

Zabezpečený elektronický dokument v prostředí VŠ

(Závěrečná zpráva projektu FR CESNET 331R1/2009)

Pavel Jindra

Západočeská univerzita v Plzni

Centrum informatizace a výpočetní techniky

e-mail: paja@civ.zcu.cz

31. 8. 2011, doplněno 17.5.2012

Abstrakt

Předkládaný projekt má za cíl nalézt vhodné řešení pro prezentaci a publikování dat pomocí zabezpečených digitálně podepsaných dokumentů. Součástí řešení je určení vhodného formátu dat umožňujícího zabezpečení el. podpisem. Dále pak určení nejvhodnějších způsobů vytváření a zacházení s takovými dokumenty. Výsledkem by měl být základ metod a postupů jak využít zabezpečených el. dokumentů v informačních systémech univerzity. Tento projekt je dalším krokem pro kompletní náhradu papírového dokumentu elektronickým a tím posouvá procesy VŠ dále směrem k e-univerzitě.

1. Způsob řešení projektu

V rámci řešení projektu bylo zakoupeno 22 ks licence na produkt *Adobe Acrobat Pro*. Tento software byl nainstalován vybraným klíčovými uživateli z Centra informatizace ZČU a část licencí byla použita pro administrátory a programátory složitějších dokumentů opatřených dokumentovou logikou. Dále proběhlo školení uživatelů a administrátorů *Adobe Acrobat Pro* zaměřené na získání znalostí a praktických dovedností při vytváření a vývoji PDF dokumentů. Značný díl prostředků projektu byl věnován na analýzu možností deklarované technologie a vznik vzorových dokumentů pro specifické oblasti použití. V rámci řešení projektu byly navrženy i postupy jak je možné využít zabezpečený PDF dokument v praxi.

1.1 PDF dokument

Je otevřený formát vyvinutý firmou *Adobe* pro archivaci a výměnu dokumentů. Soubory PDF mohou obsahovat kromě textu, obrázků i interaktivní prvky. Formát je optimalizovaný pro přenos, zobrazení a grafický výstup textových i multimediálních dat. Jeho použití garantuje vždy stejnou interpretaci a zobrazení dokumentu nezávisle na platformě a použitém zobrazovacím software. Pro dodržení těchto parametrů jsou součástí dokumentu vždy všechny prvky nutné pro jeho grafickou interpretaci (jako např. fonty, otevřené kompresní algoritmy apod.).

Obecný formát PDF je velmi široká technologie obsahující mnoho rozšíření a dodatečných funkcí. Postupným vývojem bylo ustanoveno několik norem a průmyslových standardů definujících druhy formátu PDF určené pro různé způsoby použití.

PDF/A – určeno pro zobrazování a tisk digitálních dokumentů pro dlouhodobé uchování

PDF/E - zobrazování a tisk dokumentů používaných v technických pracovních postupech, zejména pro výměnu dokumentace a výkresů ve stavebnictví

PDF/X – určeno pro tisk a věrné podání barevného prostoru, používá se pro profesionální grafiku a tisk

PDF/UA – dokumenty usnadňující přístup handicapovaným uživatelům

PRC – pro zobrazení 3D modelů

PADES – standard pro využívání digitálních podpisů v PDF

1.1.1 Pořízení PDF dokumentů

Cest k pořízení dokumentu je několik, nicméně vždy se jedná o nějaký typ grafického výstupu. Neexistuje editor, kterým by se dal dokument PDF přímo vytvořit podobně jako vytváří dokumenty textový editor např. Word. Pro získání PDF dokumentu je možné použít speciální tiskový ovladač s výstupem do PDF. Nebo využít konverzních nástrojů, které zkonvertují obrázek do PDF. Tento přístup má tu vlastnost, že není možné (jednoduše) editovat a pozměňovat již vyrobený PDF dokument. Výhoda tohoto přístupu spočívá také v tom, že dokument bude interpretován vždy stejně tak, jak ho jeho autor vytvořil. Toto je rozdíl oproti jiným formátům např. DOC, jehož interpretace a výsledná podoba může být závislá na nastavení počítače čtenáře. Pro vytvoření složitějších struktur, nebo interaktivních dynamických dokumentů je třeba využít specializovaných nástrojů, které je možné najít v balíku *Adobe Acrobat Pro*.

1.2 Nástroje Adobe pro práci s PDF

Součástí balíku *Adobe Acrobat Pro* je kromě základního programu *Adobe Acrobat* i několik efektivních nástrojů pro práci s PDF dokumenty. Následující popis uvádí nejdůležitější součásti a jejich oblast použití. Jelikož je PDF otevřeným formátem, je možné najít i velké množství více či méně kvalitních nástrojů třetích stran. Žádný však neumožňuje vkládání licencí pro otevření pokročilých funkcí široce rozšířeného *Adobe Acrobat Readeru*, který je zdarma volně k dispozici.

Adobe Acrobat Pro

Umožňuje vytvářet PDF z obrázků, nebo zdrojových souborů typu DOC a HTML. Základní nástroj pro vytváření portfolií PDF a multimediálních souborů. Umožňuje přidávat do dokumentu další meta informace jako je elektronický podpis vydavatele dokumentu, nebo metody usnadnění pro handicapované uživatele. Stejně tak je možné tímto nástrojem nastavovat práva manipulace s dokumentem, jako například znemožnit tisk dokumentu, nebo umožnit korekční a poznámkový mód v *Adobe Readeru*.

Adobe Acrobat Distiler

Nástroj pro převod dat uložených v Post Scriptu do PDF se zachováním maximální možné kvality dokumentu. Umožňuje převádět soubory vektorovým způsobem. Výsledek je závislý na kvalitě předlohy, ale vzhledem k vlastnostem PDF je vždy dosaženo optimální kvality výstupu s výrazně menší velikostí výsledného souboru.

Adobe Live Cycle Designer

Je nástroj pro vytváření interaktivních a dynamických formulářů v PDF. Umožňuje vkládat pole formuláře i textové a grafické prvky. Jedná se o komplexní vývojové prostředí interaktivních formulářů, které umožňuje vývoj JavaScriptové logiky formuláře včetně integrovaného debuggeru a pokročilých programovacích prvků.

Adobe Acrobat Reader

Multiplatformní nástroj pro zobrazení a interpretaci PDF dokumentů. Je k dispozici zdarma na Internetu k volnému použití. Umožňuje jak prohlížení a tisk dokumentů, tak i vyplnění formulářů, vkládání poznámek do PDF a další funkce, pokud je to ve zdrojovém PDF povoleno. Některé funkce jsou závislé na verzi prohlížeče, ale obecně od verze 9 jsou dostupné všechny podstatné interaktivní prvky, včetně elektronického podpisu.

1.3 Zabezpečený PDF dokument

Elektronický podpis PDF dokumentu přináší velmi důležité rozšíření. Díky němu se může dokument stát nejen prostředkem k výměně informací, ale také nástrojem k provádění úkonů s právní vahou. Při zabezpečení dokumentu el. podpisem je zřejmé kdo a v jaké podobě dokument vytvořil (případně schválil). Je možné spolehlivě autentizovat autora, ale navíc také autor nemůže popřít, vytvoření takového dokumentu.

Adobe Acrobat Pro rozlišuje dvě možnosti jak el. podepsat dokument. První je klasický „schvalovací“ **el. podpis**. Ten se využívá k vyjádření souhlasu autora s obsahem dokumentu. Zároveň také chrání před neautorizovanými zásahy do dokumentu. Při podpisu je možné nastavit zda zůstane dokument zamknutý pro další změny, nebo zda bude odemčený a bude možné jej např. opatřit podpisem další osoby. Pokud se díky tomuto případu vyskytne v dokumentu více podpisů, je možné zobrazit si dokument také podle toho jak vypadal v okamžiku podpisu jednotlivými schvalovateli.

Druhý typ je tzv. **certifikace dokumentu**. Certifikace slouží především k tomu, aby si uživatel dokumentu mohl ověřit, že dokument byl vydán konkrétním autorem či institucí. Význam certifikace je zvláště důležitý při vyplňování formulářů s odesláním dat. Uživatel si může být jistý, že daný formulář vytvořil očekávaný autor. Druhá důležitá funkce certifikace dokumentu spočívá v možnosti získat vyšší práva při interpretaci dokumentu. Pokud je dokument certifikován el. podpisem od důvěryhodné certifikační autority, jsou takovému dokumentu poskytnuta vyšší práva při prohlížení. Tím jsou automaticky povoleny některé funkce JavaScriptu např. pro přístup k síti nebo využití systémových prostředků či spouštění externích programů (např. prohlížeče po kliknutí na odkaz). Pokud není dokument certifikován a obsahuje interaktivní prvky vyžadující zvýšená oprávnění, musí uživatel potvrdit několik dialogových boxů s upozorněním na eventuální narušení bezpečnosti.

Oba typy el. podpisů je možné do dokumentu umístit jak ve viditelné formě reprezentované tabulkou se základními informacemi o použitém certifikátu, nebo ve formě skryté. Skrytá forma el. podpisu má stejnou funkci jako viditelná, pouze není zobrazena ve formě rámečku s popisem. Přítomnost el. podpisu je pak možné ověřit jen prostřednictvím menu a nástrojové lišty. Neviditelný el. podpis se používá zejména v případech, kdy by umístění tabulky s podpisem znamenalo zhoršení možnost správně dokument přečíst.

Autor dokumentu má možnost specifikovat certifikát, nebo vydávající CA, kterým je možné dokument podepsat. V okamžiku podpisu pak *Acrobat* nabídne k podpisu pouze certifikáty vyhovující zadaným pravidlům. Tato možnost se uplatní především v interaktivních formulářích generovaných pomocí *Adobe Live Cycle Designeru*.

Ověření el. podpisu v dokumentu probíhá v okamžiku načtení do *Readeru*, pokud došlo při přenosu dokumentu k nějaké změně, je zobrazeno nepřehlédnutelné varování. Stejně tak, je uživatel upozorněn na vypršení platnosti certifikátu, nebo podpis nedůvěryhodným certifikátem. Pokud není v dokumentu hodnověrným způsobem zaznamenán čas pomocí časového razítka, je taktéž zobrazeno upozornění.

Zde je třeba zdůraznit, že *Adobe Acrobat* i *Acrobat Reader* mají své vlastní úložiště důvěryhodných certifikačních autorit. Díky tomu si uživatel může jasně nastavit soubor kořenových CA, kterým důvěřuje. Naopak opačná možnost nastavení důvěryhodných CA je povolit integraci úložiště Windows, kdy jsou za důvěryhodné považovány všechny CA používané v operačním systému.

Časové razítko slouží jako důvěryhodný zdroj času. Validace dokumentu je vždy posuzována k datu jeho vzniku. Aby bylo možné důvěryhodně určit takové datum je vhodné vložit do dokumentu časovou značku. Adresu serveru poskytujícího časová razítka je nutné nastavit pomocí menu „*Další volby -> Nastavení zabezpečení*“ položka „*Servery časových razítek*“. Pokud je takto nastaven alespoň jeden funkční server je možné údaje o čase použít nejen při podpisu dokumentu, ale také při ověřování platnosti certifikátů. Pokud není možné získat časové razítko a podepsaný dokument kvůli tomu nebude opatřen důvěryhodným údajem o čase, bude zobrazeno varování, že čas podpisu byl získán z počítače autora a není důvěryhodný.

1.4 Spolupráce s čipovými kartami

Pokud má uživatel uložen osobní certifikát na čipové kartě, může i tak využít el. podpisy v dokumentech PDF. V *Adobe Acrobat Readeru* jsou k tomuto účelu dostupné dvě metody. Pokud *Reader* běží v prostředí *Windows* je možné použít MS CAPI (MS crypto API), pomocí kterého je certifikát dostupný v systémovém úložišti certifikátů. Produkty *Adobe* standardně mohou podepisovat certifikáty uloženými v systému.

Druhá možnost je využít přímo standardizované rozhraní PKCS#11 pro přístup k čipové kartě. Tímto postupem je možné používat certifikáty přímo z karty nezávisle na systému. Tato volba bývá využívána především na jiných platformách než *Windows*, nebo pokud vyžadujeme zvláštní bezpečnost přístupu ke kartě. Nastavení PKCS#11 knihovny se provádí v menu „*Další volby -> Nastavení zabezpečení*“ položka „*Moduly a tokeny PKCS#11*“.

2 Způsob řešení projektu

2.1 Publikování dokumentů v PDF

Základní skupinu zabezpečených dokumentů v prostředí VŠ tvoří dokumenty, které je nutné vystavit širokému spektru uživatelů v univerzální a srozumitelné formě. Uživatel musí dokument snadno zobrazit a musí mít možnost ověřit, že byl vytvořen důvěryhodnou osobou (nebo organizací) a nebyl pozměněn. Při řešení projektu bylo navrženo několik vhodných způsobů publikování dokumentu. Cílem bylo vytvořit takový dokument, který poskytuje uživateli možnost jednoznačně ověřit identitu autora a tím autentičnost dokumentu. Způsob validace dokumentu je závislá na jeho typu a způsobu použití. Jak již bylo uváděno, pokud se jedná o **prostý dokument** ve kterém nebudou prováděny změny je vhodné jej **elektronicky podepsat**. V našem prostředí IS vysoké školy jsou to například různé směrnice nebo prohlášení, která budou opatřena viditelným elektronickým podpisem. V případě, že by viditelný podpis narušoval správné zobrazení je vhodné použít podpis skrytý. Důležité je v tomto případě nastavit, aby byl dokument po podepsání zamknutý pro další změny. V případě vystavení formulářů, nebo dokumentů k doplnění je vhodné použít místo el. podpisu **certifikaci dokumentu**. Mechanismus certifikace dovoluje lépe řídit možnosti pozdějších úprav souboru. To se hodí např. pro formuláře a žádosti určené k vyplnění. Podrobněji bude problematika formulářů a jejich zpracování řešena v kapitole „El. oběh formulářů“. Při analýze vhodného řešení bylo vytipováno několik typů dokumentů, které by bylo účelné před vystavením el. podepisovat.

Vyhlášky a směrnice

V případě těchto dokumentů je obvykle původcem jediné oddělení pro legislativu. Na hlavním pracovišti se směrnice pomocí *Adobe Acrobatu Pro* podepíše buď přímo, nebo se do dokumentu vloží licence pro rozšíření funkcí *Acrobat Readeru*. Výsledné PDF s rozšířením podepíše odpovědná osoba (např. ředitel, rektor, apod.) pomocí volně šiřitelného *Adobe Acrobat Readeru* a zašle zpět k vystavení. Je nezbytné aby při podpisu byla zaškrtnuta volba „*Zamknou dokument po podepsání*“. Oba postupy jsou z hlediska výsledku zcela ekvivalentní, záleží jen na momentální situaci, který postup je pro dané pracoviště jednodušší.

Mechanismus tvorby vyhlášky či směrnice ze zdrojového dokumentu vyžaduje nástroj *Adobe Acrobatu Pro*. Zabezpečení se provádí el. podpisem buď přímo v okamžiku vytváření, nebo následně pomocí *Acrobat Readeru*. Dokument neobsahuje žádnou dokumentovou logiku a proto, jej může vytvářet samotný původce vyhlášky bez spolupráce administrátora. Tento typ dokumentu není možné předgenerovat, nebo vytvořit univerzální parametrizovatelnou šablonu.

Formuláře k vyplnění

V této kapitole se jedná především o velmi jednoduché formuláře pouze k vyplnění běžným uživatelem. Typickým příkladem takového formuláře je např. anketní lístek. Uživatel formulář vyplní a zašle zpět. Pro takový účel je možné dokument certifikovat, tak aby si uživatel byl jistý tím, že vyplňuje oficiální formulář.

Pro vytvoření jednoduchých formulářů (např. dotazníku) je možné s úspěchem použít automatického konverzního průvodce v *Adobe Acrobat Pro*. Tento průvodce umožňuje vytvořit formulář z elektronického dokumentu (např. ve formátu DOC), nebo dokonce detekcí formulářových polí z naskenovaného dokumentu. Tento typ formuláře je schopen vytvořit a upravit průměrně zdatný a poučený uživatel, vyžaduje pouze použití produktu *Adobe Acrobat Pro*.

Pro složitější formuláře je výhodné použít produkt *Adobe LiveCycle Designer* a vytvořit celý formulář od základu skládáním formulářových prvků. Druhý postup vyžaduje hlubší znalost práce s PDF dokumenty, ale přináší možnost opatřit formulář prvky dokumentové logiky. Podrobnější postupy pro práci s formuláři jsou popsány v kapitole „El. oběh formulářů“.

Generované výstupy

Ve studijním informačním systému *STAG* používáme generované výstupy do PDF. Jedná se například o osobní rozvrh studenta, nebo některá rozhodnutí týkající se průběhu studia. Aby měli tyto výstupy právní relevanci je nutné je opatřit elektronickým podpisem systému. Bohužel pro vytváření takových výstupů není možné použít *Adobe Acrobat*, neboť nemá automatický režim zpracování dokumentu. Tato funkcionality je obsažena až v serverové verzi produktu *Adobe LiveCycle Enterprise*. Nicméně pro tento účel navrhujeme použít open source nástroj „JSigndf“ pro podpis PDF dokumentu. Pomocí této řádkové utility je možné automaticky generované PDF opatřit el. podpisem a vyhnout se tak interaktivnímu rozhraní *Acrobatu*.

Vzhledem ke skutečnosti, že příjemci uvedených dokumentů jsou povětšinou studenti, je vhodné pečlivě zvážit jaký certifikát použít pro podpis takto vystavovaných dokumentů. Aby byl popis správně validován, musí prohlížeč PDF na stroji koncového uživatele důvěřovat certifikační autoritě, která vydala certifikát autora. Na ZČU mají uživatelé možnost získat certifikáty podepsané *CESNET CA Root*. Tyto certifikáty však nejsou pro potřeby publikování dokumentů určených studentům příliš vhodné, protože uvedenou CA koncoví uživatelé zpravidla nemají importovanou v úložišti *Acrobat Readeru*. Jako vhodnější se ukazuje použít certifikáty TCS-P vydané od fy. COMODO, která má své kořenové certifikáty ve všech hlavních operačních systémech i v certifikátovém úložišti *Acrobatu*.

2.2 PDF dokument v korekčním režimu

Korekční režim PDF dokumentu znamená, že do již hotového dokumentu je možné provádět další úpravy pomocí speciálních nástrojů *Adobe Acrobat*. Tyto funkce jsou obsaženy také ve volné verzi *Acrobat Reader*, ale vyžadují vložení licence pomocí velkého *Adobe Acrobat Pro*.

Pro vytvoření PDF dokumentu s korekčními funkcemi, je nutné nejprve vytvořit samotné PDF a otevřít jej v *Adobe Acrobatu Pro*. V menu zvolit „*Další volby -> Rozšíření funkce v Adobe Readeru*“ a dokument uložit. Tím je do PDF dokumentu vložena licence pro použití v *Adobe Acrobat Readeru* a jsou u něj přístupné rozšířené funkce. K dispozici jsou nástroje jako je psací stroj, anotace, korektury, kreslené prvky a digitální podpis. Upravený dokument je možné uložit ve formě PDF a zaslat zpět na další zpracování.

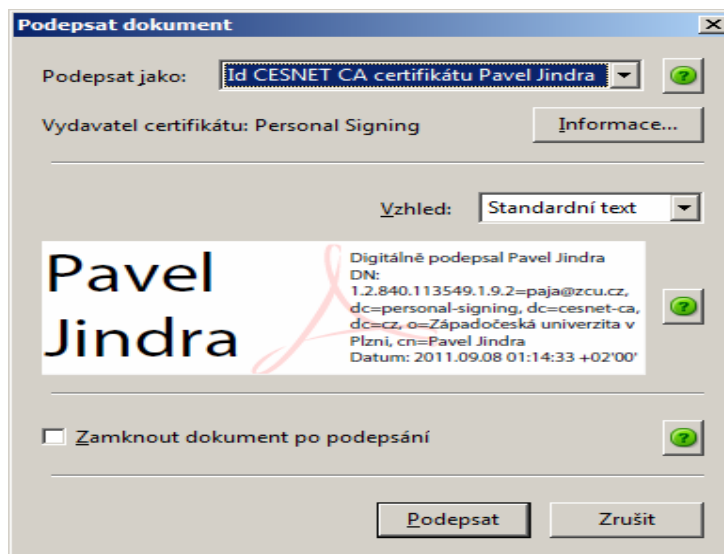
Nástroj **psací stroj** slouží pro doplňování textu na dokument. Text je vždy umístěn do samostatné vrstvy přes dokument a nijak neovlivní jeho původní podobu. Tento nástroj je možné použít např. pro vyplnění statických neinteraktivních formulářů a jejich tisk. Nebo pro psaní doplňkových textů či poznámek. Je možné nastavit typ, velikost a barvu použitého písma.

Nástrojem **anotace** je možné do dokumentu vkládat anotační poznámky. Kromě běžných anotačních značek pro textové korektury je možné využít i další méně obvyklé ale efektivní korekturní prvky. Velmi zajímavé a rychlé je vložení hlasové poznámky s nahraným vzkazem, nebo možnost vložení dalšího souboru přímo na konkrétní místo dokumentu.

Dalším efektivním korekčním nástrojem jsou **kreslená označení**, které umožňují vkládat nejrůznější grafické prvky, jako čáry, šipky, ohraničení, různé obrazce apod. Pod tuto kategorii je možné zařadit i nástroj schvalovací razítko. Jedním kliknutím lze přehledně označit dokument jako schválený, nebo např. určený k přepracování.

Po provedení korekcí a úprav dokumentu je možné celý dokument opatřit **elektronickým podpisem**. Při vkládání el. podpisu se může zvolit volba „*Zamknout dokument po podepsání*“. Tímto krokem se znemožní další úpravy, dokud však není dokument zamknutý je i po podpisu možné stále provádět korektury a také dále přidávat další

el. podpisy dalších korektorů. Ve výsledku *Adobe Acrobat Reader* umožňuje zobrazit jednotlivé verze dokumentu tak jak vypadaly v okamžiku schválení jednotlivých podpisů.



Obrázek 1: Volby el. podpisu dokumentu

Využití korekčního režimu

Korekční nástroj přináší zajímavý a rozmanitý způsob spolupráce více autorů na jednom dokumentu. Použití elektronického podpisu umožňuje garanci autora a nepopíratelnou identifikaci. Nicméně zásadní problém tohoto řešení spolupráce více autorů je **nemožnost snadné akceptace navržených změn**. Veškeré korekční poznámky jsou v dokumentu zobrazeny formou překryvné vrstvy a nemají žádný vliv na vzhled a obsah původního dokumentu. Autor tedy musí všechny poznámky zpracovat ručně do původního zdrojového souboru. Toto omezení se pro klíčové potenciální uživatele jeví jako zásadní.

Původní záměr projektu použít korekční režim pro zaznamenání zápisů z porad se ukázal jako příliš komplikovaný. Původní předpoklad byl takový, že zapisovatel vytvoří zápis v textovém editoru (např. *Word*) a převede jej do PDF s možností korekčního režimu. Takto vytvořené PDF rozešle na korekturu a schválení účastníkům schůze. Poté by zpracoval připomínky a vytvořil nový el. podepsaný výsledný zápis. Dle současné praxe je výhodnější využít režim revizí přímo ve *Wordu*. Pro publikaci pak využít až poslední krok a to vygenerování výsledného PDF a opatření elektronickým podpisem.

Využití korekčního režimu je výhodné jen v případech, kdy je potřeba schválit takové dokumenty, které nevyžadují změny obsahu. Vhodným příkladem jsou dokumenty vyžadující jen vzetí skutečnosti na vědomí nebo parafování. Výsledný parafovaný PDF dokument je možné přímo archivovat, včetně případných poznámek. U takových dokumentů odpadá ruční zapracování připomínek a vytváření nového dokumentu.

Mechanismus tvorby těchto dokumentů je obdobný jako v případě publikování směrnice. Rozdíl je v tom, že korekční režim dokumentu je možné zapnout i u existujícího PDF dokumentu vytvořeného předem.

2.3 Elektronický oběh formulářů

Stěžejním předmětem tohoto projektu bylo analyzovat možnosti formátu PDF jako prostředku pro zabezpečený el. oběh dokumentů. PDF dokument má pro tento účel všechny předpoklady, obsahuje jak metody umožňující dynamickou změnu dokumentu, tak i možnosti

elektronického podpisu a to i vícenásobného. Posledním předpokladem je možnost zpracování výsledného vyplněného formuláře i s ověřením jeho integrity a validity el. podpisů.

2.3.1 Komponenty interaktivního formuláře

Pro tvorbu složitějších interaktivních formulářů je nutné využít nástroj *Adobe LiveCycle Designer*. Tento software obsahuje pokročilé funkce pro vytváření formulářů jež obsahují množství interaktivních i grafických prvků. Dále je jeho součástí prostředí pro vývoj dynamických manipulace s prvky dokumentu pomocí funkcí v jazyce JavaScript. Formulář je vytvářený v *Adobe LiveCycle Designeru* pomocí vložení jednotlivých prvků na layout výsledného dokumentu a nastavením jejich vlastností a vzájemných interakcí pomocí dokumentové logiky. To vše je uloženo ve speciálním XML formátu *Adobe XDP* a výsledný PDF dokument se generuje až z tohoto formátu.

Následující sada prvků je jen ilustrativní přehled nejdůležitějších komponent PDF formuláře.

Prvky pro grafický vzhled formuláře

Tyto prvky je možné použít pro grafickou stavbu formuláře. Sami o sobě neumožňují žádné interaktivní akce, ale pomocí dokumentové logiky je možné tyto prvky skrývat, nebo zobrazovat.

Text - pole prostého textu. Umožňuje vložit formátovaný text na pozici.

Line/Rectangle – čára a obdélník umožňují vkládat jednoduché geometrické prvky. Je možné nastavovat tloušťku a barvu čar.

Table – tabulka s možností dynamické změny počtu prvků i velikosti. Má široké možnosti formátování vzhledu a určení typu políček. Hodnoty polí je možné dynamicky plnit.

Image – obrázek vložený do dokumentu. Specialitou je možnost vložení obrázku pomocí URL adresy. *LiveCycle Designer* umí automaticky zvětšovat a zmenšovat vkládané obrázky dle požadavků.

Prvky pro uživatelský vstup

Text Field - textové pole formuláře. Umožňuje zadat textovou hodnotu a zajistí kontrolu vložených dat. Pro vkládaná data je možné nastavit omezení délky, možnost dynamického roztažení políčka nebo omezení vkládání speciálních znaků. Pro složitější validace jsou k dispozici uživatelsky definovaná validační schémata (např. vložení uživatelského jména o 8 znacích). Pro formuláře určené k vytisknutí je vhodné použít volbu „*Limit length to visible area*“, která zaručí vytištění všech zadaných hodnot.

Numeric Field – obdobné jako Text Field jen pouze pro číselné hodnoty. Hodnoty těchto políček je možné využívat jako numerické hodnoty ve scriptech.

Date/Time Field – políčko pro zadání časových hodnot. Po kliknutí se zobrazí malý kalendář s možností výměru požadované hodnoty.

Drop Down List – pole seznamu hodnot. Je možné vybrat jednu hodnotu, nebo napsat vlastní v případě, že je to ve vlastnostech prvku povolené.

List Box – pole seznamu hodnot s možností výběru více hodnot. U tohoto pole je výhodou možnost mapování zobrazené hodnoty výběru s hodnotou ukládanou do výstupu. Např. je možné zobrazit zkratky kateder pro výběr, ale ke zpracování bude zaslána číselná reprezentace katedry.

Image Field – položka pro vložení uživatelského obrázku. Vhodné například pro přiložení fotografie do dokumentu.

Prvky pro interakci uživatele

Následující prvky slouží především k řízení interaktivních formulářů a spouštění akcí, mohou však také nést uživatelská data a předávat jejich hodnoty.

Check Box – zaškrtačací políčko s nastavením hodnot pro *true* a *false*. Hodnota může být jak uživatelem zadaná tak i automaticky nastavená skriptem.

Radio Button – přepínač seznamu prvků. Může být zvolena jen jedna hodnota ze seznamu.

Button - obecné tlačítko pro spuštění akce.

Email Submit Button – specifické tlačítko s přednastavenou funkcí odeslání formuláře pomocí e-mailu. Pomocí tohoto tlačítka se odesílají vyplněné formuláře na zadanou URL.

Signature Field – nástroj pro vložení podpisového pole. Kromě běžných voleb týkajících se vzhledu, umožňuje obsáhlé nastavení vlastností elektronického podpisu jako je volba masky podpisového certifikátu nebo CA. Použití časového razítka, nebo vložení aktuální odpovědi OCSP serveru v okamžiku podpisu. Podpisových polí může být v dokumentu více, ale je nutné správně nastavit, která pole mají zůstat po prvním podpisu odemčená.

2.3.2 Dokumentová logika formuláře

Elementární dokumentovou logiku formuláře řeší již vhodné nastavení interaktivních prvků. Příkladem může být pole podpisu, které po podpisu zamkne vybraná pole proti editaci. Také nastavení validačních vzorů vstupních polí včetně varovných upozornění vytváří interaktivní funkce formuláře bez nutnosti programování. Pro složitější konstrukce chování dokumentu je třeba sáhnout k pokročilým skriptovacím funkcím. Při běhu formuláře jsou k dispozici dva interpretované skriptovací jazyky. Prvním všeobecně používaný JavaScript přináší širokou škálu funkcí, druhý nativní skriptovací jazyk FormCalc je určený přímo pro použití v PDF.

Ve formuláři mohou být oba jazyky kombinovány, ale nelze je míchat pro funkce jednoho objektu.

JavaScript

Použití JavaScriptu v přináší široké možnosti vložení vlastní funkcionality do formuláře. *LiveCycle Designer* přináší možnost využití objektového modelu programování. Funkce JavaScriptu mohou volat metody objektu a upravovat jejich vlastnosti, umožňují psát velmi výkonné programové struktury. Obsahuje množství funkcí od běžných matematických nebo textových až k pokročilým funkcím pro interakci s okolím. (např. použití webservicess, nebo přístup k lokálním souborům). Vzhledem k potenciální nebezpečnosti některých

pokročilých funkcí je nutné v některých případech certifikovat dokument el. podpisem, nebo ručně povolit provádění pokročilých funkcí.

FormCalc

Je jazyk vyvinutý přímo pro použití ve formulářích PDF. Neobsahuje ani zdaleka tolik funkcí jako JavaScript, ale jeho hlavní výhodou je jednoduchost a přehlednost. Byl vyvinut proto, aby bylo možné co nejjednodušším způsobem použít běžné a často využívané funkce. FormCalc má základ v JavaScriptu, ale způsob použití funkcí a proměnných je značně zjednodušen. Mezi základní funkce FormCalcu patří zejména finanční a aritmetické funkce, dále pak funkce pro textové manipulace a práci s časem.

2.3.3 Vyplnění a zpracování formuláře

Jak již bylo uvedeno, dokument navržený pomocí *Adobe LiveCycle Designeru* je pro použití nutné uložit jako dynamické PDF. Pro možnost využití vyplnit a odeslat formulář pomocí *Adobe Acrobat Readeru* se použije následující postup:

1. Uložit dokument jako dynamické PDF.
2. Otevřít toto PDF v Adobe Acrobat Pro
3. V menu zvolit „Další volby -> Rozšířit funkce v Adobe Readeru“
4. Uložit takto upravený dokument a zaslat jej uživatelům

Uživatel po obdržení dokumentu formulář vyplní, opatří elektronickým podpisem a pak může např. využít tlačítko poslat přes e-mail. Vyplněný formulář je otevřen jako příloha nového mailu směřující na emailovou adresu autora. Autor obdrží kompletní vyplněný formulář a včetně el. podpisů a může jej archivovat nebo třeba vytisknout.

Jiný alternativní způsob zpracování je posílání vyplněných údajů v XML formátu. Tento způsob usnadňuje automatické zpracování formuláře. Vyplněné hodnoty formuláře se sestaví do XML a je možné jej také opatřit elektronickým podpisem. Takto připravený XML formát se odesílá pomocí e-mailu nebo webové služby autorovi ke zpracování.

Dle licenčních podmínek pro použití *Adobe Acrobat Pro* je možné tímto způsobem vytvořit maximálně 500 podání jednoho formuláře. Pokud by měl být tento limit překročen je nutné použít pro tvorbu formulářů serverové řešení *Adobe LiveCycle Enterprise Suite*.

2.3.4 Ukázkový formulář el. dovolenka

Výsledkem projektu je modelový případ elektronického oběhu dokumentů ve formě el. dovolenkového formuláře. Proces vystavení a schvalování dovolenky probíhá tak, že zaměstnanec vyplní prázdný formulář s uvedením osobních údajů, data nástupu a ukončení dovolené a samozřejmě vlastnoručním podpisem. Tento doručí vedoucímu k podpisu a po podepsání vedoucím putuje papírová dovolenka k mzdové účetní na zpracování.

V rámci řešení projektu jsme tento postup převedli do elektronického zpracování pomocí zabezpečeného PDF dokumentu. Pomocí dokumentové logiky jsme do formuláře naprogramovali možnost stažení základních osobních údajů pomocí webové služby (WS).

Zaměstnanec si otevře prázdný formulář v *Acrobat Readeru*, vyplní položku login a JavaScript pomocí webservicel doplní jméno, příjmení, katedru a zaměstnanecké číslo. Poté je možné vyplnit datum nástupu a ukončení dovolené. Takto vyplněný formulář žadatel

podepíše el. podpisem pomocí certifikátu uloženém na čipové kartě. Vyplněná pole jsou zamknuta proti další editaci a nyní je formulář připraven k zaslání vedoucímu e-mailem pomocí tlačítka „poslat vedoucímu“. Jakmile vedoucí obdrží vyplněný formulář také jej stvrdí svým el. podpisem a odešle mzdové účetní. Mzdová účtárna pomocí *Acrobat Readeru* zkontroluje oba podpisy a zanesse údaje do účetního systému. Výslednou dovolenku pak archivuje v dokumentovém úložišti.

Dovolenka

Poslat vedoucímu
Odeslat na PER

Jméno: Příjmení: Login:

Osobní číslo: Útvar: Číslo útvaru:

Žádá o dovolenou na zotavenou v době od: do:

Celkový počet pracovních dnů:

Datum a podpis zaměstnance: Datum a podpis vedoucího:

Pavel Jindra Digitálně podepsal Pavel Jindra
Dne: 1.2.2011 11:35:40 v: 0.2:zajavensou.cz
úč: personal-signing, dc:casinet-cs,
#c:cs, o: Západočeská univerzita v
Plzni, ou: Pavel Jindra
Datum: 2011.08.22 09:32:30 +0200'

Skutečný nástup dovolené Likvidoval:

Obrázek 2: El. dovolenka vyplněná a podepsaná zaměstnancem

Úpravy a změny formuláře a formulářové logiky

Pokud je formulář pro elektronický oběh dokumentů připraven pro použití, je zpravidla vystaven na důvěryhodném místě odkud si jej jednotliví uživatelé stahují a používají. Takto vytvořené formuláře mohou být parametrizovány např. podle pracoviště uživatele. Jednotlivý formulář obsahuje také e-mailovou adresu vedoucího pro zasílání vyplněných dokumentů. Při požadavku na změnu této adresy je možné, aby změnu provedl správce konkrétního pracoviště přepsáním adresy pomocí Live CycleDesigneru. Toto je jednoduchá změna nevyžadující změnu dokumentové logiky.

Pro náročnější změny, například změnu workflow dokumentu je nutné zasáhnout do příslušné dokumentové logiky. Při úpravě formuláře je nutné dbát na komplexní úpravu dokumentu a především dokumentové logiky v JavaScriptu. Mění-li se workflow dokumentu, který obashuje elektronické podpisy, je nutné důsledně dbát na to, aby upravené prvky formuláře byly zahrnuty do skupiny podepisovaných prvků tak, jak to vyžaduje nové workflow.

Npříklad v průběhu využití el. dovolenky došlo ke změně workflow pro vyplnění a odeslání. Místo odeslání vyplněného a schváleného dokumentu na personální oddělení si změna vyžadovala odeslání vyplněné a podepsané dovolenky svému přímému nadřízenému a po jeho podpisu ještě do kanceláře ředitele. Proto byla dokumentová logika dolněna o mechanismus získání čísla pracoviště a z něj pak pomocí změny hodnoty formulářového pole Drop-down-list emailové adresy přímého vedoucího. Dále pak byla změněna některá pole a viditelnost tlačítek po odeslání se řídí stavem vyplnění dokumentu. Viz. následující obrázek upraveného dokumentu „dovolenka“.

Dovolenka

Poslat vedoucímu

Login: Jméno: Příjmení:

Osobní číslo: Útvar:

Žádá o dovolenou na zotavenou v době od: do:

Celkový počet pracovních dnů:

Datum a podpis zaměstnance:

Datum a podpis vedoucího:

Skutečný nástup dovolené

2.4 Školení Adobe Acrobat Pro

V průběhu řešení projektu se uskutečnilo školení administrátorů a vývojářů zaměřené na tvorbu interaktivních formulářů. Školení provedla renomovaná firma, která je autorizovaným zástupcem fy. Adobe v ČR. Díky vstřícnosti školitelské firmy se školení uskutečnilo přímo v prostorách naší univerzity. Prostředky vyhrazené na cestovní náklady tak bylo možné použít na rozšíření rozsahu školení. Školení bylo díky tomu prodlouženo na 3 výukové dny a rozšířeno o oblast webové interakce dokumentu pomocí webservicess. Výuka proběhla praktickou formou, řešením modelových příkladů doplněných teoretickým výkladem.

Předmětem školení bylo zejména:

- Úpravy dokumentu: záhlaví/zápatí, pozadí, vodoznak, manipulace se stránkami, vkládání záložek (+ strukturované záložky).
- Odesílání souboru k revizi/komentování, vkládání komentářů, zpracování komentářů (řešení komentářů, import/export komentářů).
- Nástroje editace dokumentů
- Nástroj Adobe LiveCycle Designer
- Zabezpečení dokumentů, digitální podepisování dokumentů.
- Základní koncept oběhu formulářových dokumentů ve firmě.
- Formulářové prvky/objekty.
- Nastavení a úpravy vlastností formulářových polí.
- Hierarchie dokumentu z pohledu formuláře a jeho dalšího zpracování.
- Kontrola vstupních hodnot, chybová hlášení, formátování výstupu.
- Formulářová logika JavaScript, FormCalc
- Spolupráce s webovými službami

V rámci školení jsme využily také možnost konzultačních služeb školitele. Součástí rámec konzultačních služeb byly analyzovány možnosti využití PDF dokumentu v našem specifickém prostředí. jednalo se především o autentizační služby webservicess a spolupráce a nastavení čipových karet a certifikátů pro podpis dokumentu.

2.5 Vazba na elektronické podpisy a PKI

Pro podpis dokumentů v PDF jsou využívány elektronické podpisy v rámci PKI infrastruktury ZČU. Infrastruktura PKI je založena na certifikátech vydávaných certifikační autoritou CESNET „Peronal Signing“. Certifikát uživatele je i s privátním klíčem uložen na čipové kartě a tím je zaručena ochrana a také přenositelnost klíče. Díky použitému middleware jsou certifikáty po zasunutí karty do počítače integrovány do prostředí windows, kde mohou být využity mnoha aplikacemi včetně aplikace Adobe Acrobat.

Certifikáty podepsané certifikační autoritou CESNET CA ROOT a umístěné na osobní čipové kartě uživatele jsou v akceptovány k identifikaci uživatelů v rámci administrativních úkonů na ZČU. Akceptace, vydávání a správa elektronických podpisů a certifikátů je legislativně zakotvená ve vnitřních předpisech univerzity.

2.6 Závěry a hodnocení použití technologie Acrobat PDF

Po analýze možností, které poskytuje technologie Adobe PDF můžeme konstatovat následující závěry. Dokument ve formě PDF splňuje funkční i bezpečnostní předpoklady pro předpokládané výše uvedené oblasti použití. Díky standardizaci jsou dokumenty univerzálně přístupné pro mnoho platforem. Veškerá data k zobrazení a ověření dokumentu jsou přiložena a proto mohou být ověřena i offline.

Vkládání licence pro aktivaci funkcí Acrobat Readeru se provádí ručním nastavením v produktu *Adobe Acrobat Pro*. Toto se projevuje jako slabé místo navrženého řešení, neboť vyžaduje vybavení pracovišť pořizujících dokumenty licencemi *Acrobatu*. V případě, že jsou velmi pečlivě vybrány vhodné typy dokumentů a za cenu mnohem složitější dokumentové logiky a programování, je možné optimalizovat počet nutných pracovišť vybavených licencí *Adobe Acrobat Pro*. V takovém případě se však můžeme snadno dostat na licenční omezení max. 500 podání jednoho dokumentu s vloženou licencí rozšířených funkcí *Adobe Readeru*.

V případě širšího nasazení práce se zabezpečeným PDF dokumentem doporučujeme použít serverové řešení *Adobe LiveCycle Enterprise*, které nemá licenční omezení na 500 podání. Použití serverového řešení je sice významně finančně náročnější, ale za to otevírá široké možnosti využití PDF technologie. *LiveCycle Enterprise server* umožňuje generovat online personalizované dokumenty, má pokročilé nástroje pro automatické zpracování vyplněných formulářů a životního cyklu dokumentu. Na *LiveCycle serveru* je postaveno mnoho systémů spisových služeb a řízení firemní komunikace u nás i ve světě.

3 Změny v projektu

Během řešení projektu došlo k několika změnám. Díky výrazné slevě při nákupu produktu *Adobe Acrobat Pro* jsme za plánované prostředky nakoupily 22 ks licence tohoto produktu. V záměru projektu bylo původně zamýšleno pořídit 10 licencí software. Díky tomuto navýšení můžeme vybavit větší počet pracovišť „velkým“ *Acrobatem* a to nám umožní lépe využít zabezpečeného PDF v praxi.

Díky dobré dohodě se školitelskou firmou proběhlo školení přímo v prostorách naší univerzity. Uspořené prostředky za cestovní náklady na školení jsme využily na rozšíření rozsahu školení a konzultační práce spojené s řešením specifík prostředí naší VŠ. Uvedené změny neměly negativní vliv na uskutečnění deklarovaných cílů, naopak vedly k ještě většímu prohloubení znalostí problému a zvládnutí specifík prostředí VŠ. Nákupy licencí a platby za školení byly hrazeny z prostředků domovské organizace řešitele jako spoluúčast na tomto projektu.

4 Výstupy projektu

Závěry a výstupy projektu jsou prakticky použity na tvorbu bezpečných a interaktivních PDF dokumentů v rámci Centra informatizace ZČU. V rámci projektu byly vytvořeny ukázkové typické dokumenty pro výše uvedené typy dokumentů. Zejména se jednalo o následující kategorie a dokumenty.

- El. formuláře – el. dovolenka
- Korekční režim dokumentu – návrh normy, zápis ze schůze
- Publikování – vyhláška, el. dotazník

Podrobný přehled ukázkových dokumentů včetně možnosti vyzkoušení je uveden na stránce projektu.¹

Praktické využití dokumentů bylo dosaženo v rámci Centra informatizace ZČU v oblasti el. formuláře „Dovolenka“, který složí k hlášení záměru výběru dovolené pro vedoucí oddělení a sekretariát. Dále jsou využívány el. podpisy v oblasti publikování a to formou vyhlášek vydávaných ředitelem centra. Pro hodnocení kvality seminářů CIV, mohou účastníci vyplnit el. dotazník v pdf, který také vznikl na základě poznatků získaných v tomto projektu.

Praktické zkušenosti byly prezentovány v rámci pravidelných setkání zaměstnanců centra. Další praktické zkušenosti práce s využitím zabezpečených PDF dokumentů budou prezentovány formou semináře CIV.

Bohužel se nám nepodařilo prezentovat výsledky na konferenci EUNIS, protože v době kdy byly závěry projektu k dispozici se neuskutečnila žádná vhodně tématicky zaměřená konference. Ovšem tato obsáhlá technická zpráva včetně ukázkových dokumentů je zveřejněna na stránce projektu¹. Autoři se budou nadále snažit prezentovat výsledky projektu při vhodné akci sdružení EUNIS.

5 Přínosy projektu

Hlavním přínosem projektu je ověření možností technologie PDF pro sdílení, publikování a el. oběh dokumentů. Prakticky bylo otestováno využití produktů *Adobe Acrobat*. Byly navrženy postupy vhodného uspořádání využití nástrojů *Adobe Acrobat Pro* a volného *Acrobat Readeru* při vzniku a použití dokumentů tak, aby se minimalizovaly požadavky na licence produktu *Acrobat Pro*. Na klíčová pracoviště Centra informatizace byl nainstalován *Acrobat Pro* a tím bylo umožněno publikovat zabezpečené PDF dokumenty s vloženou možností úprav v *Acrobat Readeru*.

Díky uskutečněnému školení jsme získaly tým vývojářů schopných tvorby a dalšího rozšiřování interaktivních zabezpečených PDF dokumentů. Byly vyvinuty pilotní dokumenty pro ověření funkce technologie a ustavení postupů jak využít komponentu obsahující dokument včetně dokumentové logiky spolu s technologicko-administrativními opatřeními v prostředí informačního systému ZČU. Na základě znalostí a zkušeností získaných řešením projektu bude možné další rozšiřování využití PDF dokumentů v prostředí IS vysoké školy.

6 Tisková zpráva

Centrum informatizace a výpočetní techniky na ZČU v Plzni testuje díky podpoře Fondu rozvoje CESNET nové možnosti jak využít standardizované technologie PDF pro zabezpečený oběh dokumentů. Tento rozvojový program přinese elektronické verze schvalování běžných formulářů a pokládá základ pro kompletní náhradu papírového dokumentu elektronickým.

7 Přílohy

- Výkaz hospodaření s prostředky (list E)
- Faktury nákupu licencí a školení
- finanční vyhodnocení projektu

¹ <http://support.zcu.cz/index.php/CIV:Granty/331R1>