Zabezpečený elektronický dokument v prostředí VŠ

Pavel Jindra
Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky
e-mail: paja@civ.zcu.cz

14.října 2009

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 bude ucelená komponenta se sadou metod a postupů jak integrovat vytváření zabezpečených el. dokumentů v informačních systémech univerzity. Tento projekt pokládá základ pro kompletní náhradu papírového dokumentu elektronickým a tím posunout procesy VŠ dále směrem k e-univerzitě.

1. Současný stav řešeného problému

Západočeská univerzita již řadu let využívá kvalitní PKI infrastrukturu postavenou na technologii ENTRUST. Klíčoví zaměstnanci jsou vybaveni osobním certifikátem vydaným certifikační autoritou spravovanou ZČU. Pro zajištění podmínky nepopíratelnosti a možnosti využít PKI jako prostředek legislativní důvěry jsou všechny osobní certifikáty vydávány výhradně na čipové kartě poskytující dostatečnou ochranu soukromého klíče. V současné době připravujeme využití nové certifikační autority CESNET CA, jako náhrady všech certifikačních služeb. Tento krok přinese nejen standardizaci certifikačních služeb mezi VŠ, ale i vzájemnou důvěru a uznávání certifikátu mezi jednotlivými VŠ. Uložení certifikátů na čipové kartě zůstane zachováno tak, aby přinášelo uživatelům jasný prostředek bezpečnosti.

S využitím uvedené fungující PKI infrastruktury již několik let používáme elektronické podpisy pro aplikaci el. oběhu dokumentů (objednávek a faktur). Tento systém je postaven na technologii VERSO od fy. DERS a zahrnuje sadu webových formulářů, workflow a mechanizmy podpisu XML dat reprezentující příslušné dokumenty. Systém je s úspěchem využíván na většině pracovišť a přináší značné zjednodušení a zrychlení celého procesu schvalování dokumentů.

Popisovaný systém el. oběhu dokumentů však nepokrývá případy, kdy je nutné zpracovat a publikovat dokumenty různorodého obsahu určené širokému spektru uživatelů (např. studentům). Z hlediska bezpečnosti a především průkaznosti je nezbytné takové dokumenty opatřit el. podpisem. Každý koncový uživatel by měl mít možnost jednoduše, bez ohledu na platformu ze které přistupuje, přečíst dokument a ověřit platnost el. podpisu. Řešení, které by naplňovalo tyto požadavky a zároveň bylo dostatečně robustní a snadno použitelné nám doposud chybí.

2. Cíle projektu

Cílem projektu je najít způsob tvorby zabezpečeného elektronického dokumentu, který by byl vhodný pro prezentaci a publikování dat v rámci činnosti VŠ. Součástí řešení je určení vhodného formátu dat umožňujícího zabezpečení el. podpisem. Formát musí být standardizovaný, široce využívaný tak, aby byl akceptovatelný širokým spektrem uživatelů z řad studentů a zaměstnanců VŠ. Součástí projektu je nalezení a určení vhodných postupů k vytváření, schvalování a publikování takových dokumentů. Díky tomuto projektu by měla vzniknout ucelená komponenta pro publikování zabezpečených dokumentů snadno integrovatelná do dalších informačních systémů VŠ. Využití nalezených řešení se předpokládá ve třech hlavních funkcích informačního systému. První je publikování dokumentů pro širokou masu uživatelů ve smyslu důvěryhodném předání informací. Typickým využitím je např. el. úřední deska. Druhou funkcí zabezpečeného el. dokumentu bude el. oběh formulářů. Předvytvořené formuláře by měli sloužit jako náhrada různých papírových formulářů. Charakteristickým příkladem takového formuláře může být např. el. dovolenka. Další důležitou oblastí využití zabezpečeného dokumentu v prostředí VŠ bude el. korekční a schvalovací proces. Díky využité komponentě bude možné vytvářet dokumenty, provádět v nich korekce a potvrzovat je el. podpisem a to vše pomocí jednotné a snadno dostupné technologie. Jako nejvhodnější příklad uvedeného modelu mohou být např. zápisy ze schůzí. V rámci zavádění nových postupů je cílem projektu i intenzivní školení pro klíčové uživatele předpokládaného produktu. Na straně koncových uživatelů se předpokládá určení postupů a návodů, jak podepsané dokumenty využívat a ověřovat.

3. Způsob řešení

Předmětem realizace projektu bude nákup několika licencí produktu *Adobe Acrobat Pro* pro klíčové uživatele, kteří budou vytvářet nové dokumenty a jejich šablony. Pomocí nástroje Adobe Acrobat Pro bude možné vytvářet dokumenty PDF a vkládat do nich licence pro umožnění elektronického popisu. Dále bude možné pomocí uvedeného nástroje vytvářet i dokumenty pro revizi obsahu. Každá revidující osoba připojí na závěr ke svým poznámkám el. podpis.

První část projektu se bude zabývat:

- Analýzou možností a procesů vytváření zabezpečených el. dokumentů pomocí nástroje *Adobe Acrobat Pro.*
- Zjištěním způsobu vkládání digitálního podpisu do dokumentu a ověření funkčnosti a využitelnosti celého produktu.
- Návazností mezi nástrojem pro vytváření PDF dokumentů *Adobe Acrobat Pro* a nástrojem pro čtení a validaci předpřipravených dokumentu *Adobe Acrobat Reader.* ¨
- Zjištěním možností dokumentové logiky a skriptování zejména v oblasti tvorby formulářů.

Řešení projektu je možné rozdělit dle níže uvedených témat. Všechny kapitoly mají společný základ vycházející z použití technologie *Adobe*. Důležitá je i důkladná analýza stávajících procesů univerzity a hledání řešení, která budou přínosem používatele. Důležitou součástí výsledku, jsou i právní otázky zabývající se platností a důvěryhodností zabezpečených el. dokumentů.

Analýza technologie a prostředí

V této části projektu se řešitelský tým bude věnovat možnostem a způsobem využití použité technologie *Adobe Acrobat*. Důležité bude určení postupů instalace a integrace produktů *Adobe Acrobat Pro* a *Adobe Acrobat Reader*, tak aby umožňovaly spolupráci s čipovými kartami uživatelů a akceptovaly certifikáty vytvořené danou PKI infrastrukturou. Použitá technologie Adobe umožňuje vytváření inteligentních dokumentů opatřených i dokumentovou logikou. Takové dokumenty se vytváří programováním pomocí jazyka založeného na JAVAscriptu. V rámci projektu bude nutné, aby příslušní programátoři nastudovali tento jazyk a byli schopní vytvářet složitější dokumenty zvláště v oblasti tvorby formulářů.

Publikování dokumentů

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 a nebyl pozměněn. Uživatel tak dostane jednoduchý formát, pomocí kterého může zjistit důvěryhodnost dokumentu. Bude moci dokument stáhnout a prohlížet offline, případně jej snadno vytisknout v takové podobě, v jaké vznikl. Typické použití této komponenty bude v aplikacích úřední desky, nebo na různých katedrálních a fakultních webech. Typickým konzumentem služby bude široká masa studentů a zaměstnanců VŠ.

Nejsložitější částí této komponenty bude navržení vhodného workflow tvorby a schvalování dokumentu na straně jeho vzniku. Typické využití předpokládáme v režimu sekretářka-vedoucí, kdy sekretářka na základě podkladů zaslaných např. v textovém dokumentu vytvoří pomocí nástroje *Adobe Acrobat Pro* dokument a opatří jej licencí pro podpis. Výsledný PDF dokument zašle k podpisu vedoucímu, který již může využít jen volně šiřitelný *Adobe Acrobat Reader* a dokument schválí.

Elektronický oběh formulářů

Tato možnost využití zabezpečených dokumentů v prostředí VŠ je cílena na skupinu zaměstnanců. Předpokládáme, že v rámci projektu vzniknou el. formuláře, které bude možné vyplňovat a el. podepisovat pomocí běžně rozšířeného nástroje *Adobe Acrobat Reader*. Oběh dokumentu se bude co nejvíce blížit dosavadnímu papírovému způsobu. Programátor připraví prázdné formuláře opatřené vhodnou formulářovou logikou. Do dokumentu se vloží možnost podpisu několika osobami (typicky řetězec: žadatel – správce - příkazce). El. dokument podepsaný všemi účastníky je pak doručen zpracovateli, který buď zpracuje celý formulář, nebo z něj může získat jen formulářová data ve formátu XML. Součástí zavedení tohoto využití musí být nejen nalezení vhodných postupů pro workflow, ale také právní posouzení validity podepsaného dokumentu.

Schvalování a el. korekce dokumentů

Poslední skupina dokumentů využívá možnosti uvedené technologie pro vytváření a posuzování dokumentů v režimu korekcí. Předpokládáme nasazení zabezpečeného el. dokumentu pro využití např. pro zápisy z porad. Pomocí aplikace *Adobe Acrobat Pro* bude možné vytvořit dokument (např. zápis z porady). V dokumentu se aktivuje možnost vytvářet korekce a el. podpisy. Dokument pak postupně může projít všemi schvalovateli, kteří jej mohou opatřit poznámkami a korekcemi, popřípadě jej každý může podepsat. Hlavní schvalovatel nakonec dokument sestaví a opatří el. podpisem a zamkne. Tím bude proces schvalování ukončen a je možné dokument publikovat nebo archivovat. Výhodou tohoto řešení je možnost snadno oddělit korekturní poznámky od textu a možnost prohlížet jednotlivé verze dokumentů podle jejich schvalovatele. Navíc bude možné využít k provádění

korektur a el. podpisu jen volný *Adobe Acrobat Reader* dostupný pro široké spektrum platforem.

Školení

Součástí implementace nástroje *Adobe Acrobat Pro* je i intenzivní 2 denní školení klíčových uživatelů, které bude hrazeno z prostředků projektu. Díky tomuto školení získají pracovníci znalosti a zkušenosti s tvorbou PDF dokumentů s el. podpisem, PDF formulářů a dokumentů realizujících jednoduché schvalování. Dále se seznámí s možnostmi revize PDF dokumentů a jejich publikování.

Předmětem školení jsou především tato témata:

- Postupy tvorby PDF dokumentů.
- Úpravy dokumentu: záhlaví/zápatí, pozadí, vodoznak, manipulace se stránkami, vkládání záložek (+ strukturované záložky).
- Komentování souborů: Základní koncept komentování a oběhu dokumentů ve firmě, odesílání souboru k revizi/komentování, vkládání komentářů, zpracování komentářů (řešení komentářů, import/export komentářů).
- Nástroje editace dokumentů – nastavení pořadí čtení článku, hlasitého čtení, propojování a další nástroje.
- 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.

Budeme se snažit v rámci projektu dohodnout s dodavatelem školení individuální přístup a orientaci školení přímo na prostředí VŠ. Pokud to bude možné a kapacita školení nebude zcela naplněna budou volná místa k dispozici členům sdružení CESNET.

Obecné

Důležitou součástí celého projektu je PKI infrastruktura. Každý uživatel má osobní certifikát uložený na čipové kartě. Tím je zaručena prokazatelnost a neodmítnutelnost el. podpisu v dokumentech. Integrace čipové karty do *Adobe Acrobat Readeru* je realizována prostřednictvím standardních rozhraní MS CAPI (Crypto API). To značně rozšiřuje oblast možného využití i s ohledem na to, že na straně koncového uživatele stačí obecně rozšířený bezplatný *Adobe Acrobat Reader*.

V poslední části projektu se budeme zabývat tvorbou pracovních postupů a doporučení. V neposlední řadě tvorbou dokumentace. V rámci této části bychom chtěli v pilotním provozu převést vybrané portálové aplikace tak, aby maximálně využívaly technologické možnosti zjištěné v průběhu projektu.

Pro dosažení uvedených cílů bude nutné zakoupit několik pilotních licencí pro SW na vytváření PDF dokumentů *Adobe Acrobat Pro*. Dále se klíčoví uživatelé z řad vedoucích a administrativních pracovníků zúčastní školení se zaměřením na přípravu zabezpečených PDF dokumentů. Největší úsilí v rámci projektu bude věnováno analýzám a hledání vhodného řešení integrace této technologie do prostředí VŠ. Bude nutné analyzovat řadu aplikací, konzultovat vhodná řešení s klíčovými uživateli a nacházet uspokojivá východiska jak vhodně nahrazovat stávající papírové podklady jejich elektronickými verzemi.

4. Prezentace výsledků

V rámci projektu budou vypracovány uživatelské návody a popisy. Z realizovaných školení budou k dispozici materiály a výsledky budou předány dalším uživatelům. Možnosti a funkce tohoto systému budou podrobně představeny administrátorům v rámci pravidelných seminářů ZČU - CIV. Odborné materiály a analýzy budou zájemcům dostupné prostřednictvím WWW stránek CIV, ZČU v Plzni. Záměrem řešitelů je prezentovat obecné výsledky a přínosy projektu v rámci konference sdružení EUNIS. Volba této konference je především proto, že EUNIS stejně jako CESNET sdružuje většinu veřejných VŠ a navíc úzce spolupracuje s dodavatelem technologie fy Adobe. Sdružení EUNIS pravidelně pořádá konference zaměřené na rozvoj informačních systémů VŠ, především v oblasti e-komunikace a bezpečnosti, což přesně koresponduje s tímto projektem.

5. Charakteristika řešitelského kolektivu

Řešitelem projektu je Ing. Pavel Jindra, spoluřešitelem *Ing. Luboš Kejzlar*.

Ing. Pavel Jindra (hlavní řešitel)
je absolventem Fakulty elektrotechnické na Západočeské Univerzitě v Plzni. Od roku 2003 pracuje v Laboratoři počítačových systémů Centra informatizace a výpočetní techniky, kde je v současné době vedoucím projektu PKI. Pracovní náplň tvoří správa, provoz a konfigurace centrálního autentizačního systému Kerberos a správa certifikační autority. Zároveň se podílí na několika projektech týkajících správy uživatelských identit (IdM). Od roku 2005 je řešitelem sdružení CESNET v oblasti PKI.

Ing. Luboš Kejzlar (spoluřešitel)
je absolventem Fakulty elektrotechnické Vysoké školy strojní a elektrotechnické v Plzni v oboru Automatizované systémy řízení. Od roku 1989 je v různých funkcích členem Laboratoře počítačových systému (LPS) Centra informatizace a výpočetní techniky (CIV) ZČU v Plzni.V rámci své pracovní náplně se podílel na řešení řady rozsáhlých projektů z oblasti návrhu síťové infrastruktury a implementace distribuovaného výpočetního prostředí ORION. S několika přestávkami se od počátku podílí na realizaci projektů Superpočítačová centra VŠ a návazně MetaCentrum. Mezi jeho profesní zájmy patří problematika bezpečnostní infrastruktury a distribuovaných výpočetních prostředí. Od roku 2002 řídí ve funkci vedoucího LPS kolektiv cca. třiceti spolupracovníků, kteří se aktivně podílejí na tvorbě koncepce, implementaci a provozu komplexního výpočetního prostředí ZČU. Z povahy své funkce v současnosti řídí a podílí se na řešení řady střednědobých infrastrukturálních projektů v oblasti PKI, AAA, mobility, SSO, MOM (Message Oriented Middleware), identifikačních technologií apod.

6. Navrhovaná doba projektu

Navrhovaná doba trvání projektu je 12 měsíců.

7. Finanční rozvaha a rozsah prací

V rámci projektu požadujeme neinvestiční prostředky na pořízení 10ks licence produktu *Adobe Acrobat Pro*. Dále požadujeme prostředky pro uskutečnění krátkého intenzivního školení klíčových uživatelů produktu pro min. 5 uživatelů. K nákladům na školení je třeba připočíst i tuzemské cestovní výdaje. Vzhledem k rozsahu uváděného problému a množství aplikací, pro které je nutné zhodnotit postupy a návrhy řešení předpokládáme rozsah prací na úrovni cca 76 člověkodní. Odměna za jeden člověkoden včetně zdravotního a sociálního pojištění činí 2500,- Kč. Po úspěšném splnění cílů projektu navrhujeme za řízení projektu a konzultační činnosti vyplatit řešitelům odměnu 10 000,- Kč včetně zákonného pojištění.

Rozsah prací:

Administrativní část

Položka	**Počet MD**
Analýza technologie a prostředí	5
Instalace a integrace produktu do prostředí OrionXP	4
Interakce mezi *Acrobat Pro* a *Acrobat Reader*	2
Skriptovací jazyk dokumentu	4
Celkem	**15**

Publikování dokumentů

Položka	**Počet MD**
Analýza stávajících řešení	5
Návrh procesů a workflow pro vytváření dokumentů	3
Úprava aplikací	5
Uživatelská osvěta	2
Tvorba návodů a dokumentace	4
Celkem	**19**

Elektronický oběh formulářů

Položka	**Počet MD**
Analýza potřeb a výběr vhodných formulářů	5
Návrh workflow oběhu formuláře, návrh dokument logiky	5
Tvorba inteligentních formulářů	8
Tvorba návodů a dokumentace	4
Celkem	**22**

Schvalování a el. korekce dokumentů

Položka	**Počet MD**
Návrh workflow oběhu dokumentu	4
Tvorba šablon a vzorových dokumentů	3
Tvorba návodů a dokumentace	3
Celkem	**10**

Školení a příprava projektu

Položka	**Počet MD**
Příprava školení	2
Příprava prezentace výsledků	3
Řízení a správa projektu	5
Celkem	**10**

Rozpočtové položky:

Položka	**Počet**	**Cena/MJ**	**Cena Kč s DPH**	**Hradí**
Licence Adobe Acrobat Pro	10	5 100,-	51 000,-	ZČU
Školení Adobe Acrobat Pro	5	6 000,-	30 000,-	ZČU
Cestovné tuzemské	5	4 000,-	20 000,-	ZČU
Mzdy (včetně zákonného pojištění)			189 000,-	FR Cesnet
Odměny řešitelům		10 000,-	10 000,-	FR Cesnet

Celková částka nákladů na projekt činí **300 000,- Kč** (s DPH). Z prostředků fondu rozvoje budou čerpány náklady na mzdy a odměny ve výši **199 000,- Kč** . Z prostředků řešitele bude hrazeno školení pro min. 5 klíčových uživatelů včetně cestovních výdajů a 10 licencí *Adobe Acrobat Pro* v celkové hodnotě **101 000,-** jako neinvestiční položka. Licence zakoupené v rámci projektu zůstanou po skončení projektu v majetku řešitele.