Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Implementace dynamického biometrického podpisu

Bc. Blažek Marek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Marek Blažek

Veřejná správa a regionální rozvoj

Název práce

Implementace dynamického biometrického podpisu

Název anglicky

Implementation of dynamic biometric signature

Cíle práce

V diplomové práci bude zkoumána implementace dynamického biometrického podpisu v subjektu a úspora při jeho zavedení pro daný subjekt.

Metodika

V teoretické části bude studována odborná literatura, dostupné dokumenty a záznamy. V praktické části bude podán přehled současného stavu implementace dynamického biometrického podpisu a technologií spojených s jeho zavedením.

Doporučený rozsah práce

60 – 80 stran

Doporučené zdroje informací

POHLMANN, Norbert, Helmut REIMER a Wolfgang SCHNEIDER. ISSE 2010, securing electronic business processes: highlights of the Information Security Solutions Europe 2010 conference. 1st. ed. Wiesbaden: Vieweg Teubner, c2011, ix, 416 p. ISBN 978-383-4814-388

Smejkal Vladimír, Mates Pavel: E-government v České republice. Právní a technologické aspekty. 2. podstatně přepracované a rozšířené vydání, Vydavatelství: Leges, 11/2012,ISBN: 978-80-87576-36-6

Zákon č. 499/2004 Sb. o archivnictví a spisové službě

Zákon č.227/2000 Sb., o elektronickém podpisu

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Mgr. Ing. Vladimír Očenášek

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 05. 03. 2015

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Implementace dynamického biometrického podpisu" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne datum odevzdání _____

Poděkování

Rád bych touto cestou poděkoval Mgr. Ing. Vladimíru Očenáškovi za jeho cenné rady a trpělivosti při vedení mé diplomové práce. Současně mé báječné rodině za podporu a obrovskou trpělivost při náročném studiu.

Implementace dynamického biometrického podpisu

Implementation of dynamic biometric signature

Anotace

Cílem diplomové práce je seznámit se s možností, jak efektivně dokáže přispět zavedením nové technologie, dynamického biometrického podpisu, k progresivnímu snížení nákladů a zároveň zvýšení pružnosti fungování společnosti v obchodním světě.
Diplomová práce má dvě části. Teoretická část obsahuje vymezení od elektronického podpisu, přes princip až k dynamickému biometrickému podpisu za podpory zakotvení v právních pramenech, které byly čerpány z různých odborných publikací a právních opor. Praktická část se zabývá kladením a zodpovězením otázek, jak snížit náklady a zvýšit úspory po implementaci dynamického biometrického podpisu. Následně bude ukázáno navrhované řešení a vyčíslení úspor pro jednotlivé procesy ve společnosti po dopadu zavedení dynamického biometrického podpisu. V samotném závěru si ukážeme nové řešení za využití dynamického biometrického podpisu v České republice.

Anotation

The aim of my diploma paper is to raise awareness concerning the possibility of progressive decrease of costs and increase of more flexible everyday business routine by supporting of new technology - dynamic biometric signature introduction.
My diploma paper is divided into two parts. The first part is a theoretical part dealing with terminology concerning biometrical signature area, background of this issue on the basis of various particularly legal national acts referred in number of publications and expert articles. The other part is a practical part. This part is focused on questioning of right questions and answering them. All the questions are about decreasing of costs and increasing of savings after implementation of dynamic biometric signature. There are also examples of possible solutions and figures concerning savings for various steps and processes in companies after implementation of dynamic biometric signature in the practical part.
In the last part readers can find new solutions in using of dynamic biometric signature in the Czech Republic.

Klíčová slova:

dynamický biometrický podpis
biometrické prvky
digitální dokument
stávající proces uzavření smlouvy
náklady spojené s papírovými formuláři
proces s využitím DBP
hardware vybavení
SW a validace uživatele
archivace dokumentů
přímé úspory
benefity

Keywords:
dynamic biometric signature
biometrics elements
digital document
current process of contracting
costs associated with paper forms
process using DBS
hardware equipment
SW validation of user
archiving of documents
direct savings
benefits

Obsah

1 Úvod

Nacházíme se v 21. století, které sebou nese vlnu stupňujících se inovací ve všech směrech našeho hektického života ovládaného technologiemi. Vždyť už i lednička na nás dokáže mluvit, upozorňovat nás na stav potravin uvnitř. Musíme si pomalu uvědomovat, že pokud budeme chtít udržet krok, nezbývá nám nic jiného, něž přijmout onen valící se pokrok. Naše děti dokáží ovládat iPady, hrát a kreslit si na nich. To je ten krůček k technologiím, které jsme nuceni využívat přímo či nepřímo při komunikaci s megalomanskými společnostmi. Ty to společnosti, aby držely krok se světem, zajišťovaly větší bezpečnost svých transakcí, snižovaly své náklady, využívají různé nástroje. Jedním z nich je i dynamický elektronický podpis. Každá technologie má své pozitivní i negativní dopady ať je to ve formě snižování nákladů na jedné straně či snižování pracovních míst na straně druhé.

Toto téma diplomové práce jsem si vybral, protože mě zajímá tato nová technologie prorůstající do obchodních společností v České republice. Chci ji přiblížit širší veřejnosti a současně, jak je třeba možné přispět k ochraně životního prostředí cestou snížení spotřeby kancelářského papíru a s tím souvisejících oblastí.

Diplomová práce je rozdělena na teoretickou a praktickou část. Teoretická část bude obsahovat popis, rozdělení, vývoje a seznámení se s elektronickými dokumenty. Následně i popsání a seznámení se s dynamickým biometrickým podpisem, jeho znaleckým zkoumáním a právním zakotvením v legislativě České republiky. V praktické části se budeme zabývat samotnou implementací dynamického biometrického podpisu, poukázání na jeho samotný přínos cestou úspor nákladů. Ukážeme si i samotnou implementaci ve společnostech, které testují danou technologii a jejich zjištěné závěry. V samotném závěru diplomové práce se pokusíme nalézt návrhy a doporučení do budoucnosti v pokračování této zajímavé cestu si nacházející technologii ke koncovým uživatelům.

2 Cíl práce a metodika

2.1 Cíl práce

Podpis je nedílnou součástí lidstva a jak samo lidstvo i on procházel a prochází vývojem, vyvíjí se, reaguje na potřeby doby i rozšiřujících se technologií. Můžeme říct, že podpis „žije“. Člověk je ten, kdo jej změnil z tahu uhlíku z popela na zdi jeskyně, až po tah perem po destičce, která jej převede, znázorní na obrazovce třeba iPodu. Proto bych ve své diplomové práci zvolil za hlavní cíl přiblížit problematiku dynamického biometrického podpisu, zavedení či implementaci do života firmy. Následně poukázal na neoddělitelnost od růstu společnosti, které chtějí využívat nové technologie přinášející úspory a zvyšují legitimitu firmy a to nejen v České republice. Cílem této diplomové práce je ukázat, popsat dynamický biometrický podpis, jeho proces při implementaci, využití, vyčíslit náklady na úsporu v podniku a v neposlední řadě ukázat provázanost technologie s lidským životem a jeho nutností se stále učit a přizpůsobovat pokroku.
V diplomové práci budou použity metody podpisu, analýzy dat, schémata. Pro zpracování diplomové práce jsou využity odborné literatury, konzultace se znalci v oboru písmoznalectví, soudních znalců nebo vlastní zkušenost. Je samozřejmě využito i mnoho elektronických zdrojů, které poskytují společnosti zabývající se řešenou problematikou.

2.2 Metodika práce

Mnou zvolená diplomová práce bude zaměřena na implementaci dynamického biometrického podpisu, osvětlení historického vývoje podpisu, jeho znalecké zkoumání, popsání, vysvětlení souvisejících problematik a analýzu přehledu současného stavu využívání dynamického biometrického podpisu v České republice a sousedních státu. V teoretické části bude popsán a definován podpis, jako takový a jeho vývoj, jeho právní opora a instituce zabývající se níže uvedenou problematikou. Analytická část bude věnována popsáním před a po zavedení dynamického biometrického podpisu s vyjádřením úspor v nákladech. Tato část diplomové práce bude vypracována na základě podkladů získaných od společností, které již implementovaly dynamický biometrický podpis či jej zavádějí ve zkušebním provozu s daným očekáváním. Nadále budu čerpat z dat poskytnutými společnostmi, které zavádí dynamický biometrický podpis tzv. na „míru“ dle

požadavků zákazníka. Výzkum bude směřován na analýzu implementace dynamického biometrického podpisu a uvedení ukazatelů úspor ve společnosti. V závěru práce bude ukázán nový trend směřující k budoucnosti využití dynamického podpisu a ulehčení, tak práce s dokumenty, ale i negativní dopady pro společnost.

3 Literární rešerše

V České republice patří mezi přední odborníky, kteří se zabývají všemi existujícími právními a technologickými aspekty informačních systémů veřejné správy a dalšími složkami e-governmentu . Současně se zabývají a zároveň působí v Legislativní radě vlády, jsou autory návrhů zákonů a žádanými přednášejícími. Jedná se o JUDr. Pavla Matese, CSc. a Prof. Ing. Vladimíra Smejkala, CSc. Jsou autory a spoluautory řady odborných knih, časopisů, článků, v kterých jsou definovány základní pojmy z oblasti e-governmentu a informačních systémů, s důrazem na informační systémy veřejné správy. V jejich příspěvcích je popsáno mnoho problematik dotýkajících se i ku příkladu - základních registrů. Samostatně je zpracována problematika e-justice jako jednoho ze základních kamenů e-governmentu. Vzhledem k podílu autorů na příslušných předpisech jsou podrobně rozebrány právní předpisy o elektronickém podpisu a o elektronických úkonech a autorizované konverzi dokumentů (o datových schránkách), jakož i technologické aspekty těchto nástrojů.

Velkou pozornost věnují autoři otázkám elektronických dokumentů včetně možností jejich autentizace prostřednictvím elektronického podpisu, elektronické značky a časového razítka. Ve svých odborných knihách popisují i novinku - dynamický biometrický podpis, který bude předmětem diplomové práce. Vzhledem k rostoucímu významu elektronické komunikace je podrobně diskutováno také dokazování, znalectví v prostředí elektronických dokumentů.

Prof. Ing. Vladimír Smejkal, CSc. již přes dvacet let vykonává činnost soudního znalce, a to v závažných ekonomických, kriminalistických a autorskoprávních otázkách. V roce 1986 byl ministrem spravedlnosti ČSR jmenován soudním znalcem v oborech ekonomika a kybernetika, v roce 1995 byl jmenován ministrem spravedlnosti ČR soudním znalcem v dalších oborech, a to kriminalistika – ochrana dat a autorské právo.

JUDr. Pavel Mates CSc. se specializuje na správní právo se zaměřením na oblast ochrany

osobních údajů, správní právo trestní a e-government. V letech 1972-1994 asistent, odborný asistent, docent (1988) Právnická fakulta Masarykovy University v Brně. 1992 soudce Ústavního soudu Československé federativní republiky až do jejího zániku. 1993 Úřad pro legislativu a veřejnou správu. 1994 vedoucí katedry veřejné správy Policejní akademie České republiky. Od roku 1995 katedra veřejné správy a regionálního rozvoje Národohospodářské fakulty Vysoké školy ekonomické v Praze, nyní pověřen vedením katedry práva. Od roku 2000 přednáší také správní právo na Právnické fakultě Západočeské University v Plzni. Je předseda rozkladové komise Úřadu pro ochranu osobních údajů České republiky. Člen komise pro advokátní zkoušky České advokátní komory. Člen redakční rady časopisů Právní zpravodaj (C. H. Beck) a Právněhistorické studie. Výše jmenovaní odborníci se zasloužili o zvýšení informační gramotnosti, elektronizaci státní správy a to v oblasti e-justice (připravované e-sbírce, e-legislativě). Samotný projekt e-justice znamenal obrovský posun k přístupu informací o činnosti soudů a státních zastupitelství, což je dnes již pro mnohé samozřejmostí. Projekt znamenal i návaznost na legislativu v oblasti ověřování pravosti dokumentů, jak elektronických, tak samotných elektronických podpisů. Tato zajímavá oblast je součástí zkoumání v diplomové práci s ukázkou technologie ověřování pravosti dynamických biometrických podpisů.

Analýza využití dynamických biometrických podpisů v mé diplomové práci bude probíhat na základě zpracování dostupných údajů nebo internetových zdrojů a na samotný závěr bude uvedeno hodnocení a zjištění stávajícího stavu.

Dynamických biometrický podpis jsem se rozhodl analyzovat všeobecně, nezaměřovat se na složitou technologii kryptování, která by spíše spadala do oblasti složitých informačních technologií. Budu se zajímat o implementaci této technologie do společnosti, otázky kladené při zvažování před samotným zavedením a ukázky úspor nákladů. V neposlední řadě budou i dokladovány výstupy u již implementované technologie v různých všeobecně známých společnostech v České republice. Závěrem budou uvedeny postřehy a poznatky.

4 Přehled řešené problematiky

4.1 Základní rozdělení digitálních dokumentů

Digitální dokumenty prosté a rozšířené

Digitální dokumenty jsou v zásadě ve dvou variantách:

- prosté dokumenty, tj. bez použití jakýchkoliv nástrojů, umožňujících identifikaci a autentizaci podepsané osoby a/nebo jiných atributů (bez elektronického podpisu, značky a bez časových razítek),
- dokumenty s rozšířenými vlastnostmi, umožňující je pomocí různých, převážně kryptografických nástrojů opatřit atributem (-y) určujícím (-i) některé charakteristiky souvisejících se vznikem, případně modifikací dokumentů (elektronicky podepsané nebo označené dokumenty včetně dokumentů opatřených časovým razítkem).

Dokumenty bez elektronického podpisu či razítka

Jedná se o dokumenty nesoucí informace, u kterých není významný ani podpis ani přesný čas jejich vytvoření. Archiv, systém spisové služby atd. sice může tyto dokumenty doplnit elektronickým podpisem, značkou nebo časovým razítkem jako indicii jejich existence v konkrétním čase, ale tím nezískáme žádné další informace, natož jistotu, kdo a kdy dokument vytvořil či jej poslal. Typickým příkladem takových to dokumentů jsou e-maily, které obsahují sice údaj o datu a čase v hlavičce mailu, ale tyto údaje lze libovolně modifikovat či podvrhnout, takže například znalecké posouzení toho, kdo, kdy a komu odeslal určitý e-mail, je bez opatření e-mailu dalšími atributy (podpis, značka, razítko), nemožné.

Dokumenty s elektronickými podpisy, značkami a časovými razítky

Pro udržení síly elektronických podpisů a časových razítek je nutné zajistit možnost ověření jejich pravosti v době podpisu či „orazítkování“, tedy mít k dispozici certifikát, který platil v době provedení uvedeného úkonu. To se řeší různými způsoby – od tzv.

institucionálního ověření, nebo tím, že podpisy a razítka jsou obnovována, res. ověřována dalšími podpisy a/nebo razítky. Důvodem je skutečnost, že dokument může být z archivu vyzvednut k úřednímu jednání. K tomu vyžaduje indicie, potvrzující pravost dokumentu.

Skutečnost, že dokument může být vyzvednut z archívu a předložen jako důkazní materiál je časově závislá. U některých dokumentů se tak může dít jen řádově léta, u jiných po velmi dlouhou dobu. Konkrétně autenticita faktury je důležitá pouze po dobu, po kterou může být konkrétní osoba obviněna z daňového podvodu nebo správního deliktu. Kdežto dokumenty o nabytí nebo vyvlastnění majetku mohou být důležité i po sto letech.

Takže obnovovat elektronické podpisy a časová razítka, aby neztratily svou sílu, má smysl pouze dobu, po kterou mohou být využity jako dokumenty. Poté sice může být vyžadována jejich archivace, ale jako historické dědictví, tj. pro účely historického, resp. Obecně badatelského výzkumu. Myslíme si, že pak již není potřeba obnovovat podpisy a razítka – dikce § 69a Archivního Zákona tomu odpovídá.

U digitálně podepisovaných (resp. časově orazítkovaných) dokumentů je tedy třeba v archivačním a skartačním řádu stanovit nejen dobu jejich archivace, ale i dobu obnovování razítek a podpisů, nebo nastavit technicko-organizační opatření taková, aby bylo možno prokázat i bez výše uvedeného obnovování pravost dokumentů – např. prostřednictvím zmíněného souběžného záznamu na mikrofiše, prováděnému při skenování.

Je třeba zdůraznit, že zákon o archivnictví a spisové službě výslovně počítá s možností, že dokumenty budou primárně pořizovány v elektronické podobě a v tomto směru obsahuje též úpravu, jak s nimi má být disponováno. Co se týká jejich ukládání.

4.2 Elektronický podpis a jeho využití

4.2.1 K čemu je elektronický podpis

Elektronický podpis se dá využít všude tam, kde je dnes nutný vlastnoruční podpis. Prakticky všechny dokumenty lze převést z papírové (listinné) podoby na dokumenty elektronické (digitální) a všechny podpisy je možné vytvořit v jejich elektronické, ovšem digitální formě. Podepisovat i ověřovat podpisy lze takto nesrovnatelně rychleji a efektivněji; je možné podepsat dokonce i to, co lze ručně opatřit podpisem velmi těžko, ale

co je digitalizované – obsah jakéhokoliv datového souboru, obsahujícího fotografie, audiovizuální záznamy atd.

4.2.2 Elektronický versus vlastní podpis

Elektronický podpis není tím, zač jej určitou dobu vydávali novináři, tedy nějakým kódem, který uživatel „vyfasuje“ někde – na úřadu nebo i někoho, kdo podniká v této oblasti, aby potom uživatel tuto skupinu číslic a písmen připojoval ke každému elektronickému dokumentu coby svůj podpis.

Elektronický podpis je – stejně jako „ruční“ (vlastnoruční) podpis – výsledkem nějakého procesu, vyplývajícího z rozhodnutí podepisující osoby, jehož úkolem je stvrdit vůli této osoby, případně její identitu.

Vlastnoruční podpis je výsledkem uplatnění návyku psaní, získaného v podobě individuálního a relativně stálého písemného projevu člověka. Vznik individuálnosti písma je důsledkem vytvoření dynamického stereotypu psaní, tedy vypracování složitějšího systému podmíněných reflexů, které jsou závislé na stupni procvičování. Při vytvoření konkrétního písemného projevu – tedy např. podpisu – se uplatňují, ale i aktuální vnější podmínky, za kterých psaní probíhá a v jejichž důsledku může být získaný dynamický stereotyp narušen.

Zkoumání pravosti písma (podpisu), které je zaměřeno na grafickou stránku směřující k identifikaci pisatele, je prováděno pomocí různých metod, přičemž za základní metodu je považována metoda pozorování, dále pak to jsou metody analytická, syntetická, komparační a grafometrická.[1] Jak u podepisování, tak u zkoumání pravosti (ověřování) podpisu jde tedy o procesy převážně subjektivního charakteru, v nichž se promítají obecné a individuální vlastnosti zúčastněných osob. Tyto vlastnosti se dnes využijí i při ověřování pravosti tzv. dynamického biometrického podpisu, který kombinuje vlastnosti jak grafického, tak elektronického podpisu – viz dále.

Elektronický podpis na bázi kryptografických metod je naproti tomu od okamžiku „odstartování“ podepisování, tedy od okamžiku učinění rozhodnutí podepisující osoby až po okamžik ověření pravosti podpisu, objektivním výsledkem technologického, na zvláštnostech zúčastněných osob či situace nezávislého procesu. Je výsledkem aplikace

[1] MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. 2., přepracované a dopl. vyd. Praha: C. H. Beck, 2004, 606 s. ISBN 80-717-9878-9.

určité, pro podepisující osobu charakteristické vlastnosti (tajné informace) na podepisovaný text; jedná se tedy – na rozdíl od ručního podpisu – o podpis proměnný, tedy daleko obtížněji vysledovatelný či naučitelný (což vyplývá z jeho kryptografických principů).

Jak uvidíme dále, možnost zneužití elektronického podpisu není větší než u podpisu ručního, zatímco možnost ověření pravosti elektronického podpisu je daleko vyšší.

Podpis slouží k doložení skutečnosti, že určitá osoba projevila svoji vůli, případně že se v určitou dobu nacházela na určitém místě, popř. že stvrzuje platnost určitého dokumentu. Jak říká americké právo, podpisem je jakýkoliv znak, symbol nebo kresba, kterým osoba stvrzuje platnost dokumentu. Podle našeho základního právního předpisu, občanského zákoníku, § 40 odst. 3, písemný právní úkon je platný, je-li podepsán jednající osobou, přičemž se tímto podpisem zásadně rozumí podpis vlastnoruční; podpisem může být nahrazen mechanickými prostředky pouze v případech, kdy je to obvyklé. Jak říká Občanský zákoník dále v odst. 4, písemná forma je zachována, je-li právní úkon učiněn telegrafický, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.

V obou případech, tedy u dokumentu papírového nebo elektronického, nám jde o totéž: zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila, tedy a) zaznamenání informace písemně, tedy psaním, na nějakém hmotném nosiči trvalým způsobem, umožňující tuto informaci předat, získat, vykázat se jí apod. i s časovým odstupem, a to případně jinou osobou, nežli autorem zápisu, b) identifikace s tím související autentizace neboli ověřování osoby, jíž se informace týká (o jejíž právní úkon jde).

4.2.3 Identifikace a autentizace

Identifikací lze stručně definovat jako zajištění identity (totožnosti) subjektu, které se provádí porovnáním osobních údajů nebo projevů osobní povahy fyzické osoby s jinými, které jsou obvykle zachyceny na nějakém nosiči, zatímco autentizaci jako ověření, že subjekt je tím, za koho se prostřednictvím této identity vydává. V praxi se identifikace na písemném dokumentu provádí nejčastěji uvedením jména, příjmení, adresy, případně jiných údajů o dotčené osobě. Autentizace, tj. ověření, že dokument skutečně podepsala

uvedená osoba, se provádí podpisem, podpisem před svědky, ověřením totožnosti pověřenou osobou; nejjistější je zatím stále legalizace formou úředně ověřeného podpisu nebo notářského zápisu.[2] Pravost podpisu na papíru je v případě sporu o obsahu dokumentu prokazována následně znalecky, tj. znalcem z oboru písmoznalectví.

Poznáváme v této souvislosti, že ani úředně ověřený podpis s využitím odcizeného či padělaného občanského průkazu, případně dosažený v důsledku trestního činu úřední osoby není absolutně bezpečný, stejně jako se nelze stoprocentně spolehnout na to, že obsah listiny po jejím ověření notářem nebyl následně změněn (padělán). Z těchto důvodů je třeba absolutizování papírových dokumentů a nezlomnou víru v jejich nedotknutelnost odmítnout. Úřední ověření podpisu na listinném dokumentu zakládá pouze domněnku autentizace podepsané osoby, a to domněnku vyvratitelnou.

Autentizace (ověření pravosti proklamované identity), případně autorizace (přiřazení služeb ICT autentizované osobě) v oblasti informačních systémů a elektronických dokumentů je v současnosti velmi aktuálním problémem, který se potýká s několika protichůdnými požadavky: na uživatelskou jednoduchost, rychlost, ověřování, bezpečnost, věrohodnost a náklady.

Použité metody autentizace by měly splňovat požadavky na variabilitu jak z pohledu použitých technologií a systémů, tak i z hlediska samostatných uživatelů. Navržená řešení musí navíc vycházet z práva jednotlivých stran na komunikaci mezi oprávněnými účastníky a v případě řádného kontraktu či provedení transakce.

Informační technologie v případě autentizace uživatelů musí zajistit stejné podmínky jako při klasicky realizovaných činnostech, tzn. zajistit výměnu dat mezi oprávněnými uživateli při zajištění neodmítnutelnosti provedených činností. V případě osobního styku, tj. na obou stranách se vyskytuje člověk, který je s protistranou v přímém, fyzickém kontaktu, je identifikace a autentizace postavena na principu rozeznání entity (autentizované osoby) posuzovatelem. Tento kognitivní a rozhodovací proces je sice jednoduchý, rychlý, vyplývajícím ze subjektivního pojetí celého procesu.

Při osobním styku v případě, kdy má dojít k autentizaci na základě jiné vlastnosti, nežli osobní známosti, je bezpečnost autentizačního procesu přímo úměrná bezpečnosti použité metody. Zatímco ověřování podpisů podle podpisových vzorů je všeobecně považované za

[2] Viz §62 a násl. Zák. č. 358/1992 Sb., o notářích a jejich činností (notářský řád), ve znění pozdějších přepisů.

metodu, poskytující velmi malé záruky, rizika autentizace na bázi osobních dokladů jsou přímo úměrná kvalitě práce autentizující osoby a padělatelnosti dokladů.

Při komunikaci na dálku, stejně jako v případě komunikace člověk/stroj (či stroj/stroj) je situace ještě složitější, protože možnosti podvrhu identity jsou daleko vyšší. V případě živé hlasové komunikace (telefonní bankovnictví) je míra rizika velmi diverzifikována – od vysokého v případě identifikace opakujícím se heslem či jejich malou množinou (číslice z rodného čísla), až po zanedbatelné (při použití tabulky jednorázových hesel či autentizaci kalkulačky). Při autentizaci pomocí technologických nástrojů je riziko obvykle střední až vysoké, přičemž je funkcí nejen vlastností metody či produktu, ale i chováním uživatele a vlastnosti prostředí, v němž je autentizace prováděna.

Při distanční autentizaci a autorizaci by měly být dodrženy následující předpoklady:

- technologicky neutrální řešení elektronických operací,
- politiky, které se vztahují k řešení autentizace, by měly být odlišné od politik týkajících se zajištění bezpečnosti dat,
- navržené řešení musí být škálové a mělo by umožnit případné rozšíření bezpečnostních modelů,
- navržené řešení by mělo respektovat požadavky obecně závazných právních předpisů i interních dokumentů,
- navržené řešení musí být pro uživatele jednoduše použitelné a neklást vysoké finanční požadavky na kteroukoliv ze stran.

Při autentizaci subjektu dochází k ověření jeho identity na základě:

- vlastnictví - magnetická nebo čipová karty, autentizační kalkulačka,
- znalosti - heslo, PIN, tajný klíč;
- charakteristiky - biometrické informace.

Úspěch do jisté míry závisí na dobře propracovaném procesu využití těchto parametrů. V současné době se musíme orientovat na silnou či více parametrovou autentizaci, kdy je řešení postaveno na kombinaci 2, popř. 3 autentizačních parametrů.

Trojfaktorová autentizace pracující s biometrickými informacemi do určité míry eliminuje základní slabiny systémů s parametrem postaveným na heslech či PIN, kdy:

- při využití PIN nebo hesla uživatelé mohou neúmyslně ohrozit privátní údaje tím, že nechají ID a PIN bez dozoru,
- uživatelé s více hesly si je většinou poznamenávají a ukládají na nezabezpečených místech, případně používají tatáž hesla v různých systémech,
- čipové karty a tokeny mohou být odcizeny,
- uživatelé mají možnost diskreditovat jak hesla, tak i autentizační zařízení.

Ale ani použití biometrických informací není všespasitelnou cestou. Jednak se zvyšuje pravděpodobnost chybného vyhodnocení (nepřijetí správného rozhodnutí nebo přijetí chybného rozhodnutí, tj. odmítnutí pravé osoby nebo akceptace podvržené osoby), jednak i zde již existuje riziko falšování biometrických informací (podvržení otisku prstu, snímku duhovky apod.) Při vzdáleném přístupu se útok může uskutečnit kdekoliv na trase od autentizované osoby k autentizačnímu místu.

Útok může směřovat na:

- nástroj pro autentizaci (kartu – magnetický proužek, čip, počítač, bankomat či platební terminál, snímač otisků prstů apod.),
- prostředí, v němž se nachází autentizovaná osoba (počítač obsahující spyware, modifikovaný bankomat),
- prostředí sloužící pro přenos dat (útok na protokol atd.),
- autentizační místo (podvržení dat v procesu autentizace – změna údajů v autentizační databázi, modifikace software),
- uživatele samotného (a jeho zmatení, aby se přihlásil do systému útočníka, ne do skutečného, např. v případě phishingu nebo při tzv. sociálním inženýrstvím, spočívající v manipulaci lidí za účelem provedení určité akce nebo získání určité informace).

V rámci autentizačního místa je samozřejmě možné „posunout“ vlastní útok až do fáze autorizace, kdy správně autentizovaná, tj. oprávněná osoba, získá neadekvátní práva – např. k provádění finančních transakcí.

Při návrhu autentizace uživatele, kdy jsou autentizační údaje předávány prostřednictvím nezabezpečeného komunikačního prostředí např. Internetu, se také používají autentizační protokoly typu dotaz – odpověď, které jsou v souvislosti s používáním jednorázových hesel považovány za značně bezpečné.

4.2.4 Identifikace a autentizace s využitím elektronického podpisu

V případě, že je písemný či jiný projev zachycen na elektronickém nosiči, a to nikoliv v obrazové podobě, ale znakové (tak, jak byl napsán na klávesnici) či jinak digitálně (zvuk, obraz), pak je dnes identifikace a autentizace při tomto způsobu zpracování zajišťována především právě elektronickým podpisem. [3] Elektronicky podepsat ovšem můžeme (a v některých případech musíme) i text či obrázek, který byl oskenován a uložen jako digitální záznam.

Z hlediska výše uvedených požadavků je to právě elektronický podpis, který nám poskytuje větší míru bezpečnosti – přinejmenším co se týká možností určit podepsanou osobou a zajistit následnou ochranu proti neoprávněné modifikaci podepsaného dokumentu. Pokud jsou čas od času v mediích, zejména českých publikovány „zaručené metody“, jak obelstít elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí prostředku pro bezpečné vytváření podpisu (pro tuto variantu se začalo v zahraničí využívat zkratky „kvalifikovaný podpis“), se obvykle jedná buď o nepochopení technologických či právních souvislostí elektronického podpisu, nebo o umělou, od reálného života odtrženou konstrukci. Přesto je třeba bezpečnostní stránku elektronického podpisu neustále vyhodnocovat, neboť dosažení určité úrovně technologického pokroku by mohlo vést ke snížení bezpečnosti a tedy nutnosti určitých protiopatření (v lepším případě prosloužení délky privátního podepisovacího klíče, v horším případě změny celé stávající technologie).

Jak se ukázalo, problém masového používání elektronického podpisu je poměrná složitost technologicko-organizační, od opatřování certifikátu přes vlastní vytváření podpisu. Proto

[3] Mates, P., Smejkal, V.: *Elektronické podpisy.* Právní rádce, VII., 1999,č.9, s.17.

není používán tam, kde se nejvíce předpokládalo, že umožní přejít od listinné k elektronické dokumentaci – typicky např. ve zdravotnictví.

Alternativou by mohlo být použití biometrického elektronického podpisu, také nazývaného dynamický biometrický podpis.

4.2.5 Tři úrovně elektronického podpisu

Revoluce spočívá v nahrazení klasického podpisu na papíru podpisem elektronického dokumentu, při současném zvýšení bezpečnosti celé podpisové operace. Tato zvýšení je ale podmíněno použitím tzv. zaručeného elektronického podpisu, dnes především v kombinaci s tzv. kvalifikovaným certifikátem, což je nejnáročnější kombinace všech možných druhů elektronického podepisování. A samozřejmě tento způsob podepisování musí mít oporu v zákoně.

Existují tři stupně elektronického podpisu: „obyčejný“, „zaručený“ a „uznávaný“. Zákon o elektronickém podpisu i směrnice[4] o elektronickém podpisu říkají, že (obyčejným) *elektronickým podpisem jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě (§ 2písm. a) EPZ.* Neříkají nic o tom, jako technologií mají být tato data vytvořena a jak se má postupovat při zmíněném ověření totožnosti. S „obyčejným“ elektronickým podpisem se proto můžeme dnes setkat např. v bankách při porovnání podpisu na papíru s podpisovým vzorem, oskenovaným a uloženým v paměti počítače. Srovnání je ale pouze vizuální a záleží na momentální kondici podepisujícího i na schopnostech bankéře, aby odhalil, zda jde o padělek. Jde tedy o postup ryze subjektivní. Může, ale existovat i elektronický podpis na bázi biometriky, konkrétně dynamický biometrický podpis, o kterém budeme hovořit dále.

Tzv. *zaručený elektronický podpis* přináší zcela novou kvalitu. Jedná se o údaje, které jsou připojeny k obsahu elektronického dokumentu a které jsou vytvořeny zvláštním postupem, dnes nejčastěji využitím kryptografie neboli šifrováním. Podle §2 písm. b) EPZ zaručeným elektronickým podpisem se rozumí elektronický podpis, který splňuje následující požadavky:

[4] Směrnice Evropského parlamentu a rady 1999/93 ES ze dne 13. Prosince 1999 o zásadách Společenství pro elektronické podpisy. Citace (CELEX):399L0093, publikováno v OJ L 013.

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Tento podpis poskytuje řadu funkcí, které na papíře nemůžeme nikdy dosáhnout:

- identifikuje průvodce podpisu (tzn., že příjemce zprávy bezpečně ví, kdo je autorem či odesilatelem elektronické zprávy),
- zaručuje integritu zprávy (příjemce má jistotu, že zpráva nebyla změněna),
- zaručuje nepopiratelnost (osoba nemůže popřít, že danou zprávu s daným obsahem vytvořila) a to především proto, že je vytvořena pomocí prostředků, které podepisující osoba může mít pod svou výhradní kontrolou.

Tento poslední požadavek vyplývající ze Směrnice 1999/93/ES byl v minulosti předmětem mnoha diskuzí na téma, co dnes, v době sofistikovaných počítačů a jejich operačních systémů může uživatel udržet pod kontrolou. Současný výklad je takový, že:

a) osoba má možnost svým chováním zabránit kompromitaci tajného klíče,
b) podepisuje se prostředkem pro bezpečné vytváření elektronických podpisů, což je požadavek pro vytváření elektronického podpisu, který splňuje požadavky stanovené zákonem (EPZ).

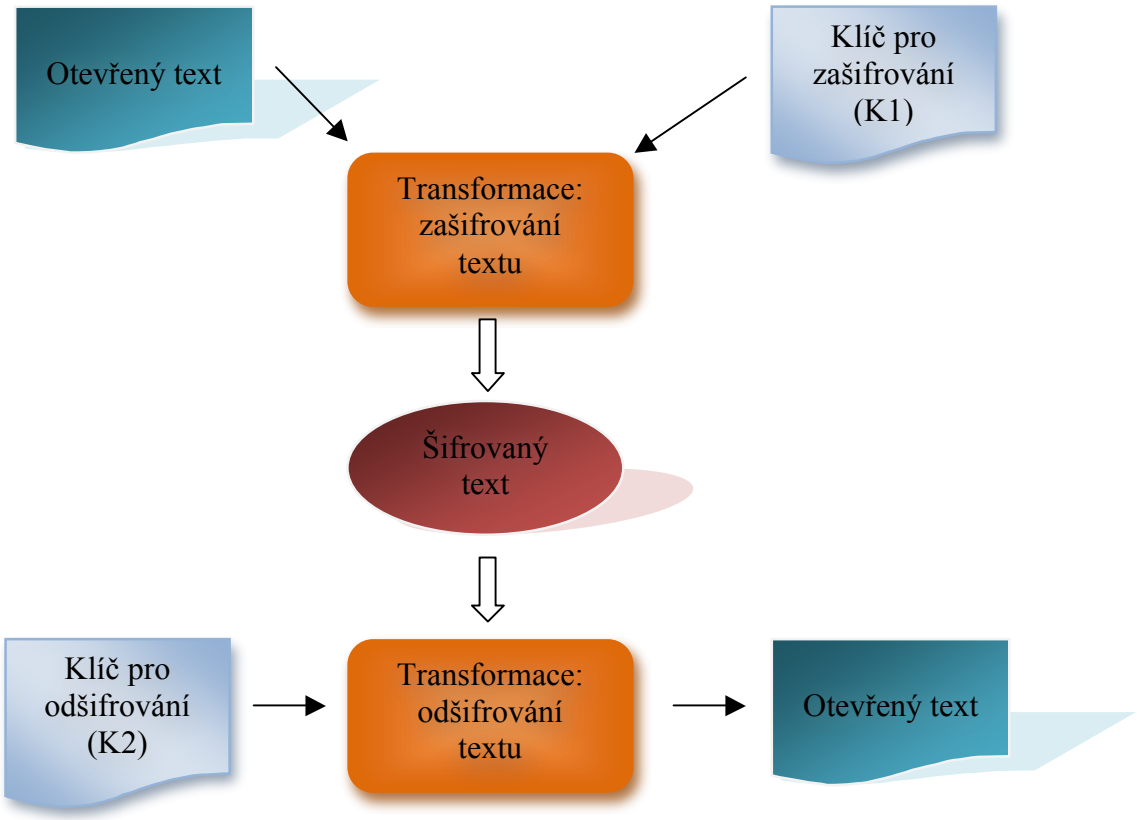
Zákon pak v § 11 zavádí tzv. „uznávaný elektronický podpis“, kterým je zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaným akreditovaným poskytovatelem certifikačních služeb. Jde o institucionální úroveň důvěryhodnosti, nikoliv již – na rozdíl od předchozích variant – úroveň technologickou.

4.3 Princip digitálního podpisu

Především, digitální podpis nemá nic společného s pojmy jako digitalizovaný podpis nebo oskenovaný podpis. Digitální podpis je totiž číslo. Pokud se řekne číslo, můžeme si představit jako číslo v desítkové, tak v dvojkové soustavě. Je to jedno, protože každý z těchto tvarů můžeme vzájemně jednoznačně převést na druhý. Snad by bylo názornější si představovat, že číslo je spíše posloupnost nul a jedniček (bitů), naopak posloupnost bitů pak můžeme přirozeně považovat za vyjádření čísla. Od „běžných“ čísel se, ale digitální podpis přece jen odlišuje. Zejména tím, že:

- to bývá velmi velké číslo (tisíce bytů dlouhý údaj), a
- jeho výpočet nebo ověření je dosti složitější úkon, který nelze provádět ručně, ale pouze s pomocí počítače.

Počítač, který umí vytvářet nebo ověřovat digitální podpis, nemusí být zrovna osobní počítač nebo notebook. Příslušné složité výpočty mohou vykonávat i miniaturní čipy, které se vejdou na čipové karty. Takové čipové karty se také už delší dobu vyrábějí. Tyto čipy mohou být umístěny v různých technických zařízeních, třeba v mobilních telefonech, klíčích od auta nebo hodinkách. To opět záleží na představivosti uživatelů, trhu a na tom, kterým směrem se celá tato oblast bude vyvíjet. Prozatím tedy zůstaňme u toho, že digitální podpis je velké číslo, které vytváří a ověřuje počítač.



Obrázek 1: Transformace a šifrování

Obecně je šifrovací algoritmus transformace, která převádí otevřená data na data zašifrovaná a naopak. Tato transformace je řízena šifrovacím klíčem. Při zašifrování se použije klíč pro zašifrování, při odšifrování klíč pro odšifrování.

Jestliže oba tyto klíče jsou totožné (K1=K2), hovoříme o symetrickém šifrovacím algoritmu. Jestliže jsou různé (K1≠K2), hovoříme o asymetrickém šifrovacím algoritmu, nebo o šifrovacím algoritmu s veřejným klíčem.

4.3.1 Hash funkce

Pojem digitální dokument by mohl být zavádějící v tom, že to je jen digitální obdoba nějakého formálního dokumentu (listiny, formuláře apod.). My budeme pod pojmem digitální dokument uvažovat libovolný soubor dat tak, jak jej známe v počítačové terminologii. Digitální dokument je tedy libovolná posloupnost dat neboli libovolná

posloupnost bitů (v zákonu o elektronickém podpisu tomuto pojmu odpovídá termín „datová zpráva“).[5]

Digitální dokumenty mohou být soubory textové, obrazové, zvukové, ale i počítačové programy, mapy, výkresy nebo jednotlivé položky v databázi apod. (Můžeme proto podepsat i svůj program tak, aby bylo zřejmé, že je náš, že jsme jej vytvořili apod.) Ve všech případech jsou to, ale „pouhé“ posloupnosti bitů – nul a jedniček. A protože posloupnost bitů můžeme chápat jako číslo, digitální dokument bude pro nás číslo. Většinou to bude opět velké číslo, třeba bude mít miliony číslic, ale na jeho podstatě to nic nemění. Tento triviální „převod“ digitálních dokumentů na čísla, nám nyní umožňuje pracovat s čísly a nikoli s papírovými dokumenty. Vše následující, například hudební skladba či kompletní písnička, zvukově-obrazový záznam apod., jsou z hlediska procesu podepsání dokumentu pouhým jedním, byť třeba velice dlouhým číslem.

Protože ale by práce s tak velkými čísly činila při požadavcích na rychlé zpracování elektronického podpisu problémy, prvním krokem při podepisování je jistá redukce tohoto čísla = celého dokumentu na jeho reprezentaci, tj. jiné kratší číslo, které je nicméně vzhledem k obsahu dokumentu jednoznačné a má pevnou délku (to je nutné pro standardizaci). Jedná se tedy o matematicko-kryptografickou metodu tzv. hashování, kdy je pomocí jednocestné funkce převedeno ono velké číslo (obsah dokumentu) na číslo kratší.[6]

[5] Elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na technických nosičích dat, používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložena netechnických nosičích ve formě datového souboru.
[6] Klíma, V. *Bezpečné kryptografické nástroje pro třetí tisíciletí.* Praha; Decros Prague Conference, 21.6.2000

4.4 Právní aspekty DBP

4.4.1 Písemný právní úkon a podpis

V současné době je stanoveno podle našeho základního právního předpisu, zákona č. 40/1964 Sb., občanského zákoníku, ve znění pozdějších předpisů, § 40 odst. 3, že písemný právní úkon je platný, je-li podepsán jednající osobou, přičemž se tímto podpisem zásadně rozumí podpis vlastnoruční; podpis může být nahrazen mechanickými prostředky pouze v případech, kdy je to obvyklé. Jak říká Občanský Zákoník dále v odst. 4, písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.

Obdobně podle nového občanského zákoníku účinného od 1. ledna 2014, zákona č. 89/2012 Sb., § 561, jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat. Podle § 562 odst. 1 písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby. Podle odst. 2 má se za to, že záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám. Byl-li záznam pořízen při provozu závodu a dovolá-li se jej druhá strana k svému prospěchu, má se za to, že záznam je spolehlivý. Je-li tedy právní úkon učiněn elektronickými prostředky, může být podepsán podle obou občanských zákoníků elektronicky podle zvláštních předpisů (jiného právního předpisu).

4.4.2 Podpis dle zákona o elektronickém podpisu

Předpisem, na který se odvolávají oba výše uvedené občanské zákoníky, je zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

Podle tohoto zákona rozlišujeme tři kategorie elektronického podpisu:

- elektronický podpis podle § 2 písm. a)
- zaručený elektronický podpis podle § 2 písm. b),
- zaručený elektronický podpis s kvalifikovaným certifikátem,
- zaručený elektronický podpis a kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb ("uznávaný elektronický podpis") podle §11.

Podle Směrnice Evropského parlamentu a Rady 99/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy, z níž zákon vychází, i zákona samotného jsou:

- Elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě (§ 2 písm. a),
- Zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky:
  - je jednoznačně spojen s podepisující osobou,
  - umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
  - byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
  - je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat (§ 2 písm. b).

Z výše uvedeného vyplývá, že elektronickým podpisem podle § 2 písm. a) zákona (dále také jen „EP“) se rozumí podpis, který slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě, a to bez další specifikace konkrétní technologické realizace. Ani zaručený elektronický podpis není podle definice v § 2 písm. b) zákona vázán na určitou technologii, jakkoliv se v současnosti používá metoda

asymetrické kryptografie se soukromým a veřejným klíčem a certifikátem, resp. kvalifikovaným certifikátem.

- Členské státy zajistí, aby zaručené elektronické podpisy založené na kvalifikovaných certifikátech a vytvořené pomocí prostředků pro bezpečné vytváření podpisu:
    - splňovaly právní požadavky na podpis ve vztahu k datům v elektronické podobě stejně, jako vlastnoruční podpisy splňují tyto požadavky ve vztahu k datům na papíře; a
    - byly přijímány jako důkazy v soudním řízení.

- Členské státy zajistí, aby elektronickým podpisům nebyla odpírána právní účinnost a aby nebyly odmítány jako důkazy v soudním řízení pouze z toho důvodu, že:
    - jsou v elektronické podobě, nebo
    - nejsou založeny na kvalifikovaném certifikátu, nebo
    - nejsou založeny na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb, nebo
    - nejsou vytvořeny pomocí prostředku pro bezpečné vytváření podpisu.

Podle Rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu, čl. 1 odst. 4. „Odstavec 2 nebrání členským státům v přijímání jiných elektronických podpisů, než jsou zaručené elektronické podpisy založené na kvalifikovaném osvědčení, ať již s prostředkem pro bezpečné vytváření podpisu nebo bez něj.“.

Dle dikce § 3 zákona – Soulad s požadavky na podpis, odst. 1 datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.

Vlastnoruční biometrický podpis (dále také jen BVP) je zcela jistě elektronickým podpisem podle § 2 písm. a), přičemž při vhodné technologické a procesní realizaci VBP

lze splnit i požadavky podle § 2 písm. b) na zaručený elektronický podpis. Použití certifikátu není podmínkou, pokud je splněn požadavek dle § 40 odst. 4 Ob. Z, tj. určení osoby, která právní úkon učinila.

Závěry

Dle právního rozboru biometrický podpis splňuje požadavky kladené na právní úkon dle zákona č. 40/1964 Sb., občanského zákoníku, ve znění pozdějších předpisů, § 40 odst. 3 a na elektronický podpis dle ustanovení § 2 písm. a) zákona č. 227/2000 Sb., tedy je elektronickým podpisem ve smyslu zvláštního zákona. Biometrický podpis pak dle našeho názoru splňuje i požadavky kladené na tzv. zaručený elektronický podpis dle ustanovení § 2 písm. b) zákona č. 227/2000 Sb. Požadavek jednoznačného spojení s podepisující osobou je dán tím, že každá osoba se podepisuje v zásadě nezaměnitelným způsobem. Biometrický podpis nelze od elektronického dokumentu oddělit a podepisující osoba může být při podpisu jednoznačně identifikována. Díky zachycení biometrických charakteristik vlastnoručního podpisu a díky možnosti porovnání těchto dat s referenčním podpisem, je možné identifikaci osoby a verifikaci jejího podpisu zlepšit a automatizovat. Z výše uvedeného plyne také jednoznačné splnění požadavku na identifikaci podepisující se osoby ve vztahu k datové zprávě (dokumentu).

S ohledem na rozbor, podle něhož je vlastnoruční biometrický podpis elektronickým podpisem ve smyslu zákona č. 227/2000 Sb., bude možné považovat elektronický dokument podepsaný biometrickým podpisem za dokument, u něhož je splněna písemná forma ve smyslu zákona č. 40/1964 Sb., občanského zákoníku.
Nasazení vlastnoručního biometrického podpisu není v rozporu s komunitárním ani českým právem a představuje rozšíření možností elektronického podepisování podle zákona č. 227/2000 Sb., o elektronickém podpisu. [7]

Z hlediska dokazování pravosti vlastnoručního biometrického podpisu umožňuje doplnit stávající způsob dokazování prostřednictvím srovnávání statických podpisových vzorů a

[7] O elektronickém podpisu a o změně některých dalších zákonů: zákon o elektronickém podpisu. In: 227/2000. 29.6.2000. Dostupné z: http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx

pomocí posudků písmoznalců o další údaje (o dynamice podpisu), které zvýší pravděpodobnost jednoznačného výroku písmoznalci. Případně je možné ještě zpracovat znalecký posudek z oboru kybernetiky a ochrany dat, umožňující doložit správnost použité technologie.

Právní rozbor vznikl ve spolupráci s Prof. Ing. **Vladimírem Smejkalem**, CSc. LL. M., Ing. **Jindřichem Kodlem** CSc. a JUDr. **Robertem Kučerou** (AK Kučera)

4.5 Dynamický biometrický podpis

Princip biometrie spočívá v rozpoznávání jedinečných biologických charakteristik osoby,[8] při čemž se tvrdí, že některé vlastnosti člověka (otisk prstů, obraz duhovky oka, žilního řečiště, tvar ucha atd.) jsou jedinečné. (Tato jedinečnost je statistického charakteru, nikoliv charakteru zcela absolutního, nicméně z hlediska velikosti lidstva se předpokládá neopakovatelnost uvedených charakteristik u více jedinců.).

Protože statické biometrické vzorky je možné dnes poměrně snadno kopírovat (typicky otisk prstu, obraz duhovky oka), v centru pozornosti jsou tedy metody dynamické, které spočívají v zachycení řady parametrů projevu konkrétního člověka v čase. Patří sem snímání podpisu, psaní na klávesnici, chůze apod.

V souvislosti s elektronickým podpisem je diskutován tzv. dynamický biometrický podpis, kterému je věnována tato část. Dynamický biometrický podpis je nejpokročilejší variantou biomechanického podpisu, využívajícího elektronických prostředků pro snímání dynamických charakteristik podpisu a pro verifikaci osoby dle tohoto podpisu.

4.5.1 Biomechanický podpis

Biomechanický proces vzniku lidského podpisu není nikterak jednoduchý. Primární vzruch vzniká v centrálním nervovém systému – v lidském mozku s předem definovanou intenzitou a trváním. Nervový systém pak aktivuje příslušné svaly v definovaném pořadí.

[8] GERGURI S., Matyáš V., Říha Z., Smolík L. *Biometriky a generování klíčového materiálu.* Data Security Management, XIII., 2009. č. 3. s. 22-26 . ISSN 1211-8737

Pohyb pera po papíře, což je výsledek stahování a uvolňování svalů, zanechává stopu hrotu psacího nástroje.[9]

Literatura[10] rozlišuje off-line a on-line systémy pro verifikaci osob podle jejího podpisu.

4.5.2 Off-line systémy pro verifikaci osob podle jejího podpisu

U off-line systémů se verifikovaná osoba podepisuje klasickým způsobem na papír. Následně je podpis digitalizován prostřednictvím optického skeneru nebo kamery. Dále pak aplikace určuje shodnost podpisu osoby s referenčním vzorkem na základě srovnávání celkového tvaru (obrazu) podpisu.

4.5.3 On-line systémy pro verifikaci osob podle jejího podpisu

U on-line systémů jsou charakteristiky právě psaného podpisu získávány v reálném čase pomocí specializovaného tabletu, nebo speciálně upraveného pera či jiným specifickým snímacím hardwarem. Všechna tato zařízení zachycují statické i dynamické charakteristiky podpisu v průběhu jeho samotného vzniku.

Pro posuzovaný případ je ale daleko podstatnější skutečnost, zda se jedná o statické nebo dynamické snímání a vyhodnocování podpisu. Pouze on-line systémy využívají jak statické, tak i dynamické informace o podpisu (obraz i jeho vytváření). Pro tento druh podpisu tedy používáme název *dynamický biometrický podpis* (DBP) a pracujeme s tímto názvem i dál v této práci.

4.6 Úvod do problematiky dynamického biometrického podpisu

Charakteristiky on-line podpisu můžeme rozdělit na statické a dynamické charakteristiky. Můžeme na ně rovněž nahlížet jako na parametry a funkce.

Podpis se skládá ze dvou částí:

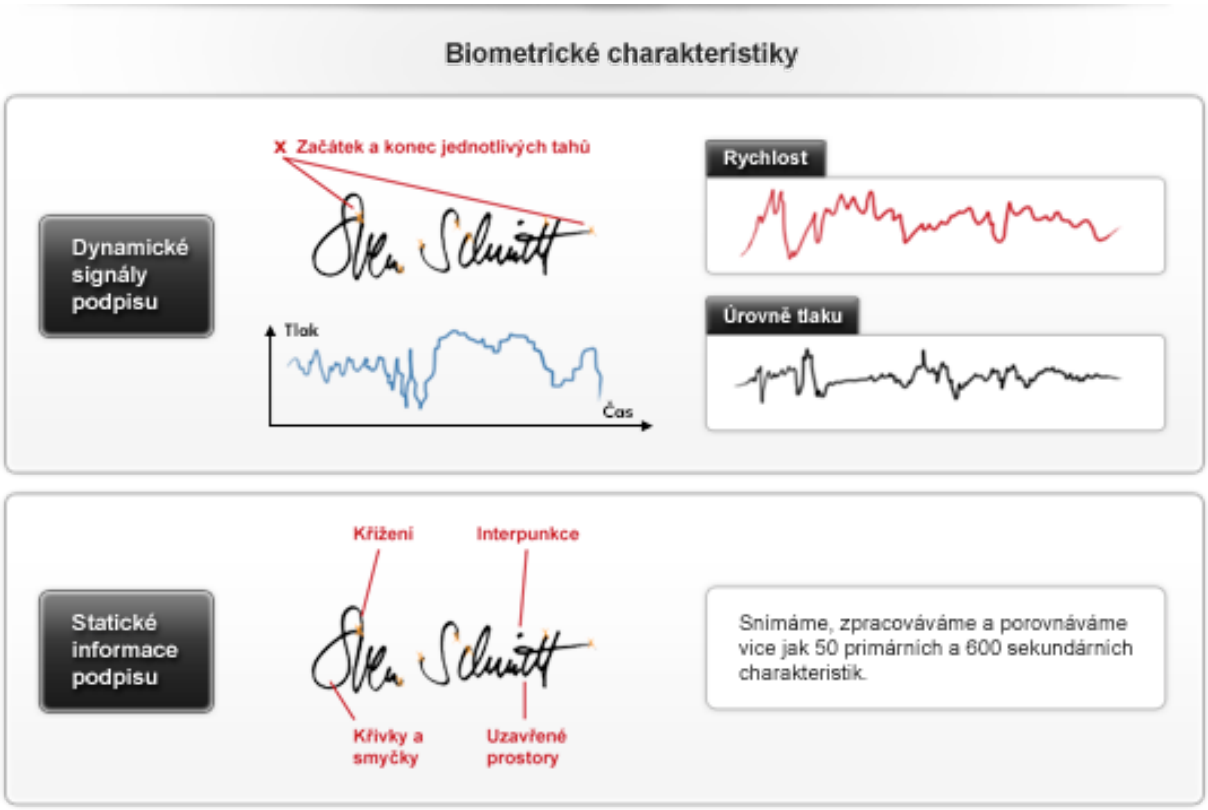
[9] BIČOVSKÝ, Radek. *Tajemství písma: úvod do grafologie*. Praha: Panorama, 1992. ISBN 80-703-8268-6.
[10] RAK, Roman. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.

- Viditelné informace: grafické znázornění, které je znázorněno na dokumentu (viditelném na obrazovce tabletu nebo pracovní stanice). Z technického hlediska není nutné, řešení obsahuje i tuto formu podpisu proto, aby podepisující se osoba viděla výsledek svého procesu podepsání. (Tím je splněn předpoklad ust. § 3 odst. 1 věta druhá zákona o elektronickém podpisu.) Grafické znázornění má tedy pouze informační charakter a není určen jako doklad podpisu.

- Neviditelné informace: Jedná se o informace, které jsou výsledkem vlastního biometrického podpisu. Tyto informace jsou vloženy do elektronického dokumentu – k jejich zobrazení je nutné využít aplikační program – např. Acrobat Reader nebo klient zvláštní aplikace DBP.

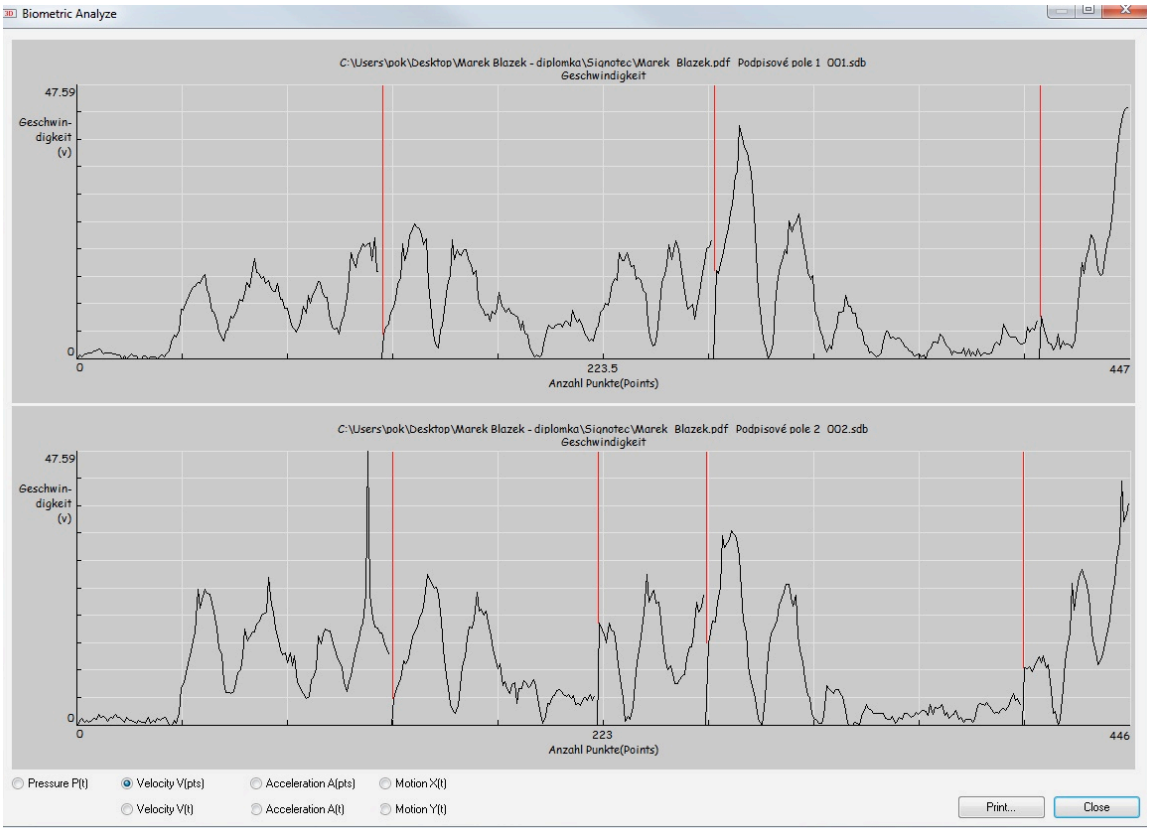
Každý podpis je určen svými charakteristickými body tahu podpisu včetně dynamických složek.[11]

[11] DOSTÁLEK L., Štíchová K. *Biometrický podpis v PDF*. Data Security Management, XVI., 2012, č. 2. 24-27



Obrázek 2: Zdroj http://signosoft.com

Tyto charakteristiky jsou obvykle extrahovány v průběhu celého procesu podepisování se. Jsou to např. průměrná rychlost psaní, maximální rychlost psaní, měření vlastností zakřivení tahů, poměr dlouhých a krátkých tahů, různé délky segmentů podpisu, doba trvání podpisování atd. Následně je můžeme přenášet do analyzačních grafů, které expert v oboru písmoznalectví analyzuje a činí závěry o pravosti podpisu samém.

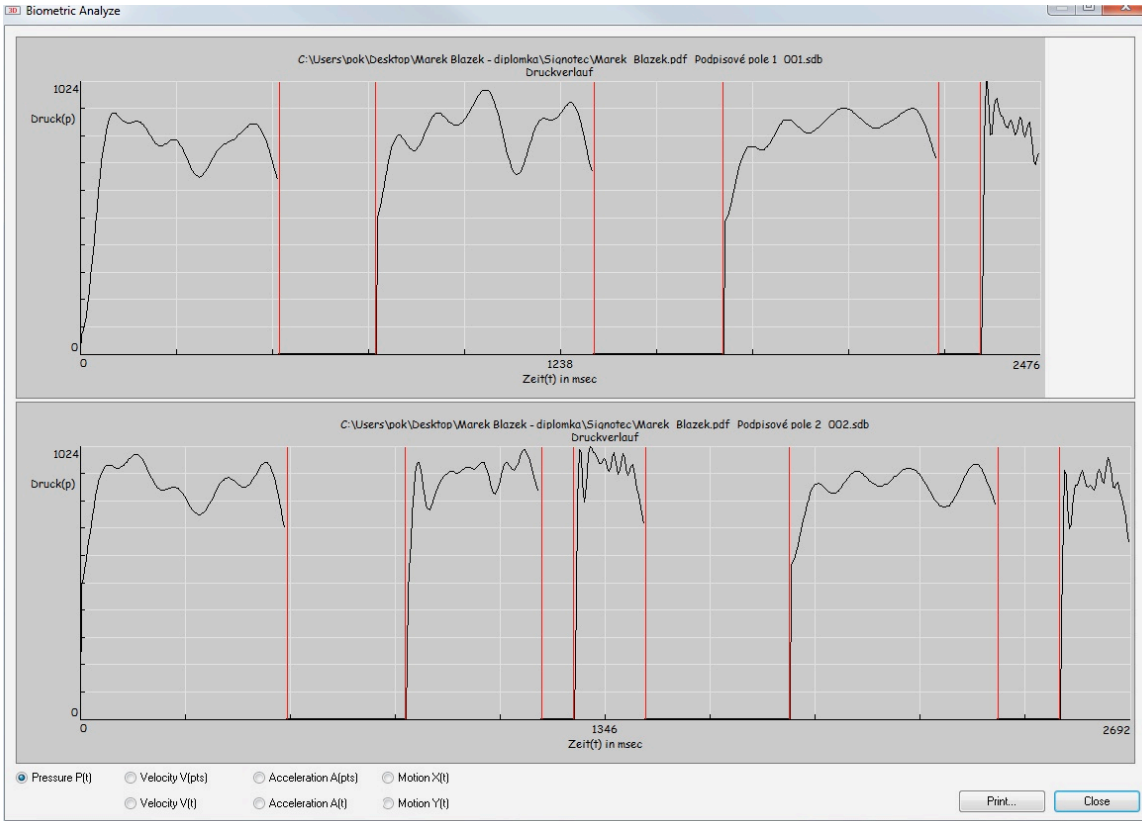


Obrázek 3: Zdroj: vlastní - graf průběhu rychlosti podepisování

Dynamické charakteristiky jsou vyjádřeny časovou funkcí, která charakterizuje podpis v každém časovém okamžiku jeho vzniku. Časové funkce podepisují souřadnicové pozice hrotu psacího nástroje: zrychlení, tlak hrotu pera na podložku apod. Další metody využívají charakteristik sklonu psacího nástroje. Lze rovněž využít charakteristik celkového pohybu psacího nástroje, tedy i pohyb nad papírem, kdy podepisující se osoba zvedá a spouští psací nástroj. Pohyb psacího nástroje je pak dynamicky (tj. v závislosti na čase) zaznamenáván a vyhodnocován v třírozměrném (3D) prostoru. Hovoříme o dynamickém zdvihu. Trojrozměrný dynamický pohyb je pro podepisující se osobu jedinečný a napomáhá k daleko větší přesnosti metody.

Dynamický podpis již sám v sobě obsahuje prvek „živosti“ objektu (pisatele), takže není potřeba vyvíjet další mechanismy testující, zda objekt je živý či nikoliv. Pohyb hrotu psacího nástroje probíhá v trojrozměrném prostoru, kde kromě souřadnic (x, y, z) se snímá tlak psacího nástroje na podložku, rychlost písma, zrychlení či časové intervaly mezi jednotlivými částmi podpisu (např. příjmení, jméno). Verifikace osoby na základě jejího podpisu je jedna z nejpřirozenějších biometrických metod, protože jsme dennodenně

zvyklí cokoliv stvrzovat našim podpisem. Metoda nikoho nijak neobtěžuje jak po stránce technické, tak i společenské či kulturní.



Obrázek 4: Zdroj: vlastní - graf průběhu intenzity tlaku při podepisování

4.6.1 Parametry dynamického biometrického podpisu

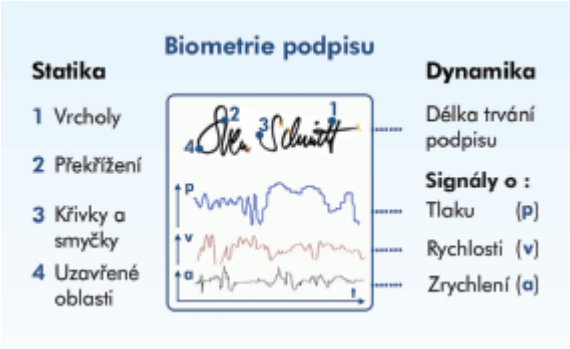
Systémy dynamických podpisů zaznamenávají vlastnoruční podpis s využitím speciálního „pera“ a digitalizačního tabletu. Digitalizační tablet poskytuje data, která umožní analyzovat jak statické, tak zejména dynamické biometrické vlastnosti podpisu spojeného s typickým chováním podepisující se osoby. Jedná se o:

- čas trvání podpisu, včetně trvání mezi jednotlivými tahy,
- body a křivky v jednotlivých částech podpisu,
- tlak působící perem na podložku v různých dobách procesu podpisu,
- celkovou velikost podpisu,
- formu a tvar podpisu,
- délku a úhel čáry, oblouky a křivky, počet smyček,

- rychlost při jednotlivých tazích, zrychlení, zpomalení,

tj. základní rysy vlastnoručního podpisu, které tvoří „biometrický vzorek. Vytvoření dynamického vzorku vychází v současné době z matematického aparátu neuronových sítí a je vesměs proprietárním řešením tvůrce.

Dynamický podpis obsahuje biometrické informace o tom, jak podpis byl tvořen, odráží charakteristické znaky podepisující se osoby, její návyky a projevy chování. Tyto vlastnosti představují biometrickou stopu, která je unikátní pro každého jednotlivce a nemůže být padělatelem reprodukována.



Obrázek 5: Zdroj http://signosoft.com

Sejmuté a zaznamenané biometrické charakteristiky vlastnoručního podpisu se využijí pro:

- grafické zobrazení podpisu v elektronickém dokumentu,
- zabezpečení elektronického dokumentu proti možnému falšování nebo padělání.

Snímací jednotky (pera) od jednotlivých výrobců se liší počtem členů vektoru biometrických informací.

Podpis je snímán ve dvou odlišných případech použití:

- jedná se pouze o podepsání dokumentu – pak postačuje sejmutí podpisu, jak je uvedeno výše,
- jedná se o využití podpisu pro autentizaci – dokumentu nebo úkonu, pro vedeného podepisující osobu. V tomto případě probíhá snímání dvou fázově:
  - fáze registrace podpisu spočívá v tom, že podepisující se osoba se několikrát podepíše na tablet (3až 12- ti podpisy). Z těchto souborů dat je pak vytvořen základní biometrický vzorek podpisu;
  - verifikace podpisu pak spočívá ve stanovení shody „vzorku“ a provedeného podpisu ve stanovených mezích. Vzhledem k tomu, že se jedná o statistické

metody, musí být při vytváření vzorku dodržena určitá pravidla, přičemž je třeba se vypořádat s několika omezeními:

- ♦ Odpovídající délka podpisu: krátký podpis → nedostatek dat, dlouhý podpis → uplatní se vliv nálady podepisovatele, může docházet k výrazně odlišným podpisům.
- ♦ Nutné stejné podmínky pro fázi podpisu – bude-li osoba stát, podpis se významně liší, než když osoba sedí.

U složitějších systémů jsou při verifikaci analyzována kromě základních charakteristik i další data, charakterizující statické i dynamické vlastnosti podpisu. Na snímací prvky jsou kladeny vysoké nároky, kdy základní požadavky (dokumentované i v normách ISO – vydaných i připravovaných) definují statické i dynamické parametry digitalizačních zařízení (tabletů i per). Musí být k dispozici dostatečné množství údajů, jak ohledně tlaku, tak i z hlediska snímání obrazce a jeho vlastností.

Mezi základní požadavky patří:

- spolehlivé sejmutí grafu křivky tlaku – kdy je nutné spolehlivé zaznamenání úrovně tlaku ve všech segmentech podpisu a tlak musí být přesně zaznamenán při různých případech tvarů (v různých tazích),
- tablet musí být ergonomický stejný jako papír,
- do podpisu nesmí být zahrnut např. otisk palce, dotek dlaně apod. – pouze musí snímat hrot,
- ukládána data musí být ve stavu umožňujícím zpětný forenzní audit, musí být zabezpečena komunikace mezi snímačem a uložištěm,
- musí být jednoznačné údaje pro autentizaci podepisující se osoby – jednoznačná vazba přístroje, času, ID osoby,
- zaručena důvěryhodnost komunikačního a výpočetního (operačního systému) systému.

Zpracovaný biometrický vzorek je přenesen do uložiště, kde vytváří základní etalon pro autentizaci osoby, která se bude následně podepisovat, a poskytuje referenční informace pro srovnávání s podpisy, které daná osoba vytvoří.

Standardně se používají u biometrických metod metody verifikace, kdy se jedná o porovnání biometrického vzorku uloženého v databázi podpisů daného uživatele s provedeným podpisem na shodu ve stanovených tolerancích.

Při této verifikaci je vznesen dotaz do databáze podpisů, která je buď zpracována prohledáním databáze na shodu s některým z uložených vzorku, nebo v návaznosti na ID příslušejícího k danému provedenému podpisu dojde k porovnání s odpovídajícím vzorkem.

Spolehlivost metod závisí jak na parametrech snímacích zařízení, tak na SW zpracovávajícího přijaté signály. Důležité je, aby použití dynamického podpisu umožnilo "zachovat standardní aspekty tradičního podpisu" bez toho, aby na uživatele byly kladeny omezující podmínky stanovující např. držení snímacího pera, limitovaná rychlost a velikost podpisu (z pohledu samotného obrazce i počtu písmen znaků).

4.6.2 Normy pro DBP

Přehled ISO/IEC norem

Vzhledem k nesporným výhodám použití dynamického podpisu jako jednoho z prvků autentizace je v současné době rozvíjena i činnost v oblasti tvorby norem. V současné době se standardizační aktivity soustřeďují zejména na vytvoření rodiny norem ISO/IEC 1974[12] Tyto normy jsou postupně začleňovány do technických norem ČR.

V současné době jedná o normy:

- ČSN ISO/IEC 19794-1 Informační technologie – Formáty výměny biometrických dat – Část 1: Struktura
- ČSN ISO/IEC 19794-7 Informační technologie – Formáty výměny biometrických dat – Část 7: data podpisových řad podpisu/značky. Norma definuje strukturu výstupních dat, která vznikají v tabletu v procesu podepisování ve formě souboru časově závislých dat.

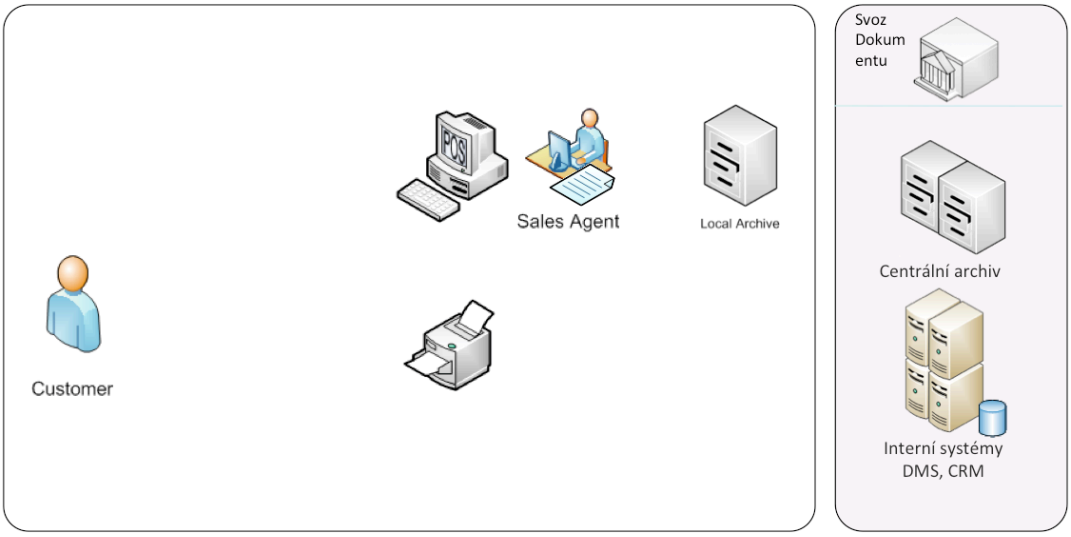
[12] INTERNATIONAL ORGANIZATION FOR STANDARTIZATION. *ISO normy* [online]. 2010 [cit. 2015-01-12]. Dostupné z: http://www.iso.org

5 Praktická část

V následujících kapitolách si názorně ukážeme a popíšeme rozdíly ve způsobech podepisování dokumentů při uzavírání smluv. Nejdříve si popíšeme standartní proces, s kterým se většina z nás běžně setkává v bankovních či pojišťovacích institutech. Následně si ukážeme a popíšeme proces za využití technologie dynamického biometrického podpisu.

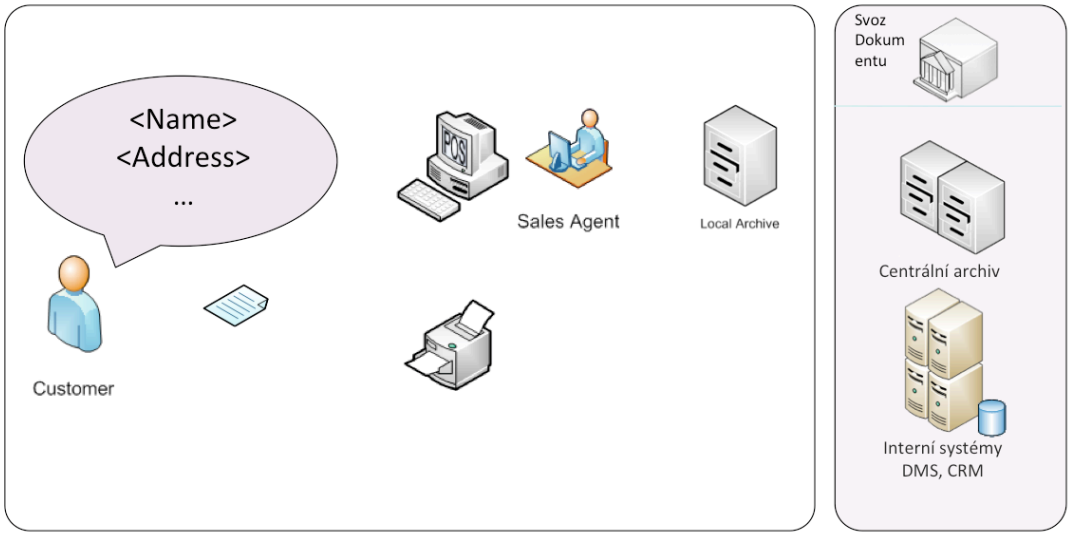
Popis stávajícího procesu uzavírání smlouvy

Nyní si ukážeme a popíšeme proces, který každý z nás zná ze své vlastní zkušenosti.
Na obrázku vidíme klienta/zákazníka, který si bude sjednávat předem obeznámený produkt u vybrané si společnosti, kterou reprezentuje obchodní zástupce. Tento zástupce má k dispozici, stolní počítač, tiskárnu a lokální archiv pro ukládání uzavřených smluv. V pravé části vidíme budovu, která reprezentuje místo, kam se sváží z více poboček dokumenty, které se následně odvážejí a ukládají do centrálního archívu. Společnost disponuje interní systémy dané společnosti pro přeposílání dat.



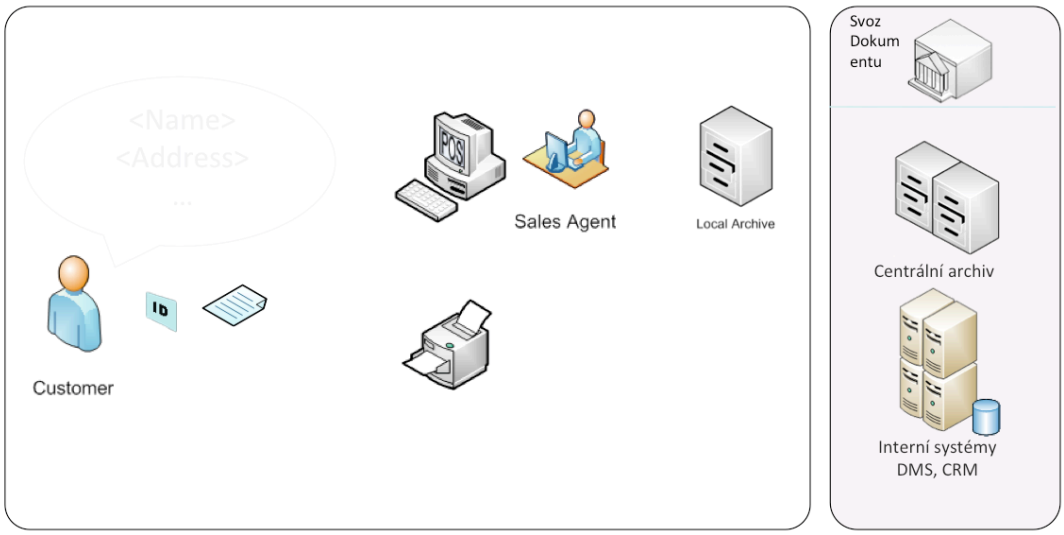
Obrázek 6 stávající proces

Na obrázku 6 si zákazník přečte koncept smlouvy a následně vypíše osobní údaje do připraveného konceptu, kterou mu obchodní zástupce vytiskl.



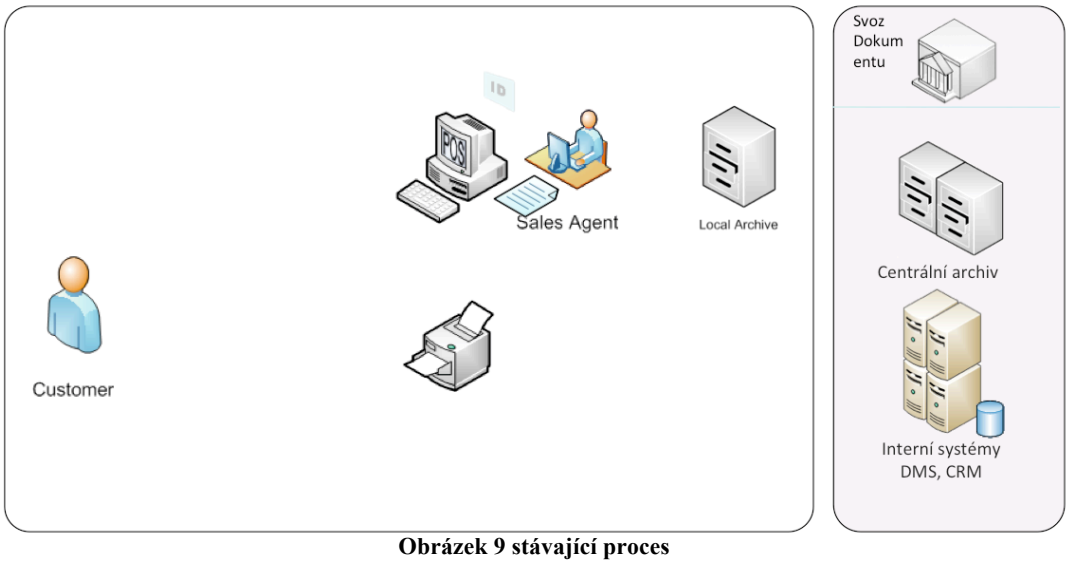
Obrázek 7 stávající proces

Následně předá vyplněnou smlouvu s platným dokladem obchodnímu zástupci.



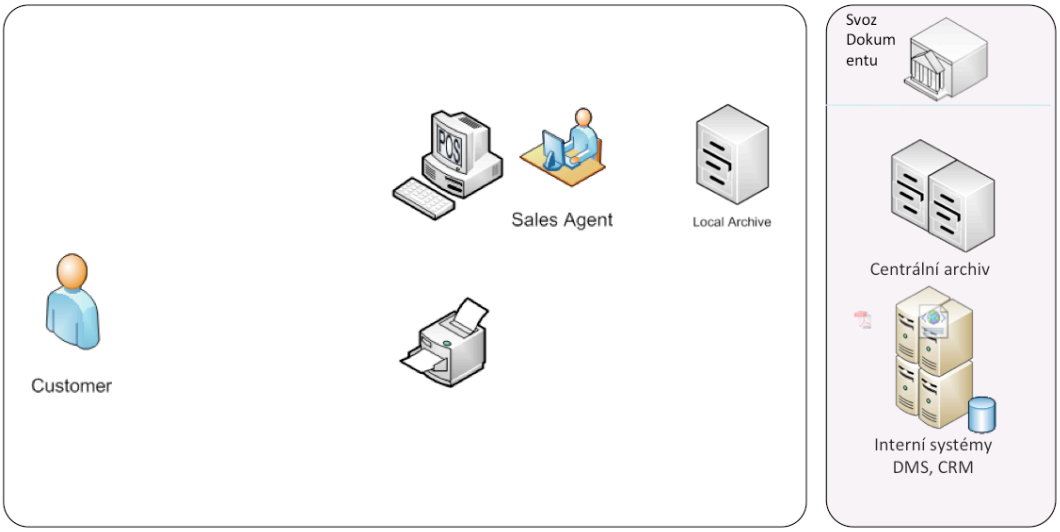
Obrázek 8 stávající proces

Ten ověří jeho totožnost a správnost uvedených údajů v uzavírané smlouvě.



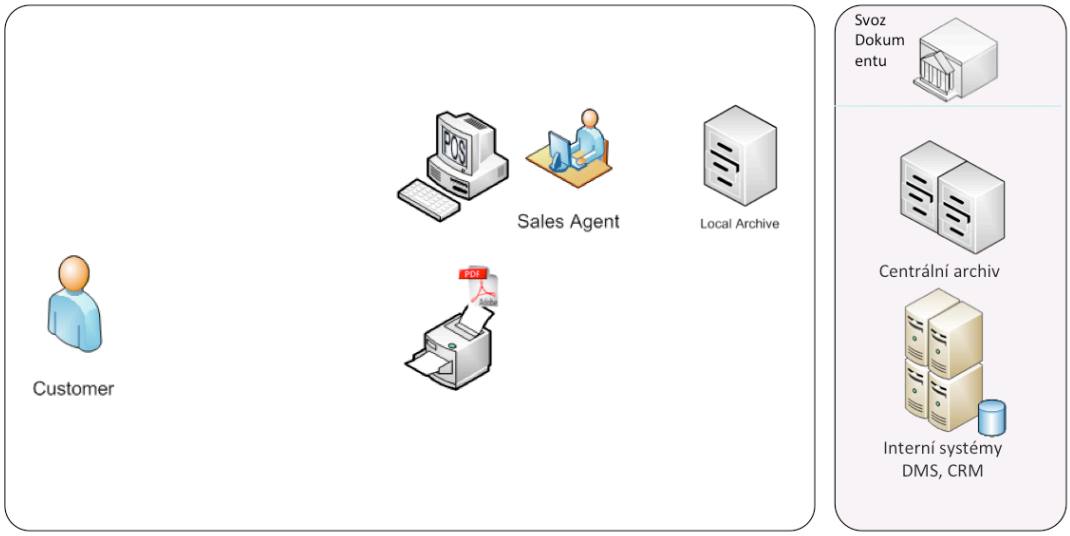
Obrázek 9 stávající proces

Po kontrole a zodpovězení případných dotazů klienta, obchodní zástupce přepíše získané údaje do stolního počítače a vygeneruje smlouvu se všemi požadovanými právními náležitostmi z interních systémů společnosti.



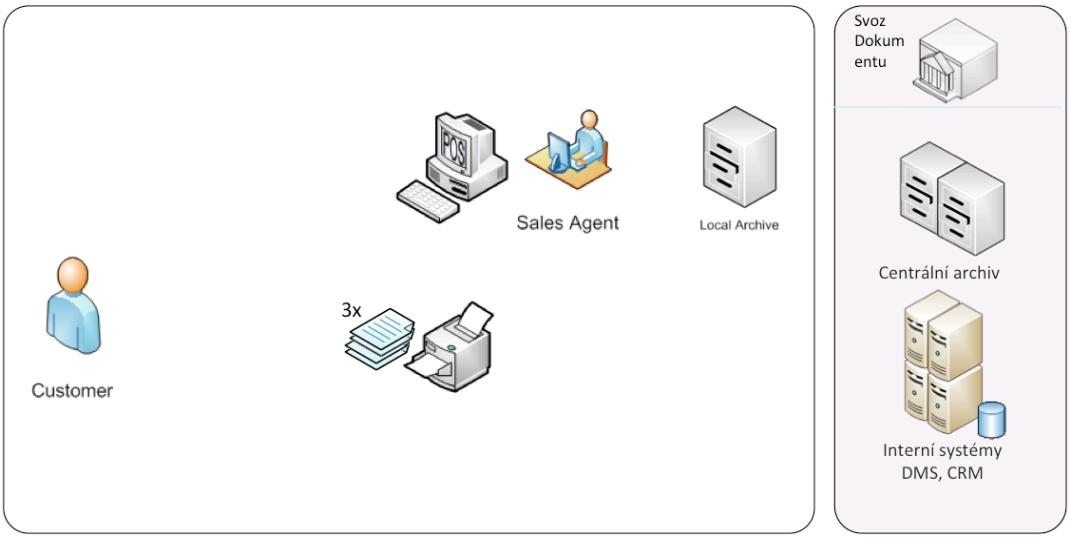
Obrázek 10 stávající proces

Ta se ve formátu Pdf zobrazí obchodnímu zástupci na monitoru, překontroluje správnost údajů.



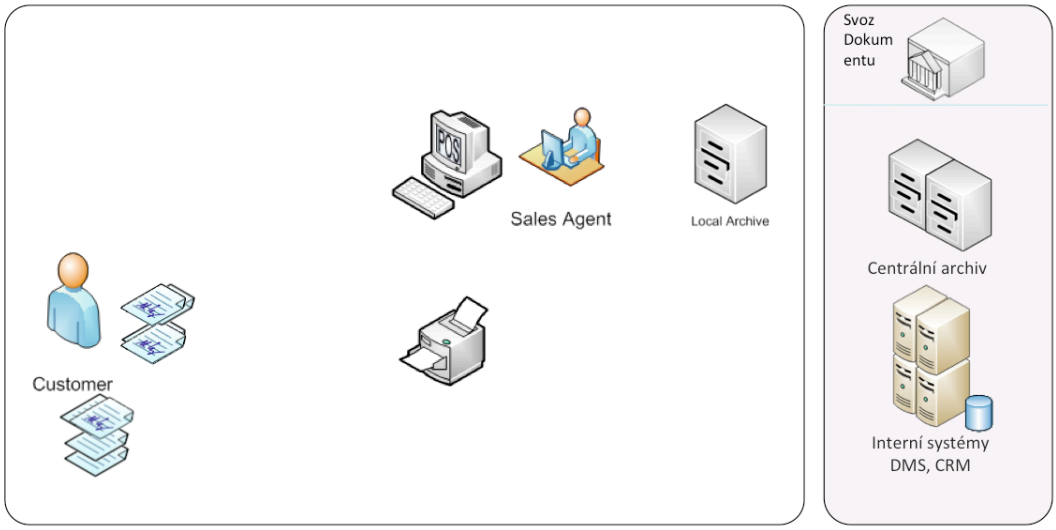
Obrázek 11 stávající proces

Vytiskne uzavíranou smlouvu v trojím provedení a dá je všechny přečíst klientovi.



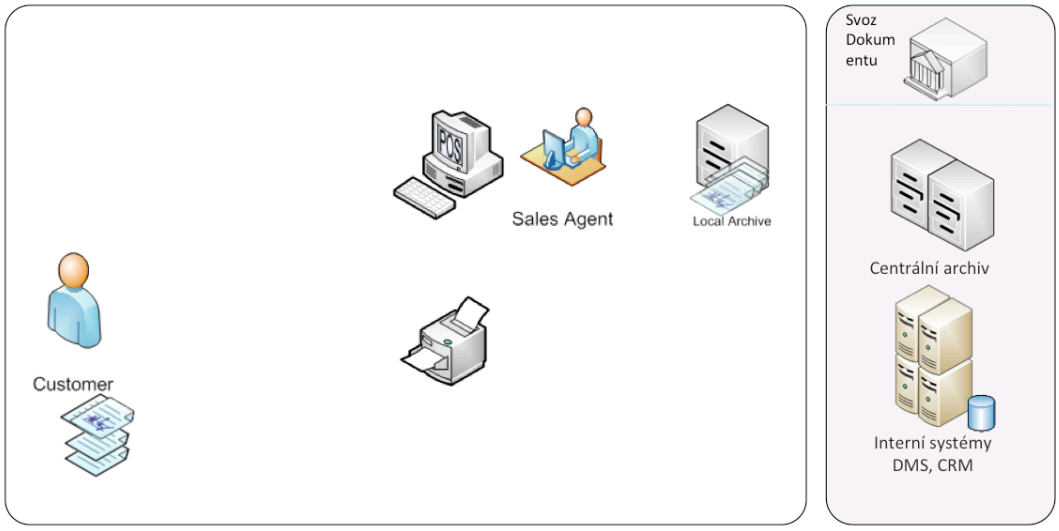
Obrázek 12 stávající proces

Klient svým podpisem potvrdí správnost údajů a vyjádří souhlas s podmínkami na všech stranách uvedených ve smlouvě u všech třech originálech.



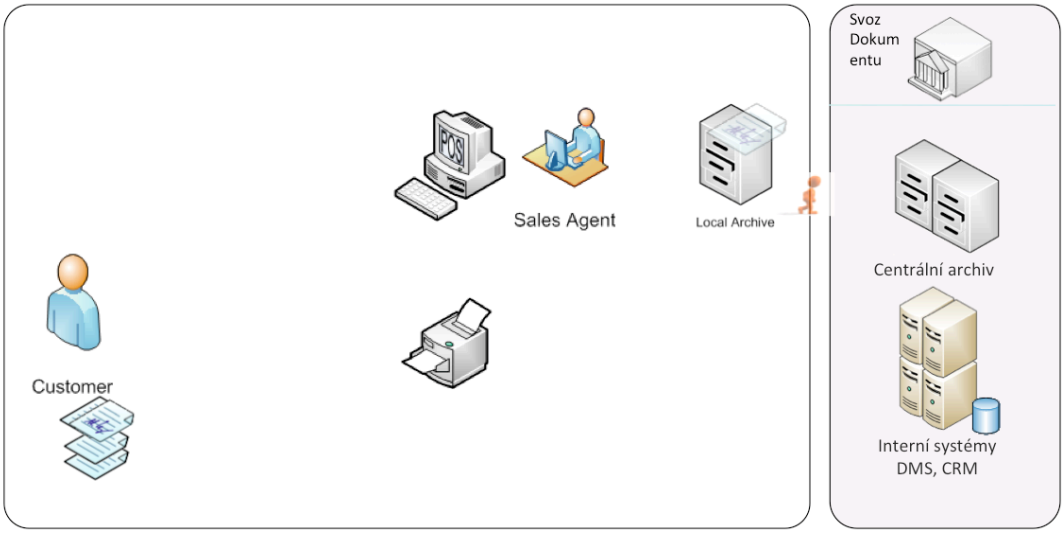
Obrázek 13 stávající proces

Jeden podepsaný výtisk smlouvy si klient nechává a další zbylé obchodní zástupce uloží do lokálního archívu pobočky.



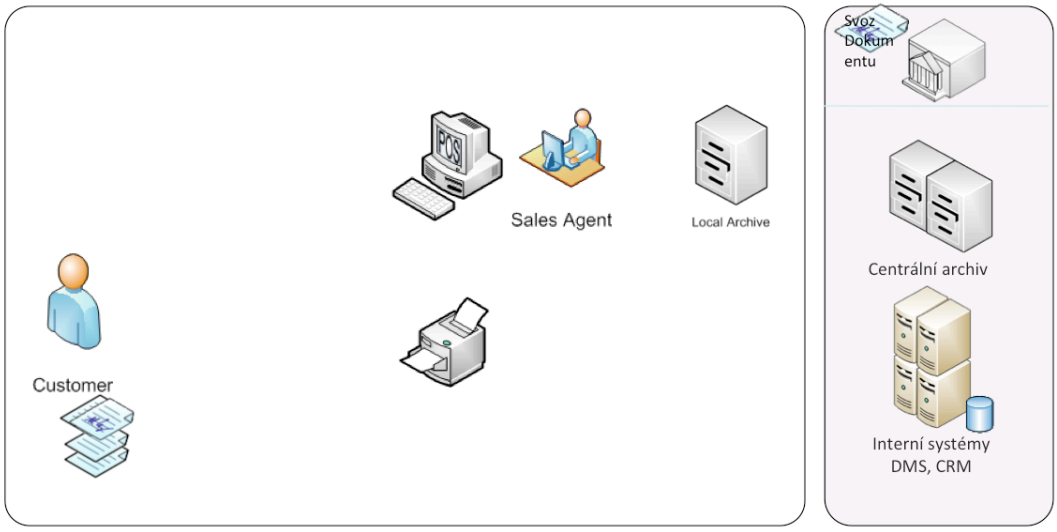
Obrázek 14 stávající proces

Zde budou uloženy do té doby, než bude proveden hromadný svoz dokumentů/smluv ze všech poboček dané společnosti.



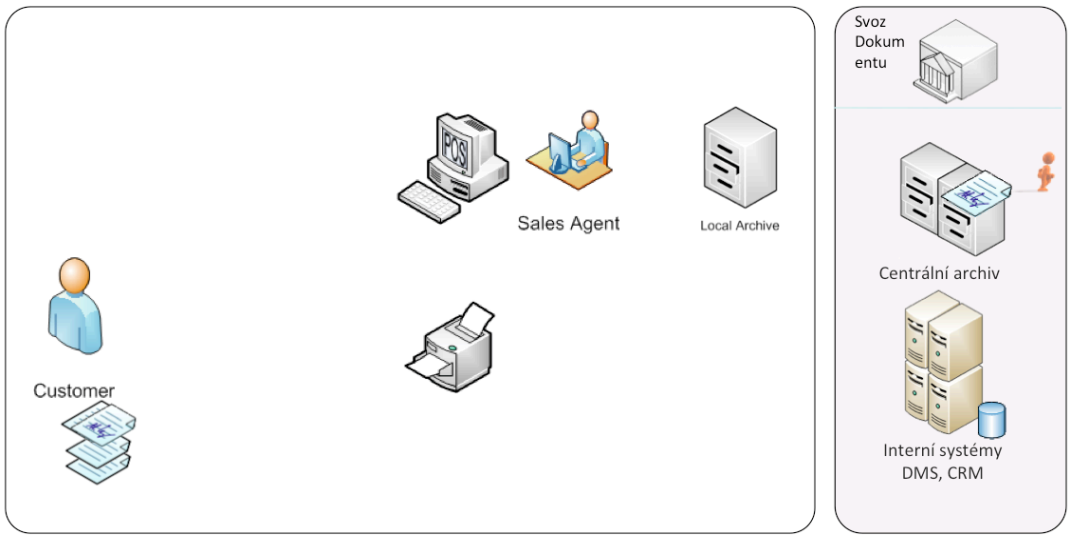
Obrázek 15 stávající proces

Dokumenty, smlouvy, listiny jsou skladovány v centrálním uložišti, než budou převezeny do centrálního archívu.



Obrázek 16 stávající proces

Do centrálního archívu se sváží veškeré smlouvy, dokumenty, listiny, které jsou pro společnost nějakým způsobem důležité, či je k tomu zavazuje zákon. V centrálním uložišti, jsou skladovány za takových podmínek, aby na písemnosti potažmo samotný papír nepůsobily okolní negativní vlivy. Ty by mohly způsobit samotné znehodnocení písemností a v jejím důsledku by nemohly být případně použity při soudních sporech nebo reklamacích klientů.



Obrázek 17 stávající proces

Shrnutí

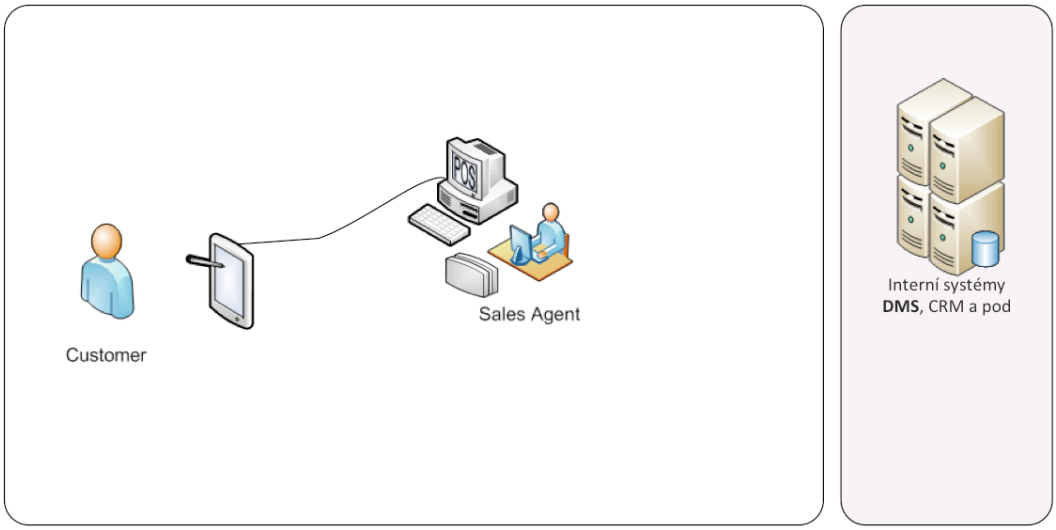
Viděli a popsali jsme si proces, kdy byl využit papír, jako nosný prostředek informací. Samotný proces je náročný pro klienta na čas, který stráví v obchodním místě, množství podkladů, které musí vyplnit, přečíst a v neposlední řadě i podepsat. Domu si odnáší jeden

originál uzavřené smlouvy, který by si měl pečlivě uschovat k případným pozdějším reklamacím ať ze strany klienta nebo společnosti v případě neplnění smluvních podmínek z jedné ze smluvních stran. Pokud se, ale podíváme z pohledu společnosti, tak jedním z negativ je čas klienta strávený na pobočce, protože další případní klienti musí čekat dokud nebude předchozí klient vyřízen k jeho spokojenosti. Při stávajícím procesu uzavírání smlouvy, dodatku, pojištění, ověření zákazníka, objednávky a samotného převzetí zboží nám rostou náklady související s oběhem dokumentu v papírové podobě. Tyto náklady se nám projevují v různých oblastech, které budou uvedeny v kapitole 5.5.

5.1 Popis procesu uzavírání smlouvy za využití DBP

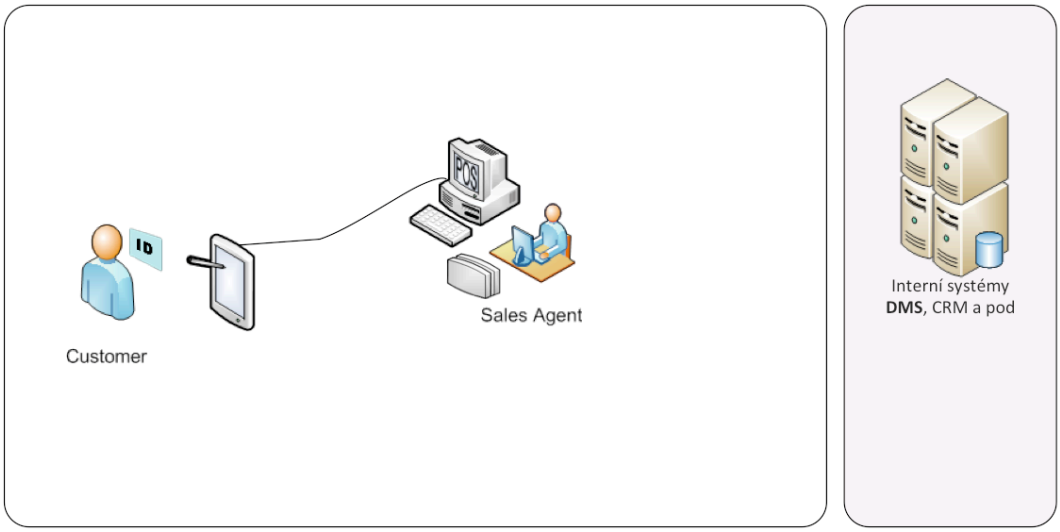
Nyní si ukážeme a popíšeme proces, v kterém budeme využívat implementaci „Dynamického biometrického podpisu“. ve společnosti.

Na obrázku vidíme klienta/zákazníka, který si bude sjednávat předem obeznámený produkt u vybrané společnosti, kterou reprezentuje obchodní zástupce. Tento zástupce má k dispozici, jak vidíme stolní počítač, čtečku identifikačních popřípadě bankovních karet a podpisovou vizualizační podložku/pad s dotykovým perem. V pravé části vidíme servery, které symbolizují uložiště dat a interní systémy dané společnosti.



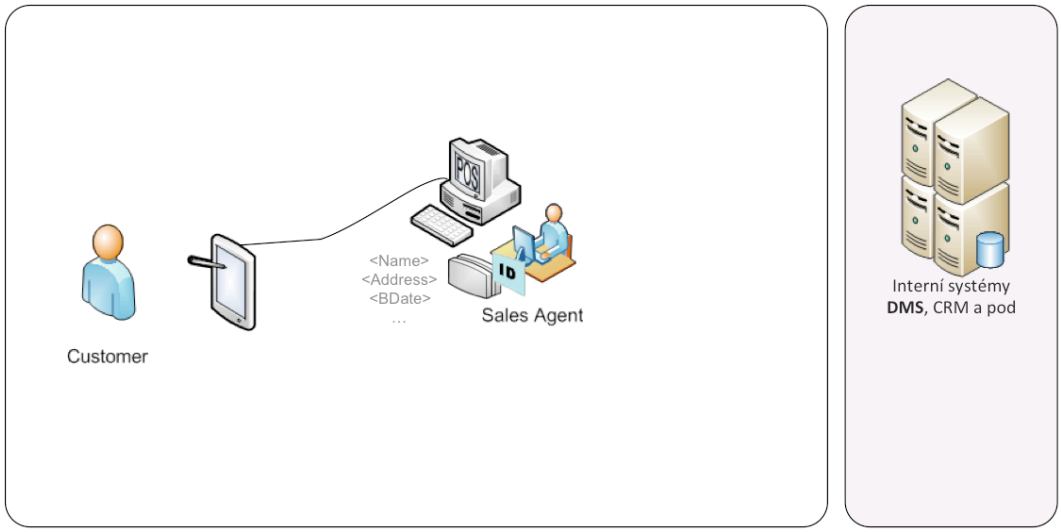
Obrázek 18 inovace DBP

Na následujícím obrázku se zákazník identifikuje platným dokladem, který ověří jeho totožnost a bude potřebný k vyplnění základních údajů do uzavírané smlouvy.



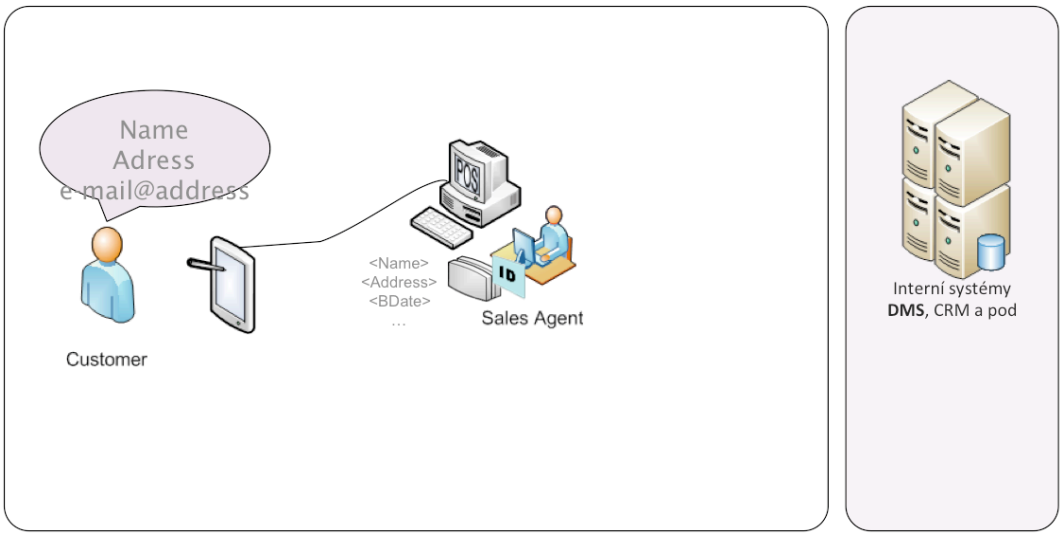
Obrázek 19 inovace DBP

Obchodní zástupce, může načíst data (jméno, příjmení, adresu, atd.) do smlouvy, kterou má aktivní ve stolním počítači z identifikační karty přímo, v tom případě ušetří čas vypisováním dat do počítače a zkrátí, tak dobu klienta na pobočce společnosti.



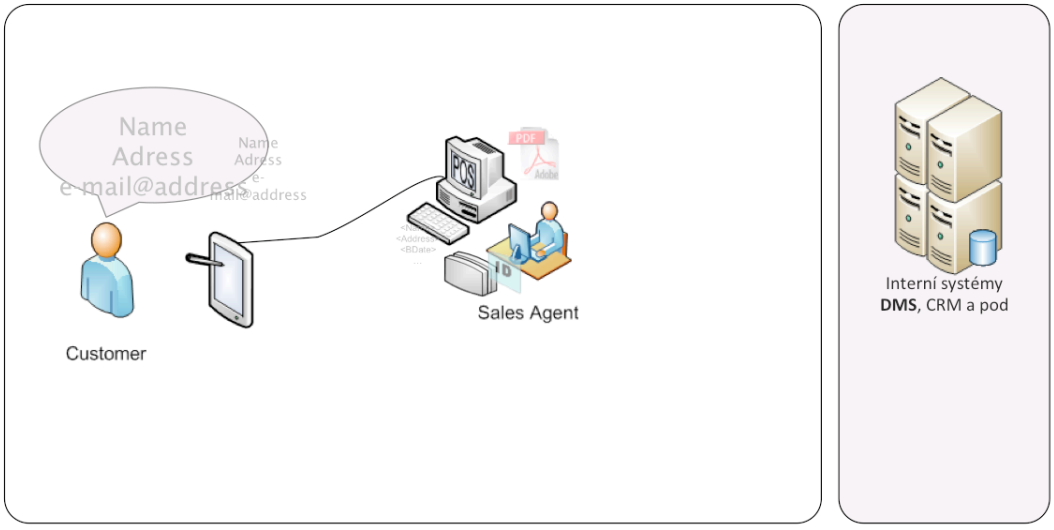
Obrázek 20 inovace DBP

Dále následuje ústní ověření načtených dat klientem a upřesnění potřebných informací ze strany obchodního zástupce.



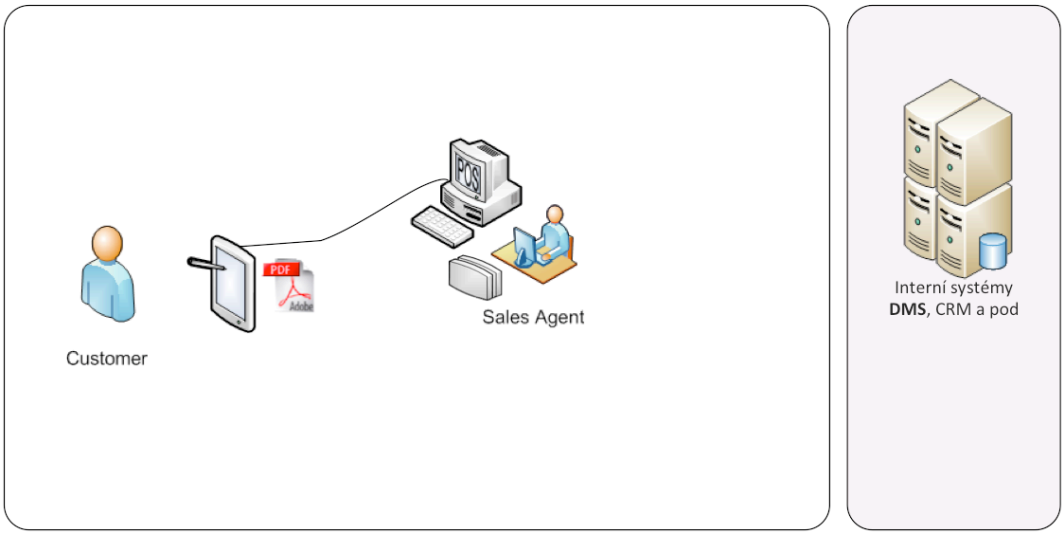
Obrázek 21 inovace DBP

Po zodpovězení dotazů klienta k danému produktu, kontrole dat a vyplnění smlouvy, je vytvořen dokument a to nejčastěji ve formátu PDF.



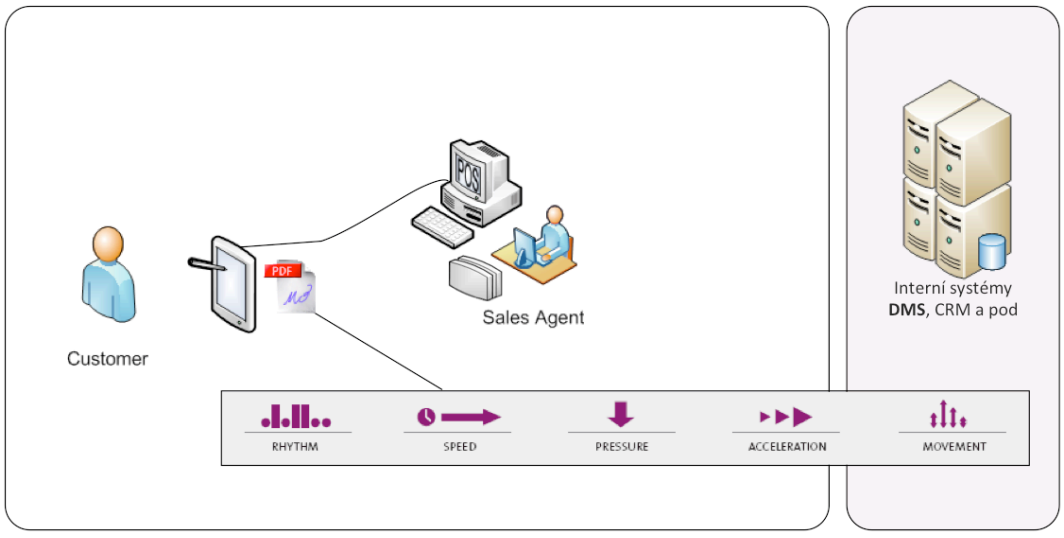
Obrázek 22 inovace DBP

Tento soubor v našem případě smlouva, je předložena elektronicky na vizualizačním zařízení, kde si ji klient přečte, projde, popřípadě dotazuje obchodního zástupce. Pokud jsou nesrovnalosti ve smlouvě, tak se okamžitě přepracuje a změnu vidí klient okamžitě.



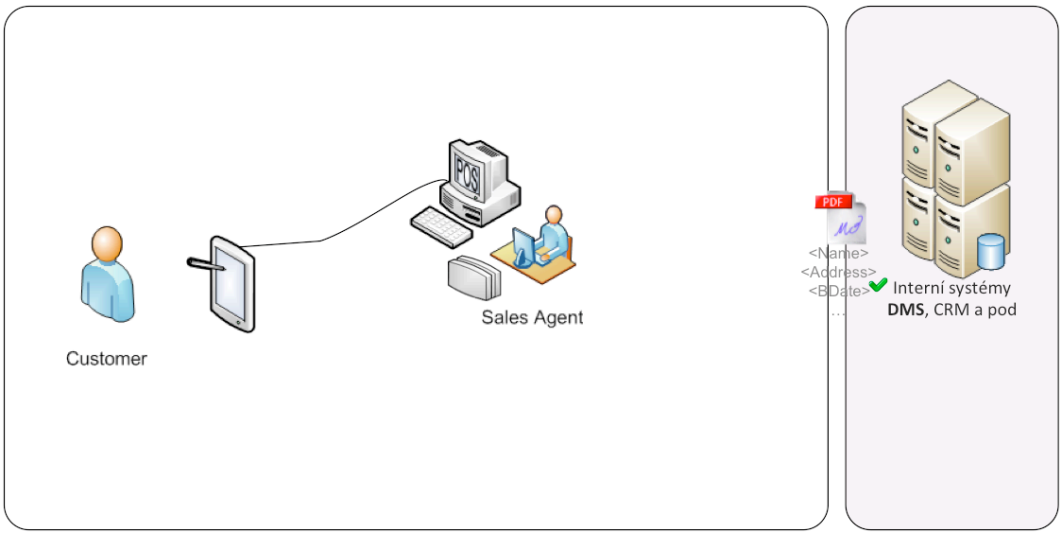
Obrázek 23 inovace DBP

V případě, že klient souhlasí s obsahem smlouvy, tak dokument/smlouvu podepíše do vyznačených aktivních polí, čímž za pomocí svých biometrických vlastností vytvoří svůj nenapodobitelný biometrický podpis. Ten obsahuje rytmus psaní, rychlost, vyvíjený tlak na podložku, zrychlování či zpomalování při podepisování a neposlední řadě i oddalování pera při samotném podpisu od podložky. To vše se zaznamenává do vytvářejícího se podpisu.



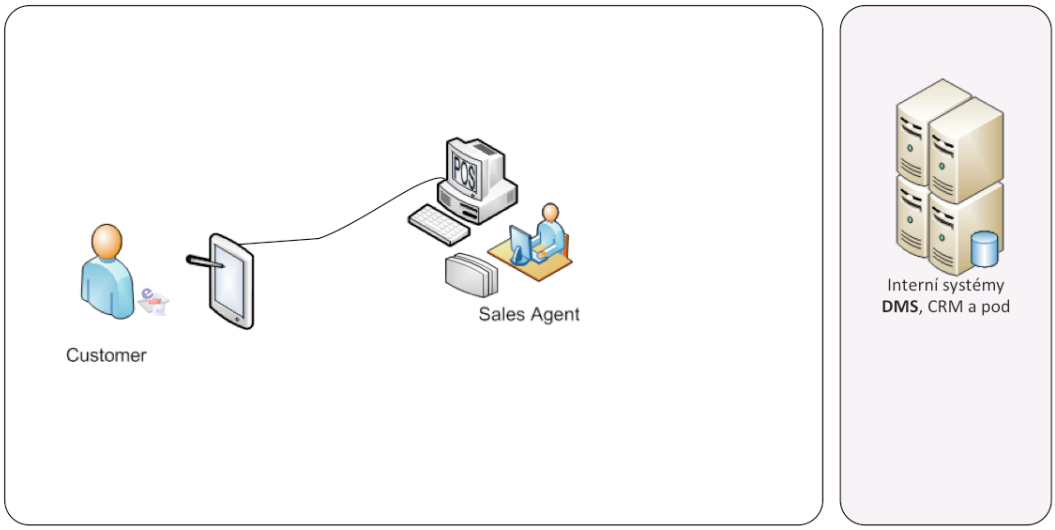
Obrázek 24 inovace DBP

Podepsaný/signovaný dokument je odeslán do interních systémů společnosti.



Obrázek 25 inovace DBP

Současně je odeslána klientovi do e-mailové schránky tzv. kopie, ale je to originál dokumentu. V případě zájmu si ji může klient kdykoliv vytisknout nebo i odnést přímo od obchodního zástupce.



Obrázek 26 inovace DBP

Shrnutí

Viděli a popsali jsme si proces, kdy byla využita podpisová podložka, jako znázorňující, přenášející prostředek informací. Samotný proces se může zdát náročný pro klienta a to ve formě práce s neznámým elektronickým zařízením, ale praxe ukazuje, že tomu tak není. Čas, který stráví klient v obchodním místě je minimalizován na nezbytně nutnou dobu, avšak ne na úkor péče o klienta samotného. Množství podkladů, které musí vyplnit, přečíst a v neposlední řadě i podepsat je v podstatě minimalizováno na jeden. Domů si v tomto případě neodnáší ve většině případech nic, protože je mu zaslán originál i s jeho podpisem do emailové schránky. V případech, že by klient trval na papírové formě, je mu to umožněno. Co se týče případných pozdějších reklamací ať ze strany klienta nebo společnosti v případě neplnění smluvních podmínek z jedné ze smluvních stran, stačí emailová komunikace a zasílaní originálu zaslané smlouvy. Pokud se, ale podíváme na proces z pohledu společnosti, tak se nám nenabízejí žádná negativa, jako u papírové formy uzavírání smluv, dodatku atd. I když by přeci jen jedno negativum mohlo případně nastat a to, že by nefungoval systém, v kterém technologie běží či na něj navazuje nebo nešel elektrický proud, který pohání všechna zařízení. Blíže budou uvedeny a popsány úspory a benefity plynoucí z implementace dynamického biometrického podpisu v kapitole 5.6.1. a následovně.

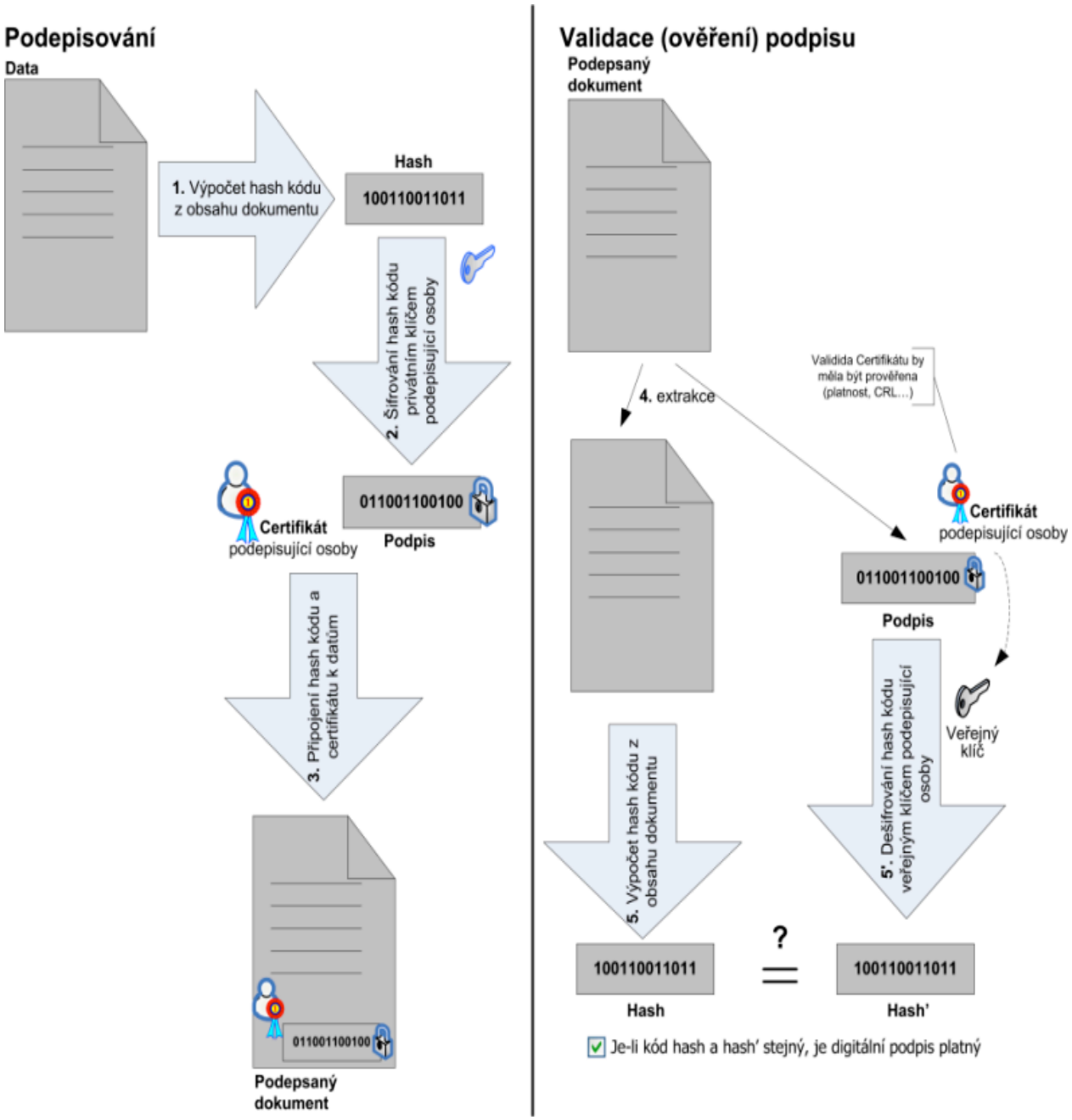
5.2 Podpis a ověření (validace) podpisu

Software využívá nejmodernější kryptografické metody pro zajištění bezpečnosti DBP včetně unikátního řešení s využitím kombinace aplikace asymetrické kryptografie a biometrického vektoru.

- **Biometrický vektor** je připojen k dokumentu v šifrované podobě pomocí mezinárodně uznávané symetrické šifry AES256 (dodnes není znám případ prolomení). SW automaticky implementuje silnější šifry dle aktuálního vývoje na poli kryptografie).
- **Integrita dokumentu** je zajištěna pomocí asymetrické kryptografie. Hash dokumentu je šifrován privátním klíčem banky, tento klíč je přístupný pouze z podpisového serveru.
- **Algoritmus RSA 2048** doposud neprolomený algoritmus asymetrické kryptografie (číslo o 617 cifrách, síla algoritmu je založena na nalezení dvou prvočísel, jejichž násobek je dané číslo). Nejvyšší prolomené číslo je RSA-768, tj. číslo o 232 cifrách.
- **Přidání časového razítka** z nezávislého časového serveru, slouží jako další záruka integrity dokumentu (založeno opět RSA).

► Podpis Digitálního dokumentu musí zajistit:

- Jednoznačnost spojení s podepisující osobou
- Identifikaci podepisující osoby k datové zprávě
- Vytvořen a připojen prostředky jež může podepisující osoba udržet pod svou výlučnou kontrolou
- Zajištění integrity dokumentu



Obrázek 27: podpis a ověření (validace)

5.3 Náklady a úspory ve stávajícím procesu

Při stávajícím procesu uzavírání smlouvy, dodatku, pojištění, ověření zákazníka, objednávky a samotného převzetí zboží nám rostou náklady související s oběhem dokumentu v papírové podobě. Tyto náklady se nám projevují v níže uvedených oblastech. A to především:

- náklady na papírové formuláře,
- nízké nasazení mobilních řešení,
- náklady na údržbu řešení:
    - Poruchovost tiskáren (teplotní výkyvy apod.),
    - Vysoké náklady na údržbu (tonery, náhradní díly apod.),
- náklady na sběr dokumentů – zasílání na centrálu,
    - Poštovné, manuální zpracování, archiv,
- náklady na manuální zpracování dokumentů,
- časové hledisko zpracování,
    - Čas zpracování (Agent – Centrála – Backend),
    - Aktivace smlouvy klientem,
    - Vyplacení provize agentovi.

Je zcela zřejmé, že se jedná o vysokou nákladovost spojenou s papírovou formou, která si vyžaduje zajištění vysokého objemu samotného kancelářského papíru, tak i zajištění samotných zařízení k tisku, jejich bezproblémového fungování a v neposlední řadě i uchovávání zpracovaných dokumentů k případné reklamaci.

5.4 Navrhované řešení a vyčíslení úspor při zavedení technologie DBP do firemního procesu

Ukažme si, co vše očekává společnost, která se rozhodné implementovat technologii zvanou „Dynamický biometrický podpis“ do svých podnikových procesů. Budou to především níže uvedené benefity ve formě snížení nákladů za kancelářský papír, navazující podnikové procesy s ním spojeny, ale také komfortnost pro zákazníka při podepisování samotných obchodních smluv.

5.4.1 Benefity ve formě úspor

Hlavní výhody jsou:

- snížení počtu papírových smluv, předávacích dokumentů, dodatků,
- žádné svážení smluvních papírových dokumentů z poboček (např. 1x týdně),
- snížení počtu tiskáren a s nimi spojená správa tiskového řešení, doplňování tonerů servis tiskového řešení…,
- vytěžování podepsaných smluv a dokumentů automaticky, integrace do BO snížení lidských zásahů a přepisování smluv a změn do interních systémů,
- snížení pracnosti na BO (případně snížení počtu FTE),
- snížení chybovosti,
- kontrola Fraudu, nemožnost oklamat a zvalidovat podpis již jednou podepsané osoby. (biometrická databáze podpisů v rámci klienta),
- validace uživatele oproti podpisovému vzoru přímo SW, nikoli pouze pohledem zaměstnance,
- kontrola interních zaměstnanců a externích partnerů - nedokáží vyměnit stránku za stránku, dokument je podepsán jako celek (pokud je požadováno),
- snížení archivace dokumentů atd.

5.4.2 Informace potřebné pro hrubý odhad řešení

Než se vůbec subjekt, který zvažuje zařadit do svých procesů výše uvedenou technologii pro ni rozhodné, měl by si dokázat zodpovědět níže uvedené ekonomické otázky. Ty mu přinesou potřebné informace pro hrubý odhad řešení.

Otázky potřebné pro hrubý odhad:

- Jaký je počet podepisovacích míst?
- Je požadovaná validace podpisových vzorů? V případě že ano, jaký je počet podpisových vzorů/profilů?
- Je požadovaný převod dokumentů do PDF/A?
- Je požadovaná integrace s časovým serverem třetí strany?
- Je požadovaná detailní analýza a návrh změny procesů pro digitalizaci a zavedení dynamického biometrického podpisu?
- Jaké je požadované HW vybavení na koncová místa (tablet PC, tablet, podepisovací zařízení, podepisovací zařízení s větším mírou bezpečnosti, monitor vhodný pro podpis, podpisový tablet s možností akceptováním platební karty apod.)?
- Jaké jsou požadavky na řešení, např. zobrazení celého dokumentu na koncovém zařízení, prezentace reklamy apod.
- Jaká je požadovaná integrace do prostředí zákazníka (DMS, BPM, Siebel, SAP, přizpůsobení obrazovek apod.)?
- Jaké jsou další požadavky na řešení ze strany zákazníka?

Pokud jsme si shromáždili potřebná data k zodpovězení otázek, můžeme si provést kalkulaci pro danou pobočku společnosti. Určitě vyvstane otázka, proč jen implementovat DBP na svou pobočku a ne rovnou do všech provozních systémů společnosti. Řešení je jednoduché. Je to z důvodu otestování si zavedené technologie do podnikových procesů a to ve vztahu k zaměstnancům, ale i také a to především k zákazníkům. Ti se budou setkávat se zavedenou technologií a měla by vyhovovat všem věkovým skupinám. Všeobecně je známo, že lidé si pomalu zvykají či přijímají něco nového. V případě, že by došlo k negativnímu přístupu, postoji ze strany zákazníku k zavedení nové podnikové technologie, nebude to mít tak výrazný ekonomický dopad, jako v případě implementace do celé společnosti.

5.4.3 Kalkulace pobočky

TCO propočet kalkulace návratnosti investice Pobočková síť

Nákladová položka	rok 1	rok 2	rok 3	rok 4	rok 5
Tisk	132000	132000	132000	132000	132000
Rozdělit dokumenty dle počtu tisku (tisk 1x, 2x, 3x)					
1x počet stran					
2x počet stran	303600	303600	303600	303600	303600
3x počet stran					
Rozdělit dokumenty dle tipu nákladů (interní - externí)					
interní					
externí					
Doplnit náklady na pořízení dokumentu - dovoz/rozvoz					
	320000	320000	320000	320000	320000
Tisk formulářů a kdo dané náklady hradí					
středisko (marketing, obchod, operation)					
Náklady na svoz dokumentů z externí sítě	4080000	4080000	4080000	4080000	4080000
počet svozů týdně / měsíčně / půlročně	8160000	8160000	8160000	8160000	8160000
Náklady na svoz dokumentů z interní sítě	2760000	2760000	2760000	2760000	2760000
počet svozů týdně / měsíčně / půlročně	5520000	5520000	5520000	5520000	5520000
Skenování					
Skenery / KAC - Maintenance	130000	130000	130000	130000	130000
Doplnit Maintenance HW	450000	450000	450000	450000	450000
Doplnit Maintenance SW	200000	200000	200000	200000	200000
Doplnit náklady na provoz skenovny - SLA smlouvy a pod	1200000	1200000	1200000	1200000	1200000
Fyzická archivace					
Manipulace s dokumentem / per dokument	33000	33000	33000	33000	33000
Skartace dokumentu / dohledání dokumentu	78000	78000	78000	78000	78000
Skartace dokumentu / per Kg	20000	20000	20000	20000	20000
Jaké jsou okamžité náklady na skartaci	800000	800000	800000	800000	800000
Jaký je procentuální poměr dokumentů které jsou k okamžité skartaci a které k dlouhodobé skartaci					

Jaký je poměr pracovníků					
interních	1150800	1150800	1150800	1150800	1150800
externích					
Lidské zdroje					
Podatelna - kolik lidí / cena FTE	1972800	1972800	1972800	1972800	1972800
skenerovna	0	0	0	0	0
Validace	3452400	3452400	3452400	3452400	3452400
Přepisování informací do dalších systémů	920640	920640	920640	920640	920640
průměrná úspora se pohybuje od 76-95%					
Lidské zdroje					
Front Office	575400	575400	575400	575400	575400
Počet FTE / cena FTE / rok	4	4	4	4	4
	2301600	2301600	2301600	2301600	2301600
průměrná úspora 2 minuty na samotný akt podpisu per dokument bez počítání času chůze k tiskárně, následně manipulace s dokumentem					
Lidské zdroje					
Back Office	353460	353460	353460	353460	353460
Počet FTE / cena FTE	70	70	70	70	70
	24742200	24742200	24742200	24742200	24742200
CELKEM / SUMA v Kč	**51 755 040 Kč**	**51 755 040 Kč**	**51 755 040 Kč**	**51 755 040 Kč**	**51 755 040 Kč**
					258 775 200 Kč

Tabulka 1: TCO propočet kalkulace návratnosti investice Pobočková síť

5.4.4 Kalkulace D2D

TCO propočet kalkulace návratnosti investice D2D

Nákladová položka	rok 1	rok 2	rok 3	rok 4	rok 5
Tisk	132000	132000	132000	132000	132000
Rozdělit dokumenty dle počtu tisku (tisk 1x, 2x, 3x)					
1x počet stran					
2x počet stran	303600	303600	303600	303600	303600
3x počet stran					
Rozdělit dokumenty dle tipu nákladů (interní - externí)					
interní					
externí					
Doplnit náklady na pořízení dokumentu - dovoz/rozvoz					
	320000	320000	320000	320000	320000
Tisk formulářů a kdo dané náklady hradí					
středisko (marketing, obchod, operation)					
Náklady na svoz dokumentů z externí sítě	4080000	4080000	4080000	4080000	4080000
počet svozů týdně / měsíčně / půlročně	8160000	8160000	8160000	8160000	8160000
Náklady na svoz dokumentů z interní sítě	2760000	2760000	2760000	2760000	2760000
počet svozů týdně / měsíčně / půlročně	5520000	5520000	5520000	5520000	5520000
Skenování					
Skenery / KAC - Maintenance	130000	130000	130000	130000	130000
Doplnit Maintenance HW	450000	450000	450000	450000	450000
Doplnit Maintenance SW	200000	200000	200000	200000	200000
Doplnit náklady na provoz skenovny - SLA smlouvy a pod	1200000	1200000	1200000	1200000	1200000
Fyzická archivace					
Manipulace s dokumentem / per dokument	33000	33000	33000	33000	33000
Skartace dokumentu / dohledání dokumentu	78000	78000	78000	78000	78000
Skartace dokumentu / per Kg	20000	20000	20000	20000	20000
Jaké jsou okamžité náklady na skartaci	800000	800000	800000	800000	800000
Jaký je procentuální poměr dokumentů které jsou k okamžité skartaci a které k dlouhodobé skartaci					

Jaký je poměr pracovníků					
interních	1150800	1150800	1150800	1150800	1150800
externích					
Lidské zdroje					
Podatelna - kolik lidí / cena FTE	1972800	1972800	1972800	1972800	1972800
skenerovna	0	0	0	0	0
Validace	3452400	3452400	3452400	3452400	3452400
Přepisování informací do dalších systémů	920640	920640	920640	920640	920640
průměrná úspora se pohybuje od 76-95%					
Lidské zdroje					
Front Office	575400	575400	575400	575400	575400
Počet FTE / cena FTE / rok	4	4	4	4	4
	2301600	2301600	2301600	2301600	2301600
průměrná úspora 2 minuty na samostatný akt podpisu per dokument bez počítání času chůze k tiskárně, následně manipulace s dokumentem					
Lidské zdroje					
Back Office	353460	353460	353460	353460	353460
Počet FTE / cena FTE	70	70	70	70	70
	24742200	24742200	24742200	24742200	24742200
CELKEM / SUMA v Kč	**51 755 040 Kč**	**51 755 040 Kč**	**51 755 040 Kč**	**51 755 040 Kč**	**51 755 040 Kč**
					258 775 200 Kč

Tabulka 2: TCO propočet kalkulace návratnosti investice D2D

5.4.5 Podatelna

Finální úspory na podatelně	rok 1	rok 2	rok 3	rok 4	rok 5	
Aktuální stav	493200	493200	493200	493200	493200	
Počet FTE	4	4	4	4	4	
Náklady na FTE / ROK	1972800	1972800	1972800	1972800	1972800	
Počet Externích pracovníků	0	0	0	0	0	
Náklady na Externí pracovníky / rok						
průměrná úspora se pohybuje okolo 80%						
CELKEM / SUMA v Kč	1972800	1972800	1972800	1972800	1972800	**9864000**

Tabulka 3: podatelna

5.4.6 Archivace a skartace dokumentů

Archivace a skartace dokumentů	rok 1	rok 2	rok 3	rok 4	rok 5	
Archivace dokumentů						
Fyzické uložení smlouvy						
Jednotková cena **x** počet ks (ks/kč/rok)						
Ad-hoc vyhledání dokumentu						
Jednotková cena **x** počet ks (ks/kč/dokument/rok)						
Vyhledání dokumentu ke skartaci						
Jednotková cena **x** počet ks (ks/kč/dokument/rok)	33000	33000	33000	33000	33000	
Skartace						
Jednotková cena **x** počet ks (ks/kč/dokument/rok)	78000	78000	78000	78000	78000	
Uložení 3tí kopie						
Jednotková cena **x** počet ks (ks/kč/rok)						
Vyhledání 3tí kopie ke skartaci						
Jednotková cena **x** počet ks (ks/kč/úložná jednotka/rok)						
skartace 3tí kopie						
Jednotková cena **x** počet ks (ks/kč/dokument/rok)						
průměrná úspora se pohybuje okolo 80%						
CELKEM / SUMA v Kč	111000	111000	111000	111000	111000	**550000**

Tabulka 4: archivace a skartace

5.4.7 Využití Dynamického Biometrického podpisu

Po implementaci dynamického biometrického podpisu můžeme očekávat úspory nákladů ve formě:

- výrazného snížení nákladů na papírový tisk,
- minimálních provozních nákladů na tiskárny (vypuštění většiny tiskáren z procesů),
- automatické integrace s backend systémy,
- zrychlení času zpracování smluv v interních systémem ON-LINE / OFF-LINE po replikaci,
- el. Archivu / snížení nákladů na fyzický archiv,
- možnosti využití POS + biometrika
    - aktivace smlouvy klientem po zaplacení,
    - rychlejší odměňování / motivace agentů,
- X - Up sell.

Úspora nákladů - na tisk, kopírování, skenování, distribuci a archivaci dokumentů. Průměrná úspora 25 Kč na dokument.

Rychlá návratnost investic - průměrně se investice vrací do 12 měsíců po zavedení řešení.

Úspora času - výrazné zrychlení obchodních a interních procesů.

Vlastnoruční podepisování elektronických dokumentů - možnost vlastnoručního podepisování různých typů elektronických dokumentů s využitím stejného zabezpečení elektronických dokumentu, jaké je požadováno pro elektronické podepisování. Pomocí našeho řešení můžete podepisovat žádosti, nabídky, objednávky, smlouvy, faktury, výkazy apod.

Rychlé nasazení a snadná integrace - naše řešení nabízí snadnou integraci se stávajícími informačními systémy, firemními dokumenty a firemními procesy.

Zvýšení bezpečnosti - dokumentů a procesů.

Uznatelnost - naše řešení pro podepisování elektronických dokumentů odpovídá legislativním požadavkům, které jsou na elektronické podepisování kladená v právním prostředí ČR i EU.

Ekologie - řešení přispívá k šetrnějšímu využívání přírodních zdrojů a energií.

5.5 HW Zařízení

Podpisové charakteristiky

Pro snímání vlastnoručního podpisu můžeme použít zařízení, která jsou **schopná snímat biometrické** (zvykové) **charakteristiky**, které se promítají do psaného projevu a tedy i do podpisu.

Mezi tato zařízení patří:

- speciální podepisovací pady od výrobce Vacom, požívající se v kamenných pobočkách,

Obrázek 28: podepisovací pady výrobce Vacom

- interaktivní (perové) grafické tablety a kiosky,

Obrázek 29: interaktivní (perové) grafické tablety a kiosky

- tablety a chytré telefony – nejrozšířenější.

Obrázek 30: tablety a chytré telefony

Podpisový 14´´(A4) LCD tablet VPad 1400 (VPSign) - novinka

Obrázek 31: podpisový 14´´(A4) LCD tablet VPad 1400 (VPSign)

Špičkový barevný velkorozměrový (14´´) podpisový tablet z produkce společnosti VPSign umožňuje zobrazování dokumentů ve formátu A4. Na rozdíl od menších podpisových zařízení, které sejmutý podpis "odesílají" do dokumentu na počítač, nabízí VPad 1400 podepsání dokumentu tak, jak jsme zvyklí na papíře - podepisujeme se přímo do zobrazeného dokumentu (podpisového pole/polí) na bázi filozofie:

What You See is What You Sign!
Podepisujete to, co vidíte!

Larry Sinclair 1982

VPad 1400 je mimořádně vhodný k podepisování smluv (dokumentů) na přepážkách organizací - klient vidí, co podepisuje, a proto není třeba vybavovat pracoviště dalším monitorem, případně řešit otázku zamezení viditelnosti textu pro další osoby stojící za

klientem. Barevný displej VPad 1400 umožňuje "v mezičase" projekci obrazových reklamních sdělení - informace, loga apod.
Hlavní oblasti určení:

- bankovnictví a finanční služby (pojišťovnictví),
- telekomunikace,
- servisní organizace,
- státní správa - úřady,
- zdravotnictví,
- služby, organizace cestovního ruchu, obchodní sféra.

Klíčové vlastnosti VPad 1400:

- zobrazuje dokument v plné velikosti, ve vysokém rozlišení a barevně,
- pracuje v souladu s legislativou platnou pro oblast elektronického podpisu,
- zpracovává vícestránkové dokumenty s více podpisy generované libovolnou lokální Windows aplikací nebo centrálním serverem pomocí generátoru dokumentů-formulářů,
- zachycuje klíčové behaviorální biometrické charakteristiky podpisu,
- podpisový SW Wizard umožňuje efektivní tvorbu formulářů,
- je kompatibilní s PKI (Public Key Infrastructure),
- v mezičase umožňuje zobrazování reklamních ploch – dokumentů,
- je připojován k pracovní stanici přes standardní USB rozhraní,
- je snadno integrovatelný do provozních systémů organizace (ERP, CRM, apod.),
- má robustní odolnou konstrukci pro použití k masivnímu provozu.

Bezpečnostní folie se používají k zamezení čtení z Vašeho zařízení nezúčastněnou osobou, která je v jeho blízkosti. Speciální povrch omezuje nežádoucí pohledy okolí na displej, to vše zajistí čtyřvrstvý ochranný štít znemožňující vidět na displej ze stran.

Podpisový LCD tablet eSignio (Wacom STU-500)

Obrázek 32: podpisový LCD tablet eSignio (Wacom STU-500)

Osvědčený špičkový tablet zvláště vhodný pro použití na obchodních přepážkách, pokladních místech a k verifikaci platebních transakcí. Vysoce ostrý 5“ displej umožňuje zobrazení doplňujících informací relevantních pro probíhající podpisový proces (např. účel podpisu, co je podepisováno, podmínky a instrukce).

Základní technické parametry

Displej:

- monochromatický reflexní TFT LCD,
- rozměr - 10,2 x 7,6 cm (5"),
- maximální rozlišení - 640 x 480 pix.,
- pozorovací úhel (horizontální/vertikální) - 120°/120°,
- povrch snímače upravený tak, že podepisující má stejný pocit jako při psaní na papír,
- úprava displeje proti odlesku, temperování,
- zobrazení podpisu v reálném čase.

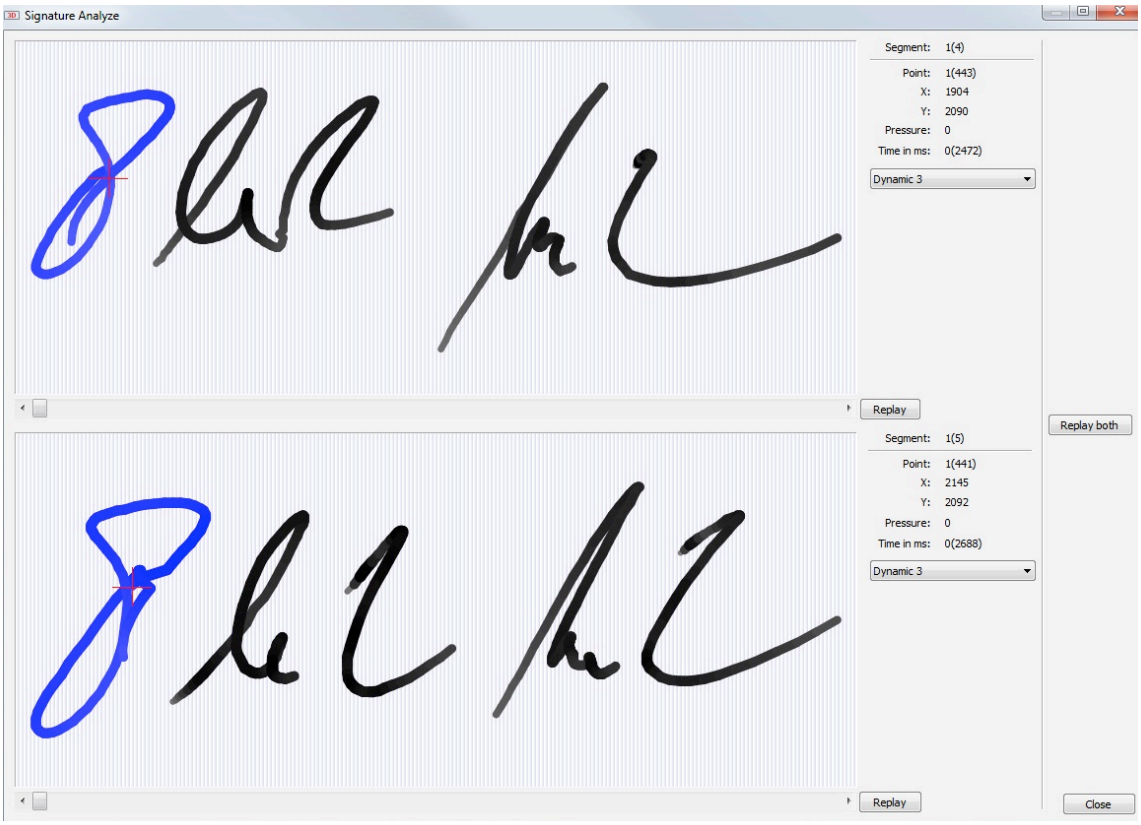
Pero a tablet:

- metoda snímání - elektromagnetická rezonance (EMR),
- 512 úrovní tlaku pera (neinterpolovaných),
- rozlišení 2,540 dpi,
- výška snímání 5mm,
- bezbateriové, bezdrátové pero,
- pero připojeno k tabletu pomocí provázku,
- přenosová rychlost snímání - 200 bodů/s (neinterpolovaných),
- integrované úložiště pro uložení pera,
- rozhraní - USB BUS power/sériově,
- napájení - prostřednictvím USB BUS power/ (volitelně AC adapter),
- stanovení, vyvolání a zrušení ikon na displeji,
- kabel USB 1,5m,
- spotřeba nižší než 1.0 W,
- provozní teplota 5° až 35°C,
- provozní vlhkost 20% až 80% RH,
- hmotnost 0,4 kg,
- rozměry tabletu 160.0 x 182,5 x 24,6 mm.

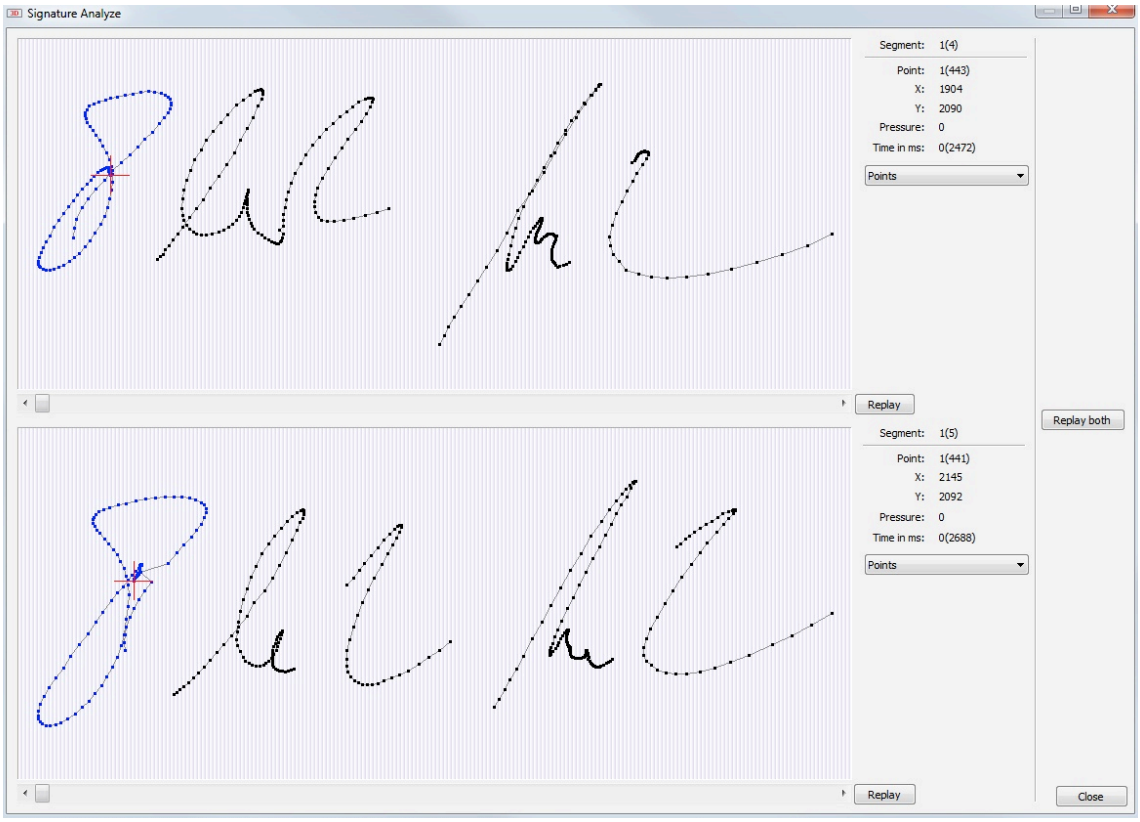
5.6 Analýza pravosti DBP

Pokud by pravost dynamických biometrických podpisů nemohla být zaručena, společnosti používající tuto technologii by pozbyly na věrohodnosti u svých klientů. Tudíž existuje nástroj, kam se může v případě pochybností ať ze strany klienta či ze strany společnosti nebo soudů obrátit. Tím to nástrojem jsou písmoznalci, kteří se zabývají zkoumáním pravosti elektronických biometrických podpisů, aby mohli vyhodnotit pravost DBP, používají software k vytvoření znaleckého posudku. Nejrozšířenější je Signotec eSig-analyze. Tím, že je každý podpis určen svými charakteristickými body tahu podpisu včetně dynamických prvků, může znalec provádět různá srovnávání, aby dosáhl jistoty v pravosti nebo ji znalecky vyloučil.

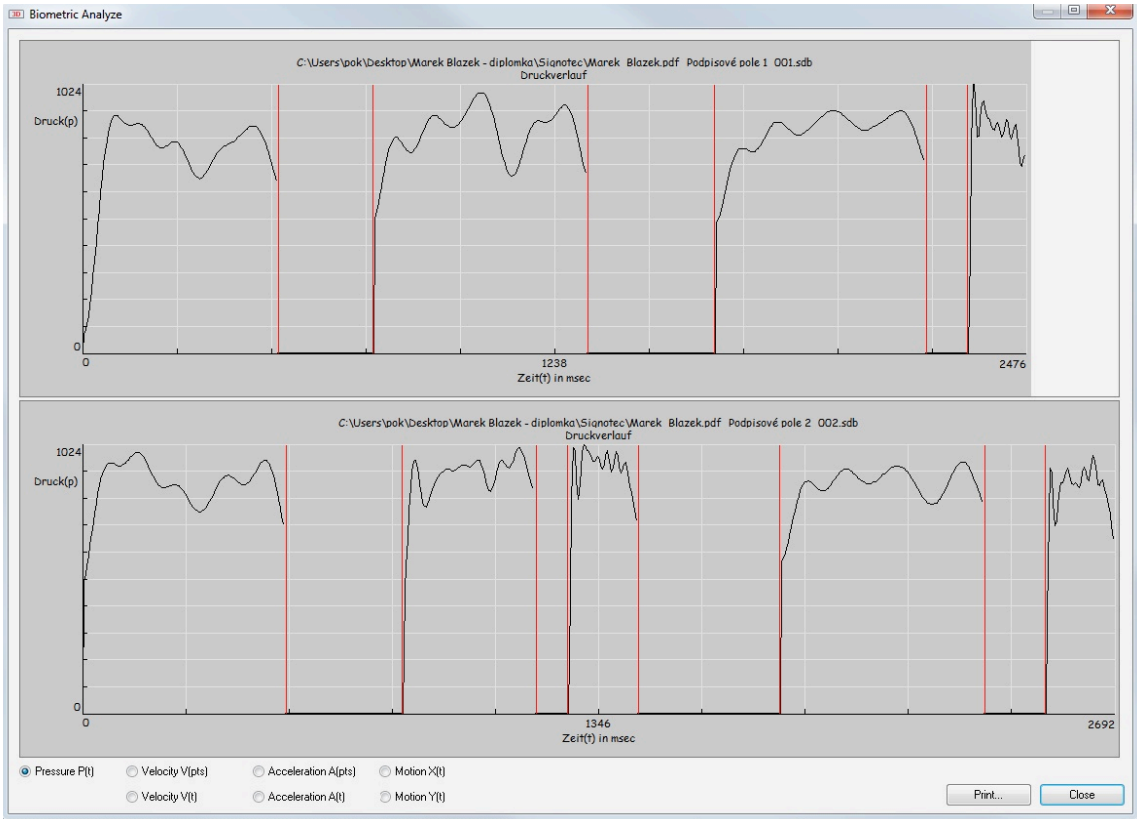
Pro potřeby simulace znaleckého zkoumání jsem oslovil znalce v oboru písmoznalectví pana Mgr. Jana Zimmera, s kterým jsem nasimuloval můj osobní podpis, který znázorňuje pouze grafické znázornění biometrických údajů a podrobil ho posudku dle dynamických znaků.



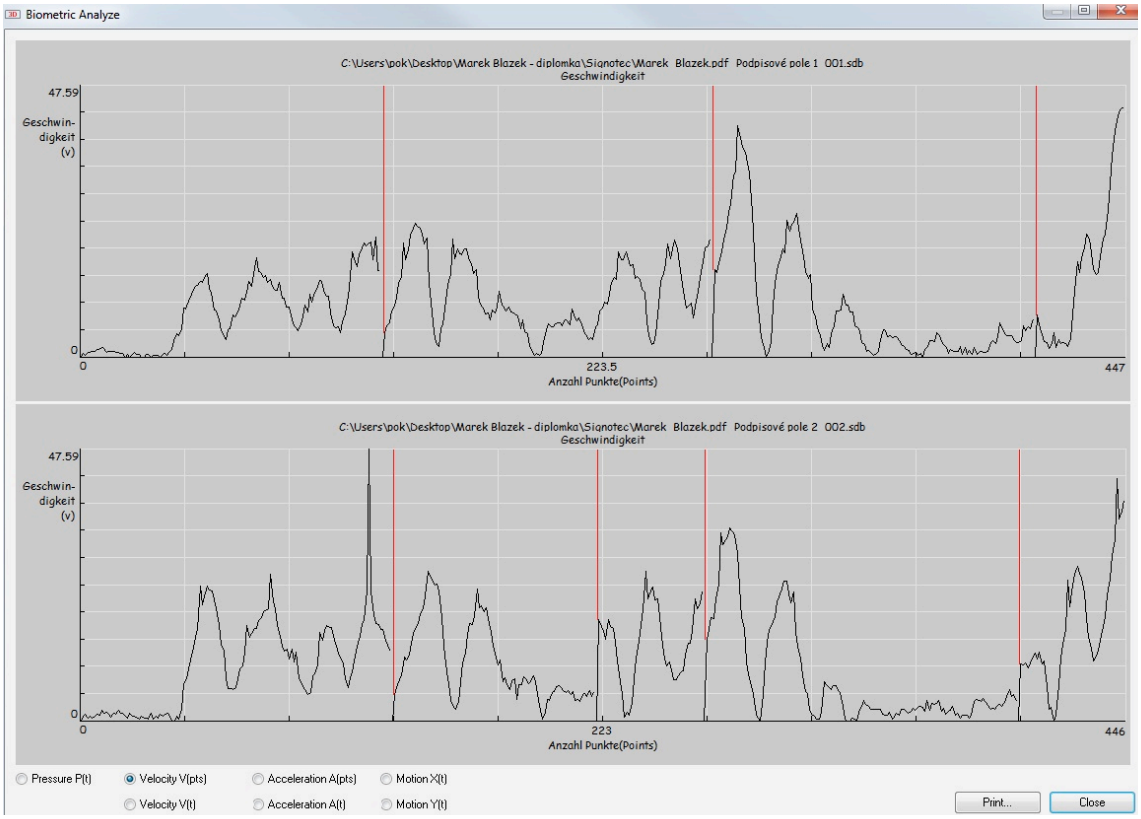
Obrázek 33: zdroj: vlastní – dva stejné podpisy od jedné osoby



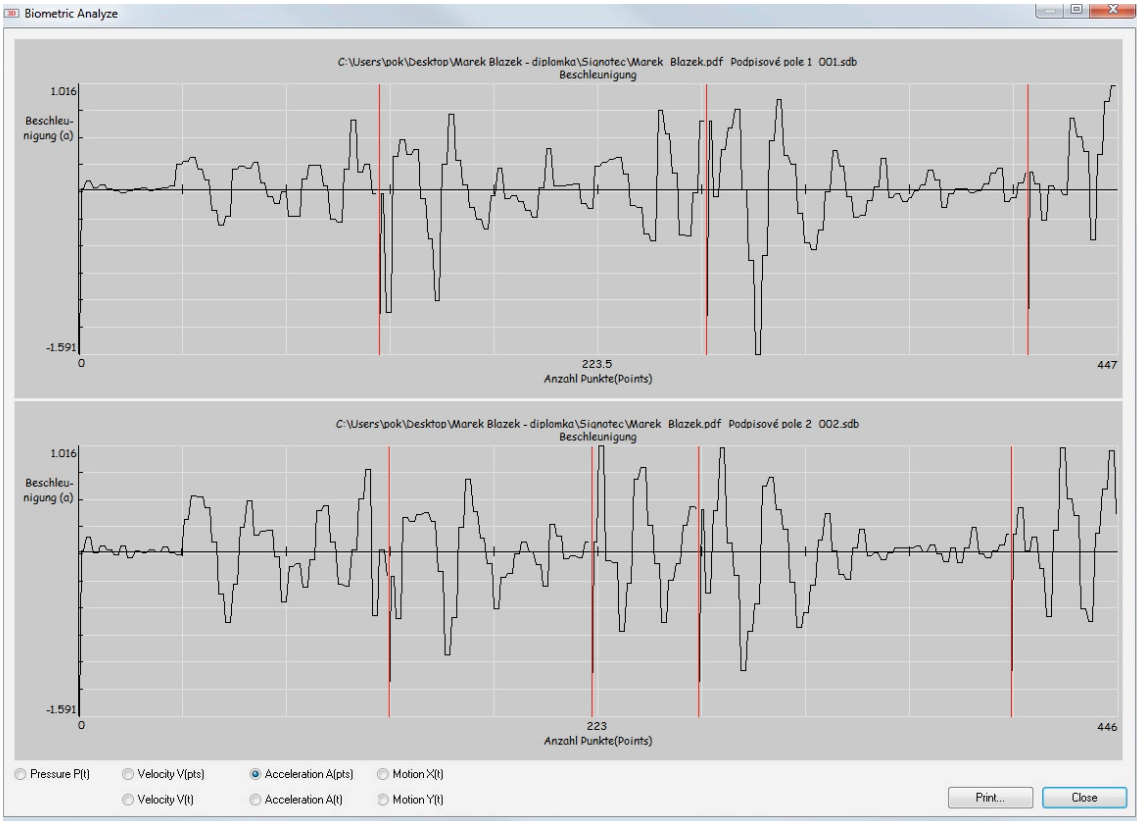
Obrázek 34: zdroj: vlastní – dva stejné podpisy od jedné osoby v bodovém znázornění



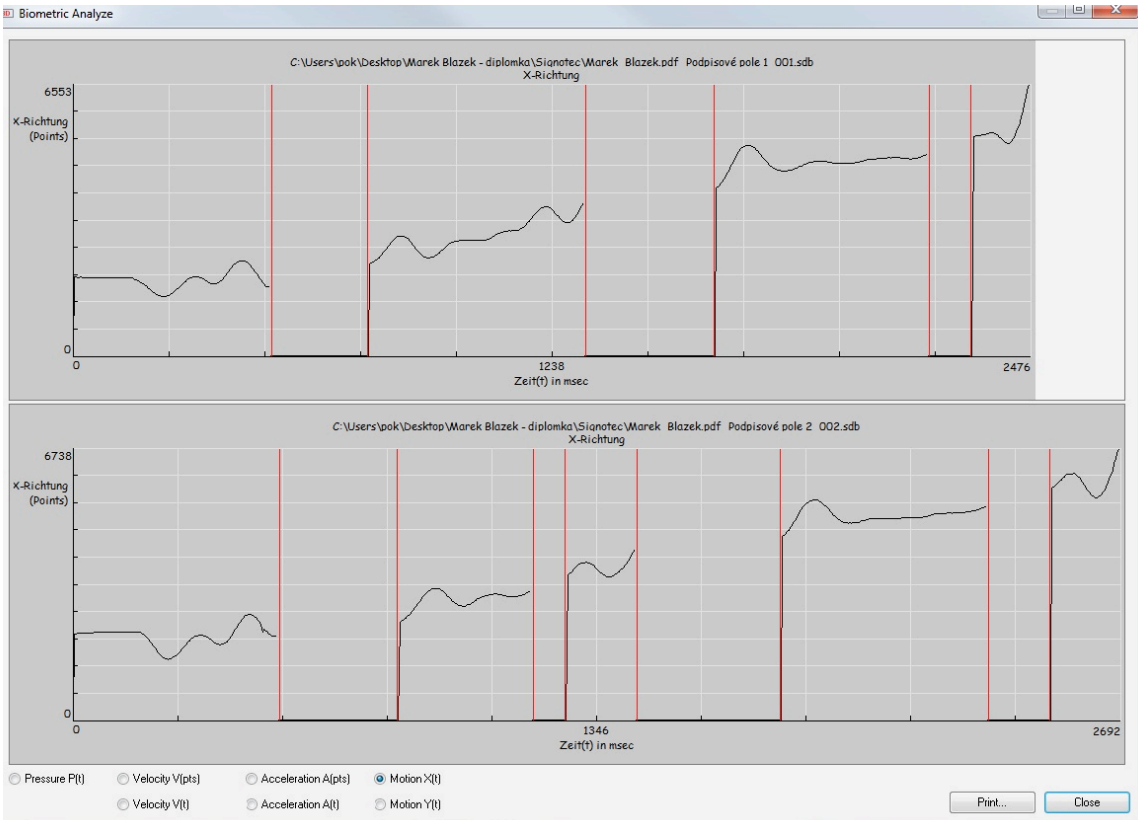
Obrázek 35: zdroj: vlastní - graf průběhu intenzity tlaku při podepisování



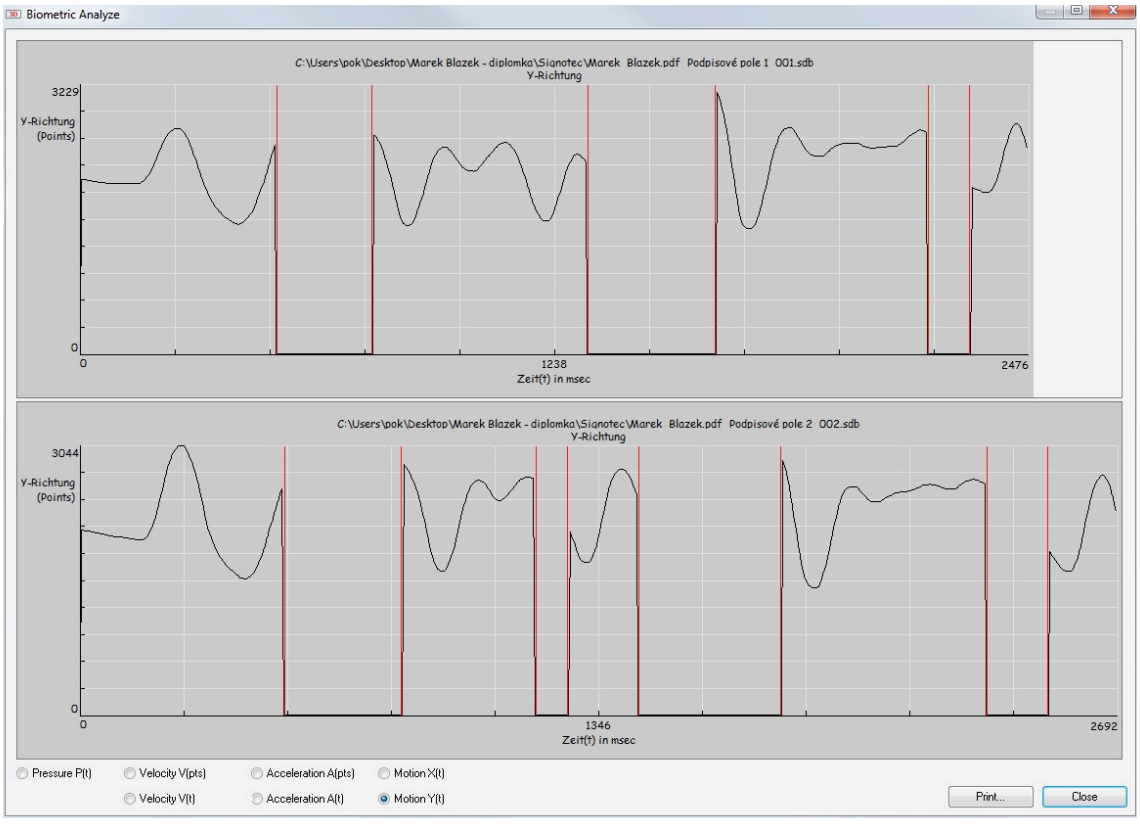
Obrázek 36: zdroj: vlastní - graf průběhu rychlosti podepisování



Obrázek 37: zdroj: vlastní - graf průběhu akcelerace podepisování

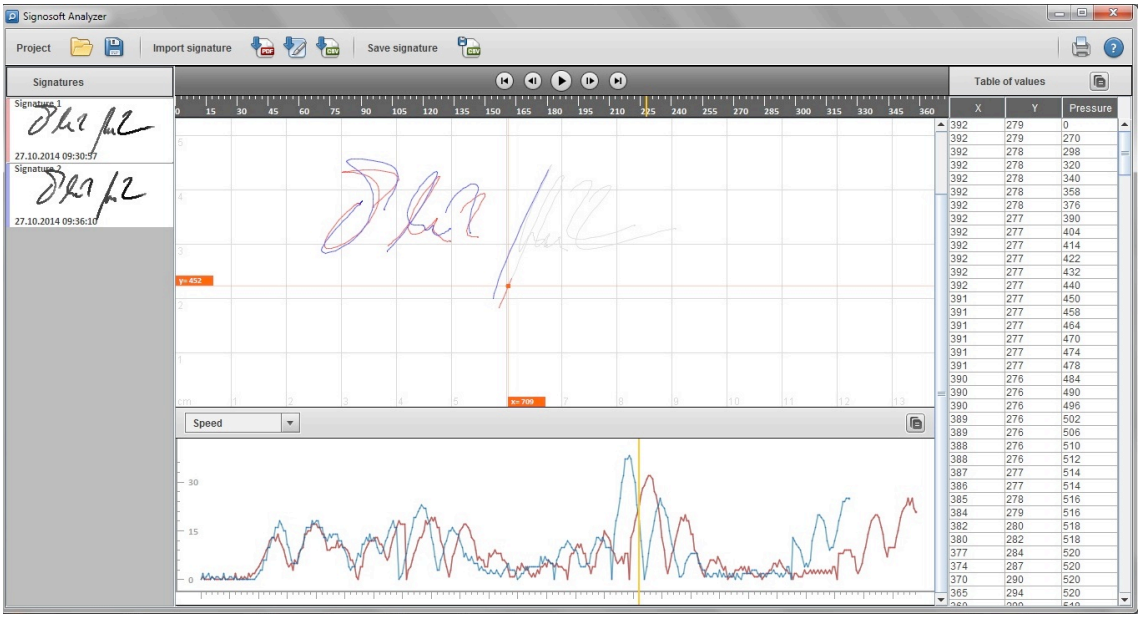


Obrázek 38: zdroj: vlastní - graf průběhu pohybu po ose X

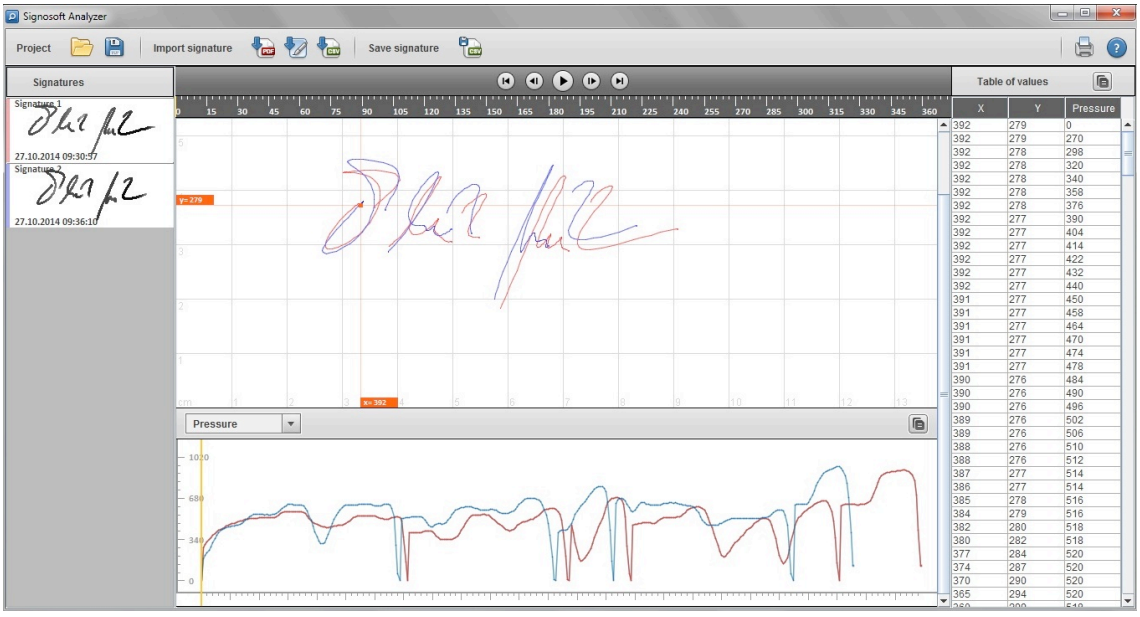


Obrázek 39: zdroj: vlastní - graf průběhu pohybu po ose Y

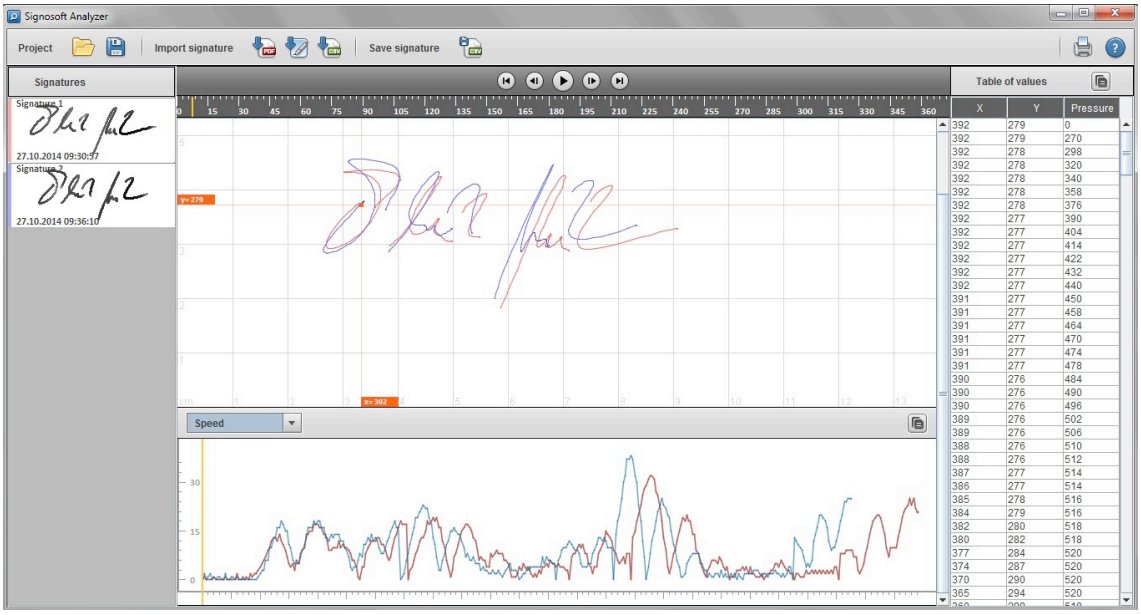
Abychom byli schopni výše uvedené grafy vytvořit, jsou čerpána z nepřeberného množství dat, na která je podpis rozložen. K znázornění můžeme využít MS Excel, který nám dokáže samotný podpis vygenerovat za pomoci software používaným znalci v oboru písmoznalectví.



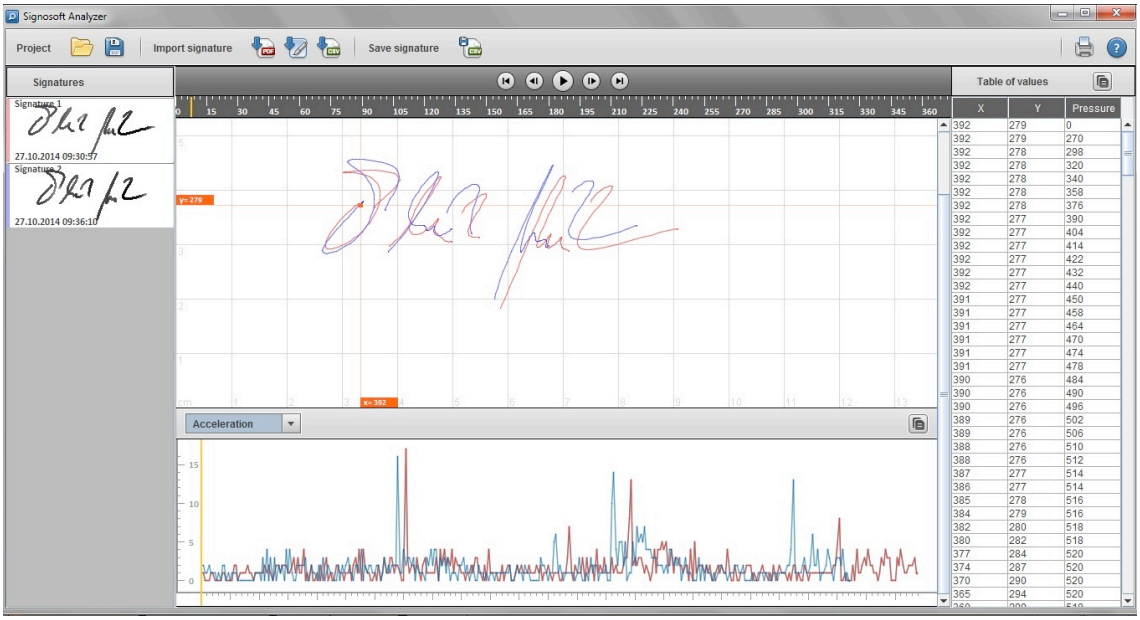
Obrázek 40: zdroj: vlastní - graf průběhu rychlosti podepisování s tabulkou hodnot



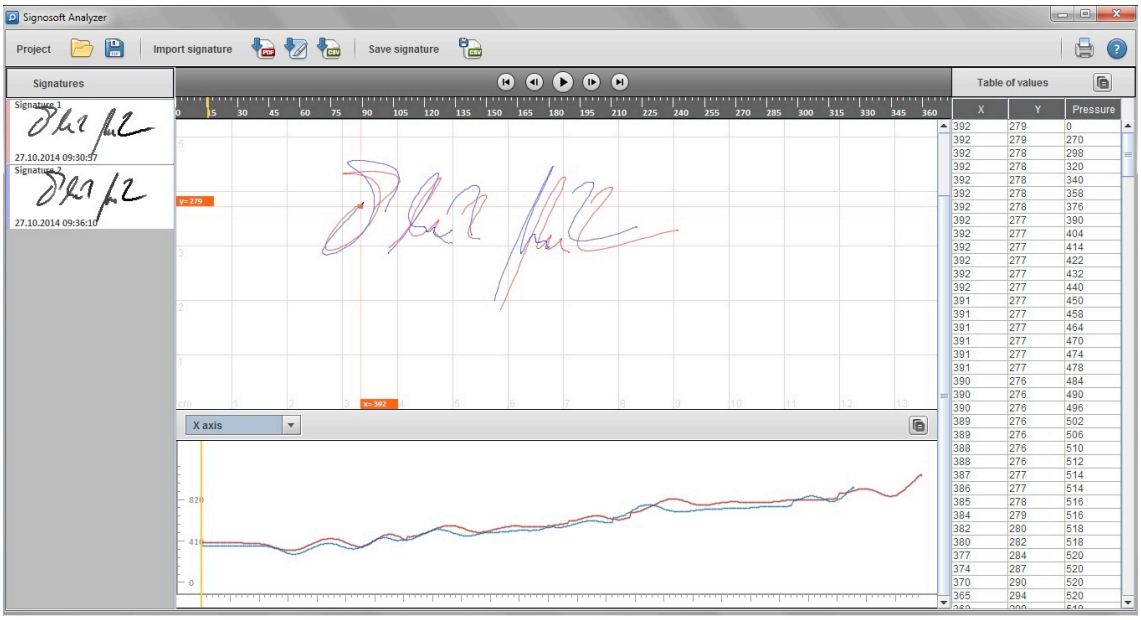
Obrázek 41: zdroj: vlastní - graf průběhu pohybu po ose Y s tabulkou hodnot



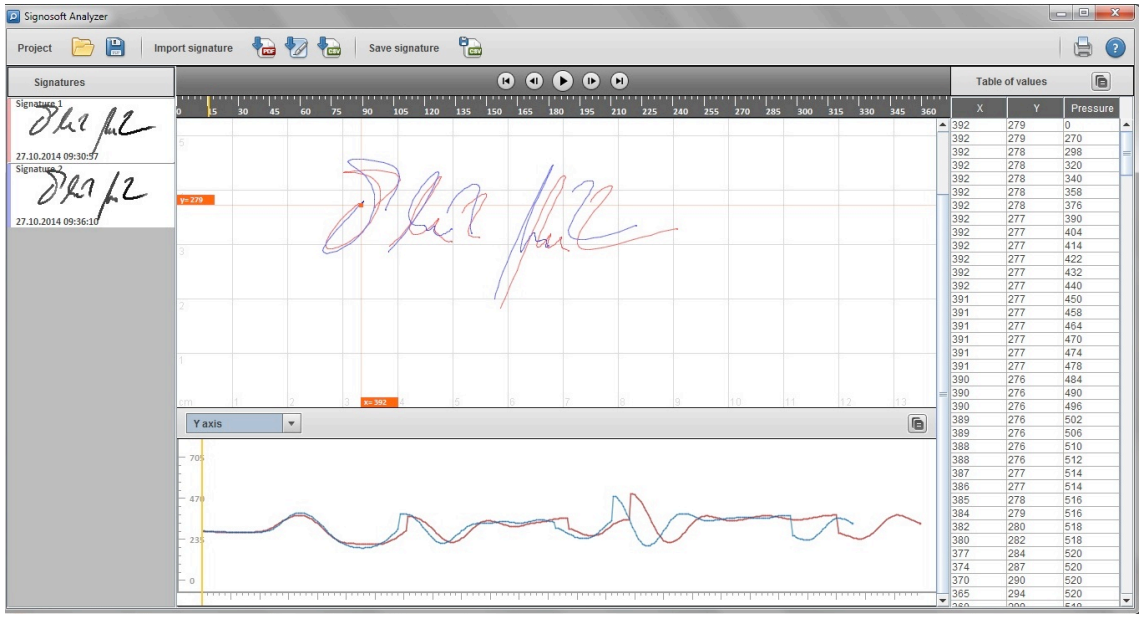
Obrázek 42: zdroj: vlastní - graf průběhu rychlosti podepisování s tabulkou hodnot



Obrázek 43: zdroj: vlastní - graf průběhu akcelerace podepisování s tabulkou hodnot

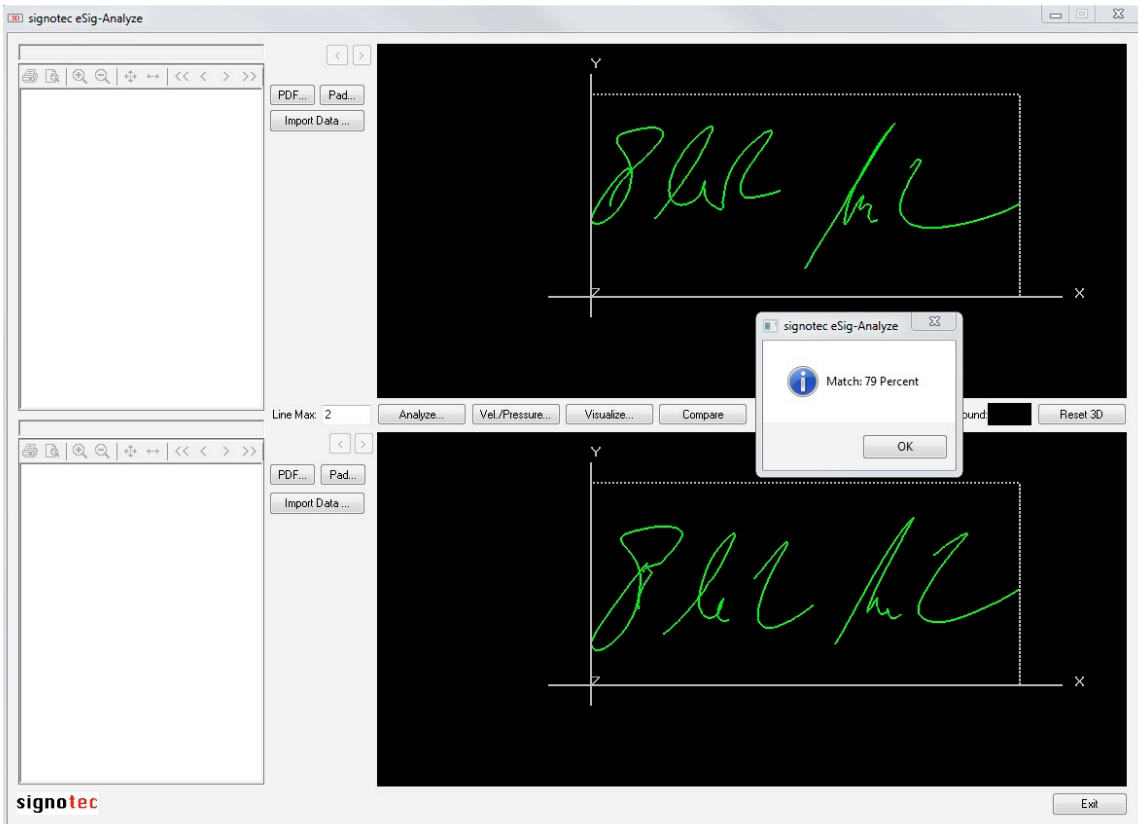


Obrázek 44: zdroj: vlastní - graf průběhu pohybu po ose X s tabulkou hodnot



Obrázek 45: zdroj: vlastní - graf průběhu pohybu po ose Y s tabulkou hodnot

Na obrázku níže je uvedeno srovnání dvou podpisů od jedné osoby s automatickým vyhodnocením shody na 79% pravosti. Vidíme, že podpisy nejsou zcela shodné, ale díky základním viditelným atributům či skrytým pro lidské oko daných technologií samotného ověřování došlo k výše uvedené shodě. Nabízí se otázka, proč není shoda 100%? Protože nikdo z nás se nedovede podepsat pokaždé absolutně stejně. Můžeme se maximálně přiblížit k hranci 90%, ale to jen ti, kteří se každý den podepisují a jsou tzv. vypsaní.



Obrázek 46: zdroj: vlastní – vyhodnocení pravosti dvou podpisů

5.7 Návrh řešení firmy SignoSoft

Využití dle SignoSoft[13]

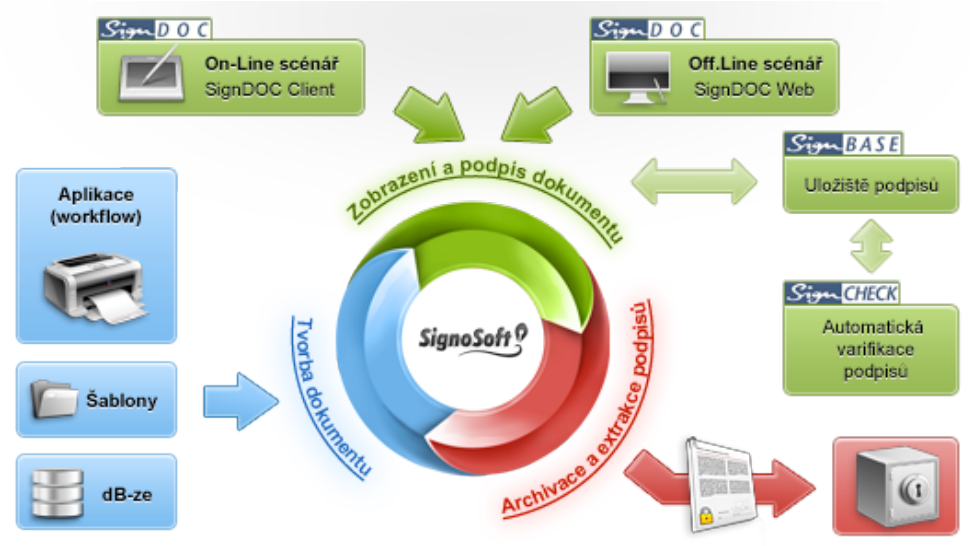
Biometrické charakteristiky

Řešení **SignoSoft** (vlastnoruční biometrický podpis) je možné využít všude, kde:

- podepisujete dokumenty při osobním jednání nebo v rámci jiného úkonu, při kterém jsou známé (ověřené) identity podepisujících se osob,
- chcete zrychlit a zjednodušit procesy,
- chcete zlevnit provoz a snížit náklady s ním související,
- chcete více zabezpečit dokumenty a informace v nich obsažené.

Všude, kde **chcete ušetřit provozní náklady** za:

- **tisk** podepisovaných dokumentů,
- **distribuci** podepsaných papírových dokumentů (poštovné a jiné doručovací a kurýrní služby),
- **kopírování, skenování** (indexování a vytěžování) podepsaných dokumentů,
- **skladování a archivaci** – papírových dokumentů.



Obrázek 47: zdroj http://signosoft.com

[13] SIGNOSOFT. *Signosoft-biometrické podpisy* [online]. 1998 - 2015 [cit. 2015-02-16]. Dostupné z: http://signosoft.com/index.html

Využití řešení SignoSoft v rámci některých odvětví:

- finanční sektor
    - **autentizace identity klienta** podle podpisu před vlastním provedením transakce metodou biometrické verifikace podpisu,
    - **automatizace** a **zrychlení procesů** – podepisování dokladů (žádosti, smlouvy, dodatky apod.),
    - zvýšení **zabezpečení proti zneužití** (zfalšování) podpisu,
    - zvýšení **zabezpečení integrity** dokumentu - nemožnost zfalšování informací uložených v dokumentu.
- obchodní sektor, služby a školy,
    - vlastnoruční podepisování různých typů elektronických dokumentů.
    - **automatizace** a **zrychlení procesů** – podepisování dokladů (žádosti, výdejky, předávací protokoly, referátníky, spisy, objednávky, faktury, smlouvy apod.),
    - zvýšení **zabezpečení integrity dokumentu** - nemožnost zfalšování informací uložených v dokumentu.
- zdravotnictví,
    - vlastnoruční podepisování elektronických dokumentů s citlivými a osobními údaji (např. neschopenky, lékařské zprávy),
    - vlastnoruční podepisování elektronických receptů,
    - zabezpečení integrity všech vlastnoručně podepsaných elektronických dokumentů,
- orgány státní správy (samosprávy) a soudy
    - využití biometrie pro interní ověřování podepisujících se osob,
    - na základě ověření podpisu provedení autentizace osoby a nastavení její autorizace – k podepsání dokumentu, nastavení přístupových práv do systémů, objektů apod.

Společnost SignoSoft má dvě varianty řešení vlastnoručních biometrických podpisů

Varianta A: Vlastnoruční podepsání elektronického dokumentu

Příprava PDF

V základním informačním systému se vygeneruje finální elektronický dokument (*.PDF) určený k podpisu. Tento PDF dokument je možné generovat z libovolných informačních systémů nebo aplikací – ERP, CRM, MS Office, HTML apod.

Vlastnoruční podpis

Vygenerované PDF se vlastnoručně podepíše pomocí speciálního podepisovacího zařízení (např. podpisového padu). Při podepisování na pad se snímají a zpracovávají biometrické (statické a dynamické) charakteristiky vlastnoručního podpisu (viz obrázek Biometrie podpisu).

Uložení a uzamčení

Během vložení vlastnoručního biometrického podpisu do dokumentu dojde k jeho elektronickému podepsání a tedy zabezpečení integrity dokumentu proti neoprávněné změně.

Sdílení

Uložený, elektronicky-biometricky podepsaný elektronický dokument je možné dále zpracovávat v rámci podnikových informačních systémů a systémů pro správu elektronických dokumentů a procesů.

Naše řešení je také možné použít pro uzavřené systémy (například bankovní sektor, zdravotnictví apod.), kde by se dalo využít nejen možnosti vlastnoručního podepisování

elektronických dokumentů, ale zároveň by se dalo využít vlastnosti ověřování vlastnoručního podpisu proti podpisovému vzoru. Tato vlastnost řešení nabízí zvýšení bezpečnosti v procesech, při kterých je potřeba ověřit, s pravděpodobností limitně se blížící 100 %, identitu nějaké osoby, která identitu předkládá a po jejím kladném ověření osobu autorizovat k další aktivitě - např. uzavření dodatku ke smlouvě.

Varianta B: Ověření vlastnoručního podpisu a podepsání elektronického dokumentu

Tvorba báze referenčních podpisů

V rámci jedné z komponent našeho řešení (SignArchive) dojde k vytvoření báze referenčních podpisů pro všechny uživatele (interní, externí apod.), kteří využívají služby uzavřeného systému. Tato báze se může v čase doplňovat o další referenční podpisy a standardně spravovat.

Příprava PDF

V základním informačním systému se vygeneruje finální elektronický dokument (*.PDF) určený k podpisu. Tento PDF dokument je možné generovat z libovolných informačních systémů nebo aplikací – ERP, CRM, MS Office, HTML apod.

Vlastnoruční podpis a ověření podpisu

Vygenerované PDF vlastnoručně podepisuje osoba, která o sobě tvrdí, že je např. osobou LM. Po zachycení jejího podpisu dojde v reálném čase k automatickému ověření tohoto podpisu proti referenční bázi a referenčnímu podpisu osoby LM, který je v ní uložený. Systém porovnává biometrické (statické a dynamické) charakteristiky podpisů. Pokud systém ověří zachycený podpis proti referenci, dochází k ověření (prokázání) identity osoby LM a systém osobu autorizuje k podepsání dokumentu.

Uložení a uzamčení

Během vložení vlastnoručního biometrického podpisu do dokumentu dojde k jeho elektronickému podepsání a tedy zabezpečení integrity dokumentu proti neoprávněné změně.

Sdílení

Uložený, vlastnoručně biometricky podepsaný elektronický dokument je možné dále zpracovávat v rámci podnikových informačních systémů a systémů pro správu elektronických dokumentů a procesů.

V případě, kdy jde o uzavřený systém a velmi kritické informace se takto podepsaný dokument (s ověřením podpisu proti referenci) může objevit např. v internetovém bankovnictví mezi uzavřenými smlouvami.

Řešení SignoSoft je zároveň integrováno s technologiemi a všemi (i bezpečnostními) standardy elektronických certifikátů a podpisů. To znamená, že řešení je primárně dodáváno a instalováno s vlastním elektronickým certifikátem. Při implementaci je ovšem možné SignoSoft integrovat s interně vytvořenou Public Key Infrastructure (PKI), která je postavená na vlastních (podnikových) elektronických certifikátech.

Řešení vlastnoručního biometrického podpisu může být také integrováno s kvalifikovanými elektronickými certifikáty vydanými kvalifikovaným poskytovatelem certifikačních služeb nebo akreditovaným poskytovatelem certifikačních služeb dle zákona č. 227/2000 Sb., zákon o elektronickém podpisu.

Z výše uvedeného vyplývá, že řešení SignoSoft je primárně dodáváno s elektronickým podpisem (EP), ale umožňuje využít i vlastností a specifikace, které nabízí zaručený elektronický podpis (ZEP) a uznávaný elektronický podpis (UEP), což dále rozšiřuje možnosti využití našeho řešení i v rámci orgánů veřejné moci (OVM).

5.8 **Konference**

AŽ 70 % velkých společností chce v příštích letech zavést biometrický podpis

13.03.2014

Dynamické biometrické podpisy SignoSoft přispívají k vyšší bezpečnosti dokumentů, zrychlují zpracování smluv, zvyšují komfort obsluhy zákazníků a firmám šetří náklady.

V následujících třech letech očekávají odborníci masivní nástup používání technologie biometrických podpisů, a to nejen v komerčním sektoru, ale i ve státní správě a samosprávě. Shodli se na tom účastníci odborné konference v hotelu Marriott, která hostila zástupce velkých firem, softwarových odborníků, soudních znalců a dalších specialistů. *„Můžeme říci, že zde nechybí zástupce žádného z oborů, kde se pracuje s velkým počtem klientů. Je to logické – rozumné firmy se v dnešní době orientují na dvě věci – úspory nákladů a vyšší komfort pro obchodníky i klienty. A to jsou přesně výhody, které biometrický podpis nabízí,“* konstatoval za organizátory **Jiří Mráz, generální ředitel největší české softwarové společnosti Unicorn Systems**. Unicorn využívá ve svých systémech technologii SignoSoft, kterou vyvinula společnost Pražská softwarová. Jedná se o nejrozšířenější řešení v oblasti biometrických podpisů na českém trhu, které používá například operátor O2. Řešení SignoSoft je založeno na světových standardech – využívá softwarové komponenty od německé společnosti Softpro a hardware (podepisovací tablety) od japonského výrobce Wacom.

Jak biometrický podpis funguje a proč je o tuto technologii rostoucí zájem? *„Toto řešení umožňuje vložit do elektronického dokumentu vlastnoruční digitální podpis, obsahující nejen obrázek podpisu, ale i jeho „skryté“ dynamické charakteristiky. Tím vznikne vlastnoručně podepsaný a zabezpečený elektronický dokument, který je po právní stránce rovnocenný s podepsaným dokumentem papírovým (s listinou). Je možné jej velmi snadno dále zpracovávat a uchovávat. A do dokumentu není možné neoprávněně zasahovat,“* přibližuje výhody řešení SignoSoft **Pavel Rousek, jednatel společnosti Pražská softwarová**. *„Vlastnoruční digitální podpis by měl postupně nahradit běžnou papírovou dokumentaci. Tímto krokem chceme zvýšit rychlost obsluhy, posílit bezpečnost smluv a díky*

poklesu objemu tisku také přispět k větší ochraně životního prostředí," uvedl na dnešní konferenci **Aleš Bernášek z O2, který zavádění této technologie ve společnosti řídí**. *„Výhodou tohoto řešení je nejen pohodlí pro zákazníky a nižší výdaje, ale i to, že celý proces zpracování dokumentů se výrazně zrychlí. Ocenili jsme i rychlé nasazení a snadnou integraci do našich interních procesů,“* konstatoval na dnešní konferenci **Santiago Uriel Arias ze španělské konfederace spořitelen CECA**, která sdružuje 12 institucí s 20 tisíci pobočkami a toto „bezpapírové“ řešení na bázi biometrických podpisů je největší v Evropě. *„Fakt, že jsme se dokázali v podstatě zbavit ručně podepsaných smluv, pokynů a dokumentů mimo jiné znamená o miliardu papírů ročně méně, což je 6750 tun papíru, neboli 28 Airbusů A380 plně naložených papírem a mimo jiné ušetření 10 km2 lesa každý rok. Úsporu času jsme vyčíslili na plných 45 tisíc hodin práce. V konečném důsledku se jedná o úsporu 40 milionů eur každý rok a investici s návratností 9 měsíců,“* doplnil Uriel.

Právní pohled na biometrické podpisy prezentoval na konferenci **Vladimír Smejkal, přední soudní znalec z oboru počítačového práva**. *„Evropské i naší legislativě dynamický biometrický podpis naprosto vyhovuje a já vidím obrovský potenciál jeho zavedení také do státní správy a samosprávy. Jeho zavedení by odstranilo stávající problémy se složitějším používáním elektronického kryptografického podpisu a jeho certifikáty s omezenou dobou platnosti. To bych považoval za jeden ze zásadních kroků k e-govermentu,“* konstatoval. Bezpečnost biometrických dat a vlastnoručních podpisů komentoval na konferenci **Jindřich Kodl, soudní znalec z oboru bezpečnosti informačních systémů** a další odborný pohled poskytl i **Jan Zimmer, soudní znalec z oboru písmoznalectví**: *"Zkoumaný podpis si můžeme i s odstupem času přehrát jako zpomalený film. To je velmi užitečná funkce pro hodnocení posloupnosti psacích tahů, pro hodnocení směru a rychlosti psacího pohybu. V tomto ohledu poskytují biometrické podpisy více spolehlivých informací pro zkoumání pravosti, než klasické podpisy psané na papír, u kterých bývá obtížné takové informace spolehlivě zjistit.“* zdůraznil J. Zimmer

„Naše zkušenosti ukazují, že tyto technologie se v současné době chystá zavést většina velkých českých firem. Tomu napomáhá i velký nástup tabletů. Důkazem zájmu je ostatně i dnešní konference, které se účastní přes 100 velkých českých firem z nejrůznějších oborů. Na papíry musíte čekat, mohou být poškozeny, zničeny, falšovány nebo se ztratí. Musíte je seřadit, chránit, skladovat a zabezpečit. To všechno zdržuje obchod, snižuje komfort prodejců i zákazníků a stojí velké peníze,“ shrnul Rousek. Zdůraznil, že z hlediska rozvoje

biometrických podpisů je klíčové zapojení společnosti Unicorn Systems, největšího dodavatele informačních systémů a řešení v ČR.

Další trend v oblasti zvyšování efektivity a komfortu obchodních procesů komentoval Vladimír Sitta ze společnosti 3M: *„Naše společnost již dlouhodobě vnímá trend západních zemí k přechodu na elektronické dokumenty, které všem jejím uživatelům přináší komfort a úsporu času. Špičková technologie k automatickému získávání dat z osobních dokladů a ověření jejich pravosti pak do světa elektronických dokumentů vnáší navíc tak zásadní pojmy, jako bezpečnost a eliminace chyb. Jsme hrdí na to, že právě 3M z pozice globálního lídra v ID autentizaci, přináší tuto technologii bezpečnostních složek i do civilního sektoru v ČR."*

Dynamický biometrický podpis Místo tradičního podpisu na papír se zákazník podepíše na speciální podložku či tablet, který umí zachytit tlak i rychlost podpisu. Takto vytvořený podpis je neoddělitelně spojen s podepisovaným dokumentem. V okamžiku, kdy zákazník podpis dokončí, je dokument zabezpečen proti jakýmkoli dalším změnám. Podpisová data jsou v dokumentu uložena v zašifrované podobě a jsou tím chráněna proti možnému zneužití. Klíč pro dešifrování podpisových údajů je bezpečně uložen a je přístupný pouze pro potřeby znaleckého zkoumání. Podpis se samostatně nikde neuchovává. Zákazník tedy nemusí mít strach, že by mohl být zneužit.

Legislativa

Z hlediska legislativy je dynamický biometrický podpis akceptován se stejnou právní validitou jako doposud používaná jediná varianta elektronického podpisu, a to s tajným a veřejným klíčem a kvalifikovaným certifikátem. Z hlediska komunitárního práva je určujícím předpisem Směrnice 1999/93/EC. Z hlediska českého práva je klíčovým zákon č.227/2000Sb., o elektronickém podpisu. Podle § 2 zákona jsou elektronickým podpisem "údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě" – což je definice, která zahrnuje i dynamický biometrický podpis. V souladu s novým občanským zákoníkem proto můžeme konstatovat, že při právním jednání učiněném elektronickými prostředky lze písemnost elektronicky podepsat i vlastnoručním dynamickým biometrickým podpisem.

5.9 O Unicorn Systems

Unicorn Systems je renomovaná evropská společnost poskytující ty největší informační systémy a řešení z oblasti informačních a komunikačních technologií. Dlouhodobě se soustředíme na vysokou přidanou hodnotu a konkurenční výhodu ve prospěch svých zákazníků. Působíme na trhu již od roku 1990 a za tu dobu vytvořili řadu špičkových a rozsáhlých řešení, která jsou rozšířena a užívána mezi těmi nejvýznamnějšími podniky z různých odvětví. Má ty nejlepší reference z oblasti bankovnictví, pojišťovnictví, telekomunikací, energetiky, průmyslu, obchodu i veřejného sektoru. Zákazníky jsou přední a největší firmy. Disponují detailními znalostmi z celého spektra podnikatelských odvětví. Rozumí principům jejich fungování, ale i specifickým potřebám svých zákazníků.
Rozsáhlé týmy systematicky vzdělávaných odborníků dokonale ovládají všechny v současnosti obvyklé produktové řady, komponenty, technologie, a proto nemají v podstatě žádná technologická omezení. Přestože při své práci uplatňují mnoho revolučních myšlenek, vlastní dodávky řešení podléhají osvědčeným kritériím – kvalita, kvantita, termín a cena.

5.10 Společnosti používající DBM

Obrázek 48: zdroj http://www.bezpecnypodpis.cz

Vlastnoruční digitální podpis existuje už několik let, šířit se ale začíná teprve nyní, a to zejména díky dostupnosti kvalitních koncových zařízení – speciálních podložek na podepisování či tabletů.

Využití najde v mnoha oblastech – ideální je například pro všechny prodejní organizace, které s klientem uzavírají smlouvy. Díky vyspělosti současných technologií ho mohou používat například i podomní obchodníci – krátce po podepsání dokumentů zákazník

obdrží e-mailem potvrzení o podepsaných dokumentech, a jím požadované služby jsou tak rychleji aktivovány.

5.10.1 V ČR je vlastnoruční digitální podpis používán

Mezi největší klienty, kteří vlastnoruční digitální podpis v široké míře využívají, patří společnost Telefónica Czech Republic. Ta jej nasadila ve svých vybraných značkových prodejnách, ale využívají ho také tzv. door-to-door obchodníci (podomní prodej).

Příklady společností využívajících vlastnoruční digitální podpis

Global Expert Česká republika

Finanční skupina Cetelem

T-Mobile Česká republika

Telefónica O2 Česká republika

Vodafone Česká republika

ORESI kuchyně

5.10.2 V zahraničí je vlastnoruční digitální podpis používán

SUNRISE (druhá největší telekomunikační společnost ve Švýcarsku)

Registr motorových vozidel v Bavorsku

IKEA (jeden z největších prodejců nábytku v Německu)

Berliner Sparkasse

Španělské konfederace spořitelen CECA

5.11 Implementace ve společnosti O 2

V roce 2013 byla realizována implementace e-Dokumentů na PC a Tabletech pro 1000+ uživatelů.

Cíl projektu

Zefektivnění stávajících postupů zpracování papírových smluv a dokumentů. Rychlejší obsluha zákazníků, posílení bezpečnosti smluv a snížení objemu tisku.

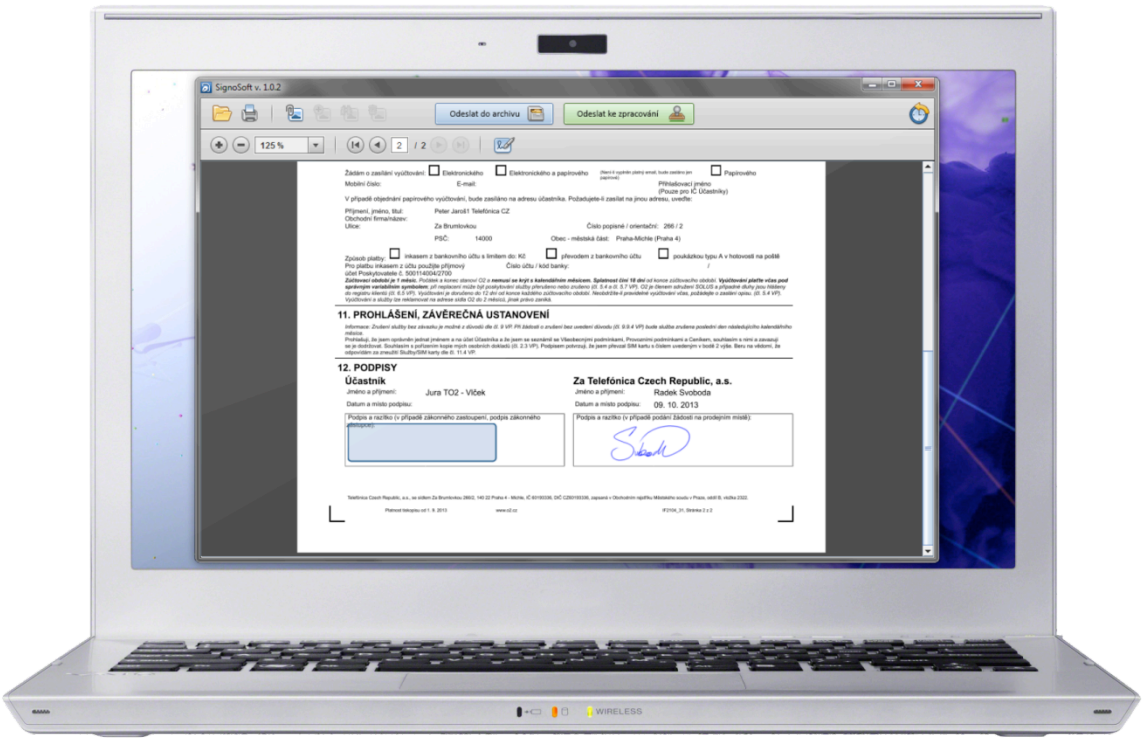
Obchodní přínosy a popis procesu:

Operátor O2 zavedl ve svých značkových prodejnách vlastnoruční digitální podpis. Ten nahrazuje běžnou papírovou dokumentaci. Tímto krokem chce společnost zvýšit rychlost obsluhy, posílit bezpečnost smluv a díky poklesu objemu tisku také přispět k větší ochraně životního prostředí. V ideálním případě úspora dosáhne 2,07 milionu listů A4, které se ve značkových prodejnách O2 ročně vytisknou.

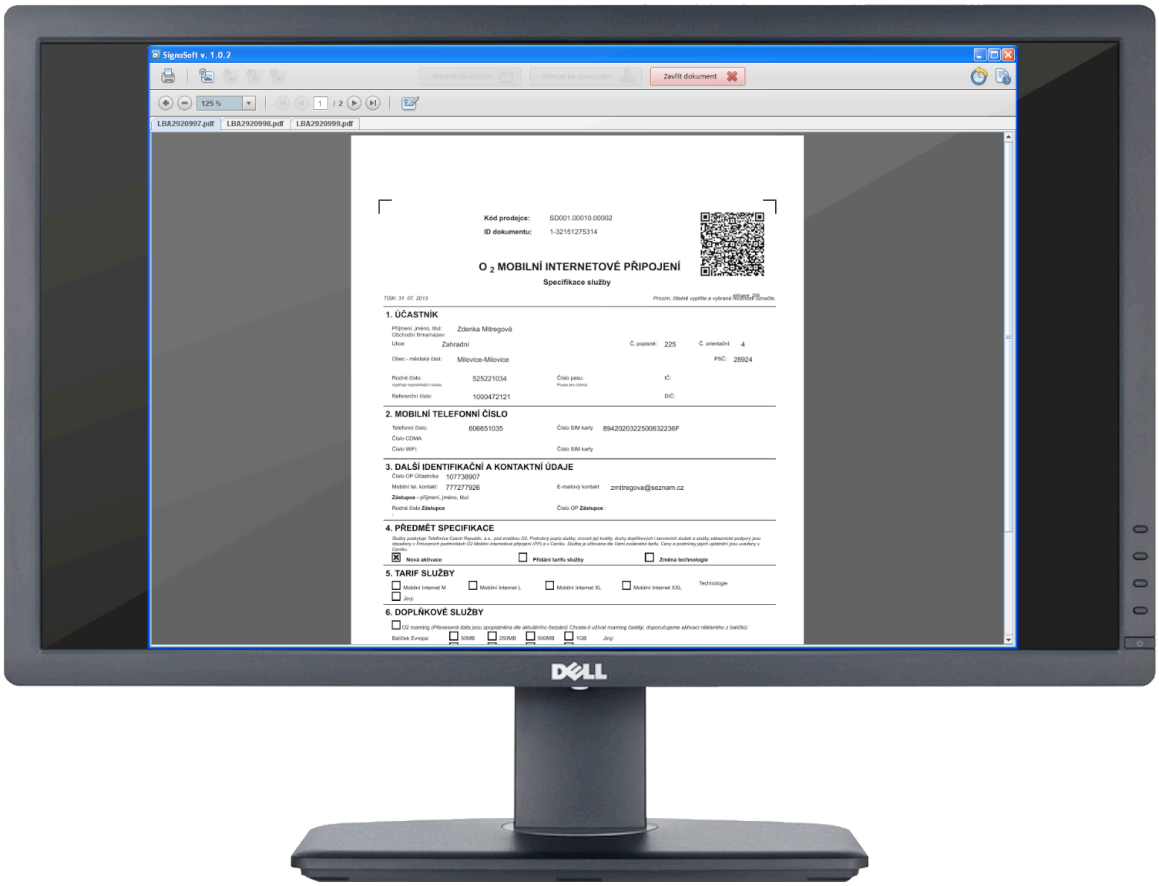
Zákazníci na celém procesu digitalizace jednoznačně vydělají. Už jen tím, že odpadne dlouhé čekání. Zatímco dnes se kvůli složitému papírování stávalo, že v případě uzavření smluv u externích partnerů zákazníci cekali na aktivaci čtyři dny, díky online přenosu na servery O2 se celý proces výrazně zrychlí.

Zde se můžete podívat na fotografie podpisové podložky (signpadu), která je nasazena na pobočkách O2 a na screenshoty aplikací SignoSoft na rozličných zařízeních.

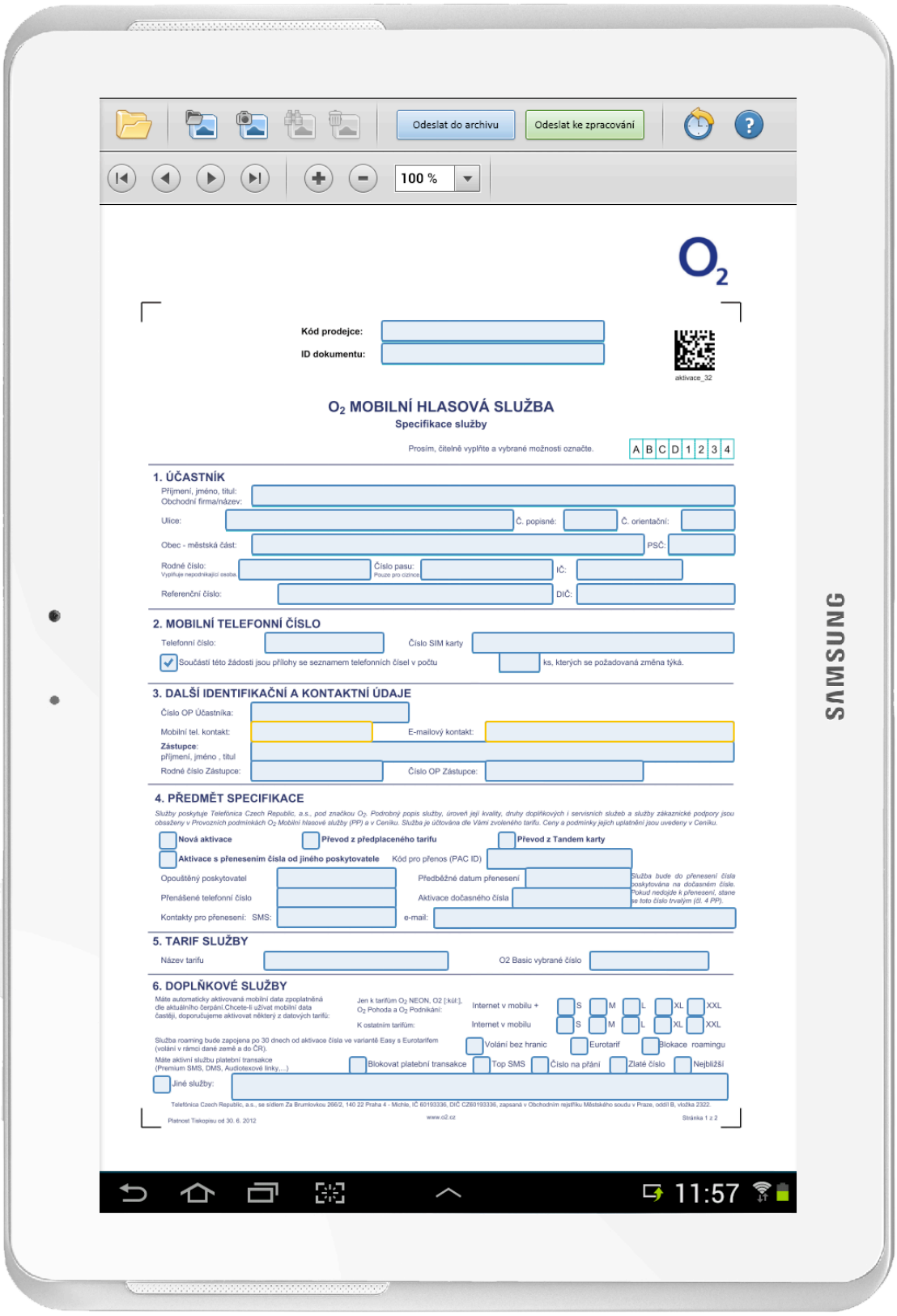
Obrázek 49: zdroj SignoSoft: Screenshot aplikace SignoSoft na speciálním podepisovacím padu



Obrázek 50: zdroj SignoSoft: Screenshot aplikace SignoSoft na notebooku



Obrázek 51: zdroj SignoSoft: Screenshot aplikace SignoSoft na monitoru pobočky



Obrázek 52: zdroj SignoSoft: Screenshot aplikace SignoSoft na tabletu Samsung – určeno k podomnímu prodeji

5.12 **Vodafone Czech Republic a.s.**

V září 2012 byla realizována implementace e-Dokumentů na PC pro 15 uživatelů.

Cíl projektu

V rámci pilotní provozu bylo cílem ověření reakce zákazníků v SMB segmentu a celkové zrychlení procesu uzavírání smluv.

Obchodní přínosy a popis procesu:

V praxi se také ověřilo, že zákazníci technologii biometrických podpisů přijímají pozitivně. Díky této technologii šetří partneři společnosti Vodafone Czech Republic čas svým zákazníkům tím, že nemusejí mít smlouvu dopředu vytištěnou, nebo pokud dojde na poslední chvíli k nějaké změně podmínek, lze vše upravit na místě a smlouvu i tak obratem podepsat, bez nutnosti ji znovu tisknout. Smlouva je poté zpracována rychleji, požadovaná služba může být aktivována v kratší době a zákazníci jsou spokojenější.

Byla použita aplikace SignoSoft na PC nebo noteboocích s OS Windows v kombinaci se podepisovacími tablety Wacom STU-300, 500 a 520.

Obrázek 53: zdroj SignoSoft - podepisovací tablety Wacom STU-500 a 520

5.13 Honeywell

V říjnu 2012 byla realizována implementace systému pro odbavování návštěv na PC pro 10 uživatelů.

Cíl projektu

Společnost Honeywell, mezinárodní koncern s bohatou a různorodou strukturou s obratem 37 miliard dolarů, využívá biometrické podepisování pro své řešení nasazované u třetích stran, které zrychluje a zjednodušuje odbavování návštěv na recepci.

Obchodní přínosy a popis procesu:

Řešení pro vlastnoruční biometrické podepisování SignoSoft umožnilo zrychlit a zjednodušit odbavení návštěv na recepcích budov. Návštěvníci se tak již nemusí podepisovat papírové knihy při udělování souhlasu s podmínkami pro vstup do objektu.

Řešení bylo realizováno pomocí SignoSoft Client (ActiveX a PDF&TIFF Converter) a použitý hardware je Wacom STU-500.

Obrázek 54: zdroj SignoSoft - podepisovací tablety Wacom STU-500

5.14 Credit Czech

V září 2013 byla realizována implementace systému pro 15 instalací na PC platformy.

Cíl projektu

Zefektivnění stávajících postupů zpracování papírových smluv a dokumentů, rychlejší obsluha zákazníků, posílení bezpečnosti smluv a snížení objemu tisku. Společnost CREDIT CZECH poskytuje komplexní služby v oblasti agenturního zaměstnávání.

Obchodní přínosy a popis procesu:

Cílem projektu bylo zavedení systému, který umožní podepisovat a uchovávat smlouvy v elektronické podobě bez nutnosti jejich tisku a následné papírové archivace. Proces podepisování byl implementován (včetně možnosti aktuálního zobrazení podepisovaného dokumentu klientovi bez náhledu do PC referenta na přepážce) přímo do zakázkového softwaru a zefektivnil tím práci referentuů na přepážkách.

V řešení byl použit SignoSoft Client (ActiveX a PDF&TIFF Converter), podepisovací tablety Wacom STU-500 (SignPad eSignio) a LCD LENOVO (jako druhý monitor). Zakázkový databázový software byl vyvíjený v Embarcadero RAD Studio a vše je provozováno na platformě Windows 7.

5.15 **Berliner Sparkasse**

Při otevření prvního účtu, polovina všech obyvatel Berlína věří stále ve spořitelny. Zákazníci a zaměstnanci jedné z největších německých spořitelen podepisují své dokumenty bez použití papíru a to pomocí SignPad eSignio SoftPro " software SignDoc a Adobe LiveCycle" s technologií zajišťující autentičnost a integritu elektronických dokumentů.

• Podpisy jsou digitalizovány v průběhu celého procesu psaní na displeji SignPad eSignio.

• SignDoc software propojuje zachycená data s podepsaným obsahem dokumentu.

Spolu s individuálními biometrickými charakteristikami podpisu je vytvořen " zaručený elektronický podpis". V průběhu podpisu se zaznamenává každá změna, je vytvořena hodnota integrity. Tato celistvá integrita a datový soubor jsou uloženy s podpisem a časovým razítkem do dokumentu pro budoucí ověření.

Obchodní přínosy a popis procesu:

Všude tam, kde je to možné, chce spořitelna snížit spotřebu papíru v jeho procesu. Proto je nutné zachytit vlastnoruční podpis a důvěryhodným způsobem ho vložit do procesu dokumentu spolehlivým způsobem, jak dosáhnout důkaz o dokazatelnosti.

Výhody

• větší důraz na spokojenost zákazníků s více času na konzultace namísto papírových workflow nabízet účinnou úlevu od rutinních úkolů,

• průchozí zpracování, takže neexistují žádné chyby vyplývající z převodu obsahu do tisku, skenování, indexování, archivaci, přepravu, atd.,

• automatická archivace, rychlý přístup k elektronickým dokumentům pro audit,

• umožnit lepší zabezpečení pro lepší kvalitu referenčních podpisů, které umožňují automatické ověření podpisu v papírové formě zpracování plateb,

• snížení nákladů jak papírových formulářů zmizí v interních procesech.

V řešení byl použit:

SOFTPROs SignPad eSignio a SignDoc Adobe Reader v kombinaci s elektronickými formuláři ve formátu PDFplusX poskytovaných Adobe LiveCycle dokumentový server Adobe Reader.

5.16 **Global Expert**

V roce 2012 byla realizována implementace systému pro 120 uživatelů do notebooků.

Cíl projektu

Zrychlení a plná automatizace procesu likvidace pojistných událostí, snížení nákladů spojených s tvorbou papírové dokumentace a zvýšení informační bezpečnosti v procesu likvidace pojistných událostí.

Obchodní přínosy a popis procesu:

Po zavedení biometrického podpisu bylo dosaženo zrychlení celého procesu likvidace pojistných událostí díky automatizaci. Pro servisního technika to znamená zjednodušení přípravy i rychlejší zpracování celého případu. Dále bylo dosaženo snížení provozních nákladů – již není třeba tisk, kopírování, skenování dokumentů nebo jejich fyzická archivace - a díky procesu přímého zpracování se odstranily chyby související s převodem obsahu do tištěné podoby, opisováním, skenováním a dopravou.

Řešení se skládalo ze 120 licencí aplikace SignoSoft, 120 ks notebooků Lenovo – X220 a implementačních prací. Technologie pro biometrické podepisování je integrována přímo do aplikací pro řešení pojistných událostí - AudaPad a SilverDAT - pomocí ActiveX technologie. Po zadání všech příslušných údajů je vygenerován „Zápis o poškození motorového vozidla“, který je přímo v aplikace následně podepsán a odeslán k dalšímu zpracování

Obrázek 55: zdroj internet notebook Lenovo – X220

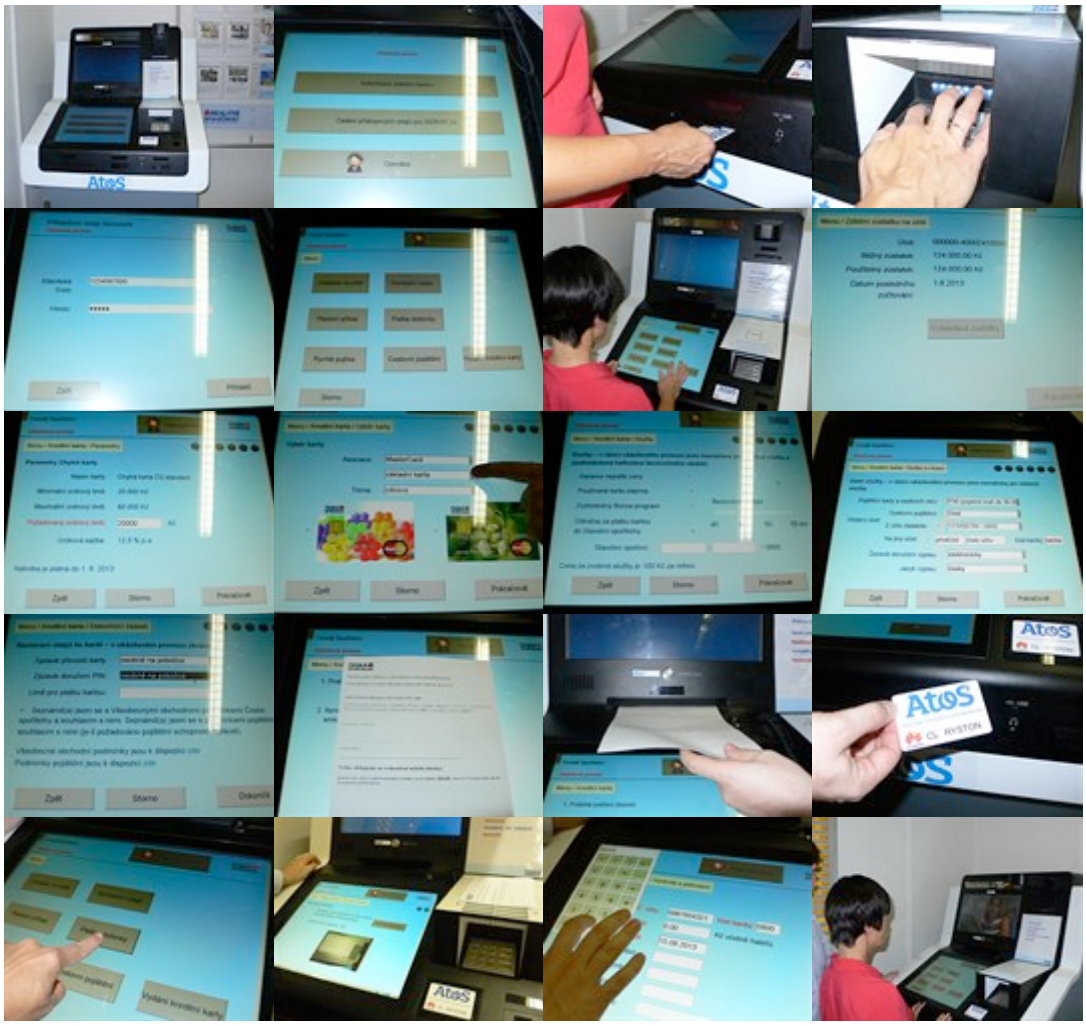
Pokud si pečlivě projdeme jednotlivé implementace výše uvedených společností, tak je zcela zřejmý pozitivní přínos a splněná očekávání u všech společností a to především v:

- ochraně životního prostředí,
- zvýšení rychlosti obsluhy zákazníka,
- posílení bezpečnosti obchodních smluv,
- zefektivnění stávajících postupů,
- zkrácení doby pobytu zákazníka na pobočce,
- více času na zákazníky,
- výrazného snížení objemu tisku smluv,
- eliminace chyb při zpracovávání papírových smluv během transformace (skenování, indexování atd.).

6 Budoucnost využití dynamických biometrických podpisů na pobočkách bank

Samoobslužný kiosek VTM

V loňském roce představila firma Huawei na českém trhu inteligentní víceúčelovou samoobslužnou pobočku eSpace Virtual Teller Machine (VTM). Přístroj bylo možno otestovat v pobočce České spořitelny, a.s. na pražském Smíchově. Níže si ukážeme několik screenshotů z této pobočky, které vystihují funkce samoobslužného kiosku.



Obrázek 56: zdroj Česká spořitelna, a.s. - souhrn náhledů inteligentní víceúčelové samoobslužné pobočky eSpace Virtual Teller Machine (VTM)

Nová experimentální pobočka byla také otevřena Českou spořitelnou, a.s. i v Plzni - Lochotín. V odkaze uvedeném níže je prezentován nový směr kudy se budou ubírat bankovní ústavy za využití nejnovějších technologií i za podpory využití biometrie, aby se zkvalitnily služby zákazníků a zpřístupnily se i o víkendech. Pokud testování proběhne dle očekávaní, budou se osvědčené postupy aplikovat do pobočkové sítě České spořitelny, a.s.

https://www.youtube.com/watch?v=DtAizMrKlGc

Přístroj je primárně určen bankám, které mají problém se zatížením poboček, ať už s přetížením (mnoho lidí ve frontě), nebo naopak s malou vytížeností pobočky. Firma Atos, která připravila software pro Českou spořitelnu a samotnou aplikaci, která umí jednotlivé funkce, jako je například uzavření smlouvy včetně elektronického a fyzického podpisu, zaplacení cestovního pojištění, uhrazení složenky, nebo díky speciální vestavěné tiskárně vydání platební karty, samozřejmostí je také zjištění finančního zůstatku na účtu.

Výhody:

- přehlednost displeje,
- velká písmena,
- jednoduchost obsluhy,
- operátor v call centru,
- vyřízeni bankovních potřeb dle svého času, kdykoliv chci 24 h,
- sdílení dokumentů, skenování originálních dokumentů pro banku,

- komunikace se svým e-mailem,
- výdej krátkodobých bezkontaktních karet,
- schválení krátkodobého úvěru.

Nevýhody:

- nevydává ani nepřijímá finanční obnosy,
- chybí člověk s kterým by zákazníci na živo komunikovali.

7 Závěr

Cílem diplomové práce bylo přiblížit problematiku dynamického biometrického podpisu, zavedení či implementaci do běžného života společnosti. Z této dynamicky se rozvíjející problematiky jsem si záměrně vybral kapitolu o samotné implementaci dynamického biometrického podpisu. O této problematice existují v povědomí veřejnosti jen kusé nebo žádné znalosti, i když se s ní v současné době setkávají a v budoucnosti budou setkávat čím dál více.

Pro dosažení stanoveného cíle bylo v teoretické části popsáno obecné rozdělení digitálních dokumentů a následně popsání elektronického podpisu a možnosti jeho využití. Dále principy digitálního podpisu a přiblížení právního rámce, na který navázal dynamický biometrický podpis a samotný úvod do této zajímavé problematiky.

Analýzou obou procesů v praxi a jejich popsáním, a to nejen z pohledu klienta, ale i z pohledu praktického zkoumání znaleckých posudků v oboru písmoznalectví z hlediska zjišťování pravosti dynamických biometrických podpisů, bylo zjištěno, že nejen v České republice dochází k pozvolné implementaci jeho využití v podnikových procesech mnoha velkých i menších společností, kterým přináší očekávanou úsporu a zrychlení jimi využívaných procesů, které navazují na uzavírání smluv i poskytovaný komfort pro zákazníky.

Při pečlivém srovnání obou procesů uplatňovaných při podpisu smluv, pojištění atd., výsledky analýzy jednoznačně hovoří ve prospěch nové technologie dynamického biometrického podpisu. Věnujeme-li se pečlivě prostudování jednotlivých implementací uvedených společností, je zcela zřejmý pozitivní přínos a splněná očekávání všech společností, a to především v oblastech:

- zvýšení rychlosti obsluhy zákazníka,
- posílení bezpečnosti obchodních smluv,
- zefektivnění stávajících postupů,
- zkrácení doby čekání zákazníka na pobočce,
- věnování více času zákazníkům,
- výrazného snížení objemu vytisknutých smluv, tzn. úspora kancelářského papíru,

- eliminace chyb při zpracovávání tištěných smluv během transformace (skenování, indexování atd.),
- ochrany životního prostředí.

Průzkumem a analýzou podkladů získaných z výzkumu byl potvrzen cíl diplomové práce, a to získat relevantní data o využití implementované technologie. Lze tedy konstatovat, že tato technologie má budoucnost i potenciál, a zaslouží si, dle mého názoru, aby byla nadále rozvíjena a inovována.

Na straně druhé bychom neměli opomíjet skutečnost, že s rozšiřujícími se technologiemi, které „vytlačují“ lidskou pracovní sílu, se podílí určitou měrou na zvyšování nezaměstnanosti a snižování pracovních příležitostí. Z toho vyplývá, že je nutné hospodárně nakládat s lidskými zdroji při zavedení jakékoliv inovace, neboť lidé a lidský potenciál jsou nadějí každé společnosti.

Téma diplomové práce jsem si zvolil záměrně. Aktivně se zajímám o „novinky“, se kterými člověk může přijít do styku, zvláště při jednáních na úřadech a ve společnostech, které ovlivňují naše životy. Pokud se pozorně podíváme kolem sebe, všude vidíme obrovskou spotřebu kancelářského papíru, což je neefektivní a nešetrné k přírodním zdrojům.

Z mého pohledu je zde určitá naděje, že i tato diplomová práce by mohla mít určitý přínos pro společnost, která se již řadu let snaží vydat cestou nových technologií s cílem snížit zatížení životního prostředí.

Seznam použitých zdrojů

BIČOVSKÝ, Radek. *Tajemství písma: úvod do grafologie*. Praha: Panorama, 1992. ISBN 80-703-8268-6.

MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2., podstatně přeprac. a rozš. vyd. Praha: Leges, 2012, 464 s. Teoretik. ISBN 978-80-87576-36-6.

MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. 2., přeprac. a dopl.vyd. Praha: C. H. Beck, 2004, 606 s. ISBN 80-717-9878-9.

POHLMANN, Norbert, Helmut REIMER a Wolfgang SCHNEIDER. *ISSE 2010, Securing electronic business processes: highlights of the Information Security Solutions Europe 2010 conference*. 1st. ed. Wiesbaden: Vieweg Teubner, c2011, ix, 416 p. ISBN 978-383-4814-388.

RAK, Roman. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.

SMEJKAL, Vladimír. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010, 354 s. Expert (Grada). ISBN 978-80-247-3051-6

VACCA, John R. *Biometric technologies and verification systems*. Oxford: Butterworth-Heinemann / Elsevier, 2007, xxvii, 625 s. ISBN 978-0-7506-7967-1.

Internetové zdroje

SIGNOSOFT. *Signosoft-biometrické podpisy* [online]. 1998 - 2015 [cit. 2015-02-16]. Dostupné z: http://signosoft.com/index.html

3M. *Full-Page Readers* [online]. 2015 [cit. 2015-02-16].
Dostupné z:
http://solutions.3m.com/wps/portal/3M/en_US/Security/Identity_Management/Products_Services/Reader_Scanner_Solutions/Document_Reader_Solutions/Full_Page_Document_Readers/

PRAŽSKÁ SOFTWAROVÁ S.R.O. *Bezpečný podpis* [online]. 2014 [cit. 2015-02-16]. Dostupné z: http://www.bezpecnypodpis.cz

SPOLEČNOST PRO PÍSMOZNALECTVÍ, o. s. *Písmoznalectví* [online]. 2013 [cit. 2015-01-16]. Dostupné z: http://www.pismoznalectvi.org

UNICORN SYSTEMS A.S. *Biometrický podpis* [online]. 2015 [cit. 2015-01-16]. Dostupné z: http://www.unicornsystems.eu

ZNALCI.CZ. *E-podpisy* [online]. 2004-2009 [cit. 2015-01-12]. Dostupné z: http://www.znalci.cz/cs/

O elektronickém podpisu a o změně některých dalších zákonů: zákon o elektronickém podpisu. In: *227/2000*. 29.6.2000. Dostupné z: http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx

Občanský zákoník. In: *Zákon č. 89/2012 Sb.,*. 1.ledna 2014. Dostupné z: http://obcanskyzakonik.justice.cz

Konference

Biometrické podpisy, 13. 3. 2014, hotel Merriott, V Celnici 8, Praha 1

Použité zkratky

BO - Business order - objednávka
BPM - business proces management - nástroj pro řízení procesů
D2D - door to door – podomní prodejci
DMS - dokument management systém - uložiště dokumentů, smluv

Fraud – podvod
OVM – orgány veřejné moci
SAP - ERP (systém na řízení zákazníků, objednávek, faktur, skladového hospodářství, vztahů se státem, se zaměstnanci, dodavateli, bankami atd.)
CRM - Siebel - Customer relationship management - nástroj k řízení pracovníků
X – Up sell – vícenásobný prodej (pozdější doprodej)

př. Prodám zákazníkovi automobil, klasický prodej. Up sell znamená, když mu k tomu prodám druhý den ku příkladu přívěsný vozík nebo další kola atd. Musí být odděleno dnem dalšího pořízení.

Seznam obrázků

Seznam tabulek

Seznam příloh

Příloha 1: Popis znaleckého zkoumání technologie xyzmo soudním znalcem v oboru písmoznalectví – Mgr. Zimmer

Znalecké zkoumání podpisů snímaných dotykovými tablety

Úvod

Dotykové tablety už delší dobu slouží jako ovládací zařízení výpočetní techniky a se zvyšováním jejich kvality se začínají uplatňovat i v oblasti zabezpečování dat tím, že umožňují pomocí dotykových senzorů zaznamenat charakteristiky ručně psaného podpisu. Ten je jedinečným projevem pisatele a je možné ho podrobit znaleckému zkoumání pravosti. Dotykové tablety zachycují nejen statické vlastnosti podpisu, tedy jeho grafickou podobu, ale i tzv. dynamické vlastnosti, jako je rychlost psaní nebo tlak na psací prostředek. Pochopitelně i v případě podpisů snímaných dotykovými tablety bude docházet ke sporům, při kterých bude třeba, aby znalec mohl pravost takového podpisu posoudit. Proto by se odborníci zabývající se identifikačním zkoumáním ručního písma měli s dotykovými tablety seznámit a posoudit možnost znalecké práce s takto snímanými podpisy.

V současnosti se dotykové tablety využívají především v zahraničí pro podepisování interní komunikace i pro podepisování dokumentů klienty. V obou případech se tím nahrazují klasické a nákladnější operace s papírovými dokumenty. V našich podmínkách je rozšíření tohoto systému podepisování otázkou času, přičemž nyní se u nás využívá zejména ve státní správě při zpracovávání žádosti o vydání cestovního dokladu s biometrickými prvky.

podpisové tablety od různých výrobců

Specifika zkoumání podpisů snímaných dotykovými tablety

Pro znalce není ideální, že podpis snímaný tabletem nemá vlastnosti originálního podpisu, resp. podpisu psaného na papír, který je v současnosti znalci označován jako originál a kterému jsou současné metody zkoumání přizpůsobeny.

S nástupem nových technologií bude ale zřejmě nutné znovu zvážit, jestli bude za originál označován i nadále jen podpis psaný na papír. V případě podpisu na dotykový tablet jde totiž také o jedinečný projev pisatele, a v tomto smyslu tedy také o originální podpis, ovšem s jinými vlastnostmi.

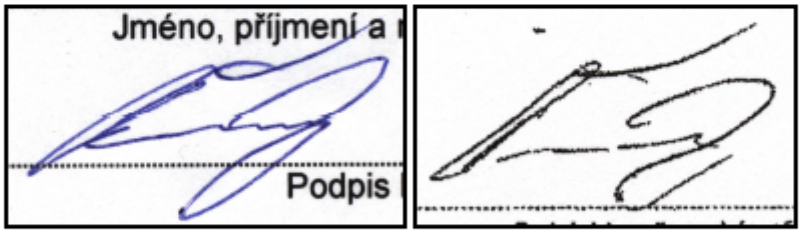
Není to tedy originál podpisu psaného na papír, který je jeho nedílnou součástí v podobě změn ve struktuře papíru a nánosu psací pasty. Současné metody znaleckého zkoumání přitom pracují především s těmito originály a informacemi, které z nich znalec dokáže pozorováním získat. V případě podepisování na dotykový tablet je mezi psací prostředek a elektronický dokument uložený v počítači navíc vložen hardware pro snímání podpisu a software pro jeho vyhodnocení. Záleží tedy v první řadě na tom, jak věrohodně dokáže hardware a software snímaná data zaznamenat a interpretovat. Je nezbytné, aby podpis osoby zobrazovaný v elektronickém dokumentu kvalitou odpovídal podpisu psanému touto osobou na papír. Pouze v takovém případě, kdy se informace jako tlak, rychlost apod., předávané při podepisování psacímu prostředku, projeví stejně v podpisu v elektronickém dokumentu a v podpisu na papíře, je možné, aby znalec mohl dospět k objektivním závěrům. Pokud by došlo ke zkreslení různých charakteristik, např. sklonu, tvarů apod., a podpis zobrazený v elektronickém dokumentu by se lišil od podpisu stejné osoby psaného na papír, potom by nebylo možné poznat, zda k odlišnostem došlo právě vlivem zkreslení dat, nebo zda jde o odlišnosti způsobené např. paděláním. Je tedy důležité, aby podpis snímaný tabletem měl stejnou kvalitu jako podpis psaný na papír, jako na následujících obrázcích.

vlevo je podpis snímaný tabletem a vpravo je neskenovaný podpis stejné osoby psaný na papír

Dále je uveden podpis stejné osoby, snímaný systémem, který v grafickém zobrazení neobsahuje rozdíly v dynamice tahu jednotlivých částí, což neodpovídá skutečnosti.

podpis bez dynamiky je pro znalecké zkoumání velmi špatně využitelný

I když není zkoumán originál podpisu psaný na papír, nejde ani o podpis, který by kvalitou odpovídal klasické elektrografické kopii. Zkoumání těchto kopií někdy bývá zatíženo problémy s jejich nízkou kvalitou bez možnosti zkoumání např. protlaku papíru nebo posloupnosti psacího pohybu, což není pro znaleckou práci optimální a nelze proto často dospět k uspokojivým závěrům o pravosti podpisu. Pokud má být podpis snímaný tabletem umístěn na papír, pak na něj musí být sice vytištěn, stejně jako bývá vytištěna elektrografická kopie, ale na rozdíl od elektrografické kopie je možné podpis snímaný tabletem na papír vytisknout ve vysoké kvalitě bez ztráty informací spojených s klasickým elektrografickým kopírováním. Navíc vedle vytištěného podpisu snímaného tabletem může mít znalec k dispozici i jeho elektronickou verzi, kterou je možné s omezením maximálního rozlišení podle potřeby zvětšovat.



srovnání originálu a elektrografické kopie podpisů jednoho pisatele – skenované ve stejné kvalitě

Existují i tablety bez displeje, které nezobrazují trajektorii podpisu, a pisatel tak může mít problémy s koordinací pohybu ruky, protože mu chybí zpětná vazba. Vhodnější je proto používat ty tablety, na kterých pisatel může sledovat průběh psaní podpisu, jako kdyby se podepisoval na papír.

Proti psaní na papír jsou tablety svými rozměry vyvýšené (u námi popisovaného tabletu níže je výška 1 cm), což může představovat pro pisatele neobvyklé písařské podmínky. To je však věcí technického řešení, vyvýšení tabletu

nakonec ani nemá na podpisy zásadní vliv a při častějším podepisování se s tím pisatel dokáže vyrovnat.

Zkoumání podpisů snímaných dotykovými tablety přináší i zcela nové možnosti, které znalci nemají ani u podpisů psaných na papír, a které se proto teprve budou muset naučit správně využívat. Pomocí speciálního analytického programu je totiž možné zkoumaný podpis přehrávat jako zpomalený film a toto přehrávání kdykoliv zastavit. To je velmi užitečná funkce pro hodnocení posloupnosti psacího tahu, což bývá i u některých originálů psaných na papír obtížné. Zároveň v případě, že by přehrávání podpisu odpovídalo reálné rychlosti podepisování, by jako další hledisko bylo možno využít i tempo psaní podpisu. Navíc lze získat informace o hodnotách tlaku na psací prostředek na kterémkoliv místě podpisu.

Experiment se systémem xyzmo

Díky spolupráci s IBM Česká republika a Design PLUS, s.r.o., která je partnerem rakouské společnosti xyzmo Software GmbH, jsme měli možnost posoudit využitelnost podpisového tabletu STU-500 od firmy Wacom, s ním dodávaného softwaru SIGNificant Client pro podepisování dokumentů ve formátu *.pdf a programu pro analýzu biometrických dat získaných při podepisování. V této souvislosti je třeba uvést, že vlastnosti nabízených dotykových tabletů i příslušného programového vybavení se mezi výrobci liší, a závěry tohoto posouzení proto nemusí platit pro všechna zařízení nabízená na trhu. Pokud jde o technické parametry námi zkoumaného tabletu Wacom STU-500, uvádí výrobce tyto hodnoty:

úhlopříčka displeje: 5 palců
maximální rozlišení: 640x480 pixelů
rozlišení tlaku: 512 úrovní tlaku
metoda snímání: elektromagnetická rezonance
citlivost snímání: 5 mm nad úrovní plochy tabletu

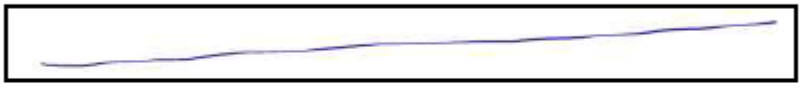
LCD podpisový tablet STU-500

Systém pracuje tak, že na uživatelem zadané místo v dokumentu umístí viditelný obraz sejmutého podpisu se skrytým obsahem dalších biometrických údajů, které je možné využít buď k zautomatizovanému porovnání s jinými již dříve uloženými podpisy, nebo právě pro znalecké identifikační zkoumání.

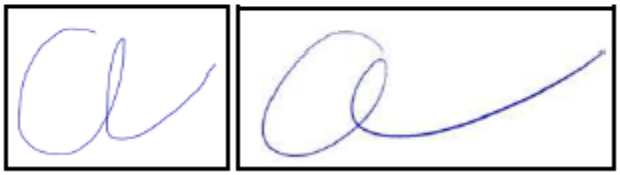
Provedené experimenty

První fáze byla zaměřena na to, jak podpisy snímané pomocí tabletu kvalitou odpovídají podpisům psaným na papír. K tomu je třeba sledovat, jaké změny v kvalitě tahu vyvolá změna rychlosti pohybu psacího prostředku. Při psaní na papír se vyšší rychlost projevuje jistými tahy a odlišením odlehčených míst, zatímco pomalé vedení psacího prostředku snižuje dynamiku a může vést až ke třesům tahu. Obdobné změny v kvalitě psacího tahu se projevily i při změnách rychlosti psaní na tablet, jak je vidět na následujících obrázcích.

rychle psaný tah snímaný tabletem

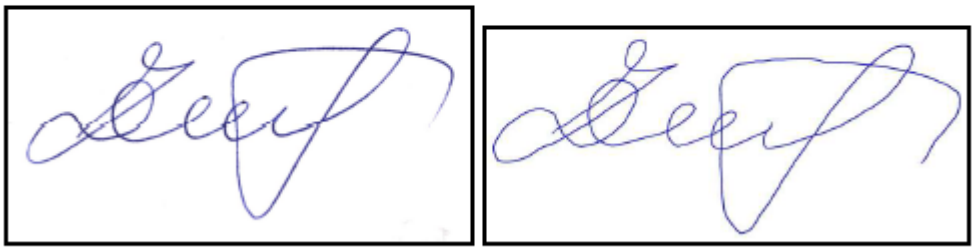


pomalu psaný tah snímaný tabletem



písmeno „a" snímané tabletem, vlevo psané pomalu, vpravo psané rychle

To je důležité např. při odhalování padělků vyhotovených napodobováním cizího podpisu. Padělatel si totiž nemůže osvojit písařský návyk jiné osoby a nemůže její podpis napsat se stejnou kvalitou a přesností jednotlivých částí jako ona. V případě padělků se to projevuje snížením kvality psacího tahu, protože padělatel většinou postupuje pomalu. Na následujících obrázcích je patrné, že i napodobenina snímaná tabletem má obdobné kvalitativní vlastnosti, jako kdyby byla psána na papír.

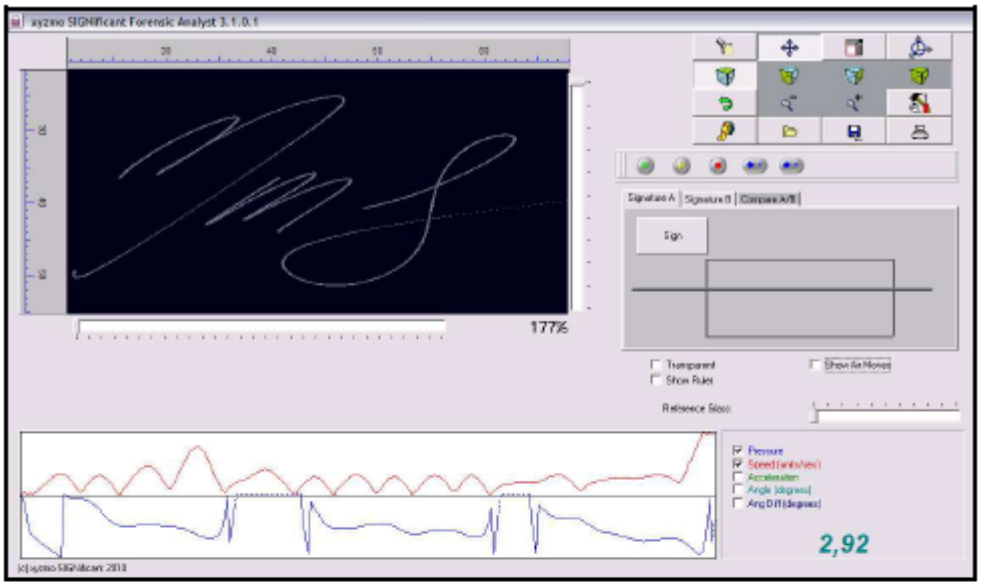


vlevo je pravý podpis a vpravo jeho pomalu psaná napodobenina na tablet

Druhá část byla zaměřena na využitelnost analytického programu, který interpretuje data snímaná tabletem, zejména pro znalecké potřeby.

Využitelné pro identifikační zkoumání je, že po nahrání biometrických dat podpisu má znalec možnost přehrávat průběh jeho psaní včetně tzv. airmoves (přemísťování psacího prostředku nad povrchem tabletu do výšky 5 mm), měřit vzdálenosti a úhly a sledovat změny tlaku na psací prostředek v jednotlivých místech podpisu. Informace, které analytický nástroj také zobrazuje, ale které zatím ke zkoumání využít neumíme, jsou např. zrychlení na jednotlivých místech podpisu, nebo prohlížení trojrozměrného obrazu podpisu.

Hlavní výhodou je, že podpis snímaný tabletem umožňuje sledovat průběh jeho psaní včetně pohybů psacího prostředku nad povrchem při přerušení tahu. Náhled okna analytického programu následuje.

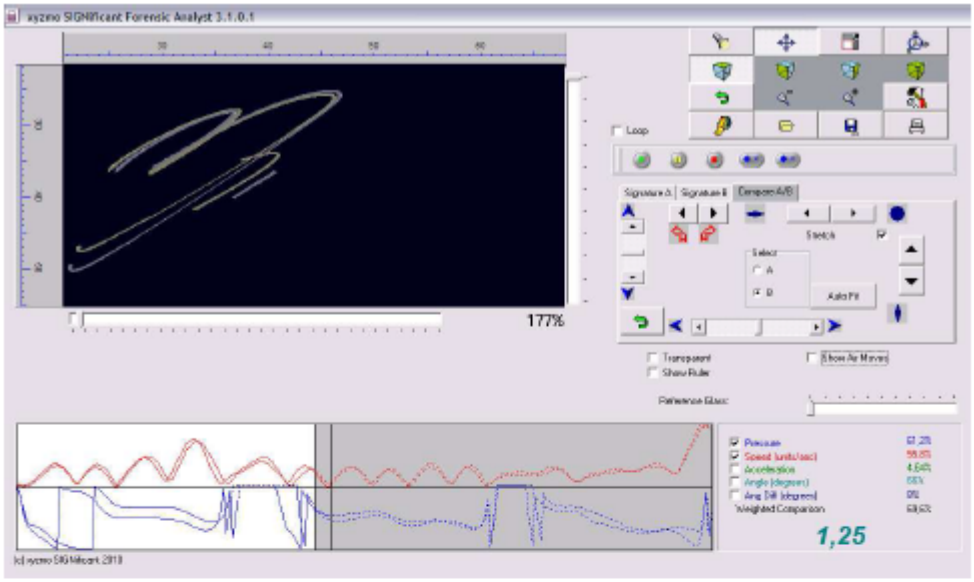


okno analytického programu se znázorněním průběhu tlaku a rychlosti psaní podpisu ve spodní části modrá křivka-tlak na psací prostředek, červená křivka-rychlost

V případě, že je psací tah rozpojen, jako je tomu v zobrazeném podpisu, je možné graficky znázornit i pohyby psacího prostředku v místech, kde se nedotýkal povrchu tabletu, a přehrát podpis, jako by byl psaný jedním tahem. Následuje zobrazení stejného podpisu včetně těchto tzv. airmoves.

graficky zvýrazněné tzv. airmoves a barevně potlačená jinak viditelná část podpisu

Pokud má znalec k dispozici nesporně pravé podpisy snímané tabletem, potom program umožňuje tyto podpisy a s nimi spojená data porovnávat včetně souběžného přehrávání průběhu jejich psaní. Na následujícím obrázku je znázorněno porovnání podpisů jedné osoby při přehrávání průběhu jejich psaní.



porovnání dvou podpisů jednoho pisatele – přehrávání průběhu psaní
ve spodní části jsou porovnané i křivky tlaku a rychlosti psacího prostředku

Závěr

Zkoumání podpisů snímaných dotykovými tablety je zcela novou oblastí, která v našich podmínkách ještě nebyla podrobně prozkoumána. Z kvalitativních rozdílů, které mezi tablety a softwarem různých výrobců existují, navíc vyplývá nutnost před vlastním zkoumáním experimentálně ověřit vlastnosti každého takového zařízení a jeho vhodnost pro znaleckou práci.

Experimenty provedené se systémem od firmy xyzmo Software GmbH zahrnujícím tablet STU-500 od firmy Wacom potvrzují, že co do kvality psacího tahu se v podpisech snímaných tabletem projevují obdobné znaky provázející spontánní i nespontánní psaní jako při psaní na papír. Analytický program navíc znalci umožňuje při zkoumání využít i další kvantifikované informace snímané tabletem, jako jsou rychlost psaní podpisu nebo tlak na psací prostředek. Nejvýraznější pozitivum však lze spatřovat v tom, že si znalec může přehrávat průběh psaní podpisu, který přitom vznikl v minulosti. To mu velmi efektivně umožní hodnotit směr, posloupnost a rychlost psacího pohybu včetně pohybů při přerušení kontaktu psacího prostředku s povrchem tabletu.

Po počáteční zdrženlivosti ohledně zkoumání podpisů snímaných dotykovými tablety lze proto na závěr uvést, že i tyto podpisy je možné zkoumat současnými

písmoznaleckými metodami. Je však důležité, aby použité zařízení věrně zaznamenávalo a interpretovalo všechny charakteristiky podpisu, které je potřeba při identifikačním zkoumání hodnotit. Není těžké si představit, že se tímto směrem budou vyvíjet komunikační technologie, které budou využívat identifikační potenciál ručně psaných podpisů, a umožňovat tak kvalifikované posuzování jejich pravosti.

Mgr. Jan Zimmer, soudní znalec z oboru písmoznalectví
2007 až 2009 oddělení grafických expertiz Kriminalistického ústavu Praha

Stanovisko JUDr. Jiřího Straky

S Mgr. Zimmerem mám možnost spolupracovat jak při znaleckém zkoumání, tak i v aktivitách souvisejících s experimentálním ověřováním nových metod a prostředků identifikačního zkoumání ručního písma. Od počátku jsem tak mohl sledovat i jeho snahu ověřit možnosti v článku popisovaných tabletů a hlavně jejich eventuální přínos pro rozvoj ručně psané komunikace v době stále výrazněji nastupujícího elektronického věku. Snažil jsem se mu také dávat podněty v tom smyslu, co by bylo zejména důležité sledovat a ověřovat. Mohu říci, že jsem byl stejně jako Mgr. Zimmer zpočátku k těmto zařízením mírně skeptický. Protože jsme ale byli jedním z výrobců osloveni, abychom tyto prostředky objektivně vyhodnotili z hlediska možnosti využití jejich produktů pro identifikační zkoumání, nemohlo se to obejít bez bližšího seznámení s nimi a bez provedení alespoň pilotních experimentů – to vše již zajišťoval Mgr. Zimmer. Musím potvrdit, že postupoval velice pečlivě a snažil se všímat si jak negativ, tak i pozitiv uvedených zařízení. Zjištění, ke kterým dospěl, mě velmi příjemně překvapila. Mohu dokonce konstatovat, že změnila můj pohled na budoucnost ručně psaných podpisů. Ještě donedávna jsem patřil k těm, kdo si mysleli, že ruční podepisování bude pomalu ustupovat a bude ho vytlačovat elektronický podpis. Ten má ale tolik negativ - z hlediska možností identifikace osoby, která ho vytvořila, dokonce velmi zásadních - že o jeho budoucnosti nyní spíše pochybuji. Popisovaná zařízení mají podle mého názoru potenciál daleko větší. Jde o to, že především zachovávají určité standardy pro pisatele po velmi dlouhou dobu obvyklé, a to je vždy příjemné – na vlastním procesu podepisování se tedy nic nemění. Navíc vytvářejí netušené možnosti také pro identifikační zkoumání. Samozřejmě že v „přechodné době“ nemusí být ideální porovnávat sporné podpisy vytvořené na

tabletech s ukázkami vyhotovenými v současných podmínkách – tedy na papír. I když podpisy vytvořené na tabletech (ať už jsou vytištěné na papír, nebo si je znalec zobrazí na monitoru) jsou kvalitativně na vyšší úrovni než elektrografické kopie, určitým omezením zkoumání je, jestliže není k dispozici srovnávací materiál pořízený zcela adekvátním způsobem. Pokud se ale podaří tuto technologii masově prosadit a využívat např. i ve státní správě, v bankovním sektoru apod., pak mohou být i ukázky v elektronické podobě (tedy již ne pouze psané na papír), a tím může být k dispozici vzorek ukázek s biometrickými údaji, které dnešní ukázky neobsahují. Potom by zcela objektivně platilo, že by se při rozhodování o pravosti takového elektronicky vyhotoveného podpisu s biometrickými údaji mohl znalec opírat o daleko přesnější informace, a že by tyto informace byly založené i na zcela zjevně a nepochybně ověřitelných matematických hodnotách. To by mohlo znamenat výrazný posun v objektivizaci písmoznaleckého zkoumání, takový posun, o kterém se nám před pár lety nemohlo ani snít.

Protože tedy podpisy, příp. i jiné ručně psané projevy na těchto zařízeních velmi úzce souvisejí s možností rozvoje identifikačního zkoumání rukopisu, považuji za nanejvýš potřebné se s nimi seznamovat, ověřovat jejich kvality a na jejich vývoji s jejich výrobci co nejvíce spolupracovat. Z tohoto pohledu hodnotím snahy Mgr. Zimmera včetně publikace tohoto pojednání jako velmi prospěšné.

JUDr. Jiří Straka, soudní znalec z oboru písmoznalectví
1975 až 2007 oddělení grafických expertiz Kriminalistického ústavu Praha
člen poradního sboru ministra spravedlnosti pro obor písmoznalectví

Příloha 2: Závěrečné vyjádření soudních znalců v oboru písmoznalectví – Mgr. Zimmer, JUDr. Straka

Mgr. Jan Zimmer
soudní znalec z oboru písmoznalectví
specializace ruční písmo
mob +420 777 024 451
e-mail zimmer@volny.cz
datová schránka dxyv2s6
adresa Marie Podvalové 939/13, 19600 Praha 9

identifikacepisatele.cz

Praha 20. března 2011

Design PLUS, s.r.o.
Zelený pruh 1560/99
140 00 Praha-Braník

Vyjádření k možnosti znaleckého zkoumání podpisů snímaných dotykovým tabletem společnosti xyzmo SIGNificant group.

V návaznosti na předběžné vyjádření znalce JUDr. Jiřího Straky jsem provedl experimentální ověření stanovených hypotéz. Předpokladem uvedeného vyjádření je, že podpisy snímané systémem xyzmo lze podrobit identifikačnímu zkoumání jako podpisy psané na papír.

Řešení, které jsem měl k dispozici, obsahovalo podpisový tablet STU-500 od firmy Wacom, software SIGNificant Client pro podepisování dokumentů ve formátu *.pdf a analytický software SIGNificant Forensic Analyst pro interpretaci biometrických dat získaných při podepisování.

Provedené experimenty potvrdily, že v kvalitě psacího tahu se v podpisech snímaných tabletem projevují obdobné znaky provázející spontánnost a nespontánnost jako při psaní na papír a že zobrazované vlastnosti zkoumaných podpisů, jako např. tvarové charakteristiky a velikostní poměry, odpovídají skutečnosti a nejsou tedy nijak zkresleny. To je základním předpokladem umožňujícím vůbec uvažovat o aplikaci současných znaleckých metod na podpisy snímané dotykovými tablety.

Výhodou pro znalecké zkoumání navíc je, že analytický program umožňuje při zkoumání využít i další kvantifikované informace snímané tabletem, jako jsou rychlost psaní podpisu nebo tlak na psací prostředek. To vede k objektivizaci zkoumání, protože při současné expertíze podpisů na papíru jsou tyto údaje získávány subjektivním hodnocením znalce.

Nejvýraznější pozitivum je ale to, že analytický program znalci nabízí možnost přehrávat průběh psaní podpisu, který přitom vznikl v minulosti. To velmi efektivně umožňuje hodnotit směr, posloupnost a rychlost psacího tahu, což je v některých případech obtížné i při zkoumání podpisů psaných na papír. Zároveň je možné analyzovat i pohyby psacího prostředku nad povrchem tabletu, které jsou systémem také zaznamenávány a které znalci poskytují další hodnotné informace, které u podpisů psaných na papír nelze získat.

V závěru zhodnocení předloženého zařízení lze proto uvést, že řešení společnosti SIGNificant group zastoupené v České republice společností Design PLUS, s.r.o. vyhovuje potřebám soudních znalců zabývajících se posuzováním pravosti ručně psaných podpisů. Na podpisy snímané pomocí tohoto řešení je možné aplikovat současné metody znaleckého zkoumání stejně jako na podpisy psané na papír.

Mgr. Jan Zimmer

Příloha 3: Vyjádření soudního znalce v oboru písmoznalectví k využitelnosti technologie xyzmo - JUDr. Straka

JUDr. Jiří STRAKA
soudní znalec z oboru písmoznalectví
specializace ruční písmo
Lysinská 1848/36, 143 00 Praha 4
tel./fax 244402390, mob. 606534634
e-mail: strakaji@volny.cz

Praha 24.9.2010

Byl jsem požádán, abych se jako soudní znalec z oboru písmoznalectví se specializací na ruční písmo vyjádřil k možnosti identifikačního zkoumání podpisů snímaných pomocí dotykových tabletů. Tedy jsou-li elektronické dokumenty obsahující ruční písmo (např. vlastnoruční podpis) vhodné k určení původce zprávy, obdobně, jako tomu je v případě podepsání papírového dokumentu obsahující ruční písmo, které obvykle v současné době zkoumám v případě soudních sporů.

Předběžně jsem se seznámil s možnostmi takového postupu a připravil podklady pro jeho laboratorní zkoumání z pohledu písmoznalecké identifikace, které bude realizováno v následujících měsících. **Ze získaných poznatků již nyní předpokládám, že podpisy snímané dotykovými tablety obsahují množství důležitých informací (biometrik), které umožní jejich identifikační zkoumání.**

Podpisy snímané pomocí dotykového tabletu jsou proti běžným fotokopiím pro forenzní zkoumání pravosti vhodnější. „Tabletové podpisy" digitalizací totiž neztrácí informace o tlaku na psací prostředek, posloupnosti a směru psacího pohybu, což je klasickým nedostatkem fotokopií. Největší výhodou je, že podpis snímaný pomocí tabletu, který je znalci předložen ve formě vytištěné kopie, může být doplněn digitální verzí podpisu ve vysokém rozlišení na datovém nosiči, pomocí které může znalec pozorovat jeho detaily. Digitální verze podpisu navíc díky softwarovému vybavení (hodnocení se vztahuje na technologii xyzmo Software GmbH, dále jen „xyzmo") může obsahovat i další biometrické údaje o jeho vyhotovení, jako např. celkový čas psaní podpisu a jeho detailní průběh, které je možné pro zkoumání pravosti také využít.

Nejlepších výsledků bude zřejmě možné dosáhnout při použití dotykového tabletu s vysokým rozlišením, záznamem tlaku na psací prostředek, s možností zobrazování trajektorie psacího pohybu, a v situaci, kdy je podpis snímán za standard-

ních písařských podmínek, tj. v sedě, s pevnou podložkou a s dostatečným osvětlením.

Pomocí správně volených postupů a maximálního využití možnosti technického zabezpečení výrobcem by také mohly být dány výrazně lepší podmínky k vyloučení, že takový podpis mohl být pořízen jiným způsobem a poté do systému implantován, což je dosud největší nevýhoda fotokopií, u nichž nelze přesně stanovit, zda byly i na původním originálním formuláři, či zda na něj mohly být přeneseny z listiny jiné.

V závěru tohoto předběžného hodnocení proto předpokládám, že zkoumáním ručně psaného podpisu v rámci elektronického dokumentu, pořízeného technologií xyzmo, bude možné identifikovat jeho pisatele, případně jeho padělatele tak, jak je to obvyklé u zkoumání ručního písma napsaného na papírových dokumentech. Z toho vyplývá, že pomocí technických prostředků xyzmo by bylo možné soudně určit původce ručního písma na dokumentu a tedy tuto technologii využít v běžné obchodní praxi.

Protože jde o novou technologii, která má ambice velmi zásadním způsobem měnit dosavadní písemné formy komunikace ve smyslu možnosti identifikačního zkoumání pisatele, resp. zkoumání pravosti podpisu, je třeba uvedené předpoklady spolehlivě experimentálně ověřit a přesně stanovit, do jaké míry platí ve vztahu k různosti zkoumaných objektů a podmínek psaní tak, jak je to známo u originálních ručně psaných projevů učiněných na papír či odpovídající materiály.

JUDr. Jiří STRAKA
soudní znalec
z oboru písmoznalectví
Lysinská 1848, 143 00 PRAHA 4
tel./fax: 244 402 390

Příloha 4: Ocenění produktů xyzmo na 11. mezinárodní konferenci biometrických systémů

2011 International Conference on Document Analysis and Recognition

Signature Verification Competition for Online and Offline Skilled Forgeries (SigComp2011)

Marcus Liwicki*, Muhammad Imran Malik*, C. Elisa van den Heuvel†, Xiaohong Chen‡,
Charles Berger†, Reinoud Stoel†, Michael Blumenstein§, and Bryan Found¶
*DFKI, Germany, Email: firstname.lastname@dfki.de
†Netherlands Forensic Institute, The Hague, The Netherlands
Email: E.van.den.Heuvel@nfi.minjus.nl, c.berger@nfi.minjus.nl, reinoud@holmes.nl
‡Forensic Science Institute, Ministry of Justice, Shanghai, China
Email: ccpccxh@hotmail.com
§Griffith University, Australia, Email: m.blumenstein@griffith.edu.au
¶La Trobe University, Melbourne, Australia, Email: Email b.found@latrobe.edu.au

***Abstract*—The Netherlands Forensic Institute and the Institute for Forensic Science in Shanghai are in search of a signature verification system that can be implemented in forensic casework and research to objectify results. We want to bridge the gap between recent technological developments and forensic casework. In collaboration with the German Research Center for Artificial Intelligence we have organized a signature verification competition on datasets with two scripts (Dutch and Chinese) in which we asked to compare questioned signatures against a set of reference signatures. We have received 12 systems from 5 institutes and performed experiments on online and offline Dutch and Chinese signatures. For evaluation, we applied methods used by Forensic Handwriting Examiners (FHEs) to assess the value of the evidence, i.e., we took the likelihood ratios more into account than in previous competitions. The data set was quite challenging and the results are very interesting.**

I. Introduction

The topic of writer identification and verification has been addressed in the literature for several decades [1], [2]. Usually, the task is to identify the writer of a handwritten text or signature or to verify his or her identity. Work in writer verification can be differentiated according to the available data. If only a scanned or a camera captured image of the handwriting is available then writer classification is performed with offline data. Otherwise, if temporal and spatial information about the writing is available, writer classification is performed with online data. Usually, the former task is considered to be less difficult than the offline classification [2]. Surveys covering work in automatic writer identification and signature verification until 1993 are given in [2]. Subsequent works up to 2000 are summarized in [3]. Most approaches are tested on specially collected data sets which were acquired in controlled environments. In the past, several competitions were organized to measure the detection rate of several classifiers:

- First international Signature Verification Competition (SVC 2004), online data, 5 reference signatures
- BioSecure Signature Evaluation Campaign 2009, online data, 5 reference signatures
- SigComp 2009 [4], online and offline data, 1 reference signature

Most of the current research in the field of signature verification does not take the real needs of Forensic Handwriting Experts (FHEs) into account. In their casework they often work with signatures produced in various real world environments. These signatures are more difficult to analyze compared to the signatures produced in controlled environments. FHEs also have to deal with possibly disguised signatures, where the author tries to disguise his or her handwriting in order to make it seem to be a forgery. The 4NSigComp2010 [5] was the first signature verification competition focusing explicitly the classification of disguised, simulated and genuine signatures.

We have now organized the Signature Verification Competition for Online and Offline Skilled Forgeries (SigComp2011). The major emphasis of this competition is not the possibility of disguised signatures but to motivate the signature verification community to enable their systems to compute the likelihood ratios instead of just computing the evidence (for more details see [6]). This is very important as it allows one to combine the FHE's evidence (from the results of an automated system) with other evidence presented in a court of law. In this competition we ask to produce a comparison score (e.g. a degree of similarity or difference), and the evidential value of that score, expressed as the ratio of the probabilities of finding that score when the questioned signature is a genuine signature and when it is a forgery (i.e. the likelihood ratio). Note that this competition has introduced a paradigm shift from the "decision paradigm" to an evidential value that impacts the task in the competition.

1520-5363/11 $26.00 © 2011 IEEE
DOI 10.1109/ICDAR.2011.294

The issue is not the pure classification, since

- The FHE cannot and was never asked to decide on authorship,
- the FHE cannot know the probability of authorship based on handwriting comparison alone, and
- classification brings with it the probability of an error of which the cost is undefined.

The true issue is to find the likelihood ratio (LR) for a comparison: the probability of finding a particular score given that Hypothesis $H1$ is true, divided by the probability of finding the score when the alternative Hypothesis $H2$ is true. $H1$ corresponds to intra-source scores (same author) and $H2$ to inter-source scores (different authors).

The relevant graphs therefore show histograms of some measure of similarity (or difference; or any continuous measure that used to be compared to some threshold in a classification task) for intra-source and inter-source comparisons. Such graphs make it possible to assess the value of the evidence given both hypotheses, which is of major importance to forensic experts and the courts. Therefore, in this competition we have had a closer look at the likelihood ratios.

II. Background

Forensic signature verification is done by visual comparison by trained FHEs. The authenticity of the questioned signature is estimated by weighing the particular similarities/differences observed between the features of the questioned signature and the features of several known signatures of a reference writer.

The interpretation of the observed similarities/differences in signature analysis is not as straightforward as in other forensic disciplines such as DNA or fingerprint evidence, because signatures are a product of a behavioral process that can be manipulated by the writer. In this competition only such cases of $H2$ exist, where the forger is not the reference writer. In signature verification research, a 100% perfect match does not necessarily support $H1$, because a perfect match can occur if a signature is traced. Also, differences between signatures do not necessarily support $H2$, because slight changes can occur due to a within-writer variation.

Since forensic signature verification is performed in a highly subjective manner, the discipline is in need for scientific, objective methods. The use of automatic signature verification tools can objectify the FHE's opinion about the authenticity of a questioned signature. However, to our knowledge, signature verification algorithms are not widely used by the FHEs. The objective of this competition is to compare automatic signature verification performances on new, unpublished, forensically relevant datasets to bridge the gap between recent technological developments and the daily casework of FHEs.

Table I
Number of Authors (A) and number of Genuine (G) (Reference (GR) and Questioned (GQ)) and Forged (F) Signatures in the Chinese data set

Training Set	Training			Test			
	A	G	F	A	GR	GQ	F
Offline	10	235	340	10	116	120	367
Online	10	230	430	10	120	125	461

Table II
Number of Authors (A) and number of Genuine (G) (Reference (GR) and Questioned (GQ)) and Forged (F) Signatures in the Dutch data set

Training Set	Training			Test			
	A	G	F	A	GR	GQ	F
Offline	10	240	123	54	648	648	638
Online	10	330	119	54	648	648	611

III. Data

Data collected from realistic, forensically relevant situations were used in this competition. Signature samples were collected while writing on a paper attached to a digitizing tablet. The collected signature data were made available in an online and offline format. Participants could choose to compete on the online data or offline data, or on both data formats.

The collection contains offline and online signature samples. Signatures were either genuine: written by the reference writer, or a simulation: simulated by another writer than the reference writer. The offline data sets consisted of PNG images, scanned at 400 dpi, RGB color. The online datasets consisted of ascii files with the format: X, Y, Z (per line) (sampling rate: 200 Hz, resolution: 2000 lines/cm, precision: 0.25 mm). For collection of these samples we used a WACOM Intuos3 A3 Wide USB Pen Tablet and collection software: MovAlyzer. A preprinted paper was used with 12 numbered boxes (width: 59 mm, height: 23 mm). The preprinted paper was placed underneath the blank writing paper. Four extra blank pages were added underneath the first two pages to obtain a soft writing surface.

Besides the detection of skilled forgeries of Western signatures, this competition also introduced a novel set of Chinese signatures. The purpose of using these two data sets was to evaluate the validity of the participating systems on both Western and Chinese signatures.

A. Data Sets

For both the online and offline cases, the data was divided in training and test sets having different naming conventions. Further details about the number of contributing authentic authors, forgers, number of authentic reference signatures and forgeries for both the training and test sets of Chinese and Dutch are provided in Tables I and II respectively. Note that due to minor problems during the acquisition the numbers of signatures in the online data sets differ from

Table III
OVERVIEW OF THE SUBMITTED SYSTEMS

ID	Institution	Mode
1	Sabanci	both
2	Anonymous-1	offline
3	HDU	offline
4	xyzmo(1)	online
5	xyzmo(2)	online
6	Qatar (Chinese optimization)	both
7	Qatar (Dutch optimization)	both
8	DFKI	offline
9	Anonymous-2	both

those in the offline data sets. However, this issue has no impact on the systems' performance, since 12 reference signatures could always be used (see below). Furthermore, while the training signatures were provided without restrictions on which signatures were used as reference signatures, the testing signatures have been divided by us into reference and questioned signatures.

IV. SUBMITTED SYSTEMS

In total, we received thirteen systems from six institutions for this competition. In the following we will list the participants and their brief descriptions. Participants were allowed to be anonymous upon request.

A. Sabanci University

After preprocessing and size normalization steps, we tesselate the image into a fixed number of zones using polar coordinate representation and extract gradient information in each zone. The extracted features of the query signature are classified using a user-dependent support vector machine (SVM) that is trained with the reference signatures of the user and negative examples.

B. Anonymous-1

The method utilizes a modified direction feature and microstructure feature, both of which are based on the signature's boundary. The modified direction feature not only extracts direction information but also detects transitions between background and foreground pixels. For each transition, the location of the transition and the direction values are stored. The grid microstructure feature records the positions of some special contour pixel pairs in every local grid, which are used to calculate the appearance probability of different position pairs and express the writing style by the probability density distribution. Then the system adopts an SVM as classifier. In the training stage, the positive samples are authentic signatures from the reference writer; the negative samples are all the offline forgery signatures. In the verification stage, using the "-b" parameter of libsvm, it will get the similarity score P1 for genuine signatures and score P2 for forgeries. Then it uses log(P2)-log(P1) as log-likelihood-ratio.

C. Hong Duc University (HDU)

The system HDUSigVerify includes two main phases: the evidence estimation phase and the calibration phase. For every two signatures, we compute two types of descriptors (a local one and a global one) in order to gain robustness as well as precision. The local descriptors are locally computed at every sampled point based on the gradient in the gray scale image. The global descriptors are computed in a skeleton image by using ShapeContext [7]. The matching step is carried out by using the technique from the Linear Assignment Problem (LAP) [8]. Particularly, we carry out the following stages in the first phase: Pre-processing: to remove noises, small blobs and the rectangle surrounding the signature (if any). The Hough transforms are employed to remove the rectangles in signature images. Binarization and thinning: we employed Otsu's technique to do binarization and then the thinning step is carried out to obtain a skeleton image of signature. The skeleton is then smoothed to remove "unwanted" segments (e.g. very short branches connecting to main lines). Sampling: there are typically about 2000-2500 pixels for each skeleton image and in order to employ the ShapeContext descriptor to find candidate matches between two signatures, we sample the skeleton image to obtain about 300-500 pixels (i.e. sampled pixels). ShapeContext descriptors and matching: The 1D matching technique (DWT) is often used in literature for signature matching. One advantage of this technique is that it is able to find optimal matches by dynamically wrapping the signals over time. However, in order to use DWT we need to transform the signature image from 2D space into 1D space. For offline signatures, this step is not reliable and causes information loss. In order to take advantage of the DWT for 2D matching, we adapt the ShapeContext descriptors and propose a postprocess to refine matches as follows. We sparsely sample for one signature and densely sample for the other one. (1) Compute ShapeContext descriptors for every sampled pixel. (2) Compute a cost-matching matrix based on ShapeContext descriptors and then apply LAP to find candidate matches. (3) Apply RANSAC [9] to remove geometry-inconsistent matches (4) Compute a cost-matching matrix based on the RANSAC model and then apply LAP again to find optimal matches. Subsequently, we compute local descriptors: A circular window is placed at every sampled pixel in the gray scale image to build up a histogram of orientation and magnitude gradients. The radius of the window is the thickness of signature at every sampled pixel (this makes the descriptors scale invariant). The histograms are then normalized to unit length in order to obtain illumination changes. For rotation invariance, the orientation of every pixel within the window is computed relative to the orientation of the sampled pixel. Combination: Compute the evidence score for optimal matches by combining three scores: the matching score based on local descriptors, the

matching score based on ShapeContext descriptors, and the matching score based on the RANSAC model. In addition, to deal with the intra-variation of each writer, these scores are normalized by using Z-Score computed from the genuine set of each writer. In the second phase, we employ the framework FoCal [10] to calibrate the evidence score.

D. xyzmo

The tool is based on a signature verification algorithm using statistical respectively empirical models and calculates the evidence score by comparing reference signatures and the questioned signature taking into account only features of the actual signatures without prior knowledge and does not require any training steps in advance as it is the case in other approaches. Mainly a biometric comparer is spanning a mathematical multi dimensional room (the tolerance border) built from extracted dynamic features of the reference signatures and evaluates the distance of the questioned signature to this room by correlation methods which is than expressed and formulated into a score with a range from 0 to 1 expressing the similarity, e.g., 1 means highest similarity possible. Input parameters into the algorithm are the native signature data because extraction and comparison steps will be done internally in the comparison component when signatures are loaded for being compared. Usually the underlying algorithm supports an extra enrollment step respectively checks which cannot be applied in the given test scenario. All signatures used as reference signatures are in the evaluated systems to fulfill defined minimum consistency criteria and a signature will be refused to go into a profile (the set of reference signatures) in case it fails to do so. In the test scenario the reference signatures will be enforced from outside and preselecting the reference set may not be allowed.

E. Qatar University and Northumbria University

The proposed method uses edge-based directional probability distribution features [11] and grapheme features [12]. These methods have previously been applied for Arabic writer identification and have shown interesting results. The classification step is performed using a logistic regression classifier trained separately on each dataset (Chinese and Dutch). The online tool combines the most discriminant features described in Nalwa's method [13] also trained separately on each dataset using a logistic regression classifier. All the tools use the proposed z-calibration method.

F. German Research Center for Artificial Intelligence

The system is based on the methods introduced in [14] However, we have modified/optimized it in order to fit in the scenarios presented in this signature verification competition. First, the signature image is spatially smoothed followed by a binarization. In the optimized version of this approach we used various combinations of local and global binarization methods and evaluated the results. After these preprocessing steps the operations of [14] have been performed.

We used means and variances for thresholds' computations. Next, the nearest neighbor approach is applied to decide on the result of each feature vector and finally a voting based classification is made. In the optimized version different voting strategies were applied that improved the overall performance.

Table IV
RESULTS FOR THE CHINESE OFFLINE COMPETITION

ID	Accuracy(%)	FRR	FAR	$\widehat{C}_{llr}$	$\widehat{C}_{llr}^{min}$
1	80.04	21.01	19.62	0.757712	0.693347
2	73.10	27.50	26.70	3.062735	0.765021
3	72.90	27.50	26.98	1.125224	0.789918
6	56.06	45.00	43.60	1.260461	0.890711
7	51.95	50.00	47.41	3.222468	0.951274
8	62.01	37.50	38.15	1.573580	0.926571
9	61.81	38.33	38.15	6.227011	0.918450

Table V
RESULTS FOR THE DUTCH OFFLINE COMPETITION

ID	Accuracy(%)	FRR	FAR	$\widehat{C}_{llr}$	$\widehat{C}_{llr}^{min}$
1	82.91	17.93	16.41	0.730387	0.573175
2	77.99	22.22	21.75	2.456203	0.674031
3	87.80	12.35	12.05	0.415796	0.386128
6	95.57	4.48	4.38	0.714976	0.133917
7	97.67	2.47	2.19	0.900352	0.075223
8	75.84	23.77	24.57	1.664745	0.722033
9	71.02	29.17	28.79	4.133458	0.794021

G. Anonymous-2

This institution did not provide us with any details.

V. EXPERIMENTS AND EVALUATION

The systems have been evaluated on the four testing sets described above, i.e., the offline and online Chinese and Dutch data set. The task was to determine if a given questioned signature has been written by the author of the n reference signatures or of it was forged by another writer. In all experiments the number of reference signatures was $n = 12$, i.e., twelve known reference signatures were presented to the systems.

We evaluated our systems according to several measurements. First, we generated ROC-curves to see at which point the equal error rate is reached, i.e., the point were the false acceptance rate (FAR) equals the false rejection rate (FRR). At this specific point we also measured the accuracy, i.e., the percentage of correct decisions with respect to all questioned signatures. Next, we measured the cost of the log-likelihood ratios $\widehat{C}_{llr}$ (see [10]) using the FoCal toolkit. Finally, the minimal possible value of $\widehat{C}_{llr}$, i.e., $\widehat{C}_{llr}^{min}$ as a final assessment value. Note that a smaller value of $\widehat{C}_{llr}^{min}$ denotes a better performance of the method.

The results of the offline competitions appear in Tables IV and V. Those of the online competitions appear in Tables VI

Table VI
RESULTS FOR THE CHINESE ONLINE COMPETITION

ID	Accuracy(%)	FRR	FAR	$\widehat{C}_{llr}$	$\widehat{C}_{llr}^{min}$
1	84.81	12.00	16.05	0.565146	0.351142
4	93.17	6.40	6.94	0.413413	0.217915
5	93.17	6.40	6.94	0.418631	0.217915
6	82.94	16.80	17.14	1.049099	0.503151
7	85.32	13.60	14.97	0.905516	0.461140
9	80.89	9.26	8.14	6.210251	0.733883

Table VII
RESULTS FOR THE DUTCH ONLINE COMPETITION

ID	Accuracy(%)	FRR	FAR	$\widehat{C}_{llr}$	$\widehat{C}_{llr}^{min}$
1	93.49	7.56	7.69	0.492844	0.237550
4	96.27	3.70	3.76	0.258932	0.122596
5	96.35	3.86	3.44	0.351189	0.122596
6	91.82	8.33	8.02	0.534542	0.290940
7	92.93	7.25	6.87	0.604641	0.241201
9	88.56	11.11	11.27	6.433622	0.408429

and VII. As can be seen, different systems performed best on different tasks. Interestingly, the system with the best FRR and FAR always turned out to have the best value of $\widehat{C}_{llr}^{min}$. The winners for the offline competitions are System 1 for Chinese data and System 7 for Dutch data. The winner for both online competitions is System 4.

Several interesting observations can be made when having a closer look at the tables. First, it is interesting, that a good EER does not always result in a good $\widehat{C}_{llr}^{min}$, e.g., System 9 performs quite well on online Chinese data when looking at the EER but has the worst $\widehat{C}_{llr}^{min}$. This might be explained by the fact that a few large errors might spoil the overall performance with $\widehat{C}_{llr}^{min}$. Second, surprisingly System 7 performs better on Chinese online data than System 6, even if System 6 has been optimized to Chinese data. Finally, the results on Chinese data are much worse than those on Dutch data. This indicates that a lot of research has to be performed on Chinese scripts and maybe that this data is more challenging.

ACKNOWLEDGEMENTS

We would like to thank Falco Schneider for performing parts of the evaluation.

REFERENCES

[1] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification – the state of the art," in *Pattern Recognition*, vol. 22, 1989, pp. 107–131.

[2] F. Leclerc and R. Plamondon, "Automatic signature verification: the state of the art 1989–1993," in *Progress in Automatic Signature Verification*, R. Plamondon, Ed. World Scientific Publ. Co., 1994, pp. 13–19.

[3] R. Plamondon and S. N. Srihari, "On-line and off-line handwriting recognition: a comprehensive survey," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 63–84, 2000.

[4] V. L. Blankers, C. E. van den Heuvel, K. Y. Franke, and L. G. Vuurpijl, "Icdar 2009 signature verification competition," 2009, pp. 1403–1407.

[5] M. Liwicki, C. E. van den Heuvel, B. Found, and M. I. Malik, "Forensic signature verification competition 4nsigcomp2010 - detection of simulated and disguised signatures," in *12th International Conference on Frontiers in Handwriting Recognition*, 2010, pp. 715–720.

[6] J. Gonzalez-Rodriguez, J. Fierrez-Aguilar, D. Ramos-Castro, and J. Ortega-Garcia, "Bayesian analysis of fingerprint, face and signature evidences with automatic biometric systems," *Forensic Science International*, vol. 155, no. 2-3, pp. 126–140, 2005.

[7] S. Belongie, J. Malik, and J. Puzicha, "Shape matching and object recognition using shape contexts," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, pp. 509–522, 2002.

[8] R. Jonker and A. Volgenant, "A shortest augmenting path algorithm for dense and sparse linear assignment problems," *Computing*, vol. 38, pp. 325–340, 1987.

[9] M. A. Fischler and R. C. Bolles, "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography," *Commun. ACM*, vol. 24, pp. 381–395, 1981.

[10] N. Brümmer and J. du Preez, "Application-independent evaluation of speaker detection," *Computer Speech & Language*, vol. 20, no. 2–3, pp. 230–275, 2006.

[11] S. Al-Ma'adeed, E. Mohammed, and D. Al Kassis, "Writer identification using edge-based directional probability distribution features for arabic words," in *IEEE/ACS International Conference on Computer Systems and Applications*, 2008, pp. 582–590.

[12] S. Al-Ma'adeed, A.-A. Al-Kurbi, A. Al-Muslih, R. Al-Qahtani, and H. Al Kubisi, "Writer identification of arabic handwriting documents using grapheme features," in *IEEE/ACS International Conference on Computer Systems and Applications*, 2008, pp. 923–924.

[13] V. Nalwa, "Automatic on-line signature verification," *kluwer International series in engineering and computer science*, pp. 143–164, 1999.

[14] P. I. S. D. D. Samuel, "Novel feature extraction technique for off-line signature verification system," *International Journal of Engineering Science and Technology*, vol. 2, pp. 3137–3143, 2010.