu je prázdný nebo předvyplněný formulář smlouvy, který je potřeba podepsat, na výstupu pak podepsaný dokument, který je nutné odeslat zákazníkovi a bezpečně uložit. Zapojené jsou postupně následující systémy či systémové domény:

CRM systém – zajišťuje vygenerování šablony smlouvy ve formátu PDF, její vyplnění včetně metadat a otevření v klientské aplikaci SignoSoft (externí prodejní kanály bez přímého přístupu do CRM pracují s editovatelným PDF formulářem).

DMS systém – zajišťuje uložení podepsaného elektronického dokumentu pro účely běžného zpracování, umožňuje náhled smlouvy na prodejních místech a předání smlouvy do automatizovaného zpracovatelského workflow dle nastaveného procesu. Pokud je ke smlouvě přiložena anonymizovaná kopie ID dokladů, dojde k jejímu uložení odděleně od smlouvy v souladu s legislativními požadavky na ochranu osobních údajů.

Integrační platforma a e-mailový systém – zajišťuje odeslání smlouvy zákazníkovi a v definovaných případech i prodejci (externí prodejní kanály). Z důvodu bezpečnosti probíhá zaslání ve dvou částech – e-mailem odchází PDF soubor komprimovaný do ZIP archivu, SMS zprávou odchází jednorázové heslo (OTP) k ZIP archivu.

O2 Důvěryhodný archiv – zajišťuje dlouhodobé a důvěryhodné uložení smlouvy, tj. označení kvalifikovaným časovým razítkem v okamžiku vstupu smlouvy a následné přetiskování v pravidelných intervalech dle nastavené politiky. Přístup je omezen na vybrané jednotlivce a je možný pouze za účelem získání originálu pro potřeby soudního či správního řízení.

Zařízení pro zachycení podpisu

Výběr podpisových zařízení (viz Tab. 1) má vliv nejen na ergonomii používání uživateli a zákazníky, ale zejména na kvalitu snímání podpisových dat, která jsou důležitá pro jejich případné písmoznalecké zkoumání. V tomto ohledu jsou klíčové parametry, jako je přesnost obrazu podpisu (jeho vizualizace), dostatečný počet detekovaných signálů v čase podepisování, rozlišení různých úrovní tlaku a precizní optická zpětná vazba v průběhu psaní.

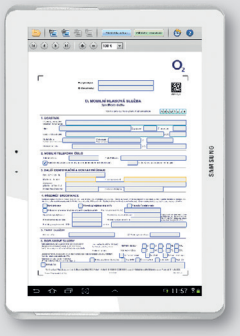
Výběr ovlivnilo také zamýšlené použití v různých prodejních kanálech a jejich stávající technické vybavení. U části

z nich bylo potřeba doplnit pouze jednoúčelové zařízení na snímání podpisu, u dalších jsme ale potřebovali komplexní zařízení schopné smlouvu nejen podepsat, ale také vyplnit a odeslat ke zpracování. Na zařízení jsme ve výsledku měli následující požadavky:

- Ergonomie – pocit při podpisu co nejvíce podobný podpisu na papír
- Displej – možnost zobrazení náhledu celé smlouvy a manipulace s ním (přiblížení, posun, stránkování), využití pro zobrazení marketingových materiálů (v barvě)
- Důvěryhodnost – sejmutí podpisu v kvalitě umožňující písmoznalecké zkoumání, porovnatelná kvalita podpisů pořízených na různých typech zařízení, okamžitá vizualizace podpisu na smlouvě v reálném čase
- Kompatibilita – možnost provozu na stávajícím technickém vybavení v jednotlivých prodejních kanálech (značkové prodejny, franšízy a externí obchodní zástupci)
- Mobilita – možnost vyplnění smlouvy, podpisu a pořízení kopie ID dokladů v terénu (mobilní prodejci)
- Cena – pořizovací náklady s ohledem na rozsah implementace a počet prodejních míst

Po zvážení všech kritérií a testování zařízení od různých výrobců jsme se rozhodli pro podpisovou podložku STU-520 od renomované společnosti Wacom a tablety Samsung Galaxy Note 10.1 založené na stejné snímací technologii.

Podložka STU-520 vyhovovala všem kritériím kromě velikosti displeje (pouze 5“), ale její výběr byl kompromisem mezi výkonem a cenou. Pro zvýšení komfortu pro zákazníky jsme všechna prodejní místa vybavili ještě otočnými držáky na LCD monitory. Zákazník si tedy může smlouvu zkontrolovat v plné velikosti a na podložce se pořizuje pouze vlastní podpis v kontextu zobrazené smlouvy.

Wacom STU-520	Špičková mobilita Barevný displej s úhlopříčkou 5” a rozlišením 800 × 480 pixelů Snímací technologie – elektromagnetická rezonance bránící nežádoucím chybným zadáním dotekem dlaně či prstů, 512 úrovní tlaku Vysoká odolnost proti poškrábání displeje Cenová dostupnost Doplněk k existujícím PC / notebookům	
Samsung GT-N8000	Špičková mobilita a ergonomie ovládání Přirozený pocit při podpisu – podpis přímo do těla dokumentu Velmi kvalitní displej 10.1" TFT s rozlišením 1280 × 800 pixelů Snímací technologie – aktivní wacom digitalizér, 1024 úrovní tlaku Aktivní stylus S Pen Použití u mobilních prodejců, kteří dosud neměli IT vybavení Potenciál využití pro další účely nad rámec vlastnoručního digitálního podpisu (prodejní, prezentační a komunikační platforma) Vyšší pořizovací náklady	

Tab. 1: Základní charakteristiky zvolených zařízení

DŘÍVE	DNES
1. Od zákazníka si vyžádáme občanský průkaz, který okopírujeme, naskenujeme a kopii pošleme k archivaci	1. Od zákazníka si vyžádáme občanský průkaz, který již pouze naskenujeme a v elektronické podobě odešleme k archivaci
2. Na základě požadavku sestavíme a vytiskneme mnohastránkovou smlouvu nebo objednávku	2. Objednávku produktů či služeb založíme výhradně elektronicky
3. Zákazník smlouvu ručně podepíše v několika vytištěných exemplářích	3. Zákazník smlouvu podepíše pouze jednou, a to výhradně elektronicky – pomocí speciální podpisové podložky nebo tabletu
4. Podepsané tištěné originály převedeme do elektronické podoby a odešleme je na back office, originály zároveň putují k archivaci	4. Podepsaný elektronický originál okamžitě odešleme ke zpracování na back office a k archivaci do DMS a O2 Důvěryhodného archivu
5. Na back office na základě naskenovaných dokumentů zpracujeme požadavek zákazníka	5. Na back office elektronické dokumenty jednoduše zpracují
6. Zákazník odchází se složkou plnou vytištěných dokumentů	**6. Zákazník odchází s prázdnýma rukama – dokumenty jsme mu automaticky doručili do e-mailu**

Tab. 2: Srovnání procesu podepisování a archivace smlouvy před nasazením řešení a po něm

E2E proces a přínosy

Nový proces s využitím elektronických dokumentů a vlastnoručního digitálního podpisu je výrazně jednodušší jak pro

zákazníky, tak pro uživatele / prodejce. Na typickém příkladu ze značkové prodejny si popišme, jak celá transakce probíhá:

- Zákazník se domluví s prodejcem na požadované službě
- Prodejce zkontroluje identitu zákazníka dle občanského průkazu a pořídí jeho sken (osobní údaje jsou anonymizované)
- Prodejce zadá objednávku v systému CRM a vygeneruje smlouvu v digitální podobě
- Smlouva se otevře v aplikaci SignoSoft a prodejce k ní jako přílohu vloží sken občanského průkazu
- Prodejce natočí LCD monitor k zákazníkovi a zkontroluje s ním parametry služby a kontaktní údaje (zejména e-mail a mobilní telefonní číslo, které jsou nezbytné pro doručení smlouvy)
- Po odsouhlasení vloží prodejce i zákazník svůj vlastnoruční digitální podpis
- Prodejce následně v aplikaci potvrzuje dokončení podpisu a odeslání k dalšímu zpracování:
  - Uložení v DMS
  - Odeslání zákazníkovi
  - Archivace v O2 Důvěryhodném archivu
  - Pokud to daná transakce vyžaduje, startuje se automatické zpracovatelské workflow
- Pokud si to zákazník vyžádá, prodejce mu před odesláním může vytisknout kopii smlouvy

Oproti původnímu procesu si zákazník z prodejny neodnáší spoustu vytištěných dokumentů, ale vše má do několika málo minut k dispozici ve své e-mailové schránce (viz Tab. 2). V budoucnu chceme zákazníkům zpřístupnit smlouvy také na portále Moje O2, což jim zajistí pohodlnou dostupnost kdykoli, stejně jako je tomu již dnes u elektronického vyúčtování.

Pro prodejce to znamená eliminaci řady administrativních činností, jako je skenování smlouvy a odesílání zásilky s originálem – vše pro ně končí stiskem tlačítka „Odeslat“ po podpisu smlouvy. Smlouva je pak během několika minut dostupná pro náhled v CRM všem prodejním místům. Ještě důležitější je přínos metadat, která každá nativně digitální smlouva obsahuje. Jejich dekódování a zpracování v návazných systémech je vždy 100% správné a umožňuje nám automatizovat workflow pro zpracování dokumentů. Smlouva se tak dostane k řešiteli na back office mnohem dříve než v případě digitalizovaných papírových smluv.

Přínosů je ale mnohem více a dají se shrnout do následujících kategorií:

- Rychlost – rychlejší podpis na prodejních místech, výrazné zkrácení doby mezi podpisem smlouvy a aktivací služby (externí prodejní kanály)
- Bezpečnost – výrazně obtížnější napodobení oproti klasickému podpisu, zabezpečení řešení na několika úrovních (přístupová oprávnění, autentizace prodejce před odesláním, asymetrická kryptografie, HASH otisky dokumentu, O2 Důvěryhodný archiv, Security Gateway, smlouva v e-mailu je chráněna heslem atd.)
- Pohodlí – vlastní způsob potvrzení smlouvy je stále stejný a přirozený – vlastnoručním podpisem, mění se pouze způsob sejmutí podpisu, žádné požadavky / bariéry pro zákazníka
- Dostupnost – smlouvu obdrží zákazník během několika málo minut e-mailem a heslo v SMS, v budoucnu bude mít smlouvu kdykoli přístupnou na portále Moje O2
- Efektivita – snížení nákladů na tisk (papír, toner, údržba tiskáren), snížení nákladů na přepravu, digitalizaci a archivaci, eliminace chyb při ručním zpracování a digitalizaci, automatické workflow pro zpracování dokumentů

Reálné zkušenosti a další rozvoj

Pilotní provoz

V pilotním provozu jsme si chtěli v reálných podmínkách ověřit zejména to, jak na nový způsob uzavření smlouvy budou reagovat zákazníci. Dále pak prověřit spolehlivost řešení, doladit procesy a získat reálná data pro znalecké posudky. Pilot jsme zahájili v listopadu 2013 na osmi značkových prodejnách a čtyřech franšízách napříč republikou tak, aby byly zastoupeny všechny typy prodejen – od malých prodejen až po Experience Center v pražském OC Chodov. Už první zkušenosti po několika dnech ukázaly, že téměř 100 % zákazníků nemá s vlastnoručním digitálním podpisem žádný problém a ani v ostatních sledovaných oblastech jsme nezaznamenali zásadní problém. Důležitá byla i pozitivní zpětná vazba od samotných prodejců, kteří oceňovali celkové zjednodušení práce s dokumenty a byli tak přirozeně motivováni nové řešení v maximální možné míře využívat.

Na základě úspěchu pilotu na značkových prodejnách jsme ho v prosinci 2013 rozšířili na vybrané mobilní prodejce a od února 2014 na zástupce externích prodejních kanálů. Tyto prodejní kanály mají svá specifika, která se promítla i ve výsledcích pilotu – u prodejce s tabletem zákazníci mnohem více vnímají jeho profesionalitu a důvěryhodnost, na druhou stranu je v cílové skupině zákazníků mnohem více těch, kteří nepoužívají e-mail nebo vyžadují papírovou variantu smlouvy (25 % vs. 10 % u prodejen). Celkově je ale i tento pilot úspěšný a pracujeme na tom, aby se podíl zákazníků s papírovou smlouvou do budoucna zmenšoval.

Komerční provoz

Vzhledem k pozitivnímu průběhu pilotu na značkových prodejnách jsme ho mohli po necelých třech měsících ukončit a spustit plný komerční provoz. Od 6. února 2014 je vlastnoruční digitální podpis nasazen na všech 71 pobočkách, což představuje zhruba 450 prodejních míst. V květnu 2014 následovaly zbývající prodejní kanály. Počet vybavených prodejních míst se blíží tisícovce. Celkem již bylo digitálně podepsáno přes 200 tisíc dokumentů a projekt začíná dodávat očekávané benefity:

- Zákazníkům jsme mohli věnovat 5 000 hodin navíc díky časové úspoře
- Ušetřili jsme již téměř milion listů papíru
- Řešení požadavků pro zákazníky se zrychlilo v průměru o 1 den a velká část požadavků je tak vyřešena v den podání

Další rozvoj

Tím ale naše aktivity v této oblasti nekončí. Podpisové podložky ve vybraných kanálech postupně měníme za plnohodnotné tablety s podporou LTE, které umožní jejich další využití nad rámec vlastnoručního digitálního podpisu (CRM a marketingová podpora). Dále plánujeme např. implementaci MDM platformy, která zjednoduší a zcentralizuje správu tabletů nebo ukládání smluv pro zákazníky na portále Moje O2. Zvažujeme také implementaci čteček identifikačních dokladů, abychom eliminovali jejich skenování, které přetrvává i v novém řešení.

Ultimátním cílem je 100% využití vlastnoručního digitálního podpisu při uzavírání smluvního vztahu se zákazníky. Nově připravované produkty už budou podporovat pouze tuto variantu.

Doporučení pro úspěšnou implementaci digitálního podpisu na základě zkušeností v O2:

- Nechat si nainstalovat demo řešení a zapůjčit si vzorky podpisových zařízení k otestování v reálných podmínkách prodejních míst
- V časovém harmonogramu dostatečně zohlednit výběrové řízení a dodržet fázování IT vývoje (prevence revizí již dokončených částí IT analýzy / architektury / designu)
- Neimplementovat digitální podpis izolovaně, je vhodné zároveň optimalizovat i navazující procesy zpracování dokumentů (využití synergií, vyšší benefity)
- Využít v maximální míře integraci se stávajícími systémy a nebudovat duplicitní byznys logiku v novém řešení, pokud to není nezbytně nutné (např. validace povinných polí a formátů hodnot ve zdrojovém CRM systému – minimalizace dodatečných validací v novém řešení)
- V případě implementace celého řešení najednou zajistit synchronizaci nasazení úprav ve všech přímo i nepřímo dotčených systémech (pro zajištění platnosti smlouvy musí fungovat celý proces end-to-end, výpadek jediné části tak může ohrozit nasazení celého řešení)
- S ohledem na komplexitu již při úvodní analýze a návrhu řešení zvažovat rozdělení na více samostatných logických celků (flexibilita s ohledem na zdroje a kapacity IT release, možnost fázování nasazení a komerčního spouštění)
- Zapojení zástupců prodejních kanálů, tj. budoucích uživatelů, do klíčových fází projektu (motivace, snazší roll-out projektu, rychlejší náběh benefitů)
- Od samého začátku zapojit do projektu právní a bezpečnostní experty (změny základních předpokladů ohledně legislativy a principů zabezpečení v pokročilých fázích projektu mají významný negativní dopad na termíny a náklady)
- Spolupracovat se soudními znalci (bezpečnost IT systémů, písmoznalectví) již v průběhu projektu a konzultovat s nimi klíčové právně-bezpečnostní otázky (korekce projektu a budování know-how znalců potřebné pro vytvoření znaleckého posudku po jeho nasazení)
- S výběrem řešení a dodavatele začít včas a využít možnosti vyhlásit RFI – Request for Information (zajištění dostatečných informací pro rozhodování a urychlení procesu výběru)

Závěr

Cílů projektu, jimiž bylo zefektivnit interní procesy i zrychlení a zjednodušení samotných zákaznických požadavků, bylo dosaženo. Potvrdilo se, že technologie vlastnoručního digitálního (biometrického) podpisu je dostatečně intuitivní pro všechny cílové skupiny.

V případové studii byl tento projekt popsán od zahájení přípravy (stanovení cílů, vymezení scope atd.) přes řešení právní problematiky, výběr dodavatele, návrh řešení a jeho vývoj, nastavení procesů, pilotní projekt po rozvoj řešení. Určitou pozornost jsme věnovali také vysvětlení principů vlastnoručního digitálního podpisu.

Aleš Bernášek
ales.bernasek@o2.cz

Ing. Aleš Bernášek

Vystudoval PEF ČZU, obor Provoz a ekonomika. Od roku 2002 působí v O2 na pozicích souvisejících s řízením kvality, zákaznickou zkušeností, procesním a projektovým řízením.