

Softwarové řešení pro e-pasy

Počínaje zářím 2006 jsou občanům České republiky vydávány nové cestovní pasy, které se významně liší od svých předchůdců: obsahují elektronický čip, na němž jsou uloženy základní údaje o držiteli pasu včetně jeho fotografie. O zavedení těchto tzv. cestovních dokladů s biometrickými prvky, zkráceně označovaných jako „e-pasy“, bylo rozhodnuto Radou EU v prosinci 2004 v souladu s celosvětovým trendem v oblasti cestovních dokladů, který s mandátem OSN koordinuje ICAO – mezinárodní organizace civilního letectví. Jedná se mj. o nutnou podmínku pro zachování, resp. zavedení bezvízového styku se Spojenými státy. Hlavním důvodem pro tuto inovaci je zvýšení bezpečnosti cestovních dokladů a dále se do budoucna počítá s automatizovaným ověřováním totožnosti držitele pasu na hraničních přechodech, letištích apod.

Hlavním dodavatelem rozsáhlého technického řešení, zajišťujícího funkce potřebné pro vydávání e-pasů pro Ministerstvo vnitra (MV), byla STÁTNÍ TISKÁRNA CENIN, státní podnik (STC). Společnost KOMIX s.r.o. se podílela na realizaci významné části systému – byl jí svěřen vývoj softwaru pro zpracování žádostí a další procesy spojené s vydáváním těchto dokladů. V dalším textu představíme základní architekturu a důležité aspekty především této části systému. Není zde hovořeno o vlastních elektronických pasech a technologiích v nich použitých. Rovněž nejsou popisovány další oblasti řešení, které spadaly pod jiné dodavatele (Siemens, IBM, Monet+, aj.) – např. detaily hardwarové architektury, vlastní výroba dokladů v STC či Národní certifikační autorita, která vydává certifikáty pro elektronické podepisování údajů v e-pasu.

ARCHITEKTURA ŘEŠENÍ

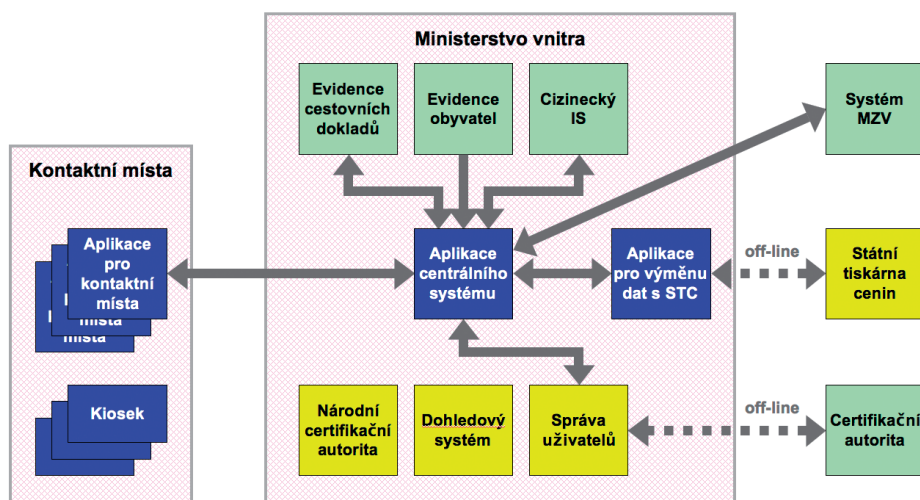
Architektura vytvořeného systému včetně vazeb na okolní systémy je patrná z obrázku. Řešení, které spadalo do naší kompetence (modře zbarvené), obsahuje: klientské aplikace pro kontaktní místa, samoobslužné kiosky, aplikace centrálního systému a aplikace pro výměnu dat s STC.

Kontaktními místy jsou obecní úřady, které zajišťují vydávání běžných e-pasů pro občany ČR, a pracoviště Oblastních ředitelství Policie ČR vydávající doklady pro cizince a uprchlíky. Klientské aplikace zde poskytují funkce pro pořízení nové žádosti o cestovní doklad, předání vyrobeného dokladu držiteli, reklamaci dokladu, zpracování žádostí přicházejících ze zastupitelských úřadů, obnovu uživatelských certifikátů uložených na čipové kartě a další doplňkové funkce. Kromě „ostrých“ klientských aplikací jsou na všech kontaktních místech instalovány ještě tzv. „školicí“ aplikace, které slouží pro



zaškolení nových úředníků a liší se tím, že nedochází k výměně dat s centrálním systémem – „školicí“ data jsou uložena lokálně. Samoobslužné kiosky na kontaktních místech umožňují držiteli e-pasu ověřit funkčnost čipu.

Centrální systém (CS) zajišťuje sběr a uložení dat žádostí vytvářených na kontaktních místech, zprostředkovává výměnu dat s externími systémy (evidenční obyvatel, evidenční cestovních dokladů, cizinecký IS, systém e-pasů Ministerstva zahraničních věcí), provádí autonomní dávkové úlohy (příprava dávek pro STC, likvidace biometrických údajů v zákonem stanovené lhůtě), obsahuje subsystém pro správu uživatelů a výměnu dat s certifikační autoritou a umožňuje monitorování systému a dat v něm uložených.



Systémy MV a STC komunikují v offline režimu z důvodu splnění požadavků na vysoký stupeň zabezpečení personalizačního centra.

KLIENSKÉ APLIKACE

Z technického hlediska jsou velmi zajímavou částí řešení klientské aplikace pro kontaktní místa. Integrují totiž velké množství komponent, které jsou nutné pro zpracování žádostí o e-pasy. Jedná se o:

- fotografický přístroj a příslušný softwarový modul, který zajistí nejen vlastní pořízení podoby obličeje žadatele, ale rovněž implementuje funkce pro automatické ověření kvality fotografie, aby vyhovovala mezinárodním standardům; jako příklad automatických kontrol uveďme: čelní pohled žadatele, otevřená ústa, zavřené oči, stíny a přešvícená místa, odlesky na brýlích, aj.;
- tablet a software pro digitalizaci podpisu žadatele; za zmínku stojí, že bylo nutno vyvinout algoritmus, který zajistí normalizaci velikosti podpisu (žadatelé různým způsobem využívají plochu pole pro podpis na žádosti), aby se dosáhlo vysoké kvality při tisku podpisu do e-pasu;
- čtečku e-pasů, která je využita nejen pro načítání údajů z čipu nově vyrobených e-pasů (kvůli kontrole), ale rovněž se používá pro automatické získání rodného čísla žadatele z dokladu obsahujícího strojově čitelnou zónu;
- čtečku čipových karet; čipové karty s uživatelskými certifikáty a privátními klíči se využívají jak pro autentizaci uživatele, tak pro elektronické podepisování vytvořených žádostí;
- 2 monitory připojené ke klientské stanici, z nichž jeden je určen pro úředníka a druhý je obrácen směrem k žadateli a slouží pro kontrolu pořízené fotografie, resp. údajů v novém e-pase;

- tiskárnu pro tisk žádostí; pro občana odpadla nutnost ručního vyplňování údajů do žádostí, naopak veškerá data jsou pořízena elektronicky a jediným manuálním úkonem žadatele je vytvoření dvou podpisů na vytištěné žádosti.

Klientské aplikace jsou vytvořeny v technologii .NET, která nejnázne umožňuje integrovat uvedené množství různorodých komponent, jejichž obslužný software je obvykle realizován v těže či příbuzných technologiích.

CENTRÁLNÍ SYSTÉM

Na straně centrálního systému se zmíníme krátce o použité architektuře, která má zajistit především dostatečnou výkonnost, spolehlivost a vysokou dostupnost. Systém je dimenzován na zpracování až 20.000 žádostí denně.

Kvůli spolehlivosti a rozložení zátěže zpracovává CS klientské požadavky ve dvou paralelních větvích propojených do clusteru, z nichž každá obsahuje hardwarově oddělený web server, aplikační server (oba typy serverů z rodiny Sun Java System) a databázový server (Informix). Data jsou pak uložena v externím diskovém poli. V případě havárie centrálního výpočetního střediska lze provoz přepnout na záložní středisko, kde je udržována replika provozní databáze.

Aplikace CS jsou postaveny nad technologií J2EE. Pro komunikaci s okolními systémy včetně výměny dat s klientskými aplikacemi se používají webové služby. Vzhledem k tomu, že žádosti v XML formátu jsou poměrně velké (řádově stovky KB) a propustnost datových přípojek obecních úřadů není vždy optimální, bylo nutno použít komprimaci dat žádostí.

ZABEZPEČENÍ DAT

Systém pracuje s osobními údaji občanů a proto je ochrana dat po celou dobu zpracování věnována mimořádná pozornost. Ke slovu přichází masivní využití PKI technologií, a sice v oblastech:

- autentizace uživatele do systému a ustanovení HTTPS spojení s CS pomocí komerčního certifikátu uloženého na čipové kartě;
- podepsání vytvořené žádosti kvalifikovaným certifikátem úředníka na kontaktním místě, který je rovněž uložen na čipové kartě;
- šifrování biometrických údajů žádosti pomocí veřejného klíče STC;
- podepsání dávek připravených pro odeslání do STC soukromým klíčem CS, uloženým v HSM modulu;
- šifrování dat na datových nosičích přenášených mezi MV a STC;
- podepsání obsahu nosiče pro STC úředníkem MV, resp. návratového nosiče zaměstnancem STC;
- podepsání údajů v čipu e-pasu pomocí klíče tzv. Document Signer (DS).

Pro ustavení bezpečné komunikace mezi CS a externími systémy je využito HTTPS se základní autentizací pomocí jména a hesla, což je dostatečný způsob ochrany vzhledem ke skutečnosti, že se jedná o komunikaci po privátní síti.

OČEKÁVANÝ VÝVOJ

Systém nasazený do produkčního prostředí průběžně doznává drobných úprav a vylepšení. Podstatná úprava chování systému bude probíhat v následující etapě, kdy přibudou mezi údaje uložené v čipu e-pasu rovněž otisky prstů držitele a nový způsob ochrany údajů v čipu. Uvedené změny si vyžádají úpravu klientských aplikací i centrálního systému a některých datových rozhraní. Zavedení otisků prstů do čipu cestovního dokladu je pro členské státy EU stanoveno do 28. 6. 2009.

Ing. Petr Sobotka
vedoucí projektu
KOMIX s.r.o.

