Single-Sign-On a jeho význam pro personalizaci

Single-Sign-On an its importance to personalization

Bc. Josef Martinák

Diplomová práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Josef MARTINÁK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Single-Sign-on a jeho význam pro personalizaci**

Zásady pro vypracování:

1. **Definice e-governmetu, popis systémů, význam a účel.**
2. **Defince Single-Sign-On, význam a účel.**
3. **Personalizace a její význam.**
4. **Analýza potřeb Single-Sign-On pro personalizaci v e-governmentu.**
5. **Věcný návrh systému Single-Sign-On, studie proveditelnosti.**
6. **Přínos práce, zhodnocení výhod a nevýhod navrženého systému.**

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government, Dostupný z: http://www.springerlink.com/content/j14331m2h184.**
2. **E-Government: Towards Electronic Democracy, Dostupný z: http://www.springerlink.com/content/wma3d67vuj60.**
3. **E-government and Public Sector Process Rebuilding, Dostupný z: http://www.springerlink.com/content/k78230.**
4. **E-Government Ict Professionalism and Competences Service Science, Dostupný z: http://www.springerlink.com/content/nw343r381406.**
5. **ANTTIROIKO, Ari-Veikko, MÄLKIÄ, Matti. Encyclopedia of digital government. [s.l.] : [s.n.], 2007. 3 sv. (290, 400, 700 s.). ISBN 9781591407904.**
6. **MATES, Pavel. E-government v českém právu. 1. vyd. Praha : Linde, 2006. 244 s. ISBN 80-7201-614-8.**

Vedoucí diplomové práce: **Ing. Radek Šilhavý**
Ústav aplikované informatiky

Datum zadání diplomové práce: **20. února 2009**

Termín odevzdání diplomové práce: **27. května 2009**

Ve Zlíně dne 13. února 2009

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá především možnostmi využití technologie Single Sign-On a s tím spojená rizika, se zaměřením na služby e-govertnmentu.

V teoretické části je nejprve přiblížena základní myšlenka e-governmentu a analýza současného stavu v České republice. Popsány jsou zde jednotlivé pilíře realizace elektronické vlády a jejich podstata. Další část je pak věnována technologii Single Sign-On, základním principům a vlastnostem jednotlivých řešení. Poslední část se pak zabývá možnostmi personalizace webových informačních systémů.

Praktická část práce se zabývá analýzou potřeb Single Sign-On pro nasazení v oblasti e-governmentu a návrhem vyhovujícího řešení.

Klíčová slova: e-government, Single Sign-On, personalizace, autentizace, Central Authentication Service

ABSTRACT

This diploma thesis is engaged first of all in possibilities of using Single Sign-On technology and its risks, focused on e-government services.

In the theoretical is at first described the main idea of e-govenrment and the analysis of current state in Czech Republic. There are described the main parts of electronic government and their principles. Another part is engaged in Single Sign-On technology, its basic principles and features of particular solutions. Last part is attended to personalization of web information systems.

The practical part deals with analyzing the needs of Single Sign-On for deployment in the field of e-government and satisfactory solution.

Keywords: e-government, Single Sign-On, personalization, autentizace, Central Authentication Service

Děkuji panu Ing. Radku Šilhavému, vedoucímu mé diplomové práce, za pomoc v průběhu jejího řešení.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

OBSAH

ÚVOD

Využívání moderních informačních technologií ve státní správě se stává trendem ve všech vyspělých státech. Často bývá spojeno s celkovou reformou fungování státem poskytovaných služeb. Cílem je zefektivnění fungování celého veřejného sektoru a především úspory v této oblasti.

Takovéto nasazování informačních technologií bývá označováno pojmem e-government. V některých případech zatím dochází pouze k elektronizaci některých úkonů, než k celkovému zlepšení fungování veřejných služeb. I toto je však významným krokem směrem ke kompletní reformě a úspěšnému nasazení e-governmentu.

Významným faktorem při zavádění elektronické vlády je zaměření na všechny občany a s tím spojené požadavky na celý systém. Musí počítat s tím, že služeb budou využívat i uživatelé s nízkou počítačovou gramotností a na druhou stranu i uživatelé zkušení. Všem by měl být poskytnut přiměřený uživatelský komfort. Elektronická forma komunikace v této oblasti navíc vyžaduje pokročilé stupně identifikace jednotlivých uživatelů. Stejně jako při běžné komunikaci s úřady, při níž se prokazujeme příslušnými doklady, je i zde nutné se jednoznačně identifikovat.

S ohledem na tyto podmínky je řešením využití technologie jednotného přihlašování (Single Sign-On) ve spojení s kvalitními identifikačními postupy a vysokým stupněm personalizace. Služeb poskytovaných v rámci e-governmentu je celá řada. Singl Sign-On umožňuje uživateli přihlásit se pouze jednou a posléze využívat všech dostupných služeb bez opětovného prokázání vlastní identity. Toto nejen šetří čas, ale také zvyšuje bezpečnost komunikace. V kombinaci s kvalitními autentizačními postupy navíc zaručuje jednoznačnou identifikaci občana, která je nutná k jednotlivým úkonům v oblasti veřejné správy.

Základní výhodou využití identifikace je možnost zobrazovat jednotlivým uživatelům personalizovaný obsah. Personalizace přináší osobní přístup ke každému z uživatelů služeb e-governmentu, kde na základě identifikovaného uživatelského profilu dochází k zobrazení relevantních informací.

Jedná se o možnost poskytnout uživatelům služeb přizpůsobení vzhledu uživatelského rozhraní. Každý u uživatelů může mít možnost si službu upravit rozložením nebo barevně do jemu vyhovující podoby.

Druhá rovina je pro účely služeb e-governmentu významnější. Jde o oblasti, kdy lze identifikovanému uživateli zobrazit jím nejžádanější služby na prvním místě. Dále lze upravovat - přednostně zobrazovat služby a informace, které budou příslušné například místu jeho trvalého bydliště nebo jeho dalším osobním informacím, které budou obsaženy v identifikaci.

Předmětem práce je prozkoumat možnosti identifikace v systémech elektronické vlády. Zkoumání je zaměřeno na oblasti možností ověřovacího principu Single Sign-On ve spojitosti k přístupu ke službám a přínos identifikace k personalizaci poskytovaných služeb.

I. TEORETICKÁ ČÁST

1 E-GOVERNMENT

V této úvodní kapitole jsou popsány důvody a cíle využívání moderních informačních a komunikačních technologií v oblasti veřejné správy, což bývá označováno pojmem e-government. Ačkoli v některých případech se jedná pouze o elektronizaci různých úkonů, než o opravdové zkvalitnění (z hlediska účinnosti a efektivity) výkonu vlády veřejnými subjekty, jsou tyto kroky přínosem a vhodným nástrojem pro postupné zavádění e-governmentu.

E-government v České republice je založen na konceptu čtyř hlavních částí. Jsou to: Zákon o e-governmentu, základní registry veřejné správy, komunikační infrastruktura veřejné správy a kontaktních místa, tzv. Czech POINTy.

V závěru této kapitoly jsou zmíněny již fungující služby poskytované občanům ČR a také ty, jejichž zprovoznění je velmi blízkou budoucností.

1.1 Veřejná správa, reforma veřejné správy

Veřejná správa je v moderních demokraciích chápána především jako služba občanům a veřejnosti.

Od této základní úlohy veřejné správy se odvíjejí její principy (jako transparentnost, publicita, povinnost skládat účty, veřejná kontrola správy), formy a metody činnosti, požadavky na odborný a nestranný výkon aj.

Těžiště veřejné správy leží v zajišťování veřejných služeb. Do této kategorie se vedle tradičních služeb (komunálních, zdravotnických, školských, dopravních apod.) dnes běžně ve vyspělém světě zařazují i některé „klasické" správní činnosti, jako je vydávání licencí, povolení, dokladů, osvědčení, poskytování informací atp. Řada těchto činností se také přestala považovat za výhradní doménu státu. Mnohé úkoly operativní povahy, odborné rozhodování, výkon dozoru, zkušebnictví apod. lze i podle našich nových zkušeností decentralizovat a přenést na samosprávné nebo soukromé subjekty.

Další z významných funkcí veřejné správy je zajišťování a posilování demokratických institucí a mechanismů. Je možné zde hovořit o dvou hlavních směrech rozvíjení politické demokracie - směrem k upevňování institucí a mechanismů reprezentativní demokracie a dále směrem k rozvíjení institucí a mechanismů participativní demokracie, to jest přímé účasti občanů a jejich organizací na řízení a správě státu. [1]

Rozvoj, rozšíření a způsob využití ICT se staly v uplynulých letech východiskem systémových, procesních i strukturálních změn na všech úrovních řízení společnosti. Nové technologie a sítě umožňují ve srovnání s minulostí kvalitativně i kvantitativně zcela odlišný přístup k informačním zdrojům a k práci s nimi. Lidé získávají stále více dovedností potřebných pro práci s novými technologiemi, přičemž pro stále větší množství oborů platí, že nedostatek této kvalifikace je důvodem pro znevýhodnění, či dokonce vyloučení z trhu práce. Zajištění příznivých podmínek pro efektivní tvorbu, správu a šíření informací má značný rozvojový potenciál na úrovni malých a středních, ale i velkých podniků, státní správy i samosprávy. Součástí těchto podmínek jsou i dostupné informační a transakční on-line služby veřejného sektoru, které svým uživatelům přinášejí konkrétní měřitelné efekty. Informační společnost mění způsob podnikání, přístup ke službám a zboží v tak velkém rozsahu, že se někdy hovoří o tzv. nové ekonomice.

Nové technologie jsou příležitostí pro vytváření moderní a efektivní veřejné správy, která nabízí nové nebo zlepšené služby, jež jsou výsledkem reformy dosud užívaných postupů. Veřejná správa je rovněž významný účastník na trhu, který podporuje jak vývoj, tak poptávku po produktech a službách v oblasti ICT. Služby veřejné správy musí být pro uživatele jednoduché a musí být dostupné všem, tedy i handicapovaným či jinak znevýhodněným skupinám obyvatel. Moderní veřejné služby musí vycházet z potřeb svých zákazníků, tj. občanů a podnikatelů. Při využívání ICT musí být zamezeno zneužívání citlivých informací a je třeba důsledně dbát na ochranu osobních údajů. [2]

1.2 Definice E-governmentu

E-government se zabývá elektronizací výkonu veřejné správy. Jedná se to transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií. [3]

1.2.1 E-government, význam, účel

Jeho hlavním smyslem a funkcí je poskytnout lidem, resp. jakýmkoli subjektům soukromého práva větší komfort při jednání se státem a jeho orgány tím, že zjednoduší a urychlí komunikaci občanů a podnikatelských subjektů s těmito orgány s cílem posílit demokratizaci veřejné správy a její funkci jakožto služby společnosti. Není to však jen jednosměrná výhoda pro adresáty, ale i pro úředníky, kteří tím získávají více času pro

strany a méně času musí věnovat papírům. Platí to jak v případě, že dotyčný něco chce od úřadu (domáhá se práva, uplatňuje požadavek, požaduje informaci), tak i v případě, že se stává z iniciativy příslušného orgánu účastníkem řízení.

Významná je ale i výše zmíněná transformační funkce. Zavádění e-governmentu může iniciovat proces re-engineeringu jednotlivých orgánů veřejné správy, tj. provést systémové změny v organizaci a řízení orgánů tak, aby došlo k odstranění duplicit a multiplicit, zlepšil se tok informací a zkvalitnila příprava podkladů pro rozhodování. Důsledkem e-governmentu by mělo být pronikavé zefektivnění výkonu veřejné moci nejen z hlediska účastníků, ale i z hlediska státu jako takového.

Patří-li mezi požadavky výkonu veřejné moci, a především pak veřejné správy v demokratických státech transparentnost, pak e-government je významným nástrojem k jejímu zajišťování. Pokud mají občané jednodušší přístup k informacím, mohou činnost orgánů veřejné moci lépe a snáze kontrolovat, což přinejmenším snižuje nebezpečí takových jevů jako jsou korupce, nehospodárné nakládání s veřejnými prostředky, protekce, neslušné chování úředníků apod. Zároveň s tím stoupá zájem občanů o věci veřejné a ochota se v nich angažovat. Prostřednictvím elektronických médií mohou lidé např. přímo sledovat zasedání zastupitelských orgánů na ústřední i lokální úrovni, vyjadřovat se k veřejným záležitostem, je možno pořádat různé ankety, diskusní fóra a průzkumy, a perspektivně se uvažuje dokonce i o volbách.

Úřadování se stává na jedné straně méně anonymní, ale současně odpadá nutnost bezprostředního kontaktu občanů s úředníky, a tím třeba jen potenciální nebezpečí z nich plynoucí (určitě bude jen málokdo riskovat a říkat si o úplatek e-mailem nebo ho tímto způsobem nabízet).

Pokud se na tuto problematiku díváme z vnějšku, tedy z pohledu občana jakožto uživatele služeb veřejné správy, který uplatňuje svá práva a očekávání v informační společnosti, a jako aktivního účastníka veřejného života, je na místě používat spíče výraz e-občanství (e-citizenship).

Není pochyb o tom, že modernizace veřejné správy prostřednictvím moderních informačních technologií je již delší dobu na pořadu dne. Objevily se pojmy jako e-government, e-služby či e-democracy, ale také již zmíněný e-citizenship, ale i e-voting (elektronické volby) či e-rights (e-práva občanů) apod.

E-government podle projektu EU „Evropská informační společnost 2010“ znamená efektivní a výkonné veřejné služby, informační a komunikační technologie umožňující občanům plně se podílet na životě společensky a kulturně tvůrčích komunit včetně demokratického procesu. [1]

1.3 E-government v ČR

1.3.1 Státní informační politika

V říjnu 1998 se vláda usnesla na sestavení Rady pro státní informační politiku, která spolu s ÚSISem předložila koncepci „Státní informační politika – cesta k informační společnosti“.
Ten byl 1. května 1999 schválen usnesením vlády č. 525. Jak již název napovídá koncepce jasně deklarovala, že je třeba ubírat se směrem k informační společnosti.

V roce 1999 vznikla „Koncepce budování informačních systémů veřejné správy“ (dále již jen „Koncepce“). Koncepce navazovala na obsah dvou vládních dokumentů: na „Koncepci reformy veřejné správy“ a na koncepci „Státní informační politika“.

„Koncepce reformy veřejné správy byla vládou vzata na vědomí usnesením č.258 ze dne 30.3 1999. Dokument „Státní informační politika“ byl vládou přijat usnesením č. 525 ze dne 31.5.1999.

V souvislosti se vstupem České republiky do Evropské unie se vláda rozhodla předložit novou strategii ISVS. Byla pojmenována Státní informační politika eČesko 2006.

Podobně jako Koncepce z roku 1999, kladl si tento dokument za cíl sjednotit postup v budování SIS. Druhým cílem bylo vytvořit systém schopný konkurovat Evropě. Bylo třeba se připravit na otevření trhu.

Cíle informační a komunikační politiky eČesko 2006 jsou shrnuty v tzv. Akčním plánu, který je součástí tohoto dokumentu. Vláda zamýšlela: zajistit bezpečné a komunikační služby, informační vzdělanost a moderní veřejné služby on-line. Dalším cílem bylo přizpůsobit povahu českých SIS těm evropským. [4]

1.3.1.1 EgovAct

Zákon o e-governmentu je normou, která přibližuje cíl projektu e-government. Tím je snížení byrokracie, elektronizace agend a šetření času občanů i úředníků. [5]

EgovAct, jak bývá zákon o e-governmentu někdy označován, respektive návrh Zákona o elektronizaci některých procesních úkonů a o změně některých zákonů, upravuje autorizovanou konverzi písemností, legalizaci elektronického podpisu, jednoznačné určení fyzické osoby při elektronické komunikaci a poskytování služeb pro komunikaci s orgány veřejné moci.

Tento zákon by měl především zrovnoprávnit listinnou formu dokumentu s elektronickou, postavit ICT do role nositele reformy státní administrativy. Ve svém výsledku by tak mělo dojít k naplnění hesla „obíhají dokumenty, nikoli občan“, neboť komunikace občanů s úřady a úřadů s úřady by byla elektronická, respektive možná i elektronicky. Návrh zákona zavádí institut autorizované konverze písemností. Umožňuje tedy použití jak elektronické, tak „papírové“ verze dokumentu a převod dokumentu z listinné do elektronické podoby a naopak. Zároveň přiznává stejnou hodnotu elektronické i papírové verzi. Přináší také institut legalizace uznávaného elektronického podpisu. To znamená, že stejně jako v případě listinné verze je možné úřední ověření podpisu, je i v případě elektronické verze možné úřední ověření elektronického podpisu. Návrh dále zavádí pro potřeby komunikace občanů a veřejné správy datové schránky. Jejich prostřednictvím budou občané moci činit potřebná podání úřadům a úřady budou moci takto doručovat písemnosti příslušným adresátům. Tyto úkony v elektronické podobě staví návrh zákona na stejnou úroveň jako tatáž podání a doručení realizovaná v papírové verzi. [6]

Zákon o elektronických úkonech a autorizované konverzi dokumentů byl vyhlášen ve Sbírce zákonů 19.8.2008 jako zákon č.300/2008 Sb. [7]

1.3.2 Základní registry

Dnes 26. března 2009 schválil Senát Parlamentu České republiky vládní návrh zákona o základních registrech a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Podle návrhů Ministerstva vnitra budou veškeré potřebné údaje o českých občanech soustředěny v těchto čtyřech základních registrech:

Registr obyvatel

V základním registru obyvatel se povedou referenční údaje o občanech České republiky a o cizincích s dlouhodobým nebo trvalým pobytem na území České republiky. Návrh počítá dále s možností, že v registru budou evidovány i další fyzické osoby, pokud tak v budoucnu stanoví jiný právní předpis. Správcem registru obyvatel bude Ministerstvo vnitra.

Registr osob

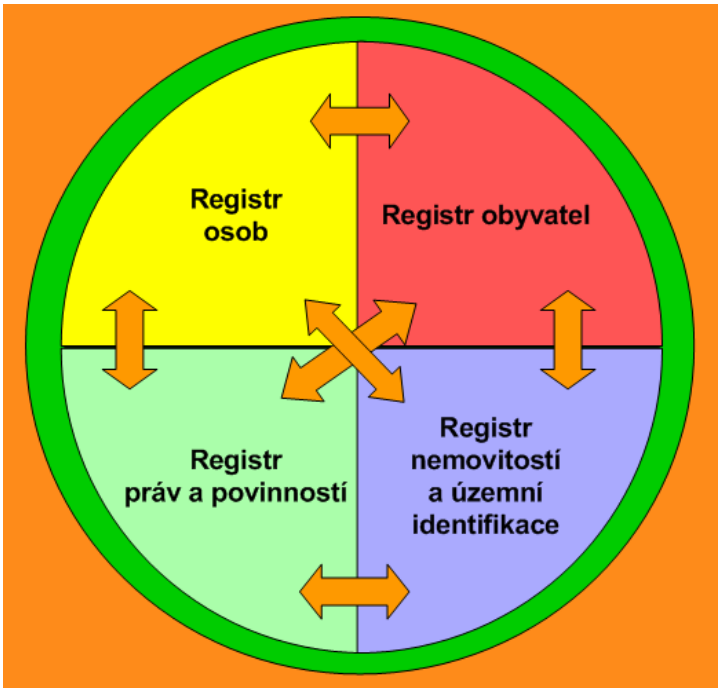
V základním registru osob se povedou referenční údaje o právnických osobách, podnikajících fyzických osobách a orgánech veřejné moci. Návrh zákona rovněž upravuje problematiku identifikačního čísla osoby (IČO) a identifikačního čísla provozovny (IČP). Registr osob, podobně jako registr územní identifikace, adres a nemovitostí, bude veřejně přístupným registrem. Správcem registru osob bude Český statistický úřad.

Registr územní identifikace, adres a nemovitostí

V tomto registru se povedou referenční údaje o územních prvcích (například území státu, území samosprávného nebo správního kraje, území okresu, území obce, katastrální území, stavební objekt, adresní místo, pozemek v podobě parcely) a referenční údaje o územně evidenčních jednotkách (například části obce, ulice nebo jiná veřejná prostranství). Správcem registru územní identifikace, adres a nemovitostí bude Český úřad zeměměřický a katastrální.

Registr práv a povinností

Základní registr práv a povinností upravuje vedení referenčních údajů o agendách orgánů veřejné moci a dále reguluje vedení referenčních údajů o některých právech a povinnostech fyzických a právnických osob a vedení oprávnění přístupu k datům vedeným v základních registrech nebo v agendových informačních systémech. Správcem registru práv a povinností bude Ministerstvo vnitra. [8]



Obr. 1. Soustava základních registrů veřejné správy

1.3.3 Komunikační infrastruktura veřejné správy

Základ budované infrastruktury je Centrální místo služeb. Zajišťuje vzájemné řízené a bezpečné propojování subjektů veřejné a státní správy, dále zajišťuje komunikaci subjektů veřejné a státní správy s jinými subjekty ve vnějších sítích, jakými jsou Internet nebo komunikační infrastruktura EU. Zároveň tvoří jediné logické místo propojení jednotlivých operátorů telekomunikačních infrastruktur poskytujících služby pro KIVS. [9]

1.3.4 Czech POINT

Czech POINT má sloužit jako asistované místo výkonu veřejné správy, umožňující komunikaci se státem prostřednictvím jednoho místa tak, aby „obíhala data ne občan“.

Cílem projektu Czech POINT je vytvořit garantovanou službu pro komunikaci se státem prostřednictvím jednoho universálního místa, kde bude možné získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů. [10]

Czech POINT v současné době poskytuje:

- Výpis z Katastru nemovitostí
- Výpis z Obchodního rejstříku
- Výpis z Živnostenského rejstříku
- Výpis z Rejstříku trestů
- Přijetí podání podle živnostenského zákona (§ 72)
- Žádost o výpis nebo opis z Rejstříku trestů podle zákona č. 124/2008 Sb
- Výpis z bodového hodnocení řidiče
- Vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů
- Podání do registru účastníků provozu modulu autovraků ISOH
- Czech POINT E-SHOP - výpisy poštou

1.4 Fungující služby e-governmetu v ČR

Kromě služeb poskytovaných na kontaktních místech czech POINT je v rámci zavádění e-governmentu občanům k dispozici celá řada dalších. V této kapitole jsou některé z nich popsány.

Fungující služby můžeme rozdělit na informační a transakční. Zatímco informační většinou pouze usnadňují přístup občana k informacím veřejné správy, transakční zprostředkovávají zaručenou komunikaci s úřady a dalšími orgány, která je rovnocenná komunikaci papírové.

1.4.1 Informační služby

portál veřejné správy

Pro občana je významným zdrojem informací portál veřejné správy. Je to portál provozovaný Ministerstvem vnitra České republiky, který vznikl na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Informační část nabízí celou řadu informací, z nichž uvedeme pouze některé: adresář úřadů ČR, postupy pro řešení více než 450 životních situací napříč veřejnou správou, mapové služby – tematické mapové úlohy, zákony, informace pro cizince atd.

e-deska

Od 1.1.2006 vstoupil v platnost nový správní řád - zákon č. 500/2004 Sb., který v §26 ukládá všem správním orgánům zřídit úřední desku, která musí být nepřetržitě přístupná. Obsah úřední desky musí být zajištěn i způsobem umožňujícím dálkový přístup (dále elektronická úřední deska). [11]

Města a obce online

Portál územní samosprávy Města a obce online poskytuje informace o úřadech měst, obcí a krajů České republiky a od roku 1996 systematicky rozvíjí nabídku řešení pro veřejné informační služby těchto úřadů s možností dálkového přístupu v souvislosti se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím. Všem obcím poskytuje bezplatně tzv. Základní stránku úřadu, která je koncipována v souladu se standardem ISVS. [12]

1.4.2 Transakční služby

Vláda schválila dne 25. 8. 2004 nařízení k elektronickým podatelnám.

Toto nařízení vlády stanoví povinnost orgánů veřejné moci zřídit e-podatelny (nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelny jiného úřadu), vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací. [13]

V současné době jsou na Portálu veřejné správy v aplikaci Elektronická podání dostupné následující služby.

- Služby České správy sociálního zabezpečení
- Služby Ministerstva průmyslu a obchodu
- Služba Ministerstva financí
- Služby Generálního ředitelství cel
- Služby Ministerstva dopravy
- [14]

Kromě podání přístupných přímo na Portálu veřejné správy existuje celá řada dalších elektronických podání. Možnosti použití i příslušné postupy jsou uvedeny na stránkách příslušných ministerstev, popřípadě jiných správních orgánů.

Pro elektronickou komunikaci s úřady je nezbytné mít k dispozici podpisový certifikát pro vytvoření elektronického podpisu. Většina úřadů vyžaduje, aby byl pro vytvoření podpisu použit kvalifikovaný certifikát od akreditované certifikační autority.

1.4.3 Datové schránky

Nejbližší budoucností v rozvoji e-governmentu v České republice jsou datové schránky. Dne 1.7.2009 vstoupí v platnost zákon o informačním systému veřejné správy, který upravuje elektronické úkony a autorizované konverze dokumentů.

Datová schránka

Datová schránka je elektronické úložiště, které je určeno k doručování a k provádění úkonů vůči orgánům veřejné moci. Datovou schránku zřizuje a spravuje Ministerstvo vnitra.

Doručování dokumentů

Pomocí datové schránky můžete posílat a přijímat úřední dokumenty v elektronické podobě (datové zprávy) orgánům veřejné moci. Tento způsob komunikace vynahrazuje klasický způsob doručování v listinné podobě. Pokud si tedy založíte datovou schránku, bude se Vám většina korespondence od orgánů veřejné moci doručovat elektronicky.

Do datové schránky jsou dodávány úřední listiny v elektronické podobě, které jsou opatřeny elektronickým podpisem odesílatele (orgánů veřejné moci). Pokud budete posílat dokument (např. odvolání k soudu) nemusíte označit Vámi vytvořený dokument zaručeným elektronickým podpisem. Identifikátor datové schránky zaručuje integritu dokumentu. V datové schránce jsou obsaženy veškeré písemnosti, které jsou již vyplněné Vašimi osobními údaji.

Datová schránka není e-mailová schránka, nemůžete pomoci ní komunikovat přímo s jednotlivými úředníky, pouze s celým úřadem. Pomocí datové schránky také nemůžete komunikovat s jinou fyzickou osobou, podnikající fyzickou osobou nebo právnickou osobou.

Jakmile je do Vaší datové schránky dodán nový dokument (datová zpráva), dle Vašeho nastavení se doručí na Váš mobilní telefon (za poplatek) popřípadě do Vaší e-mailové schránky (zdarma) oznámení o doručení. Toto je obdoba upozornění o uložení listovní zásilky.

Přístup do datové schránky

Přístupové údaje zasílá ministerstvo osobě, která o datovou schránku zažádala.

Přístup do datové schránky má pouze osoba, která zažádala o datovou schránku. Tato osoba může určit pověřenou osobu nebo administrátora, kteří budou mít určené úkony, které mohou vykonávat v zastoupení.

Pokud osoba, která má zřízenou datovou schránku, nemá připojení k internetu, může na kontaktních místech veřejné správy konvertovat do listinné podoby (vytisknout) datové zprávy ze své datové schránky. [14]

2 SINGLE SIGN-ON

Cílem všech informačních systémů a to nejen v soukromé sféře, ale i ve veřejné správě je co nejvyšší efektivita a uživatelské pohodlí. Single Sign-On umožňuje přístup a přihlášení do různých subsystémů, aplikací a sítí pouhým jedním přihlášením, tím zvyšuje nejen efektivitu celého systému ale také snižuje nároky na jednotlivé uživatele. V následující kapitole je toto řešení popsáno podrobněji.

2.1 Single-Sign-On: základní koncept

Obrovské množství služeb dostupných na síti způsobuje nárůst množství uživatelských účtů. Uživatelé se musí obvykle přihlašovat do různých systémů, z nichž každý může požadovat různé uživatelské jména a ověřovací informace. Každý tento účet může být spravován nezávisle svým lokálním správcem.

U *multiservice* domén se každý systém chová jako samostatná doména. Uživatel nejprve komunikuje s primární doménou za účelem navázání relace. To vyžaduje od uživatele poskytnutí souboru osobních údajů platných pro primární doménu. Relace s primární doménou je obvykle reprezentována nástavbou operačního systému spouštěná na počítači uživatele. Odtud může uživatel požadovat služby poskytované ostatními sekundárními doménami. Pro každý z těchto požadavků musí uživatel poskytnou další sadu osobních údajů platných pro sekundární doménu.

Z pohledu správy uživatelských účtů tento přístup vyžaduje nezávislou správu účtů v každé doméně a použití různých ověřovacích postupů. Postupem času, rozšíření služeb a bezpečnostní zájmy vyžadovaly přehodnocení přihlašovacího procesu, zaměření na koordinaci a v možných případech integraci přihlašovacích mechanizmů různých domén.

Architektura, která poskytuje takovou koordinaci a integraci se nazývá Single Sign-On (SSO). V SSO přístupu je primární doména zodpovědná za sběr a správu uživatelských údajů a informací v průběhu ověřovacího procesu, jak pro primární doménu, tak pro každou ze sekundárních domén se kterou může uživatel potenciálně komunikovat. Tyto informace jsou pak používány Single Sign-On službami uvnitř primární domény pro zajištění transparentního ověření údajů každou ze sekundárních domén, se kterou si uživatel vyžádá komunikaci. Výhodami SSO přístupu jsou:

- zredukování i) času stráveného uživateli při přihlašování do jednotlivých domén, ii) neúspěšných přihlašovacích akcí, iii) času stráveného při přihlašování do sekundárních domén, iv) nákladů a času využitých při administraci uživatelských profilů;
- zlepšení uživatelské bezpečnosti, protože se snižuje počet uživatelských jmen/hesel se kterými musí uživatel hospodařit;
- bezpečnější a jednodušší administrace, neboť s centralizovanou správou systémoví správci stráví méně času při přidávání, odstraňování nebo úpravě uživatelských práv;
- zlepšení systémové bezpečnosti pomocí zvýšené schopnosti systémových správců udržovat celistvost uspořádání uživatelských účtů, včetně možnosti změnit přístup uživatele ke všem systémovým zdrojům koordinovanou a logickou formou;
- zlepšení použitelnosti služeb, uživatel musí používat stejný přihlašovací formulář.

SSO poskytuje jednotný interface pro správu uživatelských účtů umožňující koordinované a synchronizované vedení dílčích domén.

2.2 Trust modely a požadavky Single Sign-On řešení

Definice různých trust modelů je důležitá pro vyhodnocení různých SSO řešení. Ty se mohou mírně lišit ve svých záměrech v závislosti na úkolech a trust scénářích ve kterých vystupují.

2.2.1 Trust modely

Trust model popisuje systém skrze definici výchozího prostředí a jeho chování, komponent a pravidel. Přesněji model definuje objekty zahrnuté v systému, pravidla, která řídí interakce mezi těmito objekty a charakteristiky celého systému. Pro naše potřeby, se zaměříme na definici trust modelů v prostředí SSO založených na službách které tyto prostředí poskytují. Rozlišujeme tři modely.

Autentizační a autorizační model (AAM)

Tento model představuje jeden ze základních bezpečnostně/trust modelů. Popisuje všechny struktury, které poskytují autentizační a autorizační funkce. Představuje základní mechanizmus, ve kterém uživatel požaduje přístup ke službě, která zkontroluje uživatelovy údaje za účelem rozhodnutí, zda mu bude přístup povolen nebo zamítnut. Tento model rozeznává dvě hlavní entity: *uživatele*, který požaduje přístup k prostředkům a *služby,* potenciálně složené ze sady intra-doménových služeb, které sdílejí tyto prostředky. Tento model je založen na klasické client-server architektuře a poskytuje obecně použitelný protokol pro autentizační a autorizační proces.

Federalizovaný model (FM)

Tento model představuje jeden z bezpečnostně/trust modelů, který je představován několika stejnorodými entitami spolupracujícími mezi sebou pro zajištění bezpečnostních služeb, jako jsou ochrana osobních údajů a ověření pravosti. Tento model rozeznává dvě hlavní entity: *uživatele,* který požaduje přístup k prostředkům a *služby,* které tyto prostředky sdílejí. Hlavní rozdíl oproti předchozímu modelu spočívá ve vymezení služeb a jeho kompozici: ve federalizovaných modelech jsou služby rozloženy na různé domény, které jsou postaveny na stejnou úroveň a umožňují tak vzájemnou důvěru a funkčnost cross-ověřování.

Model úplné správy identity (FIMM)

Tento model je výzvou na poli bezpečnosti a přístupových/trust modelů, který by potenciálně mohl slučovat předchozí dva modely. Navíc poskytuje mechanizmy pro správu identity, uživatelských účtů a ochranu soukromí. Tento model rozeznává tři hlavní entity: *uživatele,* který požaduje přístup k prostředkům, *služby*, které tyto prostředky sdílejí a *správce identit,* disponujícího funkcemi pro správu uživatelských identit. Hlavní rozdíl oproti dvěma předchozím modelům je, že FIMM model se snaží naplnit potřeby bezpečnosti v nově se objevujících situacích.

2.2.2 Požadavky systémů SSO

Požadavky, které by mělo Single Sign-On řešení uspokojovat jsou více či méně dobře známy uvnitř bezpečnostní komunity a bylo již vytvořeno několik SSO projektů.

První krok před realizací open source SSO systému spočívá ve vyjmenování požadavků a poučení se z předchozích projektů. Naše analýza nás vede k formulaci následujících požadavků (pro každý požadavek je uveden trust model (AM, FM, FIMM), ke kterému se vztahuje).

Autentizace (AAM, FM, FIMM). Hlavní vlastností SSO systémů je zajištění ověřovacích mechanizmů. Obvykle je ověření vykonáváno skrze klasické přihlašovací jméno/heslo, kterým je uživatel jednoznačně identifikován. Ověřovací mechanizmy by obvykle měly být spojeny s procesem přihlášení a kontrolou účtu za účelem prevence, případně odhalení útoků a neočekávaného chování. Z hlediska softwarového inženýrství je toto jediným "nutným a dostačujícím" funkčním požadavkem na SSO architekturu.

Silná autentizace (AAM, FM, FIMM). Pro prostředí s vysokým stupněm bezpečnosti nemusí tradiční přihlašování pomocí jména/hesla postačovat. Může dojít ke krádeži hesla a jeho zneužití jiným uživatelem. Nové přístupy si tak vyžádaly lepší zajištění služeb proti neoprávněným přístupům. Řešením tohoto problému může být spojení přihlašování pomocí jména a hesla s druhým, silnějším ověřovacím procesem jako např. čipovými kartami nebo biometrickými údaji uživatele (otisky prstů, sken sítnice atd.).

Autorizace (AAM, FIMM). Následně po úspěšném ověřovacím procesu, systém musí rozhodnout o nároku uživatele na informace/služby, které může žadatel vidět/používat. Zatímco aplikace založené na autorizacích pro každou specifickou doménu mohou být vymezeny a spravovány lokálně, SSO systémy mohou poskytovat podporu pro správu autorizací, které jsou aplikovány na více domén.

Provisioning (AAM, FIMM). Provisiony jsou podmínky, které musí být splněny před vydáním rozhodnutí. Provision je předběžná podmínka; je odpovědností uživatele, aby zajistil, že je požadavek v prostředí vyhovujícím všem předběžným podmínkám. Z neuspokojení provisionu vyplívají další požadavky na uživatele.

Federation (FM, FIMM). Federativní koncept je úzce propojen s trust koncepty. Uživatel by měl být schopen si vybrat služby, které chce využívat nebo zakázat za účelem ochrany vlastního soukromí a vybrat služby ve kterých zveřejní své ověřovací údaje.

C.I.M (Centralizovaná Správa Identity) (AAM, FIMM). Centralizace autentizační a autorizačních mechanizmů a především centralizace správy identit znamená zjednodušení správy uživatelských účtů. Uživatelské profily mohou být spravovány na SSO serveru a

tím mohou být sníženy nároky na lokální správce. Toto umožňuje snížení nákladů na správu uživatelských účtů, úsporu času a zlepšuje kontrolu na uživatelskými profily a ověřovacími politikami.

Client Status Info (AAM, FM, FIMM). Architektura SSO systému zahrnuje výměnu informací o uživateli mezi SSO serverem a službami zajišťujícími autentizační a autoritační procesy. Zejména při komunikaci dvou entit, musejí být tyto entity synchronizovány v tom, co má uživatelská identita obsahovat; musejí být určeny bezpečnostní a přístupové záležitosti. Řešení tohoto problému může být zahrnuto do transportu (komunikace může být šifrována) nebo do aplikační vrstvy.

Single Point of Control (AAM). Hlavním úkolem implementace SSO je zajistit univerzální přístupový bod pro uživatele, kteří požadují přístup ke službám a aplikacím zplnomocnit některé funkce vzhledem k ověřovacímu serveru. Tento bod kontroly by měl být jednoznačný, aby striktně oddělil autentizační bod od obchodních implementací za účelem vyhnutí se zmnožením a ad-hoc implementacím ověřovacích mechanizmů pro každou doménu. Je nutné mít na paměti, že každý poskytovatel služby může vyvinout svůj vlastní ověřovací mechanizmus.

Standart Compliance (AAM, FM, FIMM). Pro širokou škálu aplikací je důležité, aby podporovaly známé a ověřené protokoly a umožnily tak komunikaci a integraci mezi různými prostředími. V SSO záměru existují protokoly pro výměnu zpráv mezi ověřovacími servery a poskytovateli služeb a mezi technologiemi uvnitř téhož systému, které však mohou být různé. Z toho důvodu každá entita by měla používat standardní technologie (např. X.509, SAML pro vyjádření a výměnu ověřovacích informací a SOAP pro přenos dat) pro zajištění kompatibility různých prostředí.

Cross-Language availibility (AAM, FM, FIMM). Široké rozšíření internetu jako infrastruktury pro přístup k mnoha službám ovlivnilo definici různých jazyků/technologií používaných k vývoji aplikací. V tomto případě je důležitý vývoj SSO řešení, která dovolují integraci implementací služeb založených na různých jazycích, bez dalších podstatných změn kódu. Prvním krokem v tomto směru je zavedení standardních komunikačních protokolů založených na XML.

Password Proliferation Prevention (AMM, FM, FIMM). Dobře známým důvodem pro zavádění SSO systémů je prevence nárůstu počtu hesel tak, aby byla zvýšena bezpečnost a byl zjednodušeno přihlašování a systém správy uživatelských účtů.

Scalibility (AAM, FM, FIMM). Důležitým požadavkem na SSO systémy je podpora a správné řízení růstu počtu uživatelů a subdomén, které na nich závisejí bez podstatných změn v architektuře systému. [15]

Tab. 1. Kategorizace požadavků založená na jednotlivých trust modelech

Požadavek	AAM Model	FM Model	FIMM Model
Autentizace	**X**	**X**	**X**
Silná autentizace	**X**	**X**	**X**
Autorizace	**X**		**X**
Provisioning	**X**		**X**
Federation		**X**	**X**
C.I.M	**X**		**X**
Client Status info	**X**	**X**	**X**
Single Point of Control	**X**		
Standart Compliance	**X**	**X**	**X**
Cross-Language availibility	**X**	**X**	**X**
Passwor Proliferation Prevention	**X**	**X**	**X**
Scalability	**X**	**X**	**X**

2.3 Open source Single Sign-On systémy

Následující open source systémy jsou popsány na základě výše uvedených a dalších požadavků.

Central Authentication Service. Central Authentication Service (CAS) je open source systém vyvinutý na Univerzitě Yale. Realizuje SSO mechanizmus zaměřený na poskytování centrálního ověřování na jediném serveru a HHTP přesměrování. Když neověřený uživatel odešle požadavek na službu, je tento požadavek přesměrován z aplikace na server (CAS Server) a pak po ověření uživatele zpět do aplikace. CAS server je tedy jediným objektem, který spravuje hesla pro ověřování uživatelů, přenosů a potvrzuje jejich pravost. Informace je předána serverem aplikaci během přesměrování pomocí session cookies. CAS je založen na modulárních JAVA servletech, které mohou běžet nad jakýmkoli servlet enginem a poskytuje autentizační služby na bázi webu.

SourceID. SourceID, poprvé uvolněn v roce 2001 Ping Identity Corporation Company, je open source multi-protokolový projekt umožňující federativost identit a cross-boundary zabezpečení. SourceID je zaměřený na jednoduchou integraci a rozšíření v existujících web aplikacích a poskytuje vysoký stupeň vývojářských funkcí a přizpůsobení. SourceID také implementuje specifikace Liberty Alliance Single Sign-On a jedná se o systém, který integruje SSO jak do nových, tak do stávajících webových portálů. Nižší úroveň implementace Liberty specifikací jako např. SOAP, SAML, hlavní části Liberty, protokoly a schémata metadat jsou transparentní pro vývojáře webu. Z hlediska architektury je SourceID složen ze tří modulů zakomponovaných do Web aplikací za účelem zajištění SSO funkcí: i) *Profil,* implementuje Liberty Single Sign-On vlastnosti, jako například Federativnost, Single Sign-On a Log-Out., ii) *Zprávy*, zpřístupňují vlastnosti pro vytváření typických XML zpráv (např. Liberty protokol a ověřování), iii) *Utility,* zabezpečuje funkce jako zpracování výjimek.

Shibboleth. Shibboleth je open source projekt Internet2/MACE, zaměřený na vývoj architektury, politiku a praktické využití technologií pro podporu sdílení webových zdrojů a přístupu k nim. Shibboleth není pouze implementací SSO technologie, ale spíše obecnou architekturou, která se snaží chránit soukromí a spravovat uživatelské informace. Nicméně v tomto případě uvažujeme Shibbolet SSO řešení, které má velmi blízko k Liberty Single Sign-On řešením. Realizace na nižší úrovní závisí na různých standardech jako jsou HTTP, XML, XML Schema, XML Signature, SOAP a SAML. Stejně jako přístup Liberty Aliance, Shibboleth používá mezi identitami a poskytovateli služeb federativní koncept, pojmenovaný Shibboleth Club.

Java Open Single Sign-On (JOSSO). Java Open Single Sign-On je Open Source SSO implementací na bázi J2EE zaměřená na poskytování řešení v oblasti centralizovaného ověřování uživatelů nezávisle na platformě. V JOSSO architektuře rozeznáváme tři hlavní objekty: i) *Partnerskou aplikaci,* webovou aplikaci , která využívá služby SSO brány pro ověřování uživatelů; ii) *SSO bránu,* reprezentovanou SSO serverem, který poskytuje ověřovací služby uživatelů, kteří žádají o ověření u partnerské aplikace; iii) *SSO Agent,* je klientem SSO brány instalovaný na spravovaných službách.

Open Web SSO. Open Web SSO projekt nabízí základní služby pro realizaci transparentního Single Sign-On jako bezpečnostní komponenty. [16]

3 PERSONALIZACE

V obecném smyslu slova můžeme chápat personalizaci jako individuální přístup nebo přizpůsobení vlastním potřebám. V současné době nabývá tento pojem stále většího významu a to především v oblasti rozsáhlých informačních systémů s využitím technologie Single Sign-On. Následující kapitola je proto věnována personalizaci a také základním pojmům z oblasti webových informačních systémů.

3.1 Filozofie informačního systému

Při návrhu, vývoji a implementaci informačního systému je nutné si nejprve ujasnit několik aspektů, které mají pro životnost a úspěšnost informačního systému zvláštní význam:

- čemu bude informační sytém sloužit - v jakém oboru lidské činnosti se bude používat
- komu bude informační systém sloužit - kdo a jací budou jeho uživatelé
- způsob implementace

Předmět zájmu informačního systému

Výchozím bodem při návrhu každého informačního systému je vymezení oboru lidské činnosti, které se bude informační systém týkat (univerzitní IS, podnikový IS, IS v nemocnici, webový portál atd.). O tomto kroku v podstatě nikdo nepřemýšlí, protože je to vlastně automatický, logický základ celého budovaného informačního systému. A právě z tohoto základu vycházejí všechny ostatní výše uvedené aspekty.

Uživatelé informačního systému

Uživatelské hledisko je velmi důležité. Právě uživatelé jsou totiž zpětnou vazbou a zejména oni určují úspěšnost používaného informačního systému. Skladba uživatelů informačního systému úzce souvisí s jeho předmětem. Musíme vědět, zda uživateli našeho informačního systému budou profesionálové z oblasti informačních technologií či naopak lidé, kterým je svět počítačů značně vzdálen. Skutečnost však není v naprosté většině případů takto černobílá. Informační systémy se zpravidla zaměřují na širší okruh uživatelů, mezi nimiž jsou zástupci jedné či druhé strany, ale jinak se zkušenosti a počítačové znalosti potenciálních uživatelů pohybují někde mezi těmito dvěma póly. Proto by mel být informační systém navržen tak, aby práci s ním zvládli víceméně intuitivně i nezkušení

uživatelé, a naopak, aby odborníci nebyli zdržováni záležitostmi, které jim připadají samozřejmé a jasné (podrobná nápověda, systém navigací apod.). [17]

Způsob implementace

Webová technologie a tedy i webové informační systémy jsou založeny na funkčním oddělení klienta a serveru. Platí pro ně tedy stejná pravidla jako pro ostatní webové aplikace a stejným způsobem je postavena i infrastruktura. Základem jsou protokoly HTTP/HTTPS.

3.2 Designové prvky

Efektivita každého informačního systému závisí nejen na jeho efektivitě ale i na tom, jak uspokojuje potřeby uživatelů. Tato efektivita závisí na čitelnosti, snadnosti prohlížení a snadnosti vyhledávání v informačním systému.

3.2.1 Čitelnost informačního systému

Citelnost informačního systému představuje spojení přitažlivého grafického designu a správného rozvržení stránky. Všechny informační systémy bez ohledu na jejich velikost by mely dodržovat principy dobrého grafického designu. Velmi snadno lze odradit mnoho uživatelů, pokud nejsou data prezentována vizuálně přitažlivě a přehledně.

Při návrhu systému je proto nutné mít na paměti následující zásady:

- Používat shodný vzhled stránek
- Nevypouštět bílá místa
- Uspořádat stránky vizuálně
- Zachovávat krátké stránky
- Zahrnovat zvýrazňující prvky
- Používat všechny stylistické prvky umírněně

3.2.2 Snadnost prohlížení informačního systému

Snadnost prohlížení informačního systému je dána logickým tříděním dat a informací. S růstem velikosti systému roste i potřeba logického uspořádání dat v systému obsažených.

To zahrnuje seskupování podobných pojmových skupin. Snadnost prohlížení se zdůrazňuje, je-li spojena s hypertextem a logickým seskupením informací.

Snadno prohlížitelný informační systém má radu výhod:

- Uživatelé vidí zběžně celý systém už „na první pohled“
- Není nutná znalost speciální slovní zásoby
- Podobné položky tvoří jednu skupinu
- Jednoduchá navigace v systému
- Systém podporuje myšlení uživatelů

Na druhou stranu se však výhradně „prohlížitelný“ systém neobjede bez určitých nevýhod:

- Uživatel se může lehce ztratit
- Klasifikace systému může být uživateli cizí
- Klasifikace se narušuje s růstem kvality informací
- Klasifikace se může časem měnit

Obecně vzato je každý snadno prohlížitelný systém logicky roztříděn podle obsažených témat. Důležité pravidlo pro tvůrce každého informačního serveru (a přenositelné na tvůrce každého informačního systému) zní: „Efektivní organizace informací je pro úspěch serveru rozhodující. Má-li se náš server stát účinným informačním prostředkem a mají-li jej uživatelé často používat, musí být vhodně organizován. Filozofie třídění informací vychází z nutnosti organizování informací, jako součástí lidského bytí.

Řídí se následujícími zásadami:

- Znát své uživatelské publikum
- Nabízet vysvětlující prvky
- Používat navigační prvky
- Užívat slovní zásobu potenciálních uživatelů
- Vytvořit hierarchický systém pojmů
- Vytvořit systém, který je současně přizpůsobivý i vyčerpávající

Znalost uživatelského publika — Pokud uživatelé nebudou rozumět organizačnímu schématu informačního serveru, budou jej využívat jako informační zdroj, pouze pokud nenaleznou jiné východisko. Proto je zásada vytvoření vhodného organizačního schématu první a nejdůležitější. Organizační schéma musí být uživatelům srozumitelné. Je třeba zamyslet se nad lidmi, kteří budou náš informační systém používat. Pokud si zodpovíme otázky typu:

Pro jaké uživatele systém navrhujeme? Jaké je jejich zázemí? Co chtějí? Jakou terminologii užívají? Tedy obecně: Jak přemýšlejí? a odpovědi na tyto otázky zakomponujeme do struktury informačního systému, pak většině uživatelů bude organizační schéma našeho systému pochopitelné.

Vysvětlující texty - Systém by měl obsahovat co nejvíce vysvětlujících (nápovědných) textů - popisujících organizaci systému, způsoby použití, nápovědu k prováděným operacím atd. Přesto je nutné zařazovat vysvětlující texty s mírou, aby nebyla narušena dobrá čitelnost systému.

Navigační prvky - Aby se uživatel v systému neztratil, je vhodné na stránky umisťovat navigační prvky (zpět na hlavní stránku, návrat na předchozí nabídku, vpřed, vzad apod.). Tyto prvky mohou být součástí standardního záhlaví, zobrazujícího se na každé stránce, součástí textu stránky nebo na obou místech současně.

Užití slovní zásoby potenciálních uživatelů - Po zjištění, kdo a jací budou naši uživatelé, je vhodné používat jejich terminologii. Tak se uživatelé lépe ztotožní s informačním systémem a budou jej raději a častěji využívat.

Hierarchický systém pojmů - Základem hierarchického systému myšlenek (pojmů) jsou široké termíny, které se pak dělí do užších pojmových skupin. Dokonalá hierarchie pojmu neexistuje, je však možné se co nejvíce přiblížit myšlení naší uživatelské klientely.

Přizpůsobivý a kompletní systém - Informační systém by mel být kompletní (úplný, vyčerpávající), ale i přizpůsobivý. Jinými slovy by systém mel být současně výčtový i spojující (syntetický).

3.2.3 Snadnost vyhledávání v informačním systému

Možnost snadného vyhledávání v systému znamená pro uživatele možnost přímého přístupu k informacím. Rozsáhlejší informační systémy musejí obsahovat vyhledávací služby. Tyto služby pomáhají překlenout nedostatky špatně prohlížitelného systému.

Mají několik jasných výhod:

- vytvářejí alternativní logické třídění informací;
- zjednodušují vyhledávání známých položek;
- pracují nezávisle na velikosti systému.

Při seskupování logicky souvisejících pojmů se „logika uživatelů může lišit. Systém s usnadněným vyhledáváním však pomáhá tyto rozdíly překonat. Možnost snadného vyhledávání vybízí k přímému vyhledání známých položek a je v takových případech vhodnější než dlouhý seznam nabídek v prohlížeči, mezi nimiž uživatel hledá požadovanou informaci. Stejně tak v případech, kdy uživatel jednou použije určitou položku, ale nezapamatuje si její umístění. Pokud je však k dispozici vyhledávací mechanismus, snáze se k dané položce dostane. Vyhledávání informací pracuje nezávisle na velikosti systému. Kvalita snadno prohlížitelných systému se snižuje s rostoucí velikostí systému, ale efektivita vyhledávání není velikostí systému přímo narušena. Je však nutné připustit, že systémy, které berou ohled pouze na snadné vyhledávání,

mají i své nevýhody. Uživatelé musejí:

- znát syntaxi vyhledávání;
- vědět, co hledají - frázi, pojem, atd.;
- znát strukturu dat.

Aby mohli uživatelé účelně prohledávat informační systém, je nutné, aby znali dotazovací jazyk vyhledávacího prostředku. Ten může zahrnovat například booleovské či Unixové regulární výrazy. Pro běžné uživatele je tento způsob použití systému, jenž vyžaduje „nadstandardní“ znalosti, překážkou. Možnost prohledávat informační systém předpokládá, že uživatel ví, co chce nalézt. To může často představovat problém. Uživatel musí vyhledávat podle konkrétních výrazů nebo pojmů, které popisují žádaná data. Může se však stát, že se místo zadaných pojmů naleznou pouze jejich synonyma, z kterých je někdy obtížné vybrat ta pravá. Systémy zaměřené pouze na vyhledávání často požadují po

svých uživatelích také znalost datové struktury, například zda jsou data rozdělena do skupin, případně jakých, aby bylo možné správně formulovat dotaz k získání žádaných dat.

Stejně jako v případě předcházejících vlastností grafického designu informačního systému i v případě vytváření snadno prohledávatelného systému je vhodné dodržovat následující principy:

- vkládat nápovědné texty;
- vzájemně propojovat složky;
- nabízet jednoduchý i složitější (ale mocnější vyhledávací mechanizmus).

Vkládání nápovědných textů - Nápovědné texty jsou pro snadno prohledávatelný systém nezbytné. Popisují charakteristické znaky a omezení systému, strukturu dat v systému včetně oblastí pro vyhledávání a obsah těchto oblastí. Nápovědné texty také uvádějí příklady pro vyhledávání a vysvětlují, jak má uživatel pokračovat, je-li na jeho dotaz nalezeno příliš mnoho či příliš málo položek.

Vzájemné propojení položek - Poté, co vyhledávací mechanismus systému nalezne příslušné položky, uživatelé často vyžadují vyhledání dalších podobných položek. Proto je vhodné ke každé nalezené položce připojit odkaz (odkazy) na položky podobné.

Jednoduché i mocné vyhledávací mechanismy - Jednoduchý vyhledávací mechanismus je nejužitečnější pro začátečníky a příležitostné uživatele. Bohužel právě tento způsob vrací často příliš mnoho či příliš málo výsledků. Tuto nevýhodu lze vyvážit poskytnutím mocného vyhledávacího mechanismu (prohledávání oblastí, booleovské výrazy, omezení počtu položek atd.). [17]

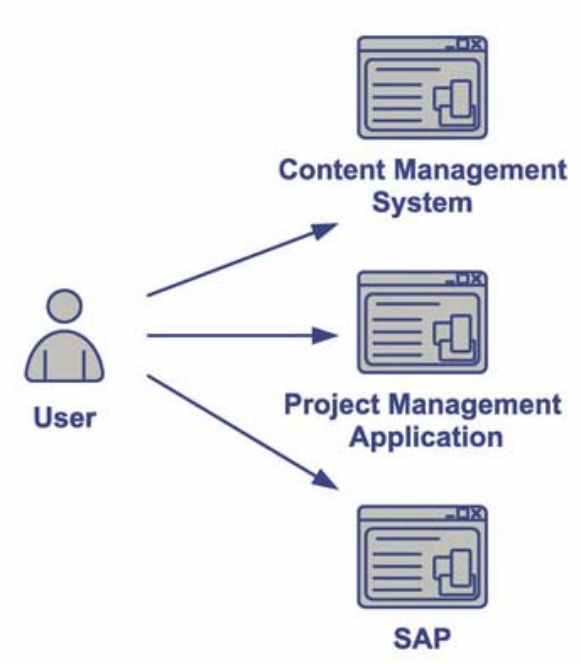
3.3 Personalizace webových portálů

Webové informační systémy velmi často využívají pro přístup tzv. portál.

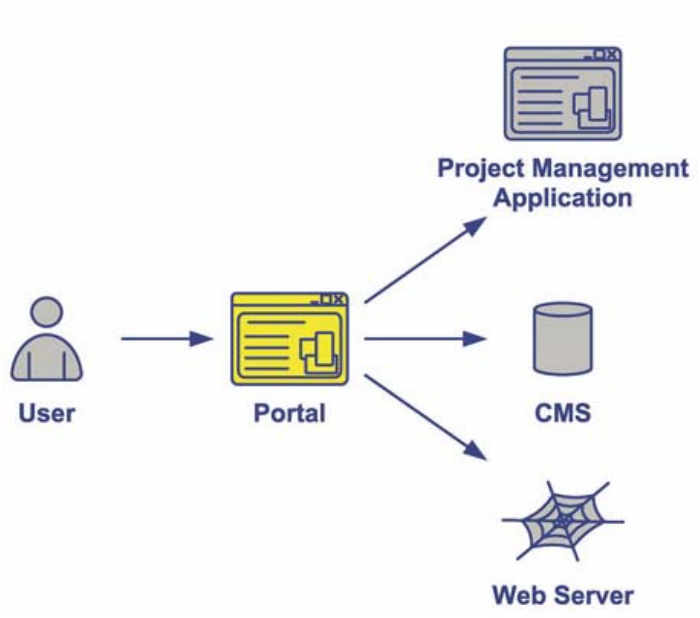
Zpravidla se jedná o webovou aplikaci, jejímž základním úkolem je integrovat informace z různých zdrojů a obsah poskytnout uživateli v přehledné formě. Všichni uživatelé internetu portály znají a zpravidla je portál první místo, kde své výlety po internetu začínají. Příkladem mohou být stránky Yahoo nebo Seznamu. Možnosti portálů jsou ovšem mnohem širší.

Portál je webová aplikace, která agreguje obsah z různých zdrojů, představuje prezentační vrstvu informačních systémů a obvykle uživatelům poskytuje personalizaci a výhody prostředí Single Sign-on (SSO).

Každý uživatel má jiný vkus a jiné priority. Portál by měl umožnit nastavení vzhledu a chování podle specifických potřeb uživatele. Nastavit lze nejen barvy, font nebo velikost písma, ale například i jazyk portálu, rozložení informací na stránce nebo výběr obsahu, který uživatele zajímá. Uživatel má nástroje, jak si přizpůsobit stránku tak, aby mu vyhovovala a jeho práce byla efektivní. Spolu s jiným barevným řešením se může stejný portál na první pohled jevit jako úplně odlišná aplikace. Portál agreguje obsah z různých zdrojů a aplikací. Umožňuje konzistentní pohled na data a jejich vztahy napříč hranicemi oddělených aplikací.



Obr. 2. Přístup k jednotlivým aplikacím



Obr. 3. Přístup k aplikacím s využitím portálu

Pro zvýšení škálovatelnosti a dostupnosti je vhodná multiplikace zdrojů, mezi které rozděluje požadavky load balancer. Autentifikační software řeší SSO a přístup k portálu. Statický obsah portálu, jako jsou obrázky nebo skripty, je vhodné umístit na samostatný webový server, který je rychlejší než samotný portál a pro poskytování statického obsahu je dostatečný. (Obr. 13)

Výsledkem je HTML stránka, která je interpretována prohlížečem klienta. Pro zkrácení času odpovědi se často používají cache. Tyto cache lze použít na libovolné úrovni infrastruktury. Použití cache musí mít ale silný důvod, protože na oplátku za zrychlení reakcí aplikace zhoršují správu aplikace. Přidáním cache se do infrastruktury přidává software, který může vykazovat nějaké chyby, a proto je nutné se o něj starat. Navíc je nutné mít na paměti aktuálnost informace. Ne každý obsah lze cachovat, obzvláště ten dynamický.

Portálových řešení existuje celá řada, ať jsou to produkty komerční nebo open source. [18]

Stupně personalizace

Někteří provozovatelé informačních systémů považují za personalizaci poskytnutí autentizovaného vstupu (přihlášení uživatele jménem a heslem), po přihlášení uživateli nabízejí či zpřístupňují jemu relevantní údaje. Navíc někteří provozovatelé umožňují uživatelům osobní nastavení některých komponent.

V chápání personalizace je však třeba jít dále. Autentizace uživatelů je samozřejmostí, neboť pro nepřihlášené (tedy neznámé) uživatele není možné evidovat jakákoliv osobní data a nastavení (nejvýše lze využívat cookies v prohlížeči). To, co bylo v předcházejícím odstavci chápáno jako personalizace, nyní chápeme pouze jako formulaci práv a rolí uživatele v příslušném systému. Na základě definice práv a rolí pro jsou uživatelům zpřístupňovány relevantní odkazy. Jednotlivým odkazům na konkrétní dokumenty či aplikace jsou přiřazeny informace (strukturované záznamy) popisující, kteří uživatelé smějí tento odkaz užívat.

Rozšíříme-li toto pojetí, skutečná personalizace přichází v okamžiku, kdy si uživatel může sám nastavovat určité parametry vzhledu či chování systému. Základním nastavením může být například povolení nebo zákaz zobrazování určitých informací o uživateli ostatním, případně si uživatel může o sobě doplnit údaje další, jako např. kontakty, konzultační hodiny, klíčová slova pro snadnější vyhledávání apod. Do personalizace řadíme i nastavení systémových politik, které souvisí s chováním systému. Uživatelé si mohou například definovat tiskárny (směrování tiskových výstupů), nejčastěji používané výstupní formáty, režim zobrazování nápovědy apod. Dalším stupněm osobního přizpůsobení systému je pak nastavitelný navigační systém (volba zobrazení a typu navigačních prvků, možnost sestavování vlastních menu). Možnost volby designů uživatelům zpříjemňuje pracovní prostředí (mohou si definovat vlastní barvy, tvary, obrázky a dokonce i rozmístění objektů na stránce podle vkusu a zvyklostí). [19]

V našem pojetí však chceme dovést personalizaci ještě dále. Uzpůsobení obsahu a služeb poskytovaných portálem není závislé pouze na uživateli, jeho právech a rozhodnutích, ale i na provozovateli portálu. V následující podkapitole jsou popsány některé způsoby získávání relevantních informací o uživatelích.

3.3.1 Metody komunikace s uživateli

Při vývoji i provozu informačního systému je nutné neustále spolupracovat s uživateli a získávat od nich cenné informace, které pomohou při tvorbě a zdokonalování systému. Pro tuto zpětnou vazbu můžeme použít několik metod:

- osobní setkání;
- kontaktní e-mail, infolinka, linka podpory apod.;

- dotazník;
- logování uživatelských operací;
- školení.

K *osobním setkáním* zástupců uživatelů (nejčastěji odpovědného managementu) se zástupci vývoje systému dochází zejména v prvních fázích vývoje nového systému a v případech, kdy je potřeba projednat klíčová rozhodnutí dalšího postupu.

Nejpřirozenější způsob komunikace mezi uživateli zavedeného informačního systému a jeho tvůrci, případně správci, je použití *kontaktního e-mailu* (případně telefonické infolinky či linky podpory). Tento komunikační kanál uživatelé používají zejména tehdy, když jim není něco jasné, neví si s něčím rady nebo něco nefunguje, jak by mělo. Pro vývojáře je to první impuls, aby chyby opravili a aby se zamysleli nad vylepšením nejasných částí systému. Často totiž postup, který se zkušenému vývojáři může zdát naprosto logický, nezkušeného uživatele zaskočí. Uživatelé však kontaktní e-mail nepoužívají jen jako „linku pomoci, ale někteří, zejména ti počítačově zdatnější, zasílají i návrhy na vylepšení, zpříjemnění práce v systému apod. Tyto ohlasy jsou velmi důležité, neboť informační systém není jen prací vývojářů, ale měl by být výsledkem spolupráce jeho vývojářů a uživatelů [19].

Tvůrci informačního systému však nemohou (nebo by alespoň neměli) spoléhat pouze na reakce uživatelů. Získat potřebné informace od uživatelů je možné například pomocí *dotazníku*. Dotazník v elektronické formě se umístí přímo na stránky informačního systému. Pokud to povaha systému umožňuje, je dobré uživatele nějakým způsobem motivovat k jeho vyplnění (nabídkou bonusu, výhodnějšího nákupu, losování apod.). U systému orientujících se na určitý uzavřený okruh uživatelů (univerzitní, podnikový IS) lze uživatele požádat o vyplnění klasického tištěného dotazníku.

Každý informační systém by měl provádět logování uživatelských operací. To umožňuje sledovat posloupnost práce jednotlivých uživatelů, jak z hlediska podpory uživatelů, tak i z hlediska bezpečnosti. Často opakované sekvence kroků pak lze nahradit zástupnou aplikací. U systému s autentizovaným přístupem (kdy známe i totožnost uživatele) můžeme tápající uživatele nasměrovat, proškolit, případně jim nabídnout alternativní řešení problému.

V případě specializovaných informačních systémů je vhodné čas od času pořádat školení uživatelů, na kterých se vysvětlují a předvádějí nové či složitější aplikace. Pokud je dostatečný zájem uživatelského publika, mohou se pořádat i školení, kde se probírá obecná problematika a formou diskuze se objasňuji a řeší připomínky a nejasnosti. [20]

II. PRAKTICKÁ ČÁST

4 ANALÝZA POTŘEB SINGLE SIGN ON V E-GOVERNMENTU

Nasazení Single Sign-On v různě velkých podnikových systémech se stává stále oblíbenější. Řada nejen předních softwarových firem nabízí své Enterprise Single Sign-On řešení, které splňuje veškeré požadavky firem. Využití SSO v e-governmentu je však specifickým případem. V následující kapitole jsou popsány potřeby a postupy umožňující nasazení této technologie v oblasti e-governmentu.

4.1 Potřeby identifikace a autentizace

Každý úkon ve styku s veřejnou správou je podmíněn jednoznačnou identifikací všech zúčastněných stran. Je nutné, aby identifikace proběhla nejen rychle, ale i spolehlivě (žádná ze stran se nemůže vydávat za někoho jiného). U běžné formy styku s úřady k slouží těmto účelům osobní doklady, případně rodné číslo, ale pro oblast e-governmentu je nutné zavést spolehlivou formu elektronické identifikace a autentizace.

Při běžné komunikaci a v některých systémech je dosaženo žádoucí bezpečnosti již použitím technologie Single Sign-On. Uživateli stačí jedno heslo (které může být specifikováno délkou, obsahem speciálních znaků atd.) místo několika jednodušších hesel. Jednoduchá hesla jsou lehčeji prolomitelná a také často dochází k tomu, že uživatelé nechtějí opakovaně vyplňovat přihlašovací údaje a tak nechávají tyto úkony na aplikaci. Může pak snadno dojít k tomu, že při ztrátě např. notebooku, zloděj získá přístup ke všem aplikacím ve kterých jsou přihlašovací údaje takto uchovávány bez větší námahy. Jediné a dostatečně dlouhé heslo poskytuje dostačující ochranu nejen proti prolomení, ale rovněž snižuje nároky na uživatele. Ten si musí pamatovat pouze jedno heslo a navíc ve spojení s technologií Single Sign-On není nucen heslo opakovaně zadávat.

V elektronickém styku s veřejnou správou však ani toto není dost velkou zárukou bezpečnosti a jednoznačné identifikace. Uživatel nemůže vystupovat pod přezdívkou a také je nežádoucí aby konkrétní osobní údaje (byť v zašifrované formě) často putovaly systémem.

Nejen z tohoto důvodu je nutné uvažovat model, který zajistí nejen jednoznačnou a bezpečnou identifikaci, ale také zaručí dostatečnou ochranu osobních údajů a pověřeným orgánům umožní efektivní získávání informací.

V následujících bodech jsou uvedeny některé důvody a požadavky na takto fungující systém:

- občan je v jednotlivých agendách representován tzv. bezvýznamovým identifikátorem, z toho plynou i další dva body;
- občan vystupuje vůči agendě „anonymně“, tzn. při zpracovávání v rámci agendy ani úředník pracující s daty neví o jakou konkrétní osobu se jedná (jméno, příjmení atd.), vidí pouze jeho identifikátor v rámci agendy;
- získat informace z jiné agendy není možné s identifikátorem agendy jiné a jejich převod je povolen pouze se souhlasem vlastníka nebo v zákonem stanovených situacích;
- v zákonech stanovených případech umožní orgánům efektivní vyhledávání (např. hledaných osob);

Je jasné, že systém musí najít kompromis mezi ochranou osobních údajů, oddělením jednotlivých agend a zároveň nebude kolidovat s požadavkem na efektivní sdílení informací mezi úřady.

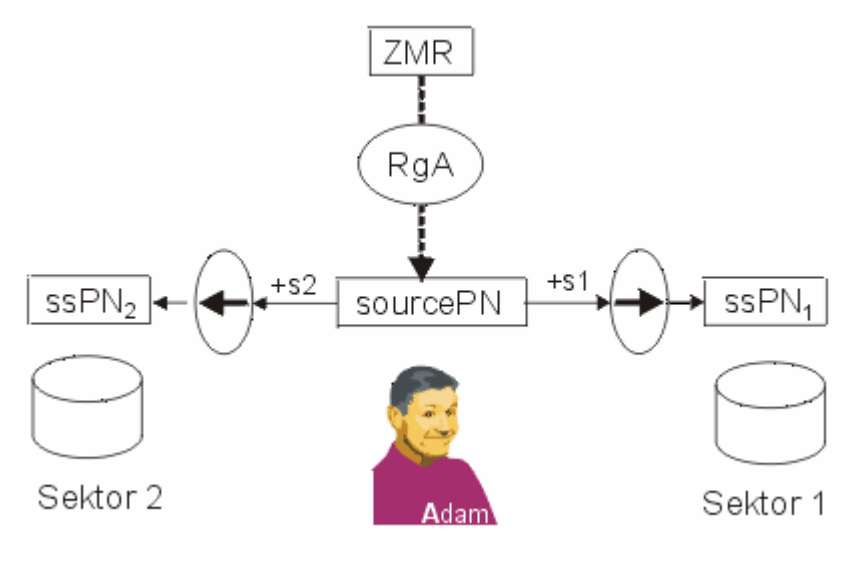
4.1.1 Rakouský model e-governmentu

Rakousko je zatím zřejmě v zavádění tohoto modelu e-governmentu nejdále. Je tedy velmi pravděpodobné, že model v České republice bude podobný nebo dokonce bude z tohoto modelu vycházet. V této kapitole je pro lepší pochopení uveden stručný popis rakouského modelu.

Rakousko vytvořilo kvalifikované expertní týmy a ty posléze navrhly jeho unikátní architekturu e-governmentu. Její tvůrci přitom byli od počátku omezeni tím, že v Rakousku je zákonem apriori zakázáno, aby záznamy osoby v různých databázích byly spojitelné společným identifikátorem. Zároveň se braly do úvahy i existující evropské předpisy, zejména o elektronickém podpisu, s nimiž bylo nutné architekturu rovněž skloubit.

V ČR se někdy za reformu v „mezích možností“ vydává to, že se stávající rodné číslo nahradí tzv. bezvýznamovým identifikátorem. V Rakousku takové číslo mají a označují ho jako ZMR. Pod tímto číslem však klient v databázi veden být nesmí. Ze ZMR se proto

vytváří zvláštní mezičíslo sourcePN osoby a z něj další, specifické identifikátory. Cílový stav znázorňuje obr. 4 níže.

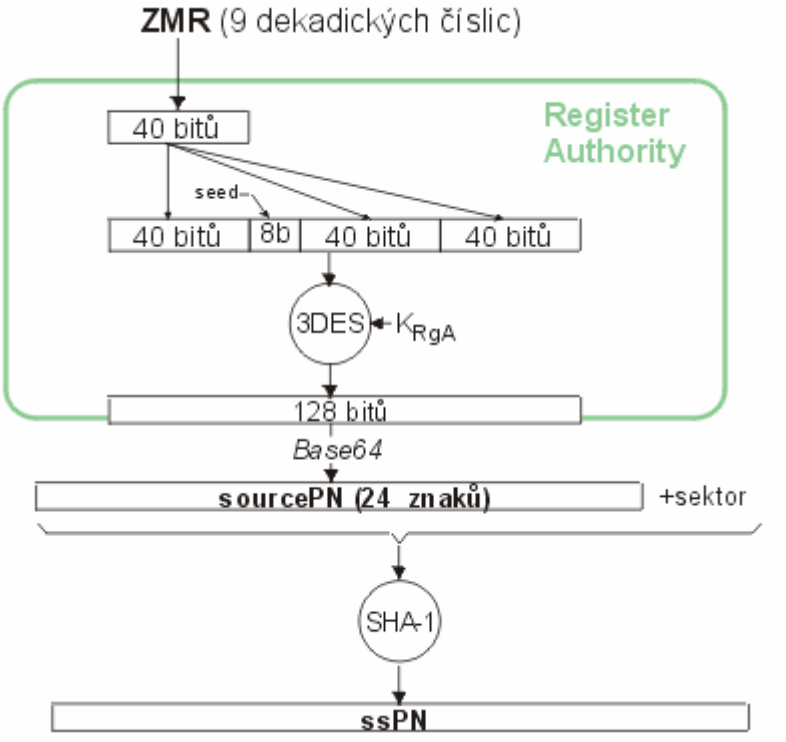


Obr. 4. Jedna osoba - mnoho identifikátorů

Jedna osoba (zde „Adam“) je v databázích každého sektoru vedena pod jiným identifikátorem (klíčem, číslem apod.). Čísla ssPN1 a ssPN2 tedy musí být různá. Navíc ze znalosti ssPN (sector specific Personal Number) v jednom sektoru nesmí být možné odvodit číslo ssPN v jakémkoliv jiném sektoru. Přitom musí být možné Adama spolehlivě identifikovat při jeho příštím přihlášení a operacích vůči databázím daného resortu (a to pokud možno i v případě, že by agendu vyřizoval pro změnu opět papírově).

Rakouský systém vychází z osobního čísla ZMR, přiděleného každému občanovi, ze kterého úřad registru (Register Authority) vytváří speciální číslo, unikátní pro každou osobu, tzv. sourcePN. Toto číslo si musí každá osoba podržet na svém zvláštním elektronickém průkazu (Bürgerkarte), který si lze představit třeba jako zvláštní čipovou kartu, ale jsou připuštěny i jakékoliv jiné, občanu milé formy, např. mobilní telefon, bankovní platební karta atp. Na průkazu je místo též pro klíčový a certifikační materiál pro kvalifikovaný elektronický podpis, pro pomocný podpis, pro autentizaci atd., ale to není pro tento výklad podstatné.

Číslo sourcePN je třeba chránit, neboť z jeho znalosti lze odvodit jakékoliv ssPN. Konkrétní implementace systému je znázorněna na dalším obrázku č. 5.



Obr. 5. Generacování sourcePN a ssPN

Číslo ZMR je překódováno do binární hodnoty ve 40 bitech. Pro vytvoření sourcePN se používá symetrický šifrovací algoritmus 3DES. Vstupní hodnota ZMR je zkopírována třikrát a mezi hodnoty je vložena konstantní hodnota seed (8 bitů), čímž vstupní blok dosáhne potřebné délky 128 bitů. Výstup představuje ono sourcePN, které je rovněž 128bitové a pro lepší čitelnost se zapisuje v Base64, čímž jeho délka dosáhne 24 znaků včetně dvou závěrečných „= =“.

Vytváření ssPN se děje vysloveně triviálně. Dostačuje k sourcePN znakově zřetězit předdefinované označení urn: daného sektoru a předat hašovací funkci SHA-1, na jejímž výstupu je sektorově specifický ssPN.

Takové použití SHA-1 je umožněno tím, že sourcePN je relativně dlouhé a v podstatě nikomu známé číslo. Pokud by se hašovací funkce používala přímo na ZMR, pak by bylo možné přes malý prostor vstupních hodnot vytvořit úplný slovník vstup-výstup, z něhož by se provedlo zpětné mapování hodnot vstupů z ssPN, ačkoliv SHA-1 je jinak kryptograficky odolná (byť již neperspektivní).

Kódování ze ZMR do sourcePN provádí jen a pouze tzv. „Registrační úřad“ (Register Authority), přičemž se uvádí, že tento registr je pouze virtuální. To znamená, že vytvoření sourcePN by se nemělo zanášet do žádné tabulky, spravované úřadem. [21]

4.1.2 Možná realizace v ČR

Jak již bylo řečeno, český model bude nejspíše v základních myšlenkách vycházet z toho rakouského. Není ještě jasné, jaké kryptografické metody budou použity k získávání jednotlivých agendových identifikátorů (obdoba ssPN), ani z jakých informací se budou získávat. Nicméně je jasné, že systém bude založen na sytému soukromých a veřejných klíčů a na kvalifikovaných certifikátech.

Základní myšlenka je specifikována v následující kapitole s využitím zdroje [22].

Identifikátory

Identifikace jednotlivých osob (fyzických, právnických i orgánů veřejné moci) je navržena pomocí identifikátorů.

Pro potřeby jednoznačné identifikace osob, a pro potřeby odvození agendových identifikátorů těchto osob, budou existovat tzv. základní identifikátory (ZI). Každá osoba bude mít vždy jen jeden základní identifikátor (na celý život).

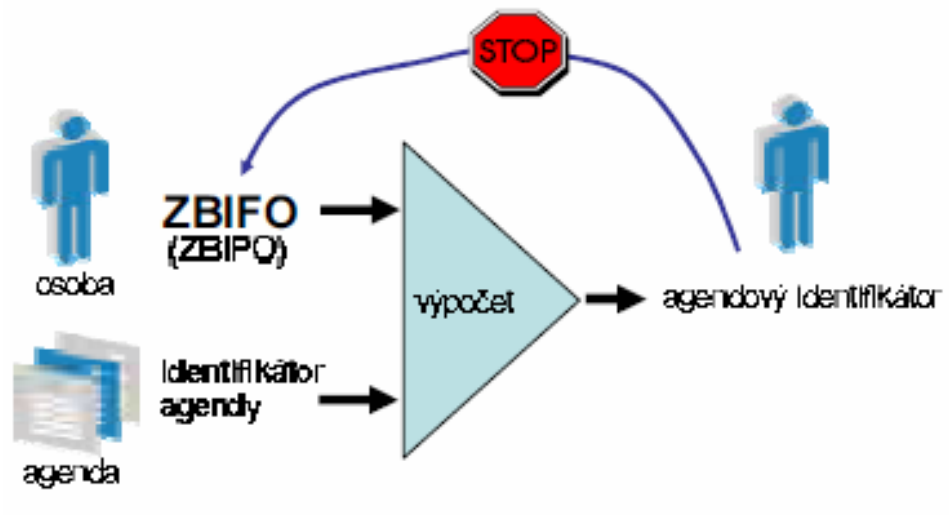
Základní identifikátor může být (ale nemusí) odvozen z jiného identifikátoru a dalších údajů (např. jména, data narození, rodného čísla atd.), pomocí kryptografických postupů. Ze základního identifikátoru fyzické, či právnické osoby proto nelze zpětně odvodit výchozí údaje, ze kterých je konstruován, bez znalosti klíče použitého k zašifrování. Tento klíč má k dispozici pouze CSI (Centrální správce identit).

Centrální správce identit je jedinou institucí oprávněnou k vydávání identifikátorů.

Pro potřeby identifikace jednotlivých agend budou existovat identifikátory agendy (sector code):

- každá agenda e-governmentu má přiřazen jeden identifikátor agendy
- obecně platí, že agendový identifikátor konkrétní osoby lze odvodit kryptografickým postupem ze základního identifikátory osoby a z příslušného identifikátoru agendy. Tento proces není obousměrný, ze znalosti agendového identifikátoru konkrétní osoby a identifikátoru agendy (sector code) nelze vypočítat základní identifikátor této osoby.
- pouze Centrální správce identit má schopnost převádět agendové identifikátory mezi sebou.

- Centrální správce identit zajišťuje převody mezi agendovými identifikátory pro potřeby vzájemné komunikace mezi agendami, ovšem pouze tam, kde to povoluje seznam tranzitivních identifikací (který je „maticí povolených převodů“). Obsah tohoto seznamu je dán legislativou, která určuje vzájemné vztahy a vazby jednotlivých agend.



Obr. 6. Představa výpočtu agendového identifikátoru

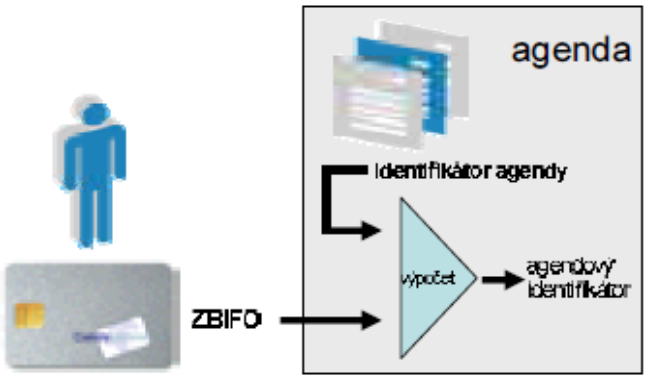
Pro potřeby ověřování identity (autentizace) bude pro každou osobu existovat tzv. identifikační záznam (identity link, fakticky datová položka XML), spojující základní identifikátor osoby s jejími podpisovými certifikáty (event. dalšími údaji).

Jako fyzické zařízení pro uchovávání základního identifikátoru a ostatních certifikátů by měla existovat tzv. karta občana. Karta občana je role, kterou mohou plnit různá zařízení na principu čipové karty (např. jednoúčelové čipové karty, platební čipové karty, klubové karty apod.), terminály či jiné formy technického řešení s tím, že žádná není apriorně vyloučena.

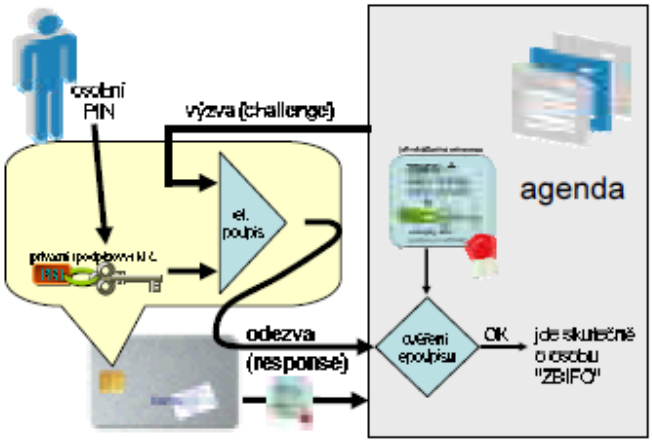
Princip identifikace a autentizace osoby vůči agendě

Vůči agendě veřejné správy se občan identifikuje svým základním identifikátorem. Agenda jej získá tak, že si z jeho karty přečte celý identifikační záznam, ve kterém jsou kromě základního identifikátoru obsaženy také podpisové certifikáty osoby. Autentizace pak proběhne tak, že agenda pošle kartě challenge (výzvu) a vyžádá si její elektronický podpis. Ten je proveden přímo na kartě, a podmínkou k jeho provedení je to, aby držitel zadal správný PIN. Agenda následně ověří pravost podpisu podle certifikátu, který je obsažen v identifikačním záznamu (a podle základního identifikátoru, který je obsažen na

identifikačním záznamu, ověří, komu podpis patří, a tím i kdo se vůči této agendě autentizuje). Pak si agenda sama vypočítá odpovídající agendový identifikátor (na základě základního identifikátoru a svého vlastního identifikátoru agendy). Dále již pracuje jenom s agendovým identifikátorem, zatímco základní identifikátor zapomene. Takovouto manipulaci se základními identifikátory má nařízenu zákonem.



Obr. 7. Identifikace osoby vůči agendě



Obr. 8. Autentizace osoby vůči agendě

4.1.3 Možnosti využití biometrických systémů

Technologie Single Sign-On byla nejdříve nasazována v soukromé sféře s cílem ušetřit prostředky, zvýšit efektivitu a bezpečnost systémů a také komfort uživatele. Stejně tak firmy kvůli obavám z bezpečnostních rizik začali zvažovat zavádění co nejkvalitnějších systémů pro zabezpečení svých prostor a sítí obsahujících citlivá data. Novým trendem v tomto směru je biometrika. Její využití pro zvýšení bezpečnosti se tak nabízí i v oblasti

elektronických systémů veřejné správy. Následující kapitola je zpracována na základě [23] a nabízí stručný pohled na technologii biometrie.

Metody autentizace uživatelů se obecně dělí do tří kategorií podle toho:

- co mají – typickým příkladem autentizace tohoto typu jsou magnetické nebo čipové karty, které běžně nezpracovávají informace, pouze je ukládají a vyžadují na straně ověřujícího subjektu příslušné čtecí zařízení.
- co znají – hesla v podobě alfanumerických řetězců, např. PIN na kartě.
- kdo jsou – na základě rozpoznávání vzorku trvalé fyzické, nebo psychické vlastnosti jedince; mezi fyzickými charakteristikami se využívají nejčastěji otisky prstů a struktura oční duhovky nebo sítnice, zkoumá se využití vlastností jako je tvar ruky nebo obličeje; z charakteristik pak lze využít hlas, způsob podpisu či způsob chůze.

Biometrika se využívá v nejrůznějších oblastech. Zpočátku samostatné biometrické systémy používané pro fyzický nebo logický přístup se dnes integrují do podnikových sítí, adresářových systémeů a také do systémů jednotného logování Single Sign-On.

Jednotlivé instituce mohou biometriku využívat samostatně nebo v kombinaci s jinými metodami autentizace. Obecně platí, že čím více metod současně použijeme, tím je dosaženo větší bezpečnosti. Můžeme tak využít všechny tři způsoby současně, čipovou kartu, PIN a některou z biometrických metod.

Biometrických systémů existuje celá řada, a jejich nasazení závisí na každém konkrétním případu. Organizace si musí nejprve stanovit potřebnou míru zabezpečení, které chtějí dosáhnout, a podle toho zvolit nejvhodnější typ. Biometrické systémy na bázi fyzických charakteristik slouží od maximálního zabezpečení ke střednímu, zatímco systémy využívající charakteristiky chování poslouží pouze pro nižší stupeň zabezpečení. Parametry některých metod jsou uvedeny v následující tabulce.

Tab. 2. Porovnání hlavních metod biometrie

	Otisk prstu	Obličej	Dlaň	Duhovka
Podíl chybných odmítnutí	0,2 – 36 %	3,3 – 70 %	0 – 5 %	1,9 – 6 %

Podíl chybných přijetí	0 – 8 %	0,3 – 5 %	0 – 2,1 %	Pod 1 %
Doba transakce	9 – 19 s	10 s	6 – 10 s	12 s
Velikost šablony	250 – 1000 B	84 – 1300 B	9 B	512 B
Počet hlavních výrobců	25+	2		1
Náklady na zařízení	Nízké	Střední	Střední	Vysoké
Faktory ovlivňující výkon	Špinavé ruce, suché horké prsty	Různá osvětlení orientace obličeje, sluneční brýle, make – up a další změny vzhledu obličeje	Zranění ruky, artritida, pocení	Špatné vidění, odrazy

Zavádění biometrických systémů však není pouze otázkou soukromých institucí, které chtějí zvýšit svoji bezpečnost. EU se rozhodla, že standardně implementuje čipy s biometrickými daty do pasů, konkrétně otisky prstů a sken oční duhovky. Jen prováděcí studie přišla na 140 milionů euro. Evropa tímto krokem také vyhovuje požadavkům americké strany, která od zemí bez vízové povinnosti požaduje biometrické identifikátory v pasech. Podobně EU bude požadovat od všech návštěvníků pocházejících ze zemí mimo unii otisk prstu ve vízu a také v povolení k pobytu, pokud cizinci žijí na území některé členské země. Podle Evropské komise je otisk prstu nejlepším řešením pro záložní kontrolu v databázi. Členské země mají v rámci imigrační politiky také rutinně ukládat fotografie žadatelů o vízum nebo o dlouhodobý pobyt jako primární biometrický identifikátor. Pomocí kombinace otisků prstů a fotografie se má zamezit zneužití dokladů a také zvýšit bezpečnost. Znamená to také nutnost sjednotit používané biometrické systémy a zajistit jejich vzájemnou spolupráci pro jednotnou evropskou politiku.

4.2 Požadavky na portál

Kromě požadavků na autentizaci a identifikaci uživatelů, což je hlavní pilíř každého Single Sign-On řešení, jsou na něj kladeny také další požadavky. V našem případě implementace v oblasti e-governmentu je dalším úkolem volba vhodného portálového řešení, které uspokojí naše požadavky na personalizaci. Bez něj by byl celý přínos tohoto řešení značně ochuzen, i když přínos použití samotného Single Sign-On je neoddiskutovatelný.

Výběr vhodného portálového řešení v našem případě není nic jednoduchého. Jak již bylo zmíněno celý informační systém a především prezentační vrstva (portál) se odvíjí od toho, pro jaký typ uživatelů je určen. Je nutné najít kompromis mezi uživatelskou přívětivostí pro nezkušené uživatele a tím, aby zkušenější uživatelé nebyli obtěžování záležitostmi, které jim připadají samozřejmé. Toho lze docílit vysokým stupněm personalizace. Portál může také obsahovat různé stupně nastavení, podle toho, jak uživatel sám sebe ohodnotí ve vztahu k informační gramotnosti a toto nastavení může samozřejmě dále upravovat. Budou mu tak nabídnuty informace a nástroje, které bude umět používat a na druhou stranu zkušeným uživatelům poskytne pokročilejší funkce, které jim usnadní práci. Samozřejmostí je pak možnost uzpůsobení vzhledu uživatelského rozhraní. Každý z uživatelů může mít možnost si službu upravit rozložením nebo barevně do jemu vyhovující podoby.

Personalizaci informačního systému, kdy si uživatel může zvolit konkrétní informace, které chce dostávat a v jaké podobě umožňuje komponentová realizace portálu. V komponentově stavěném systému jsou vzájemně odděleny stránka obsahová a prezentační.

Reakce sytému na požadavek uživatele probíhá ve třech fázích:

- zpracování parametrů vstupního požadavku aplikační, případně datovou logikou;
- generování výstupních dat nezávislých na formě prezentace (výstupní parametry udávají, která data jsou poslána na výstup, ale neříkají, jak budou zobrazena);
- zformátování výstupu a jeho prezentace uživateli;

Současně s požadavkem přicházejícím od uživatele jsou předávány i parametry popisující prostředí (např. typ a možnosti klienta), které umožňují správnou interpretaci výstupních

dat. Může být nastavena také jazyková varianta a na základě preferencí uživatele je připraveno prostředí pro výstup.

Následuje fáze zpracování vstupních údajů a provedení požadovaných akcí (např. změny v databázi či obecně stavu systému). Tato fáze většinou neprodukuje žádná výstupní data, typicky pouze chybová hlášení, příp. zprávu o úspěšně provedených změnách.

V další fázi procesu vybírá aplikace požadované údaje z databáze a sestavuje je do vhodného formátu. Nejčastěji jsou data formována jazykem XML do výstupního proudu, který je pak dále zpracován prezentační transformací, příp. je možné data poslat přímo na výstup. Aplikace mohou ukládat uživatelské preference a nastavení, které se pak používají při opětovné prezentaci dat uživateli. V autentizovaných systémech je možné tyto informace uchovávat v databázi, jinde mohou podobně posloužit např. cookies.

Výhody tohoto způsobu zpracování vstupních požadavků a výstupních dat jsou zřejmé. Pro výstup na různých zařízeních či v různých jazykových variantách potřebujeme jedinou aplikaci. [24]

Portál představuje hlavní bránu k informacím. Sám může obsahovat řadu informací, zprostředkovávat je z dalších zdrojů nebo obsahovat odkazy na další aplikace. Pro uživatele je podstatné, že si musí pamatovat pouze jednu adresu, případně ji může mít dokonce nastavenou jako domovskou stránku a ve spojení se Single Sign-On také jediné přístupové údaje, aby se dostal ke všem aplikacím, které chce využívat.

4.2.1 Základ portálu - portlety

Základním stavebním kamenem portálových frameworků jsou portlety. Portlety jsou znovupoužitelné komponenty uživatelského rozhraní založené na technologiích Java, které přijímají požadavek, zpracují jej a vygenerují dynamický obsah. Technologie portletů je standardizována specifikací JSR168 a novější JSR286 a podobně jako jiné technologie JEE i portlety jsou založené na konceptu kontejnerů. Kontejner poskytuje portletu prostředí a služby. Portálová stránka při tomto přístupu připomíná desktop, kde obsahy jednotlivých portletů jsou vykreslovány v portletových oknech. Podobně jako okna desktopu mají i portletová okna hlavičku, kde jsou umístěny ovládací prvky okna, mezi něž patří například minimalizace, maximalizace okna nebo spuštění portletu v různých režimech, jako jsou konfigurační, editační nebo prezentační.

Protože jsou portály častou a užitečnou aplikací, existují frameworky pro jejich rychlý a snadný vývoj. Tyto frameworky se zaměřují na klíčové funkčnosti portálu jako je personalizace nebo single sign-on.

Na první pohled se nabízí podobnost mezi technologií portletů a servletů. Stejně jako servlet i portlet je Java komponenta, což s sebou automaticky nese vlastnosti jako nezávislost na platformě. Obě komponenty běží v prostředí kontejneru, který řídí i jejich životní cyklus. Komponenty jsou založeny na request/response paradigmatu a generují dynamický obsah.

Nicméně portlet není servlet a mezi oběma komponentami jsou zásadní rozdíly. Zatímco úkolem servletu je vygenerovat celou HTML stránku, portlety generují pouze fragmenty stránky a samotnou stránku sestavuje portál na základě zvoleného layoutu. Portlety mohou být spuštěny pouze pomocí URL, která jsou generována pomocí portlet API. Weboví klienti přistupují k portletům pomocí portálu. Portlety rozlišují mnohem více typů požadavků, jako jsou požadavky pro provedení akce, událostí, vykreslení fragmentu. Portlet může být na jedné stránce použit vícekrát a má definovány různé módy a stavy, které ovlivňují fungování portletu.

Jak již bylo řečeno, portál poskytuje služby běžícím portletům. Mezi ty nejdůležitější služby patří:

- personalizační služba, která umožní portletu využití rule enginů (systémů pravidel) a uživatelských profilových informací k modifikaci obsahu zobrazovanému uživateli;
- zpracování událostí;
- komunikace mezi portlety, kdy lze sdílet nebo posílat data mezi portlety a umožnit tak pohled na data napříč jednotlivými zdroji;
- vyhledávací služby, které usnadní práci s obsahem portálu;
- správa uživatelů a skupin.

Výsledkem je HTML stránka, která je interpretována prohlížečem klienta. Pro zkrácení času odpovědi se často používají cache. Tyto cache lze použít na libovolné úrovni infrastruktury. Použití cache musí mít ale silný důvod, protože na oplátku za zrychlení reakcí aplikace zhoršují správu aplikace. Přidáním cache se do infrastruktury přidává software, který může vykazovat nějaké chyby, a proto je nutné se o něj starat. Navíc je

nutné mít na paměti aktuálnost informace. Ne každý obsah lze cachovat, obzvláště ten dynamický.

Portálových řešení existuje celá řada, ať jsou to produkty komerční nebo open source. Komerční portálové řešení nabízí samozřejmě lídři enterprise trhu – IBM se svým WebSphere Portal Server, Oracle s produktem Oracle Portal 10g nebo Sun s Java System Portal Server. Jako zástupce open source světa jmenujme alespoň JetSpeed od Apache nebo JBoss Portal. [18]

5 NÁVRH SYSTÉMU

Při návrhu jakéhokoli systému je dalším krokem po stanovení požadavků zjištění, zda již podobný systém, ze kterého by bylo možné vycházet neexistuje nebo zda na trhu není dostupné odpovídající řešení . V řadě případů tomu tak je. Stačí pak pouze systém doplnit, či pozměnit tak, aby splňoval naše požadavky.

Jak již bylo zmíněno existuje několik open source Single Sign-On řešení. Některé z nich však nejsou pro náš případ vyhovující. Jsou to hlavně ty, které jsou postaveny na federativním modelu (Shibboleth, SourceID).

Je nutné aby navržený systém SSO splňoval všechny požadavky AAM modelu uvedené výše. Takovým řešení, odpovídajícím našim požadavkům je open source varianta CAS. E-government, ačkoli se jedná o decentralizovaný systém, by měl být vzhledem k identifikaci a autentizaci spravován centrálně. Především pokud se jedná o správu uživatelských účtů a samotnou identifikaci.

Při porovnání našich požadavků (např. centralizace správy uživatelských účtů, jediná autorita pro vydávání certifikátů - Centrální Správce Identit, atd.) je vidět, že pro potřeby a navržený systém e-governmentu je vhodné řešení CAS.

Central Authentication Service existuje ve více verzích. V této kapitole je popsána základní verze, ze které všechny další vycházejí a také verze CAS++ publikovaná v [15], která lépe splňuje naše požadavky a její modifikací lze dosáhnout odpovídajícího řešení pro nasazení v e-govenmentu.

5.1 Central authentication service

Základní verze central authentication service byla vyvinuta na univerzite Yale. V této podkapitole je na základě [25] popsána hlavní koncepce CAS, tzn. jeho základní verze.

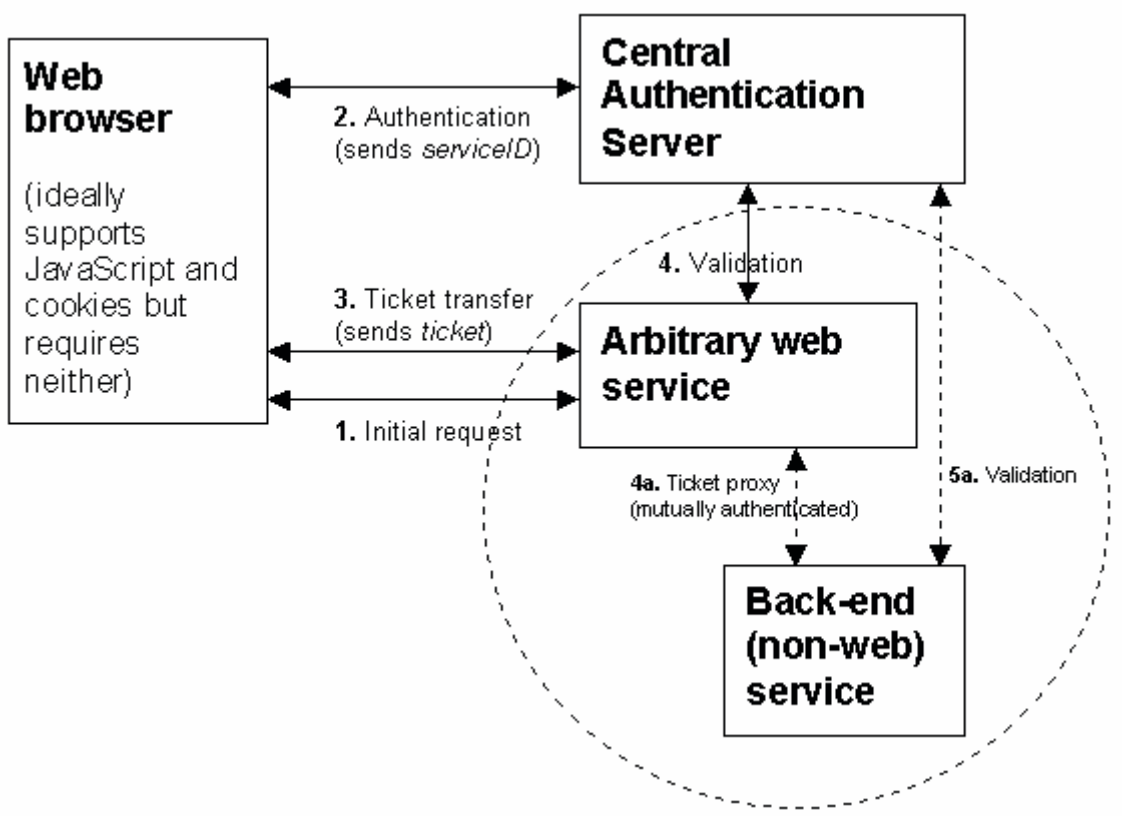
Central Authentication Server je navržen jako soběstačná webová aplikace. Je implementován jako několik JAVA servletů a běží prostřednictvím HTTPS serveru. Přístup k němu je řešen pomocí tří URL: přihlašovací URL (login URL), ověřovací URL (validation URL) a případnou odhlašovací URL (logout URL).

Pro přístup ke službě CAS aplikace přesměruje uživatele nebo jednoduše vytvoří hyperlink na přihlašovací URL. Uživatel také může zadat URL manuálně.

Přihlašovací URL spravuje prvotní autentizaci. Tzn., vyžádá si od uživatele NetID a heslo a ověří ho vzhledem k autentizační autoritě.

Aby byla umožněna pozdější opětovná autentizace CAS odešle in-memory cookie (její platnost skončí ihned po zavření prohlížeče) zpět do prohlížeče. Tato cookie, označována jako Ticket Granting Cookie (TGC), identifikuje uživatele, který je již úspěšně přihlášen.

Stojí za zmínku, že tato cookie je volitelnou částí autentizačního mechanizmu CAS. Právě s jejím přispěním uživatel získá výhody Single Sign-On, to znamená, že pouze jednou zadá svoje NetID a heslo a získá tím přístup do všech služeb pod správou CAS. Bez této cookie by byl uživatel nucen vždy když by byl aplikací přesměrován na CAS zadávat svoje údaje. Uživatelé si můžou vyžádat zrušení této cookie přesměrováním na odhlašovací URL.



Obr. 9. Schéma Central autehtication service

Navíc, při zpracovávání prvotní autentizace zaznamenává CAS také službu, ze které byl uživatel přesměrován. To je umožněno tím, že aplikace, které přistupují k přihlašovací URL musí poskytnou CAS identifikátor služby (serviceID na obrázku 9). V případě úspěšné autentizace, CAS vytvoří náhodné číslo tzv. ticket. Následně asociuje tento ticket s uživatelem, který požaduje autentizaci. To znamená, pokud je uživatel přesměrován

službou S, CAS vytvoří ticket T, který povoluje uživateli přístup. Tento ticket je možné použít pouze jednou a platí pouze pro konkrétního uživatele a službu S. Jeho platnost končí jakmile je použit k přístupu ke službě.

Po prvotní autentizaci CAS přesměruje prohlížeč uživatele zpět do aplikace. Zná URL na kterou přesměrovat, protože serviceID slouží také jako zpětná URL. To znamená že, identifikátor použitý aplikací musí reprezentovat URL, které je součástí. CAS přesměruje prohlížeč uživatele zpět na tuto URL spolu s požadovaným parametrem (ticket).

5.1.1 Využití CAS a jeho modifikace

Návrh našeho systému vychází z myšlenky open source systému CAS++ publikovaného v [15]. Ten je založen na využití certifikátů totožnosti a spojuje myšlenku CAS s využitím mechanizmů PKI. CAS++ realizuje zcela samostatný server, který poskytuje jednoduchý, efektivní a spolehlivý SSO mechanizmus využívající HTTP přesměrování.

CAS++ umožňuje centralizovanou správu uživatelských profilů a přístup ke všem službám v systému s využitím jednoznačných přihlašovacích údajů. Úložiště uživatelských profilů je pouze na SSO serveru a jsou jediným bodem přístupu k těmto informacím (případně ještě Centrální Správce Identit), čímž snižuje nebezpečí rozptylování osobních informací.

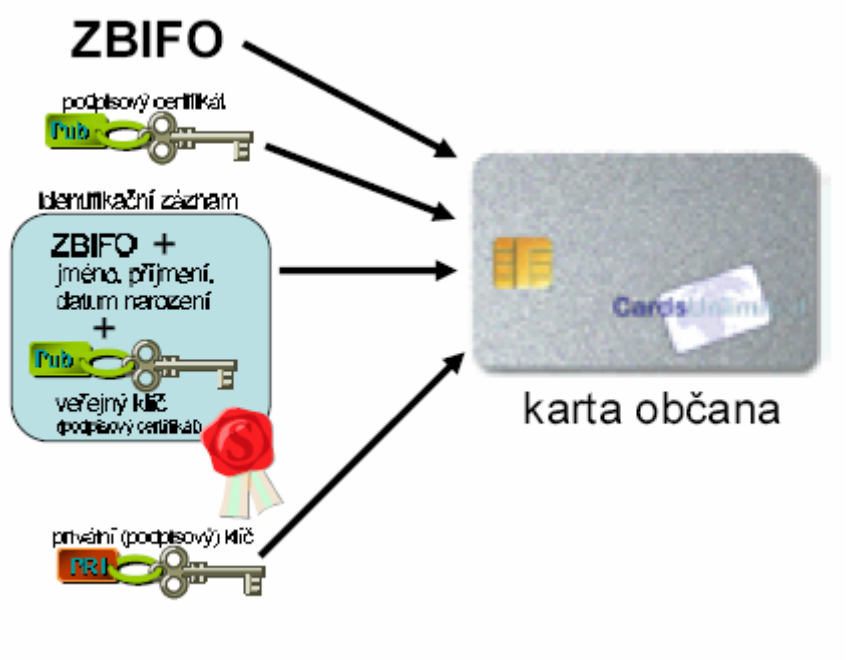
CAS++ je založen na standardních protokolech jako SSL, pro zabezpečenou komunikaci, a X.509 certifikáčních mechanizmech. CAS++ je čistokrevným JAVA modulem a je plně integrovatelný s standardními webovými aplikacemi.

Obohacuje CAS architekturu o využití:

- PKI;
- fyzické zařízení pro uchovávání certifikátů (karta, token atd.);
- volitelně o využití biometrických údajů.

Proces ověřování identity v našem systému je založen na následujících krocích:

I. Uživatel zažádá příslušnou CA (v našem případě Centrální Správce Identit) o vydání karty občana se všemi jejími náležitostmi. Představa obsahu karty je znázorněna na obrázku 10.



Obr. 10. Karta občana

II. Uživatel obdrží kartu občana se svým X.509 certifikátem podepsaným CISem, který zaručuje identitu občana. Tomu odpovídající privátní (podpisový) klíč je uložen na kartě v zašifrované podobě (např. 3DES) a jeho získání je možné pouze po identifikaci uživatele. Identifikace probíhá zadáním PIN uživatele nebo u silnějšího zabezpečení ověřením jeho biometrických údajů. Celý obsah karty občana je následující – základní identifikátor (ZBIFO), kvalifikovaný certifikát, veřejný klíč (podpisový certifikát), privátní (podpisový) klíč a identifikační záznam.

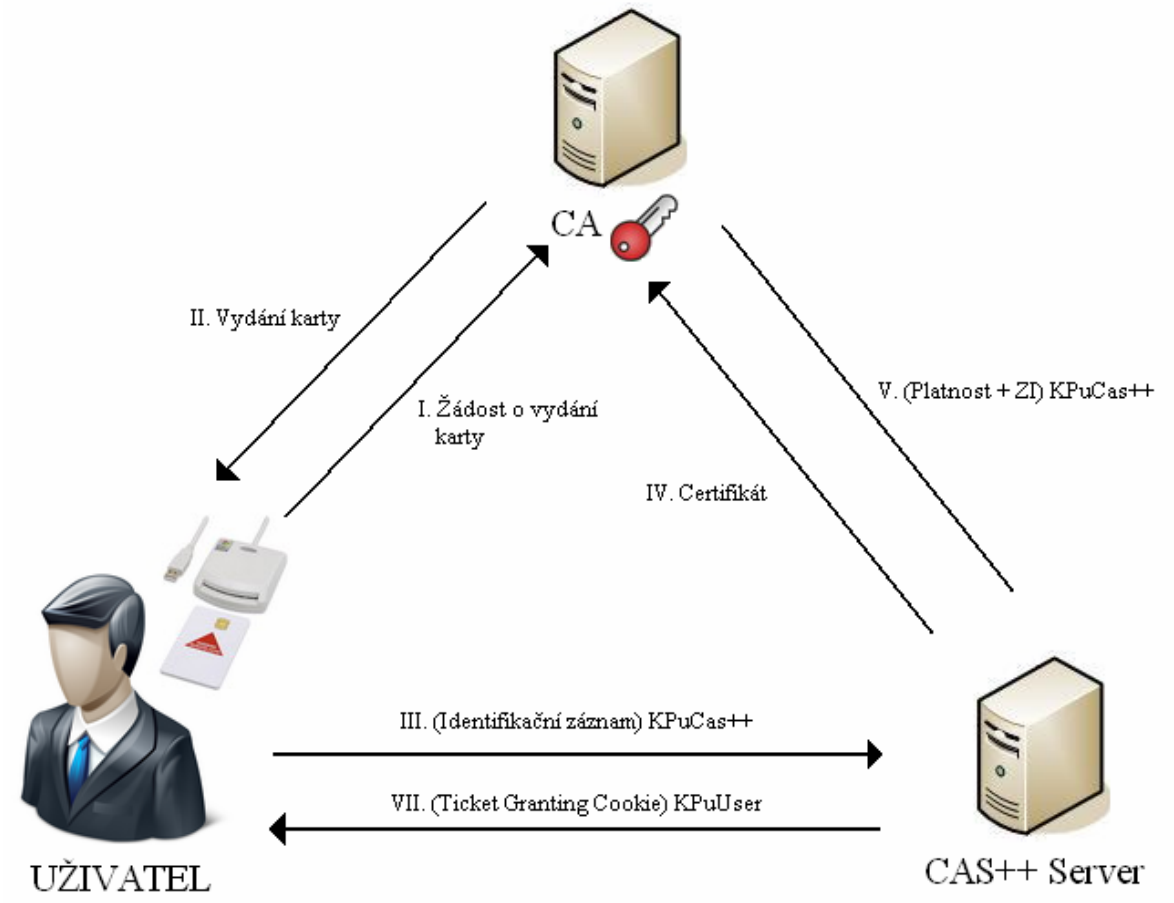
III. Při prvním navázání spojení mezi uživatelem a portálem e-governmentu je uživatel přesměrován na ověřovací server nebo může využít přímo login URL serveru. Po úspěšném navázání spojení putuje z karty občana jeho identifikační záznam zašifrovaný veřejným klíčem CAS++ (KPuCas++), ve kterém jsou kromě základního identifikátoru obsaženy také podpisové certifikáty osoby .

IV. CAS++ dešifruje přijatá data svým soukromým klíčem a ověří platnost certifikátu u CISu.

V. Centrální správce identit ověří platnost certifikátu a odešle na CAS server základní identifikátor osoby svázané s certifikátem zašifrovaný veřejným klíčem CAS++ (KPuCAs++).

VI. Pokud je certifikát platný CAS++ porovná identifikátor získaný od CISu s identifikátorem získaným z karty občana a provede tak ověření jeho identity.

VII. V případě kladné autentizace vytvoří CAS++ cookie (TGC) a odešle ji uživateli zašifrovanou jeho veřejným klíčem. V tomto bodě, pro přijetí TGC musí uživatel získat ze své karty svůj privátní klíč k rozšifrování TGC. Ten získá zadáním PIN nebo kontrolou biometrických údajů. Jakmile dojde k odemčení karty, je získán klíč a TGC rozšifrována. Ta je pak použita pro každý další přístup ke službám v rámci CAS++ Single Sign-On serveru.



Obr. 11. Proces ověřování identity

V tomto okamžiku pro každý další přístup ke službě v rámci relace je použita TGC pro autentizaci bez zadávání jakýchkoli dalších informací.

Proces ověřování vůči jednotlivým agendám probíhá zabezpečenou komunikací a je obdobný procesu ověřování identity. Probíhá v několika krocích:

I. Uživatel si vyžádá přístup k některé z agend.

II. Agenda vyšle požadavek na autentizaci pomocí HTTP přesměrování ne server CAS++.

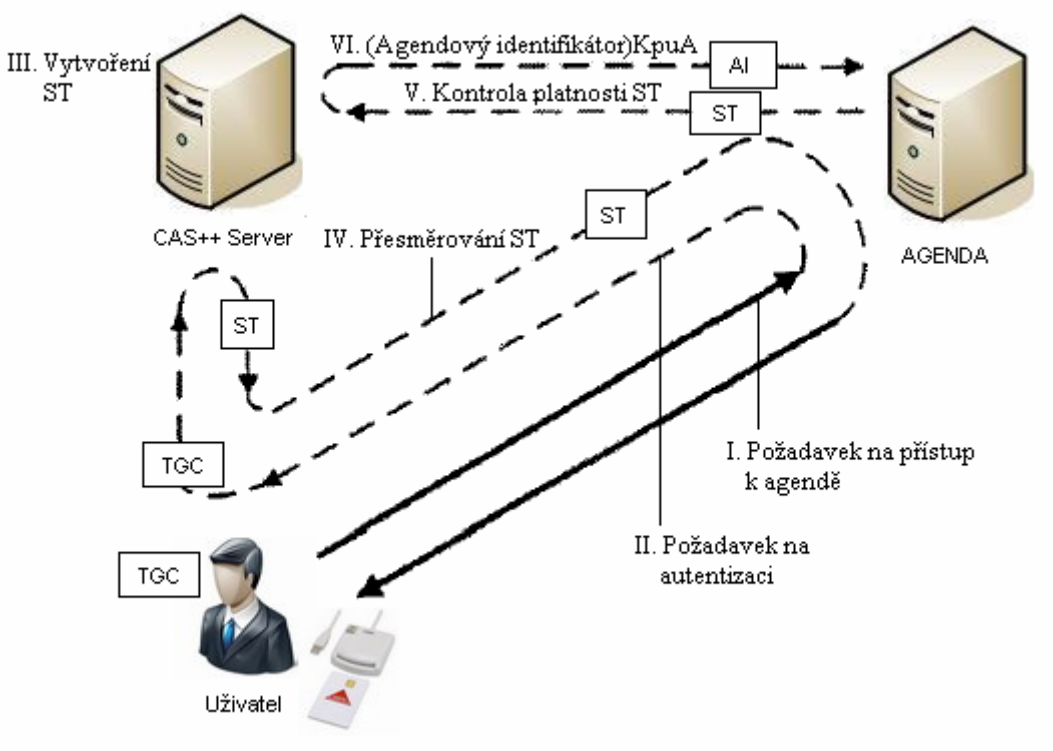
III. CAS++ server získá identifikátor agendy a TGC uživatele, pokud existuje. V případě, že byl uživatel již dříve úspěšně identifikován a má práva pro přístup k příslušné agendě, je vytvořen tzv. Service Ticket (ST).

IV. CAS++ přesměruje prohlížeč uživatele spolu s ST na příslušnou agendu.

V. Agenda obdrží ST a zkontroluje platnost jeho zasláním na CAS server.

VI. Pokud je ST platný, CAS++ vytvoří ze základního identifikátoru a identifikátoru agendy příslušný agendový identikátor uživatele. Ten je zašifrován veřejným klíčem příslušné agendy (KPuA) a odeslán agendě.

VII. Uživatel získá přístup a je jednoznačně identifikován vůči agendě svým agendovým identifikátorem.



Obr. 11. Proces ověřování vůči agendě

Důležitým faktem je, že CAS++ server uchovává příslušné základní identifikátory jednotlivých uživatelů pouze po dobu existence příslušné session. Stejně tak TGC je uložena v prohlížeči pouze po tuto dobu.

V případě zákonem daných podmínek, kdy má agenda právo získávat informace o uživateli z jiných zdrojů se může obrátit na Certifikační autoritu (Centrálního správce identit) s požadavkem na poskytnutí příslušného agendového identifikátoru. CIS tedy zajišťuje převody mezi agendovými identifikátory pro potřeby vzájemné komunikaci mezi agendami.

V navrženém systému se vstupní portál e-govermnetu chová vzhledem k CAS++ stejně jako ostatní agendy. Jednotlivý uživatelé jsou reprezentováni agendovými identifikátory pro agendu portálu a ta spravuje jejich uživatelské účty s nastavením portálu. Portál by měl poskytovat možnost přidávat do účtů informace samotným uživatelem, v případě, že s tím uživatel souhlasí. To může zvýšit možnosti personalizace, například uživateli mohou být zobrazovány informace vzhledem k jeho trvalému bydlišti nebo ve vztahu k jeho zaměstnanosti (nabídka úřadu práce). Na druhou stranu systém zachovává soukromí uživatele a takovéto informace od něj primárně nevyžaduje.

5.1.2 Zhodnocení CAS++ ve vztahu k AAM modelu

CAS++ je založen na Autentizačním a autorizačním modelu AAM. V tabulce 3 je vidět zhodnocení CAS++ ve vztahu k tomuto modelu. Jak je vidět z tabulky CAS++ naplňuje většinu požadavků AAM modelu; poskytuje centrální bod pro správu autentizací, autorizací a uživatelských profilů. Na nižší úrovni je CAS++ systém založený na tradičních a ověřených standardech jako HTTP, SSL a X.509 a dalších jako SOAP a SAML. Konečně s ohledem na Client Status Info, všechna komunikace mezi serverem, prohlížečem uživatele a jednotlivými agendami v architektuře CAS++ je založena na bezvýznamových cookies a využitý šifrovaných kanálů.

Tab. 3. Zhodnocení CAS++ ve vztahu k AAM modelu

Požadavek	CAS++
Autentizace	ano
Silná autenzizace	ano
Autorizace	ano

Provisioning	plánovaný
Federation	ne
C.I.M.	ano
Client Status Info	ano
Single Point of Control	ano
Standart Copmliance	ano (HTTP, SSL, X.509)
Cross-Language availibility	ano
Password Proliferation Prevention	ano
Scalability	plánovaný

5.2 Studie proveditelnosti

Studie proveditelnosti (Feasibility Study), někdy též označovaná jako technickoekonomická studie, je dokument, který souhrnně a ze všech realizačně významných hledisek popisuje investiční záměr. Jeho účelem je zhodnotit všechny realizační alternativy a posoudit realizovatelnost daného investičního projektu, jakož i poskytnout veškeré podklady pro samotné investiční rozhodnutí. Studie proveditelnosti bývá zpracovávána v přípravné, tedy předinvestiční fázi projektu.

Studie je zpracována na základě metodické příručky pro studie proveditelnosti [26].

1) Úvodní informace

V našem případě není studie proveditelnosti kompletním materiálem celého projektu. Je spíše materiálem, který je zaměřen na smysl projektu a jeho přínos pro potenciální uživatele. Je to způsobeno tím, že celý projekt je jen částí většího celku nasazování e-governmentu v ČR, jehož základní koncept je již znám, nicméně konkrétní řešení a použité technologie jsou zatím pouze ve fázi příprav. Všechny kroky při zavádění e-governmentu musejí mít navíc pevnou oporu v zákoně. Nebylo by moudré navrhovat systém pouze s ohledem na současný stav, i když by to umožnilo vytvořit v krátké době fungující systém, ale je nutné vzít v úvahu budoucí rozvoj a legislativní podmínky.

Také některé finanční otázky a analýzy nejsou v možnostech rozsahu této práce a vyžadovaly by hlubší zkoumání. Všechny oblasti jsou však v následující kapitole zmíněny a jsou alespoň nastíněny jejich dopady na případný projekt.

2) Stručné vyhodnocení projektu

Navržené řešení bylo vybíráno s ohledem na všechny současné i možné budoucí požadavky. Cílem bylo také aby navržený systém kladl co nejmenší nároky na potenciální uživatele a to především vzhledem k nutnosti pořizování potřebných zařízení či dalších dodatečných nákladů.

Také na straně provozovatele a zajišťovatele celého systému bylo dbáno na co nejmenší náklady a využití buď již existujících služeb nebo služeb, které budou součástí e-governmentu.

Přínos Single Sign-On v této oblasti je nesporný a to nejen vzhledem ke komfortu zájemců o službu ale také ke zvýšení poptávky po elektronických službách veřejné správy.

3) Stručný popis myšlenky projektu

Název projektu – Využití Single Sign-On a jeho přínos v oblasti e-governmentu.

Smyslem celého projektu je využití technologie Single Sign-On v elektronické formě komunikace s orgány veřejné správy. Návrh je také zaměřen na spojení této technologie s personalizačními službami které mohou přinést velký uživatelský benefit.

Systém by měl poskytovat služby jednotného přihlášení a přístup ke službám veřejné správy přes jednotný portál. Personalizace vstupního portálu by měla poskytovat nejen vzhledovou úpravu ale také úpravu obsahovou a vybraným poskytovatelům služeb možnost zasílat informace a upozornění tak, aby důležité oznámení nepřehlédl.

Zadavatelem a provozovatelem celého systému je Ministerstvo vnitra České republiky.

Z jednotlivých fází investičního záměru jsou pro tento projekt nejdůležitější fáze investiční a fáze provozní. Mezi těmito fázemi bude nejspíše probíhat ještě takzvaná mezifáze. Za typický příklad takovéto smysluplné mezifáze můžeme považovat zaváděcí provoz. Bývá typický pozvolným přechodem od procesů, organizace a toků investiční fáze směrem k fázi provozní. Tento se může vyznačovat i určitými dočasnými opatřeními, která nebyla na pořadu dne ani v předchozí fázi investiční ani nejsou součástí plné provozní fáze. Příkladů je možné nalézt celou řadu: povolání určitých expertních skupin, které mohou být nápomocny při záběhu plného provozu (IS/IT specialisté apod.), dočasně omezená velikost provozu atd.

V našem případě je pravděpodobné, že dojde k zaváděcímu provozu, v němž bude současně fungovat jak elektronická komunikace tak běžná papírová. A to nejen z důvodu doladění technických záležitostí ale také s ohledem na uživatele, kteří nemají možnosti elektronické komunikace nebo ji zatím z nějakého důvodu nechtějí využívat. V provozní části projektu by však měla být papírová komunikace omezena na nejmenší možnou míru a pouze na případy ve kterých není jiná možnost.

4) Odhad poptávky

Přestože trh v případě veřejných statků (silnic, veřejných sportovišť aj.) negeneruje přímo cenu takovéhoto výstupu, po každé službě či výrobku existuje určitá poptávka (někdy se hovoří o poptávce společenské) a ta je dána potřebami subjektů, které ji tvoří a které hodlají tyto svoje potřeby prostřednictvím dané služby či produktu, ať již veřejného či komerčního, uspokojovat. Stejně tak je tomu i u našeho návrhu.

Navíc v našem případě je určitá část poptávky zaručena zákonem. Elektronická komunikace s úřady bude brzy zákonem nařízena všem obchodním subjektům. Z toho plyne, že obchodní subjekty nebudou mít jinou alternativu uspokojení potřeby. Odhad této poptávky se pohybuje v rozmezí 2 500 000 až 2 800 000 a vychází z údajů z roku 2004 kdy bylo u nás registrováno 2 300 000 obchodních subjektů.

V oblasti fyzických osob je odhad poptávky složitou záležitostí. Odvíjí se od více faktorů, především pak od výsledné ceny produktu. Tj. certifikátu vydaného CA nutného pro přístup a využívání služeb e-governmentu.

Dalším ukazatelem možné poptávky je počet domácností disponujících potřebným vybavením pro přístup ke těmto službám. Tzn. počítač s přístupem k internetu. Tento počet neustále stoupá a podle ČSÚ je v současné době připojeno 1,8 milionu uživatelů, tedy 42 procent domácností.

Výsledná poptávka se bude odvíjet od faktu, zda se uživatelům vyplatí upřednostnit elektronickou variantu před klasickou návštěvou úřadu, případně písemnou formou komunikace. A to jak z hlediska finančního tak z hlediska úspory času a rychlosti vyřízení požadavku.

5) Management projektu a řízení lidských zdrojů

Vlastníkem projektu je stát. Provozovatel systému bude vybrán ve výběrovém řízení stejně jako tomu bylo například u projektu datových schránek. Pravděpodobně se bude jednat o některou z velkých firem na poli telekomunikačních technologií.

Všechny záležitosti řízení lidských zdrojů budou tak přeneseny na vybranou společnost a stát, resp. ministerstvo vnitra bude pouze dohlížitelem.

6) Technické a technologické aspekty

U projektů jako tento, je podklad a jeho kvalita zcela zásadní. Zvolená technika a technologie v té či oné fázi projektu zásadním způsobem ovlivní investiční nebo provozní finanční toky projektu.

Podstatou celého provozu projektu je internet, technologie s ním spojené a výhody které poskytuje.

Celá technologie je založena na open sourcové variantě autorizačního návrhu, využití šifrovacího systému veřejných klíčů a kvalifikovaných certifikátů. Je otázkou dalšího řešení, zda stát pro toto řešení zřídí svou vlastní CA. Pravděpodobnější je, že využije služeb některé z již existujících certifikačních autorit.

Zvolené řešení vyhovuje legislativním požadavkům a navíc nabízí využití již osvědčených technologií.

Jelikož se předpokládá v průběhu celého projektu postupný nárůst počtu uživatelů a také postupné zastarávání zvolených technických prostředků, především hardwaru, je nutné podrobně plánovat nutné reinvestice.

7) Finanční stránka projektu

Každý projekt před svým uskutečněním prochází řadou finančních analýz v rámci studie proveditelnosti. Součástí by měly být:

- Zajištění investičního a oběžného majetku;
- Finanční plán a analýza projektu;
- Hodnocení efektivity a udržitelnosti projektu
- Analýza citlivosti a řízení rizik

Hlavními dvěma body projektu z hlediska investic fáze investiční a fáze provozní. Investiční fáze je období od začátku výstavby projektu do zahájení provozu. V tomto období zpravidla převyšují výdaje nad příjmy. Významnějším finančním faktorem projektu je však fáze provozní. Ta zajišťuje projekt po celou dobu jeho životnosti a v našem případě tvoří hlavní část finančních nároků na navržený systém.

Zhodnotit projekt z hlediska výnosnosti není prakticky možné. Jedné se o projekt poskytující veřejné služby a tudíž negeneruje žádný zisk, popřípadě velmi malý, který ale není vzhledem k vynaloženým prostředkům podstatný. Hlavní hodnota projektu je ve zjednodušení a zrychlení vykonávání státní správy, což samo o sobě přináší úspory (např. menší potřebný počet pracovníků).

8) Harmonogram projektu

Nedílnou součástí studie proveditelnosti je časový plán jednotlivých činností a fází projektu. U všech projektů týkajících se veřejné správy existuje posloupnost jednotlivých fázi zavedení systému. Prvním krokem je přijetí příslušných zákonů, následuje výběr vhodné technologie, která odpovídá přijatým zákonům a posledním krokem je zavedení technologie.

9) Závěr studie proveditelnosti

Celý projekt je realizovatelný za předpokladu některých kroků, které musí předcházet nasazení technologie Singl Sign-On v e-governmentu. Je to především dořešení legislativních otázek a pokračování v realizaci dalších projektů spojených s e-governmentem, které umožní uvedení projektu do praxe.

ZÁVĚR

Předmětem této práce bylo prozkoumat možnosti využití technologie Single Sign-On pro použití v oblasti elektronické vlády.

Úvod teoretické části je věnován základním myšlenkám e-governmentu a definici samotného pojmu. Hlavním bodem této kapitoly je analýza a seznámení se stavem elektronizace veřejné správy v České republice. Nasazování informačních technologií ve správě veřejných věcí je neodvratným krokem v reformě celé veřejné správy. Jsou zde popsány jednotlivé služby dostupné v současné fázi nasazování e-governmentu, jejich funkce, přínosy a dostupnost.

Teoretická část pokračuje vymezením základních principů technologie Singl Sign-On a zabývá se požadavky, které jsou na tuto technologii kladeny. Jednotlivé v současné době dostupné řešení jsou popsány podrobněji.

Přínos technologie Singl Sign-On nejen v oblasti e-governmentu jak pro uživatele, tak i pro provozovatele informačních systémů je značný, nabízí se další obohacení tohoto systému a to o funkce personalizace. Tomuto tématu je věnována poslední část teoretické části. Zabývá se nejenom různými stupni personalizace, ale i technikám návrhu informačních systémů s ohledem na potřeby uživatelů.

Základem veřejné správy jsou služby. Cílem praktické části bylo seznámení s potřebami návrhu jednotného přihlašování Single Sign-On v rámci e-governmentu s ohledem na požadavky jednotlivých služeb, podmínky dané zákonem a vhodnost řešení vzhledem k celé architektuře elektronické vlády.

Bylo zvoleno open source řešení CAS vyvinuté na Univerzitě Yale, které nejlépe vyhovuje podmínkám e-governmentu v našich podmínkách. Byly prozkoumány jeho funkce a princip fungování Single Sign-On v této architektuře. Při dalším zkoumání byla jako základ celého řešení vybrána verze CAS++ a ta byla následně modifikována, aby lépe vyhovovala nejen legislativním požadavkům ale také poskytovala potřebnou úroveň bezpečnosti.

Byl navržen systém jednotného přihlašování vyhovující navrženým podmínkám a princip celého řešení byl podrobně popsán.

Závěrečná kapitola praktické části je věnována studii proveditelnosti, která zkoumá možnosti nasazení tohoto projektu v našich podmínkách. Zkoumá některé překážky a aspekty ovlivňující možnosti využití tohoto sytému.

Tato práce nabízí komplexní řešení nasazení technologie Single Sign-On v rámci e-governmentu v ČR založené na systému CAS, včetně zkoumání všech aspektů nasazení tohoto řešení.

SEZNAM POUŽITÉ LITERATURY

[1] MATES, Pavel. E-government v českém právu. 1. vyd. Praha : Linde, 2006. 244 s. ISBN 80-7201-614-8.

[2] Státní informační a komunikační politika [online]. Dostupný z WWW: http://www.isvs.cz/user_data/zpravodajstvi/obrazky/File/ISVS-eCesko2006/MICR-eCesko-2006.pdf.

[3] E-government [online]. Dostupný z WWW: http://cs.wikipedia.org/wiki/E-Government.

[4] E-government - strategické dokumenty (1. díl) [online]. Dostupný z WWW: http://www.isvs.cz/e-government/e-government-strategicke-dokumenty-1-dil.html.

[5] Česká vláda dnes schválila zákon o e-governmentu [online]. Dostupný z WWW: http://www.itapa.sk/index.php?ID=4925

[6] E-governmentAct - zákon o e-governmentu [online]. Dostupný z WWW: http://www.egovernment.cz/best/PDF%2007/EgovAct.pdf.

[7] eGon jako symbol eGovernmentu - moderního, přátelského a efektivního úřadu [online]. Dostupný z WWW: http://www.mvcr.cz/clanek/egon-jako-symbol-egovernmentu-moderniho-pratelskeho-a-efektivniho-uradu-252052.aspx?q=Y2hudW09NA%3d%3d.

[8] Zákon o základních registrech [online]. Dostupný z WWW: http://www.mvcr.cz/clanek/zakon-o-zakladnich-registrech-prosel-tretim-ctenim.aspx.

[9] Efektivní veřejná správa [online]. Dostupný z WWW: http://vladaprovas.vlada.cz/sprava.html.

[10] Co je Czech POINT [online]. Dostupný z WWW: http://www.businessinfo.cz/cz/clanek/registry-databaze/co-je-czech-point/1000430/47112.

[11] Úřední deska [online]. Dostupný z WWW: http://www.softhouse.cz/default.aspx?Obsah=UredniDeska.

[12] Veřejná správa online [online]. Dostupný z WWW: http://www.obce.cz.

[13] Nařízení vlády č. 495/2004 Sb, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů [online]. Dostupný z WWW: http://www.mvcr.cz/clanek/narizeni-vlady-c-495-2004-sb-kterym-se-provadi-zakon-c-227-2000-sb-o-elektronickem-podpisu-a-o-zmene-nekterych-dalsich-zakonu.aspx.

[14] O datových schránkách [online]. Dostupný z WWW: http://www.datoveschranky.info/o-datovych-schrankach.

[15] CAS++: An Open Source Single Sign-On Solution for Secure e-Services - http://www.springerlink.com/content/j22n0j53nu163228/?p=648750eb711a4512a2ad8981bd2935f9&pi=3.

[16] Adopting Open Source for Mission-Critical Applications: A Case Study on Single Sign-On - http://www.springerlink.com/content/3662765481621467/?p=546252593ed9487bb8a3d1ff4ab8445e&pi=6.

[17] NETREFOVÁ , Hana. *Nové postupy uplatňované při návrhu uživatelsky přívětivých informačních systémů*. [s.l.], 2002. 26 s. Teze dizertační práce.

[18] *Portálová řešení nejen pro agenta 007* [online]. 2008 [cit. 2009-04-22]. Dostupný z WWW: <http://www.systemonline.cz/sprava-dokumentu/portalova-reseni-nejen-pro-agenta-007.htm>.

[19] BRANDEJS, Michal, et al. Univerzitní IS: předsudky, pověry a realita. *RUFIS 2000* [online]. 200 [cit. 2009-04-22]. Dostupný z WWW: <https://is.muni.cz/clanky/2000_rufis.pl>.

[20] NETREFOVÁ, Hana, ŠORM, Milan. Metody personalizace webových informačních systémů. *UNIFOS 2003* [online]. 2003 [cit. 2009-04-22]. Dostupný z WWW: <https://akela.mendelu.cz/~hanac/papers/uninfos03_netref_sorm.pdf>.

[21] *Měli bychom převzít rakouský e-government?* [online]. 2007 [cit. 2009-05-03]. Dostupný z WWW: <http://www.lupa.cz/clanky/vidensky-e-government/>.

[22] *Výstup Klubu SPIS - Scénáře možné realizace eGovernmentu v ČR* [online]. [2000] [cit. 2009-05-06]. Dostupný z WWW: <http://www.spis.cz/index.php?id=1056>.

[23] *Biometrické systémy v praxi* [online]. 2001-2009 [cit. 2009-05-06]. Dostupný z WWW: <http://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm>.

[24] NETREFOVÁ, Hana. Využití portálového řešení při personalizaci webových informačních systémů. *EDAMBA 2004* [online]. 2004 [cit. 2009-05-06]. Dostupný z WWW: <https://akela.mendelu.cz/~hanac/papers/uninfos03_netref_sorm.pdf>.

[25] *CAS 1 Architecture* [online]. 2009 [cit. 2009-05-19]. Dostupný z WWW: <http://www.jasig.org/cas/cas1-architecture>.

[26] SIEBER, Patrik. *Studie proveditelnosti (Feasibility Study) metodická příručka*. [s.l.] : [s.n.], 2004. 43 s. Dostupný z WWW: <http://extranet.kr-vysocina.cz/download/gs/MET_STUD_PROV.pdf>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT	Informační a komunikační technologie
ÚSIS	Úřad pro státní informační systém
ISVS	Informační systémy veřejné správy
SIS	Státní informační systém
KIVS	Komunikační infrastruktura veřejné srpávy
Czech POINT	Český Podací Ověřovací Informační Národní Terminál
SSO	Single Sign On
AAM	Authentication and Authorization Model
FM	Federated Model
FIMM	Full Identity Management Model
CAS	Central Authentication Service
HTTP	Hypertext Transfer Protocol
SOAP	Simple Object Access Protocol
SAML	Security Assertion Markup Language
XML	eXtensible Markup Language
J2EE	Java Enterprise Edition
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
CMS	Content management system
DES	Data Encryption Standard
SHA-1	Secure Hash Algorithm
PIN	Personal identification number
ZBIFO	Základní identifikátor fyzické osoby
JEE	Java Enterprise Edition
HTML	HyperText Markup Language

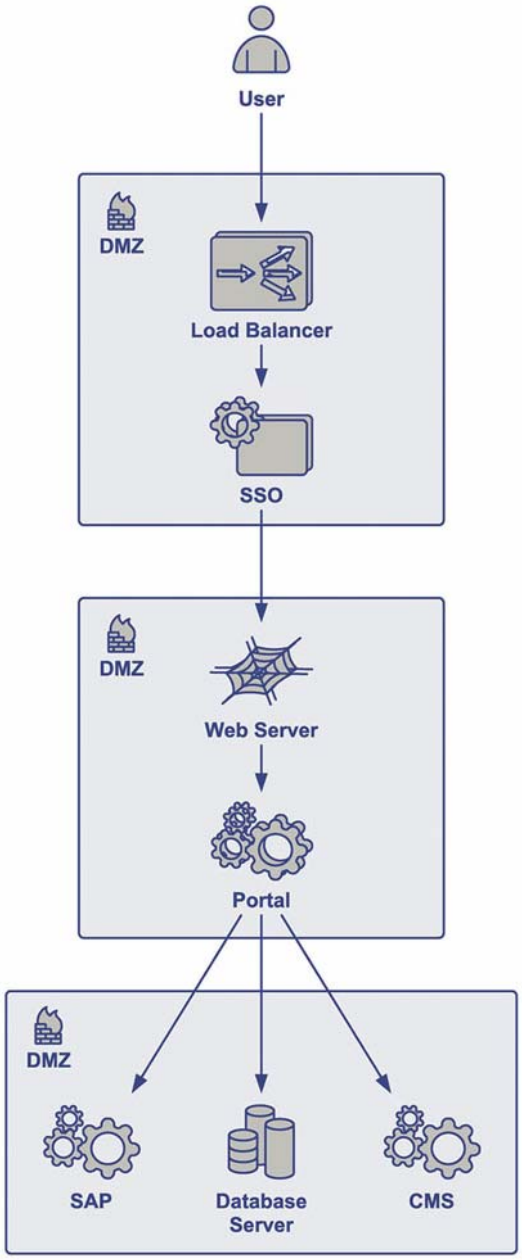
URL	Uniform Resource Locator
API	application programming interface
TGC	Ticket Granting Cookie
PKI	Publik Key Infrastructure
CA	Certifikační autorita
ZBIPO	Základní identifikátor právnické osoby
ST	Service Ticket
ČSÚ	Český statistický úřad

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OBRAZOVÁ DOKUMENTACE



Obr. 13. Schéma využití SSO a portálového přístupu