Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Rozvoj e-Governmentu typu G2G

Bc. Jiří Grünseisen

Česká zemědělská univerzita v Praze

Fakulta provozně ekonomická

Katedra informačních technologií

Akademický rok 2007/2008

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jiří Grůnseisen

obor Veřejná správa a regionální rozvoj - k.s. Hradec

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název tématu: **Rozvoj eGovernmentu typu G2G**

Struktura diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Vývoj a standardy eGovernmentu
4. Bezpečnostní standardy státní správy
5. Bezpečnost dat při komunikaci mezi úřady státní správy a samosprávy
6. Závěr
7. Seznam literatury
8. Přílohy

Rozsah původní zprávy: 50 - 60 stran

Seznam odborné literatury:

1. Dostálek, L. a kolektiv, Velký průvodce protokoly TCP/IP: Bezpečnost, Praha: Computer Press, 2003, ISBN 80-7226-849-X
2. Microsoft Corporation Inc., Windows 2000 Server Resource Kit, Sítě TCP/IP, Praha, Computer Press, 2000, ISBN 80-7226-291-2
3. Microsoft Corporation Inc., Windows 2003 Server Resource Kit, Distribuované systémy, Praha, Computer Press, 2004,
ISBN 80-7226-951-1
4. on-line materiály

Vedoucí diplomové práce: **Ing. Jan Jarolímek, Ph.D.**

Termín odevzdání diplomové práce: duben 2009

L.S.

ČZU Česká zemědělská univerzita v Praze - Provozně ekonomická fakulta

..... Vedoucí katedry

..... Děkan

V Praze dne: 9.1.2008

Evidováno děkanátem PEF pod č.j.: KIT-117-08D

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Rozvoj e-Governmentu typu G2G " jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 10.4.2009 Jiří Grünseisen

Poděkování:

Děkuji svému vedoucímu diplomové práce Ing. Janu Jarolímkovi, Ph.D. za poskytnuté rady, podněty a odborné vedení celé práce. Dále bych chtěl poděkovat Ing. Petru Mikulkovi za cenné připomínky a poskytnuté materiály.

V neposlední řadě chci také poděkovat mým blízkým, kteří se mnou po celou dobu studií měli trpělivost.

Rozvoj e-Governmentu typu G2G

Developement of e-Government type G2G

Souhrn:

Předmětem této diplomové práce je rozbor hlavních pilířů, které výrazným způsobem ovlivňují rozvoj e-Governmentu v České republice a analýza využívání kvalifikovaných certifikátů jako základního prvku bezpečnosti ve státní správě. Teoretické závěry analýzy jsou následně demonstrovány na praktických příkladech elektronické komunikace orgánů státní správy s využitím zaručeného elektronického podpisu a je provedeno srovnání s novými možnostmi komunikace, které má dnes státní správa k dispozici.

Závěr práce obsahuje zhodnocení nových trendů, které jsou spojeny s probíhajícími změnami v legislativě, a které významnou měrou ovlivní způsob a možnosti elektronické komunikace občanů, daňových subjektů či orgánů státní správy.

Summary:

The subject of this diploma theses is the analysis of the main aspects that significantly influence developement of e-Government in the Czech Republic and analysis of the electronic signature usage in the communication with the public service. The theoretical conclusions are demonstrated on practical examples of electronic communication in public service using a qualificated certificate. There is a comparison of the new communication means done; these are on the disposal of the public services.

The conclusion of this diploma theses is to evaluate the new trends that are connected with the legislation changes and will significantly change the way and options of citizens´, tax subjects or body service bodies communication.

Klíčová slova

Egovernment Act, datová schránka, zaručený elektronický podpis, daňová schránka, kvalifikovaný certifikát, sdílené registry, elektronické podání, zabezpečená komunikace, asymetrická kryptografie, kvalifikovaná certifikační autorita, bezvýznamový identifikátor, čipová karta Smart Card

Key words

Egovernment Act, data box, verified electronic signature, tax box, qualified certificate, sharable register, e notice, conditioned communication, asymetric cryptography, qualified certificated authority, unsubstential identifier, Smart Card chip card

Seznam zkratek

CA – Certifikační autorita

ČDS – Česká daňová správa

e-OP – Elektronický občanský průkaz

EP – Elektronický podpis

EPO – Elektronické podání

GIS – Geografický informační systém

ICT - Information and Communication Technologies

IČO – Identifikační číslo organizace

ISDS – Informační systém datových schránek

ISOH - Informační systém odpadového hospodářství

ISVS – Informační systém veřejné správy

KIVS – Komunikační infrastruktura veřejné správy

MF – Ministerstvo financí

MPSV – Ministerstvo práce a sociálních věcí

NDA – Národní digitální archív

OAIS - Open Archival Information System

OS – Operační systém

OSVČ – Osoba samostatně výdělečně činná

OVM – Orgán veřejné moci

PIN - Personal Identifications Numbers

RČ – Rodné číslo

Rezort - Rezort Ministerstva financí České republiky

ROB – Registr obyvatel

ROS – Registr osob

RPP – Registr práv a povinností

RUIAN – Registr územní identifikace, adres a nemovitostí

RŽP – Rejstřík živnostenského podání

SRSIS - Strategie rozvoje služeb pro informační společnost

SSP – Státní sociální podpora

Obsah

1 Úvod

V dnešní době většina lidí využívá mobilní telefon, hledá informace na internetu, či komunikuje s bankou prostřednictvím počítače. Přesto však, potřebujeme-li něco od úřadů, jako bychom se ocitnuli o několik let zpět. Tento stav neznamená, že by úřady nevyužívaly moderní technologie, bohužel je ale prozatím z větší části využívají pouze pro svůj interní chod a ne pro komunikaci s občany. Potřebu tento stav změnit prezentovala česká vláda tím, že se již před více než deseti lety přihlásila k myšlence budování e-Governmentu. Slibovala si od jeho zavedení efektivnější výkon veřejné správy, přiblížení kvalitnějších veřejných služeb občanům a v konečném důsledku i omezení nárůstu pracovníků ve veřejné správě. Žádná vláda neopomněla potvrdit toto úsilí, pravdou však je, že zatímco v roce 2000 zaměstnávala veřejná správa 175 tisíc osob, v roce 2007 jich už bylo 293 tisíc. Možné vysvětlení tohoto jevu se uvádí v bilančním dokumentu sdružení eStat.cz – „*Nesprávně zvolený způsob implementace informačních a komunikačních technologií do veřejné správy může mít za následek opačný efekt a místo k efektivnější veřejné správě může vést k velice nákladnému chaosu*“ [1]

Dnešní rychlý rozvoj výpočetní techniky, elektronizace většiny odvětví a vysoké požadavky na velké množství informací vyžadují nový přístup ze strany státní správy a samosprávy směrem k občanům a ke komerční sféře. V souvislosti s těmito požadavky je často zmiňováno slovo e-Government. Pod tímto pojmem si lze představit širokou skupinu aktivit, které jsou určeny jak pro občany, tak i pro instituce veřejné správy. Celý systém by měl v důsledku představovat ucelený komplex služeb a zdrojů informací snadno dostupných pro všechny občany s cílem efektivního a levnějšího fungování veřejné správy.

Vlastnímu budování e-Governmentu však musí předcházet důkladná reforma legislativy, která nám umožní stanovit jasný legislativní rámec a transparentní pravidla.

[1] Vladimír Pick, Professional Computing, www.procomputing.cz

Na základě těchto pravidel bude následně možné realizovat takové projekty, které budou pro občany přínosem, budou znamenat zefektivnění a zvýšení výkonu veřejné správy a v neposlední řadě přinesou zmenšení byrokracie.

2 Cíl práce a metodika

Cílem diplomové práce „Rozvoj e-Governmentu typu G2G“ je analyzovat úroveň a možnosti využívání kvalifikovaných certifikátů pro bezpečnou komunikaci a ochranu dat ve státní správě. Dalším cílem práce je shrnout změny v e-Governmentu, které přináší nové formy elektronické komunikace prostřednictvím datových schránek v souvislosti s přijetím zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Diplomová práce se v úvodní části zabývá obecnou definicí veřejné správy a tvorbou základních pilířů e-Governmentu, které v souvislosti s úpravou legislativy umožnily provedení zásadních změn v systému veřejné správy. V této části jsou také zmíněny nejvýznamnější projekty e-Governmentu a možnosti jejich zařazení do systému elektronické veřejné správy s cílem dosáhnout jejího efektivního fungování.

Následující část práce je zaměřena na používání karet Smart Card k autentizaci zaměstnanců do jednotlivých rezortních systémů či k bezpečnému ukládání zaměstnaneckých, případně kvalifikovaných certifikátů pracovníků státní správy. Na základě studia odborné literatury a s využitím praktických zkušeností s nasazováním a využíváním prvků asymetrické kryptografie v rezortu ministerstva financí je provedena analýza využívání kvalifikovaných certifikátů, které jsou uloženy na čipových kartách a mohou být používány jak pro autentizaci uživatelů v Rezortu, tak i pro přidělování oprávnění k přístupu k jednotlivým aplikacím, které jsou využívané státní správou.

Další část diplomové práce je věnována využívání zaručeného elektronického podpisu při komunikaci s orgány veřejné správy. Pomocí příslušných výzkumných metod, jako je studium písemností a zákonů, jsou shrnuty změny, které přineslo schválení nových zákonných ustanovení, které se vztahují k e-Governmentu, a které výrazným způsobem upravují možnosti elektronické komunikace orgánů veřejné správy.

V závěru diplomové práce je poukázáno na hlavní problémy a možnosti řešení, které jsou spojeny jak s využíváním kvalifikovaných certifikátů při elektronické komunikaci

ve veřejné správě, tak i se zaváděním nových trendů a zákonných ustanovení e-Governmentu.

3 Vývoj a standardy e-Governmentu

Elektronická veřejná správa má v prostředí střední a východní Evropy poněkud specifické postavení. Není to jenom záležitost více méně technokratické modernizace veřejné správy a veřejných služeb jako ve většině vyspělých zemí. Na významu jí přidává zkušenost s nefungující správou socialistického typu a snaha dosáhnout co nejdříve standardů běžných v západní Evropě. A právě e-Government je jednou z oblastí, která k tomu může významně přispět, a tato očekávání sdílejí nejen političtí představitelé, ale i občané. V regionu střední a východní Evropy lze proto vysledovat v posledních letech tendence směřující k nasazování výpočetní techniky na všech úrovních správy, automatizaci administrativních úkonů a procesů a zlepšení komunikace mezi státem a občany.

První služba, kterou mohli občané v České republice vyřizovat elektronicky prostřednictvím elektronické pošty, bylo v roce 1999 podávání žádostí o informace podle zákona o svobodném přístupu k informacím[2]. V roce 2000 pak byl implementován do českého právního řádu institut elektronického podpisu, který měl umožnit občanům komunikovat s orgány veřejné moci elektronickou cestou. Bohužel však trvalo další téměř rok a půl, než byl vydán prováděcí právní předpis k tomuto zákonu, jenž tuto funkci elektronického podpisu fakticky umožnil realizovat v praxi. V souvislosti se zavedením institutu elektronického podpisu bylo umožněno novelou správního řádu používat elektronickou komunikaci v řadě správních agend. V té době však řada úřadů na tuto činnost nebyla připravena a ani nebyly provozovány elektronické podatelny, jejichž prostřednictvím by bylo možné činit elektronická podání.

V roce 2000 byla také schválena úprava, která měla umožnit, tehdy nově zřízenému Úřadu pro veřejné informační systémy, koordinaci informačních systémů ve veřejné správě tak, aby spolu tyto systémy mohly vzájemně komunikovat a vyměňovat si data.

[2] Zákon č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

V tomtéž roce byl zřízen Úřad na ochranu osobních údajů, který má kompetenci dohlížet nad zpracováváním osobních údajů.

Další změna nastala k datu 1.1.2003, kdy zanikl Úřad pro veřejné informační systémy a jeho místo zaujalo nově zřízené Ministerstvo informatiky, které se primárně snažilo, aby co největší množství jednotlivých podání bylo možno učinit elektronicky. To, že občan pak často sice elektronicky dokument podepíše, elektronicky podá, ale následně bude muset vložit do aktovky dokumenty a na úřad se s nimi vypravit, aby je osobně doložil, bohužel nebylo předmětem až takového zájmu. Tato snaha byla vedena politickým prohlášením tehdejšího ministra informatiky z října roku 2002, kdy na veletrhu INVEX v Brně deklaroval, že jeho cílem je do roku 2006 zpřístupnit 25% agend veřejné správy online.

Ministerstvo informatiky v té době podcenilo vnitřní správu elektronických dokumentů na úřadech. Docházelo tak stále k situacím, že na úřad dorazila prostřednictvím elektronické podatelny písemnost v elektronické podobě, příslušný úředník ji však přesto vytisknul a vložil do šanonu a spis již poté po úřadě, případně i mezi úřady, putoval v materiální podobě. Toto bohužel nebylo překonáno ani novým zákonem o archivnictví a spisové službě[3], který vypracovalo Ministerstvo vnitra. Tento zákon sice umožňoval vést spisovou službu elektronicky, bohužel však stále preferoval vedení spisové služby v podobě materiální než v podobě elektronické. Úřady tak nadále setrvávaly u vedení spisů v listinné podobě a místo elektronických dokumentů, tak stále obíhaly po úřadech lidé s dokumenty.

Dalším problémem, který částečně přetrvává do dnešní doby, je sdílení dat mezi jednotlivými státem vedenými registry. Nebyla explicitně stanovena elektronická forma vedení příslušného registru a navíc údaje v registrech, které byly vedeny v elektronické formě, nebyly považovány za právně závazné. Příliš roztříštěná byla také místa provádějící registraci, zaevidování nebo zápisy do evidencí. Tato místa často vzájemně nekomunikovala (někdy ani v rámci jednoho informačního systému), často také chyběla

[3] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů

podpora těchto míst kvalitní výpočetní technikou. Ministerstvo informatiky dokonce během prvního roku své existence pozastavilo práce na zajištění sdílení dat mezi jednotlivými registry a věnovalo se hlavně vytvoření portálu veřejné správy, který se v té době stal jeho vlajkovou lodí.

Vedle výše uvedené činnosti Ministerstvo informatiky připravilo a prosadilo několik novel právních předpisů, jako byla novela zákona o elektronickém podpisu[4], která uložila povinnost všem úřadům provozovat elektronické podatelny a zavedla institut elektronické značky, či novelu zákona o informačních systémech veřejné správy.

Rozvoj e-Governmentu v letech 2004 až 2006 byl iniciován spíše nabídkovou stranou[5] a předpokládalo se, že při dostatečně velké nabídce se bude stimulovat také poptávka a dojde k určitému stavu „dynamické rovnováhy".

K datu 1.1.2007 zaniklo Ministerstvo informatiky jako ústřední orgán státní správy a jeho kompetence byly rozděleny následovně:

- Ministerstvo vnitra se stalo ústředním orgánem státní správy pro eGovernment, mimo to je také zřizovatelem České pošty a provozuje portál veřejné správy.
- Ministerstvo průmyslu a obchodu se stalo ústředním orgánem státní správy pro elektronické komunikace a získalo dohled nad poštovním trhem a digitalizací, s výjimkou věcí svěřených do působnosti Českého telekomunikačního úřadu.
- Veřejné dražby přešly pod Ministerstvo pro místní rozvoj.

---

[4] Zákon č.486/2004 Sb. (227/2000 Sb.), Úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn.

[5] Nabídka služeb e-Governmentu je měřena jako on-line dostupnost 20 základních veřejných služeb na různých úrovních (např. služby pro nezaměstnané, dostupnost dokumentů pro vyřízení žádosti o sociální dávky, možnost registrace osobního automobilu, vyřízení stavebního povolení, služby veřejných knihoven apod.).

Dále vznikla Rada vlády pro informační společnost jako poradní orgán vlády, která navrhuje vládě, jak koordinovat rozvoj e-Governmentu a definuje a formuluje strategie, cíle a politiky vlády v oblasti informační společnosti.

Dne 11.7.2007 schválila vláda strategii „Efektivní veřejná správa a přátelské veřejné služby Smart Administration[6]. Součástí tohoto dokumentu je i Strategie rozvoje služeb pro informační společnost (SRSIS), která zastřešuje veškeré aktivity vlády v oblasti rozvoje e-Governmentu. Specifické cíle této strategie jsou zpracovány ze dvou úhlů pohledu – z pohledu občana a z pohledu infrastruktury.

Z pohledu občana:

- Umožnění komfortní, bezpečné a důvěryhodné elektronické komunikace s veřejnou správou na všech úrovních a v maximu životních situací

Z pohledu infrastruktury:

- Konsolidovaná datová základna, využitelná pro konstrukci informačního obsahu a aplikací
- Ucelený balík zákonů jako právní základ a opora e-Governmentu
- Robustní, bezpečná a efektivní infrastruktura, schopna zprostředkovat přístup k datovým zdrojům s potenciálem dalšího rozvoje
- Sada klíčových aplikací, usnadňující řešení běžných životních situací, podnikání a komunikaci se státní administrativou (s přesahem do komerční sféry)
- Snížení administrativních nákladů spojených s chodem veřejné správy v souvislosti se zaváděním e-Governmentu o 20% do roku 2013

Základní milníky strategie:

1) V roce 2009 budou zprovozněny datové schránky, bude existovat rozvinutá síť univerzálních kontaktních míst veřejné správy, kde bude možno získat ověřené výpisy z vybraných rejstříků

[6] Strategie realizace Smart Administration v období 2007 – 2013, schválená usnesením vlády č. 757/2007

2) V roce 2010 budou zprovozněny centrální registry, v rámci existující sítě kontaktních míst veřejné správy bude možno učinit veškerá podání vůči veřejné správě
3) V roce 2010 bude ukončen legislativní proces všech norem souvisejících s realizací cílů Strategie
4) V roce 2012 budou funkční aplikace pro oblast zdravotnictví, sociální péče, správního, soudního a daňového řízení, bude funkční infrastruktura pro dlouhodobé ukládání a archivaci elektronických dokumentů
5) V roce 2015 bude dokončen proces elektronizace datové základny, včetně elektronizace geografických informací

Strategie SRSIS je prováděna prostřednictvím jednotlivých projektů, které jsou realizovány v úzké spolupráci se všemi angažovanými aktéry, především ústředními správními úřady a zástupci místních samosprávných orgánů. Očekává se, že stále více agend veřejné správy bude přístupných on-line způsobem a občané budou moci těchto služeb využívat pro vyřizování svých úředních záležitostí z pohodlí svého domova a navíc 24 hodin denně bez poplatků a vyplňování listinných formulářů. Rozvoj informačních systémů veřejné správy umožní díky využití moderních komunikačních technologií lepší spolupráci orgánů veřejné správy, usnadní občanům a podnikatelům kontakt se státem a učiní tak veřejnou správu průhlednější a efektivnější.

3.1 Základní pilíře rozvoje e-Governmentu

Mezi nejdůležitější prvky dalšího rozvoje e-Governmentu z pohledu legislativy v současné době patří následující kroky:

Zákon o elektronizaci některých procesních úkonů – často nazývaný EGA či Egovernment Act. Jde o jeden z hlavních zákonů umožňujících vykonávání moderní veřejné správy, který staví na roveň dokumenty v papírové i elektronické podobě, umožňuje jejich oboustrannou konverzi a definuje standardy elektronické komunikace občana se státem a naopak. Zákon mimo jiné počítá se zavedením tzv. datových

schránek, na nichž bude postaven elektronický způsob doručování dokumentů mezi právnickými a fyzickými osobami, ale i občanem na straně jedné a státem na straně druhé. Datová schránka by tak měla existovat pouze jedna, ať už bude subjekt komunikovat s jakýmkoliv úřadem státní správy. Tento zákon Poslanecká sněmovna ve třetím čtení již schválila a nabude účinnosti *1. července 2009*.

Zákon o registrech veřejné správy[7] – umožňuje vytvoření specifikovaných centrálních registrů veřejné správy, mezi něž patří registr obyvatel, registr osob, registr územní identifikace adres a nemovitostí a registr práv a povinností. Základem využívání a průběžné aktualizace základních centrálních registrů bude možnost bezpečného sdílení dat příslušnými orgány veřejné správy pro potřeby informačních systémů a zároveň umožní veřejnosti oprávněný přístup k informacím, a to z jednoho místa a například i dálkovým přístupem. Právě dotažení registrů je nezbytným předpokladem naplnění základního cíle e-Governmentu a stavu, kdy se namísto žadatele (občana) bude mezi jednotlivými úřady přesouvat pouze soubor potřebných informací. Úspěšné naplnění základních registrů bude mít i značný dopad na efektivitu výkonu veřejné správy a úsporu prostředků za administrativu – jednou pořízené a zapsané informace již nebude třeba získávat, zapisovat a ani vyžadovat znovu, neboť již budou součástí systému. Zákon o základních registrech byl schválen Senátem Parlamentu ČR dne 26. března 2009

Výhody a obrovské možnosti práce se společně sdílenou databází jako jediného datového skladu informací můžeme dokumentovat například u projektu, který je nazván SIS – Schengenský informační systém. V Evropě je SIS největší sdílenou databází věnovanou udržování veřejné bezpečnosti a zajišťování ochrany vnějších hranic. Zúčastněné státy poskytují záznamy o hledaných nebo pohřešovaných osobách, ztraceném a odcizeném majetku a zákazech vstupu. Je okamžitě dostupný všem

[7] 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. (dne 13.2.2009 jej ve třetím čtení schválila Poslanecká sněmovna Parlamentu ČR)

řadovým policistům a jiným oprávněným úředníkům, kteří tuto informaci potřebují k plnění svých úkolů. Pokrývá většinu zemí Evropské unie společně s Norskem a Islandem.

Strategie rozvoje informační společnosti v ČR pro období 2008-2013 – tento strategický dokument současného rozvoje e-Governmentu se zcela jistě stane podkladovým materiálem pro přípravu dalších zákonů. Ne náhodou se definované období kryje s novým programovacím obdobím fondů EU, které jsou jedněmi ze zdrojů, odkud by právě na modernizaci veřejné správy v ČR mohlo přitéci nemálo finančních prostředků.

Komunikační infrastruktura veřejné správy – v oblasti komunikační infrastruktury veřejné správy došlo v poslední době k řadě výrazných změn a v současné koncepci MV ČR hraje KIVS mimořádně důležitou roli. Centralizovaná komunikační infrastruktura ve spolupráci s nově definovaným „centrálním místem služeb“ je jediným místem výměny dat mezi jednotlivými informačními systémy veřejné správy a zároveň jediným místem propojení k veřejné internetové síti i ke specifickým neveřejným sítím.

Dle vyjádření Evropského statistického úřadu si v některých bodech vedeme při budování e-státu až překvapivě dobře. Například z porovnání podílu využívání internetu ve vztahu k veřejné správě z pohledu firemní sféry jsme dokonce třináct procent nad průměrem Evropské unie. Tady se zcela určitě projevují některé často využívané rutiny, jako například využívání Obchodního rejstříku ČR na internetu nebo naprosto běžná elektronická komunikace firemní sféry s Českou správou sociálního zabezpečení či úřady práce.

Portál veřejné správy[8] – v současné době je hlavním zdrojem pro výměnu informací mezi veřejnou správou a občany, respektive mezi podnikatelskou a firemní sférou a obráceně. Rozsahem poskytovaných služeb tvoří jeden z hlavních pilířů

[8] Portál veřejné správy, ***http://portal.gov.cz***

e-Governmentu v ČR a je místem, kde občané vyhledávají informace o veřejné správě a firmy a podnikatelé zasílají informace.

Portál veřejné správy významným způsobem přispívá k potřebě kvalitních služeb při poskytování důvěryhodných a garantovaných informací širokému spektru občanů ČR, včetně poskytování relevantních informací cizincům, a zjednodušení komunikace s úřady. Jeho cílem je stát se místem, které bude „integrovat a zpřístupňovat všechny zveřejňované a veřejně přístupné informace veřejné správy“. Mimo jiné například zpřístupňuje připravované návrhy legislativních dokumentů, včetně možnosti sledovat celý proces vývoje daného legislativního materiálu. Obrovskou výhodou je, že veškeré zde uvedené informace jsou přístupné dálkově, prostřednictvím internetu, přičemž je důležité, že všechna data uvedená na portálu jsou pravidelně aktualizována subjekty veřejné správy a tím je garantována integrita a aktuálnost zobrazovaných informací. Bohužel, stále se nejedná o sdílení základních dat či registrů z jednoho centrálního datového skladu a kvalita zobrazovaných informací je závislá na pečlivém vedení a zpracování údajů mnoha subjektů státní správy.

V roce 2007 jej využily více než tři milióny návštěvníků a díky více než 750 tisícům uskutečněných podání, se ušetřilo několik miliónů papírových formulářů a tisíce hodin času potřebného pro administrativu. Využívání Portálu veřejné správy neustále roste a dá se předpokládat, že i v dalších letech bude jeho role v rámci e-Governmentu v ČR velice důležitá.

3.2 Nové projekty e-Governmentu

3.2.1 Projekt Czech Point

Projekt CZECH POINT vznikl jako reakce na obtížnou situaci při komunikaci občanů s úřady veřejné správy a umožňuje jim tímto získávat veškeré potřebné dokumenty pouze na jediném místě: nejbližším krajském, městském či obecním úřadě. Projekt CZECH POINT je svým názvem slovní hříčkou vycházející z anglického CHECK POINT, tedy jakéhosi kontrolního stanoviště. Ve skutečnosti se však jedná o zkratku - Český Podací Ověřovací Informační Národní Terminál a označuje jednotné

kontaktní místo, na kterém může občan získat údaje, opisy a výpisy, které jsou vedeny v centrálních veřejných evidencích a registrech. Z Czech Pointu tak může dotazovaná osoba získat aktuální informace o průběhu řízení ve věcech, které k jeho osobě vede stát, může učinit podání k úřadu státní správy, případně má možnost ověřit elektronickou podobu dokumentů, listin a podpisů.

Ostrý provoz projektu Czech Point byl zahájen od 1.10.2007 a v současné době umožňuje asistovaný přístup občanů k veřejné správě v následujících agendách:

- Výpis z Katastru nemovitostí
- Výpis z Obchodního rejstříku
- Výpis ze Živnostenského rejstříku
- Výpis z Rejstříku trestů
- Přijetí podání podle živnostenského zákona (§ 72 [9])
- Žádost o výpis nebo opis z Rejstříku trestů podle zákona č. 124/2008 Sb.
- Výpis z bodového hodnocení řidiče[10]
- Vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů
- Podání do registru účastníků provozu modulu autovraků ISOH

Je třeba si uvědomit, že projekt Czech Point neznamená konec příslušných úřadů, např. Katastrálních úřadů; ty budou nadále spravovat data a zapisovat do registru. Pouze už nebudou vydávat výpisy a ušetřené prostředky se mohou vložit například do digitalizace všech spravovaných dat.

3.2.2 Projekt základních registrů dat

Na konci roku 2004 vláda schválila dva klíčové dokumenty, které zahájily rozsáhlé práce na vybudování registrů veřejné správy a zavedení systému sdílení dat ve veřejné

[9] Zákon č. 455/1991 Sb., o živnostenském podnikání

[10] Zákon č. 480/2008 Sb., kterým se mění zákon č. 274/2008 Sb.

správě: věcný záměr zákona o sdílení dat a návrh dalšího postupu budování registrů veřejné správy. Tato myšlenka vychází z konsensu přijatého již ve strategickém dokumentu Státní informační politika – cesta k informační společnosti a následně byla rozpracována v dokumentu „Koncepce budovaní informačních systémů veřejné správy“ a potvrzena dokumentem „Státní informační a komunikační politika, e-Česko 2006“. Vláda se zde zavázala připravit zákon o výměně dat ve veřejné správě a rozšířit využitelnost informačních systémů veřejné správy tím, že budou propojeny subsystémy a registry veřejné správy využitelné i pro potřebu veřejnosti s cílem dosáhnout nejen úspor, ale zejména zrychlit správní procesy, odstranit duplicity a zúžit státní aparát.

Proto po přijetí zákona o elektronických úkonech a autorizované konverzi dokumentů, neboli Egovernment Act, za účinnosti zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění všech novel (ISVS), bude tvořit další pilíř budovaného e-Governmentu skupina zákonů, týkajících se tzv. *základních registrů veřejné správy*.

Jedním z cílů věcného záměru tohoto programu je vytvoření spolehlivé datové základny klíčových údajů užívaných v ISVS tak, aby orgány veřejné moci (OVM) měly k dispozici správné údaje a veřejnost nebyla při jednání s OVM obtěžována opakovaným dokládáním stejných skutečností. K tomu je potřeba vytvořit legislativní předpoklady. Chystá se sada pěti zákonů o registrech veřejné správy, na něž budou navazovat prováděcí vyhlášky. Mají být zavedeny čtyři základní registry veřejné správy: registr obyvatel (ROB), registr osob (ROS), registr územní identifikace, adres a nemovitostí (RUIAN) a registr práv a povinností (RPP).

Nutnost zavedení základních registrů je dána skutečností, že v současné době není možné se spolehnout na aktuálnost údajů, které jsou v jednotlivých databázích obsaženy a není možné různé databáze navzájem bezpečně sdílet. To vede k situaci, kdy veřejnost, občané a firmy jsou opakovaně nuceni dodávat veřejné správě údaje, které jí již mnohokráte poskytli, případně veřejná správa pracuje s chybnými podklady. Orgány veřejné moci si tak verifikují data ve svých „lokálních“ informačních systémech nebo kompenzují handicap, že si nemohou samy dálkovým přístupem jednoduše získat či ověřit potřebné údaje. Tento stav je nutné řešit, to znamená vytvořit odpovídající legislativu zakládající a podporující základní registry veřejné správy. Paralelně s tím

probíhají analýzy současných registrů, vyhodnocují se postupy přebírání a slučování dat do „nových“ registrů, zkoumají se a plánují postupy verifikace a čištění dat, které budou převedeny do základních registrů veřejné správy.

Jaké jsou tedy základní cíle základních registrů veřejné správy?

a) Zavedení základních registrů VS by mělo zejména umožnit efektivní, mnohonásobné využívání již jednou pořízených dat, přispět ke zrychlení správních procesů, ke zjednodušení správy a údržby stávajících evidencí orgánů veřejné správy. To by mělo v konečném důsledku přinést úsporu prostředků státního rozpočtu.
b) Základní údaje pro ISVS budou vedeny v určeném základním registru, tj. na jednom místě, kde budou též pružně a bezpečně aktualizovány. Budou pro ostatní ISVS údaji referenčními. Referenčním údajem rozumíme jedinečný a důvěryhodný údaj, který bude veden v jednom ze základních registrů. Tento základní registr bude následně určen ke sdílení v příslušných ISVS podle jednoznačně vymezených pravidel, jejichž dodržování též zajistí potřebnou úroveň zabezpečení dat.
c) Referenční údaje budou považovány za důvěryhodné a úřady již nebudou muset jejich správnost a platnost ověřovat. Každý referenční údaj bude mít zákonem stanovené editory, kteří budou odpovědní za nápravu zjištěných nepřesností v údajích.
d) Úředník veřejné správy bude mít zajištěn přístup jenom k těm osobním údajům občana či firmy, které budou potřebné pro výkon jeho vlastní agendy.
e) Základní registry veřejné správy budou spolupracovat i mezi sebou jako ucelený integrovaný systém. Je nutno mít na paměti, že převody, čistění a verifikace dat převáděných ze stávajících registrů a evidencí, budou náročné na pečlivou práci i na finance.

Navrhovaný zákon o základních registrech prochází procesem schvalování v Parlamentu České republiky. Dne 20. 1. 2009 Výbor pro veřejnou správu a regionální rozvoj Parlamentu České republiky doporučil Parlamentu České republiky, aby

původně, Ministerstvem vnitra navrhovaných pět samostatných zákonů o základních registrech bylo schváleno v podobě jednoho komplexního zákona. Zákon o základních registrech by měl nabýt účinnosti k 1. červenci 2010. Registry, ve své konečné podobě a funkcionalitách, vytvoří jednotný, vzájemně provázaný a ucelený systém, který umožní sdílet data v dané oblasti z jediného datového zdroje. Návrh zákona právně zakotvuje čtyři základní registry (registr obyvatel, osob, územní identifikace a registr práv a povinností), jejichž přínosem bude i skutečnost, že údaje v nich obsažené a označené jako referenční údaje budou považovány za důvěryhodné (neprokáže-li se opak) a úřady již nebudou muset jejich platnost a správnost ověřovat, případně jejich doložení požadovat po dotčených subjektech.

Registr obyvatel (ROB) – bude obsahovat základní identifikační a lokační údaje o všech státních občanech ČR, cizincích s povolením pobytu v ČR a občanech jiných států vedených v základních registrech, tedy asi v obdobném rozsahu, jako je dnes Informační systém evidence obyvatel podle zákona o evidenci obyvatel.
Registr osob (ROS) – bude obsahovat identifikační a další základní údaje o všech podnikajících fyzických osobách, právnických osobách, organizačních složkách státu a organizačních složkách zahraničních právnických osob, tedy o všech ekonomických jednotkách s právní subjektivitou; jde tedy o subjekty, které mají přiděleno IČO - o obdobu dnešního Registru ekonomických subjektů (RES) vedeného podle zákona o státní statistické službě Českým statistickým úřadem (do RES dnes přichází data z Registru živnostenského podnikání a dalších evidencí).
Registr územní identifikace, adres a nemovitostí (RÚIAN) – registr by měl obsahovat základní identifikační a lokalizační údaje k územním prvkům, údaje o objektech v území a jejich vzájemné časové a územní vazby. V rámci tohoto registru by měly být sjednoceny adresní části z následujících, dnes existujících registrů:

- Informační systém katastru nemovitostí
- Informační systém evidence obyvatel (údaje o adrese)
- Registr sčítacích obvodů
- Územně identifikační registr základních sídelních jednotek
- Územně identifikační registr adres.

Registr práv a povinností (RPP) – zde by měly být uchovávány informace o právech a povinnostech veřejnosti a orgánech veřejné moci, tedy o právech a povinnostech obyvatel i osob. Tyto informace musí splňovat obecně platné právní předpisy, podzákonné normy, samosprávní rozhodnutí a rozhodnutí orgánů veřejné moci, která zakládají určitá práva a povinnosti. Gestorem je pověřeno Ministerstvo vnitra České republiky, spolupracující jsou potom všechny ústřední správní úřady i orgány samosprávy.

3.2.3 Projekt Národní digitální archiv[11]

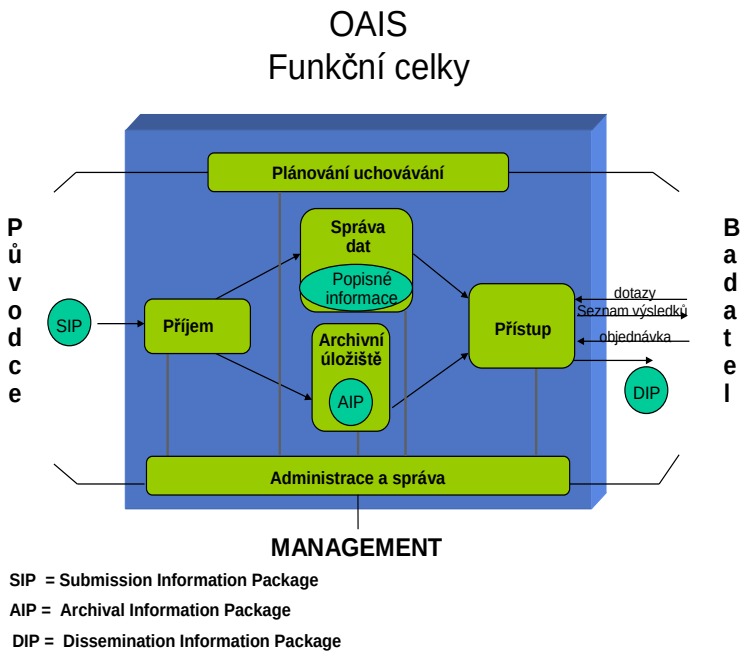
Nutnou podmínkou rozvoje e-Governmentu je zajištění dlouhodobého uchovávání dokumentů v digitální podobě. Proto vláda ČR uložila svým usnesením č. 11 ze dne 7.1.2004 místopředsedovi vlády a ministru vnitra zpracovat ve spolupráci s ministrem informatiky tuto problematiku a vytvořit digitální archiv k 31.12.2011.

Problematiku digitálního archivu řeší na základě příslušného ustanovení zákona č. 499/2004 Sb., o archivnictví a spisové službě, Národní archiv. Vypsal proto veřejnou soutěž na projekt (zadávací dokumentace viz http://www.nacr.cz), ve které zvítězila díky nejlepší nabídce firma ICZ, a.s. Tato firma tedy zpracovala Technologický projekt, na jehož základě by mělo dojít k zadání vybudování pracovišť digitálního archivu jako součásti Národního archivu, zkráceně Národního digitálního archivu (NDA). Jeho primární funkcí bude ukládat odborně vybrané dokumenty (archiválie) a zajistit jejich dlouhodobé uložení (nad 50 let), jejich čitelnost a přístupnost při zachování integrity a nezbytné míry autenticity. Sekundární funkce jsou vyjádřeny součástí NDA zvanou „chráněné úložiště“, které umožní přípravu digitálních dokumentů před výběrem, zpřístupněním digitalizovaných archiválií (originály existují v čitelné analogové podobě), uložením, případně skartačním řízením.

Návrh řešení, předkládaný v projektu, vychází ze standardu OAIS (ISO 14721:2003 - Open Archival Information System). Tento standard vymezuje základní koncepci archivu pro uložení elektronických dokumentů a je na něm budována většina digitálních

[11] Národní archív, ***http://www.nacr.cz***

archivů. Standard definuje hlavní funkce, které má archiv zajišťovat. Jedná se o příjem, správu dat, archivní uložení, přístup, administraci a plánování uchovávání. Základní model OAIS je na následujícím obrázku.



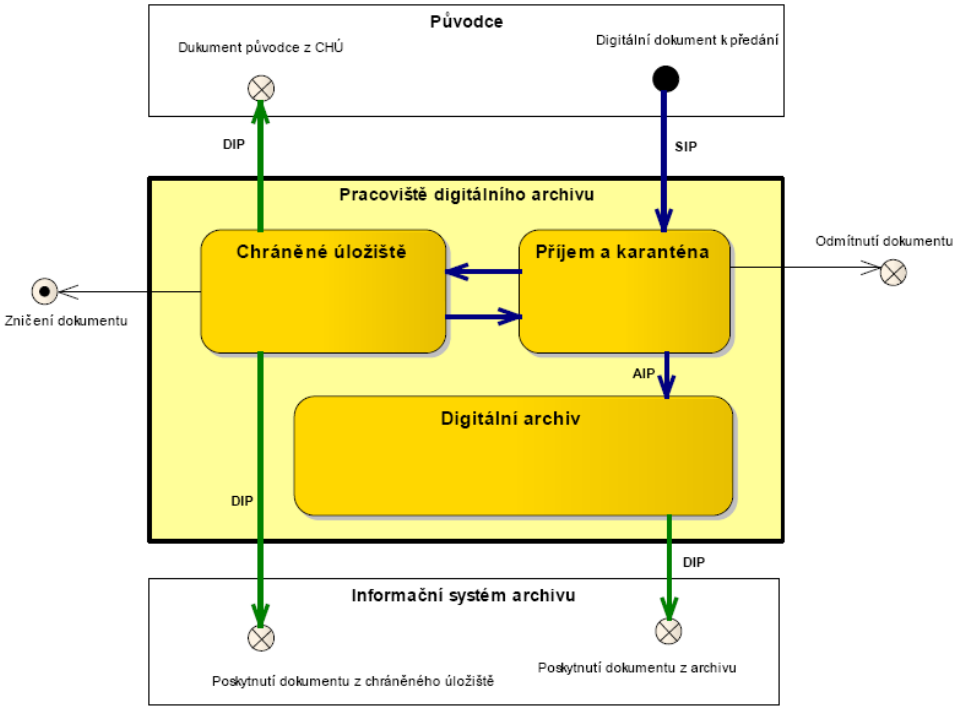
Obrázek 1 - Základní model OAIS

Podle standardu OAIS je elektronický dokument a všechny informace (metadata) zabaleny do balíčku s jednotnou strukturou. Tyto balíčky jsou nazývány SIP – Submission Information Package (balíčky přijímané od původců), AIP - Archival Information Package (archivní balíčky) zahrnující ukládaný obsah a jeho příslušné popisné informace pro uchovávání (archivní a technické informace) a DIP - Dissemination Information Package (balíčky vytvořené na základě badatelského dotazu, pro využívání).

Digitální dokument je nejprve připraven u původce do vhodné podoby pro předání do archivu. Balíček SIP může být např. exportován ze systémů Elektronické spisové služby nebo prostřednictvím rozhraní ze specializovaných informačních systémů. Stanovení struktury SIP proto *musí být ošetřeno legislativně*: jde o základní předpoklad

pro přejímání dat do NDA. Vzhledem k finanční a odborné náročnosti bude vybudován jeden digitální archiv uchovávající digitální dokumenty v péči všech veřejných archivů. Půjde tedy v podstatě o servis ostatním archivům v oblasti dlouhodobého uchovávání digitálních dokumentů. Posouzení v rámci skartačních řízení či mimo skartační řízení, archivní zpracování a zpřístupňování uložených digitálních dokumentů zůstane v kompetenci příslušných archivů. Vyhne se tím duplicitním činnostem v situacích, kdy by u jednoho původce prováděli výběr dva archiváři z různých archivů.

Základní navržené schéma digitálního archivu je následující:



Obrázek 2 - Schéma digitálního archívu

Proti ztrátě bude dokument zajištěn uložením na dvou geograficky oddělených místech a dvou typech médií s rozdílným fyzikálním principem. Předpokládá se, že hlavní úložiště bude nově vybudováno v Praze v sousedství Národního archivu a pro záložní úložiště bude využit stávající objekt. Obě úložiště budou od sebe vzdálena nejméně 50 km. Ukládací média digitálního archivu reprezentují disková pole

(magnetický princip) a UDO disky (optický princip). Ukládacím médiem chráněného úložiště bude diskové pole zálohované na pásky.

Čitelnost dokumentu bude zajišťována metodou migrace. Touto metodou nelze v současné době řešit dlouhodobé uchování veškerých digitálních dokumentů. To ostatně nedokáže zajistit žádná metoda. Migrace se v současnosti jeví jako velmi efektivní způsob zachování čitelnosti většiny digitálních dokumentů. Prostřednictvím relativně levných migračních nástrojů je možno zajistit převod mnoha formátů primárních dokumentů do menšího množství formátů pro dlouhodobé uchovávání. Uchovávání bude nejprve vyzkoušeno na „jednodušších" typech dokumentů (rastrová grafika, texty) a poté se budou řešit složitější dokumenty (GIS).

Často skloňovaným problémem digitální archivace je autenticita. V současné době jde o nevyřešený problém a z tohoto důvodu NDA předpokládá, že po určitou dobu budou do archivu přicházet v nutných případech souběžně klasické i digitální archiválie a autenticitu elektronických dokumentů bude možno ověřit proti klasickým dokumentům.

Autenticitu chápeme jako prokázání, že dokument je tím, čím má být, že nebyl v průběhu uložení v archivu změněn a že procesem migrace nedošlo ke ztrátě žádné podstatné informace.

Zvoleným principem zachování autenticity v NDA je fyzické a procesní zajištění uložených dokumentů oproti změně a transparentní, dokumentovaný způsob migrace. To vyžaduje certifikaci NDA jako důvěryhodného úložiště. Projekt předpokládá certifikaci archivu třetí stranou, že splňuje požadavky takového úložiště a to jak po stránce fyzické bezpečnosti, tak po stránce procesní včetně zajištění dostatečných finančních prostředků pro jeho dlouhodobou činnost. Certifikace proběhne podle aktuálních standardů či předpisů. Jednou z navržených možností je posouzení archivu Národním bezpečnostním úřadem.

Archiv bude považovat dokumenty předané původcem za autentické a zachová informace, jakými prostředky a s jakým výsledkem byla certifikace ověřena. Například

u dokumentu podepsaného zaručeným elektronickým podpisem bude zachována informace, kdo dokument podepsal, že byl podpis ověřen a s jakým výsledkem. Dokument pak bude uložen v archivu spolu s těmito informacemi, ale v podstatě nepodepsaný. Autenticita dokumentu po uložení v archivu bude zajištěna vnitřními prostředky archivu.

Projekt počítá s použitím elektronického podpisu na úrovni NDA pouze pro kontrolu integrity dat při přenosu od původce ke zpracování. To znamená, že platný zaručený elektronický podpis (či elektronická značka) autora dokumentu (i s časovým razítkem odeslání) má svůj význam v prvotních fázích životního cyklu digitálního dokumentu, kdy po určitou dobu potvrzuje autenticitu digitálního dokumentu. Používá se maximálně do úrovně původce. Je na původci, aby ověřil primární autentizační údaje o dokumentu a výsledek ověření uvedl do popisných metadat. Součástí metadat informačního balíčku je sekce pro vložení údajů o ověření elektronického podpisu.

Projekt NDA jsem považoval za nutné zařadit do kapitoly o vývoji e-Governmentu, protože řešení problému digitální archivace je úzce spojeno s rozvojem a zabezpečením elektronické komunikace s veřejnou správou.

3.2.4 Elektronická identifikace občana[12]

Prostředky informační a komunikační technologie v dnešní době nabízí snadný přístup k informacím, snadnou komunikaci s úřady a institucemi a mnohdy není ani nutná osobní návštěva občana na úřadu při vyřízení administrativního úkonu. Jedinec se při takové komunikaci nemusí druhé straně prezentovat osobně, ale musí svoji fyzickou přítomnost nahradit takovou informací, které jej spolehlivě a pokud možno přesně identifikuje. Takovým jednotným nástrojem bude elektronický občanský průkaz ve formě identifikační karty, který je doporučován Evropskou unií v souvislosti s možným zaváděním elektronických identifikačních dokladů tzv. „Elektronické karty občana“.

Tento elektronický občanský průkaz bude mít charakter jedinečného a univerzálního prostředku, jehož užitím jak ze strany občana, tak ze strany orgánů veřejné správy bude

[12] www.estat.cz

možné realizovat přístup do základních registrů veřejné správy a dalších informačních systémů veřejné správy. Elektronický občanský průkaz (e-OP) by měl sloužit k jednoznačnému určení totožnosti občana, navíc v rámci zemí Evropské unie by měl být využíván jako cestovní doklad. Průkaz by neměl obsahovat rodné číslo, ale zabezpečený čárový kód a číslo daného občana. Problematika jednotné identifikace občanů je poměrně rozsáhlá hlavně proto, že pro identifikaci občanů se využívá více číselných řad a proces sjednocení bude finančně a hlavně organizačně velice náročný. Úprava a vydávání elektronických občanských průkazů bude tak reálná nejdříve se zavedením sdílených registrů státní správy v roce 2010.

3.2.4.1 Identifikátor s vnitřní informací

Z hlediska ochrany osobních údajů a ochrany soukromí občanů je vytvoření dalšího, konstrukčně jednoduchého, zapamatovatelného a tedy i snadno zneužitelného identifikátoru, který bude takto široce využíván, velkým rizikem. Dostatečným varováním může být dnešní situace v používání a nadužívání rodného čísla. Moderní aplikace e-Governmentu by měly fungovat nezávisle na struktuře identifikátoru občana.

Na druhé straně rozhodnutí o novém způsobu identifikace jedince je spojeno s mnoha problémy. Bude nutno zvážit důsledky finanční, technické, organizační, ale také různé přístupy a reakce osob. Mnoho občanů si své rodné číslo pamatuje, k čemuž vnitřní informace o datu narození pomáhá. Bude nutno zvážit, jak se nový identifikátor začlení do elektronických komunikací s občany. V neposlední řadě je nutno posoudit vývojové trendy technických prostředků tak, aby nový identifikátor vyhovoval novým typům komunikace příštích generací.

Používání rodného čísla k identifikaci občana v ČR se pomalu dostává ke svému zenitu. Narůstající námitky a nespokojenost občanů s vnitřní informací uložené v RČ (datum narození, pohlaví), blížící se vyčerpání použitelné číselné řady, ale také určitá míra nepřesností či duplicit v databázích státních orgánů, vysoká míra zneužitelnosti identifikátoru, značná nedůvěra v dostatečné zabezpečení, obavy, aby se identifikátor nestal snadným propojovacím klíčem pro sdílení osobních informací mezi různými informačními systémy, to vše jsou argumenty, které nutí k zamyšlení nad novými možnostmi identifikace občana.

S právními předpisy pro zavádění e-Governmentu v České republice je spojen závažný problém tvorby a zavedení nového univerzálního identifikátoru pro každou fyzickou a právnickou osobu, které je v návrzích těchto předpisů nazýváno „osobní číslo“. Toto číslo má být konstrukčně shodné s identifikátorem fyzické osoby, který je využíván Ministerstvem práce a sociálních věcí, je součástí certifikátů elektronického podpisu a má být také využíván pro informační systém datových schránek.

Velice zajímavě je řešena Identifikační karta občanů Estonska, která má v sobě, kromě identifikačních údajů ve strojově čitelném formátu, navíc ještě standardně integrovaný procesorový čip. Na tomto čipu však nejsou uložena duplicitně data, která lze zjistit ze strojově čitelné zóny, ale certifikát, příslušný privátní klíč, jméno držitele karty a jeho identifikační číslo. Soukromé klíče jsou chráněny PIN a slouží pro autentizaci držitele karty a pro elektronické podepisování dokumentů. Za velice zdařilé považuji, že autentizační certifikát obsahuje unikátní emailovou adresu, která je přiřazena držiteli karty a má neměnný tvar: jméno.příjmení_NNNN@eesti.ee, kde NNNN je náhodně generované číslo. Tato e-adresa by měla být neměnná a měla by platit po dobu života držitele karty. Adresa neslouží přímo pro použití v internetových službách, ale je jakýmsi směrníkem na reálnou e-adresu, kterou si držitel karty může libovolně měnit. Slouží však pro komunikaci mezi občanem a státem a může být rovněž využívána pro soukromou komunikaci s privátními subjekty. Tato adresa je veřejně dostupná a nachází se v centrálním registru poskytovatelů certifikačních služeb.

Obrázek 3 - Integrovaná integrační karta občana Estonska

3.2.4.2 Současný stav vydávání občanských průkazů

Držitelem občanského průkazu je v současné době přibližně 8 miliónů občanů. V roce 2008 proběhla zatím poslední etapa výměny občanských průkazů bez strojově čitelných údajů s dobou platnosti do 31.12.2008 za občanské průkazy se strojově čitelnými údaji (s tištěnou podobou občana a jeho tištěným podpisem). Výrobu občanských průkazů se strojově čitelnými údaji má Ministerstvo vnitra zajištěnu smlouvou se Státní tiskárnou cenin, jejíž platnost končí v roce 2010.

Předpokládá se, že o vydání e-OP bude možné požádat v lednu roku 2010 s tím, že dosavadní typ občanského průkazu se strojově čitelnými údaji bude platný do doby vyznačené v dosavadním občanském průkazu. V souvislosti s jeho postupným zaváděním se navrhuje možnost vydání e-OP občanům mladším 15 let. V současné době se občanský průkaz vydává od 15 let.

Nový elektronický občanský průkaz by měl splňovat následující požadavky:

- umožnění jednoznačné určení totožnosti občana
- využitelnost e-OP jako cestovního dokladu v rámci EU
- využitelnost při elektronické komunikaci s orgány veřejné správy, např. zajištění přístupu do datových schránek, do evidencí zdravotního pojištění či důchodového zajištění
- využitelnost pro výkon volebního práva

Předpokládá se vydávání dvou typů e-OP, standardní varianta se strojově čitelnými kódy a nebo bude možné za poplatek 500,-Kč získat e-OP s kontaktním elektronickým čipem. Elektronický občanský průkaz by měl tedy sloužit nejen k fyzické identifikaci občana jako je tomu dnes, ale také ke vzdálenému přístupu ke všem službám státu, včetně služeb v oblasti zdravotnictví, sociální péče či školství, při současném zvýšení ochrany občanů v případě ztráty nebo odcizení tohoto dokladu.

3.3 Egovernment Act[13]

V této kapitole se budeme podrobně zabývat zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, který vstoupil v platnost dne 19. srpna 2008 a nabude účinnosti 1. července 2009. Realizace tohoto zákona, který se taktéž nazývá Egovernment Act, se více či méně dotýká všech zde uvedených projektů a s jeho uvedením do praxe by mělo dojít ke zlepšení dostupnosti úřadů, ke snazší komunikaci mezi fyzickými či právnickými osobami a veřejnou správou a zejména ke zrychlení a zlevnění výkonu veřejné správy v České republice. Zcela zásadní vliv bude mít zákon na provoz elektronických spisových služeb.

Jak již ze samotného názvu vyplývá, řeší tento zákon dva zásadní problémy:

- První polovina „o elektronických úkonech“ je věnována datovým schránkám. Prostřednictvím datové schránky lze činit podání kterémukoliv úřadu nebo naopak úřady mohou prostřednictvím datové schránky doručit své písemnosti příslušným adresátům (fyzickým nebo právnickým osobám). Stejným způsobem mohou komunikovat s jinými orgány veřejné moci, přičemž veškerým úkonům, které jsou prostřednictvím elektronické přepážky činěny, je přiznána ekvivalence k úkonům učiněným písemně.
- V druhé části „o autorizované konverzi dokumentů“ je postavena na stejnou úroveň papírová a elektronická verze dokumentů, jsou stanovena pravidla převodu dokumentů z listinné podoby do podoby elektronické a naopak, přičemž dokumentu, který je výstupem, se přiznávají stejné právní účinky jako ověřené kopii.

Datové schránky znamenají zcela zásadní přelom ve fungování veřejné správy, protože zavádějí povinnost pro každý orgán veřejné správy provozovat datovou schránku jako místo, do něhož se ve smyslu správního řádu a ostatních předpisů dá

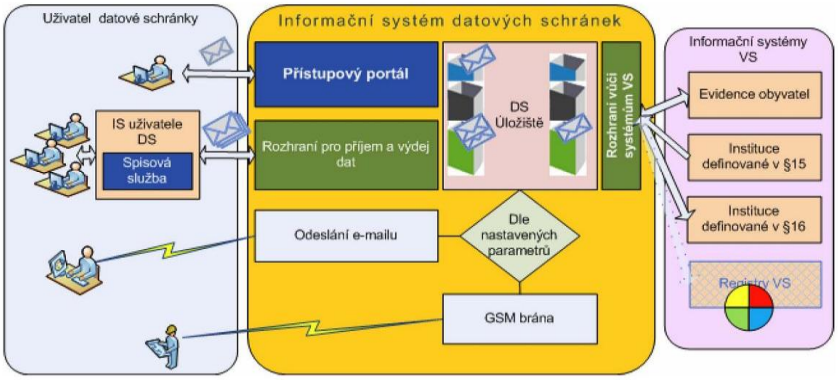
[13] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

zcela oficiálně podat jakýkoli dokument. A to dokonce i dokument bez elektronického podpisu. To znamená, že ke dvěma klasickým způsobům podání (přes poštu a do podatelny) se přidává třetí způsob v podobě **podání do datové schránky**.

Zákon o e-Governmentu zavádí od 1.7.2009 povinnost orgánů veřejné správy dokumenty podané do datové schránky přijmout a navíc zavádí povinnost orgánů veřejné správy v případech, kdy má klient zřízenu datovou schránku, tímto způsobem také doručovat. V praxi to znamená, že všem právnickým osobám povinně v okamžiku zřízení datové schránky, která jim přísluší ze zákona, bude muset veřejná správa doručovat elektronicky, a to včetně ostatních úřadů a organizací veřejné správy.

Je zřejmé, že v důsledku tohoto ustanovení dojde k razantnímu navýšení elektronických transakcí mezi veřejnou správou a okolím a bude nutno tomu přizpůsobit všechny stávající procesy v každé organizaci veřejné správy. První náraz pocítí **spisová služba**, která bude muset zvládnout veškerou evidenci a ukládání elektronických dokumentů. Dokumenty bude muset umět zpracovat, evidovat jednotlivé fáze při vyřizování dokumentu a v případě potřeby dokument zase zpátky doručit. Jde o zcela zásadní změnu dosavadního fungování spisových služeb. Systém datových schránek je z tohoto pohledu nejméně důležitou komponentou, protože z technického hlediska je to systém, který musí zaručit, že se dokument bezpečně a důvěryhodně podá a bezpečně a důvěryhodně bez jakékoli modifikace doručí.

Datové schránky nahradí tradiční doručování v listinné podobě. To znamená, že od data účinnosti výše uvedeného zákona budou firmy případně občané komunikovat s úřady elektronicky. Postačí jediné – elektronický podpis a internet a dopisy nám budou chodit domů, přímo na náš počítač. Kdo si datovou schránku zřídí, bude již s úřady jednat, kdy a odkud bude on sám chtít, přičemž doručení do schránky bude mít stejnou právní záruku jako doručení do vlastních rukou. Navíc, přes kontaktní místa budou datové schránky moci využívat i lidé, kteří doma internet nemají. Zatímco běžní lidé a fyzické osoby se budou moci sami rozhodnout, zda novinku využijí nebo zda si chtějí dál vystát frontu na poště, pro právnické osoby ani úřady už žádná jiná volba než datové schránky nebude. Právnické osoby, ale také úřady samy mezi sebou budou muset povinně komunikovat prostřednictvím datových schránek.



Obrázek 4 - Systém komunikace s datovou schránkou

Datovou schránku zřizuje Ministerstvo vnitra. Vyplněnou žádost lze donést osobně na kontaktní místa veřejné správy (Czech POINT), v případě, že žádost nepodepisujeme přímo před úředníkem, je třeba přiložit úředně ověřený vlastnoruční podpis. Žádost je možno také zaslat elektronicky, v takovém případě je nutno zprávu podepsat zaručeným elektronickým podpisem.

Pokud doručujeme pomocí datové schránky dokumenty určené adresátům veřejné moci, uplatní se zde příslušné procesní předpisy (např. občanský soudní řád nebo správní řád). Pokud tyto předpisy požadují opatřit dokument zaručeným elektronickým podpisem, který je založen na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb, je nutno tento k zasílanému dokumentu přiložit. V této souvislosti je nanejvýš vhodné si uvědomit, že dopis, který byl doručen do datové schránky je považován do deseti dnů za vyzvednutý.

Definujme si nyní několik hlavních zásad, které se vztahují k datovým schránkám:

- Datová schránka umožňuje přijímání datových zpráv od orgánů veřejné moci a odesílání datových zpráv těmto orgánům.
- Datová schránka bude mít přiděleno osobní číslo jako jednoznačný identifikátor.
- Nejméně jedním komunikujícím je úřad.
- Datová schránka není určena pro vzájemnou komunikaci fyzických či právnických osob.
- Datová schránka je občanu zřízena pouze na jeho žádost (je možné využít sítě Czech POINT).

- Občan má možnost požádat o tzv. znepřístupnění datové schránky a později o její opětovnou aktivaci.
- Datová schránka je podnikající fyzické osobě rovněž zřízena pouze na její žádost.
- Datové schránky se povinně zřizují orgánům veřejné moci, právnickým osobám zřízeným zákonem a zapsaným v obchodním rejstříku (včetně zahraničních).
- Pokud má fyzická či právnická osoba zřízenu datovou schránku, musí orgán veřejné moci doručovat v elektronické formě do datové schránky dané osoby.
- K jedné datové schránce může mít přístup více osob, ovšem všechny osoby nemusí mít přístup ke všem datovým zprávám, které jsou do schránky doručeny.
- Dokument dodaný do datové schránky je doručen okamžikem, kdy se do datové schránky přihlásí osoba mající dle svého oprávnění přístup k dodanému dokumentu.
- Nepřihlásí-li se do datové schránky oprávněná osoba ve lhůtě 10 dnů ode dne dodání do datové schránky, považuje se dokument za doručený posledním dnem této lhůty.
- Datová schránka není email ani archív !!!

V souvislosti s provozováním datových schránek je třeba zmínit, že nutnou podmínkou provozování takovéto elektronické agendy je spolehlivá, bezpečná, a současně rychlá a pohodlná *identifikace* fyzických i právnických osob a orgánů veřejné moci (tj. zjištění „o koho jde“), a jejich *autentizace* (tj. ověření, že „jsou skutečně tím, za koho se vydávají“).

Základem pro identifikaci je v našem případě použití *bezvýznamových identifikátorů* (tj. takových, které samy o sobě nevypovídají nic o tom, koho označují), a základem pro autentizaci je využití *metod elektronického podpisu*.

Druhým velice důležitým důsledkem tohoto zákona je, že každý občan nebo každá organizace má právo žádat (s několika málo výjimkami) *konverzi jakéhokoli dokumentu* do elektronické podoby a vlastně zkonstruovat celé elektronické podání včetně všech příloh.

Základním prvkem většiny procesů státní správy a samosprávy je dokument a jeho právní závaznost, která je zajištěna podpisem. Přestože se při komunikaci s úřadem používá něco mezi 100 – 200 formuláři, má značná část přijatých a vytvářených dokumentů formu nestrukturovaného textu a je vyžadován i vlastnoruční podpis.

Zavedení institutu autorizované konverze písemností nám umožní použití jak elektronické, tak „papírové“ verze dokumentu a převod dokumentu z listinné do elektronické podoby a naopak, přičemž hodnota elektronické i listinné verze dokumentu je stejná. Zákon dále umožňuje „legalizaci“ elektronického podpisu, takže stejně jako je možno u listinné verze dokumentu provést úřední ověření podpisu, bude možno stejným způsobem provést úřední ověření elektronické verze dokumentu zaručeným elektronickým podpisem.

V právní úpravě týkající se autorizované konverze dokumentů jsou poprvé upraveny podmínky a postupy, za kterých bude mít dokument převedený z listinné do elektronické podoby (či naopak) stejnou právní sílu jako dokument původní. Zákon rovněž taxativním výčtem stanoví, u kterých dokumentů konverzi nelze provádět, a definuje subjekty, které jsou oprávněny k provádění autorizované konverze dokumentů, přičemž provedením autorizované konverze dokumentu se nepotvrzuje jeho správnost ani pravdivost údajů, pouze jejich shoda.

Princip je v zásadě následující: oprávněný subjekt provede příslušnou konverzi a výsledek sám „posvětí“ (autorizuje) svoji elektronickou značkou, čímž současně ověřuje shodu obsahu v obou formách. Pro převod z elektronické formy na listinnou ("papírovou") je přitom nutné, aby elektronický originál byl opatřen buď uznávaným elektronickým podpisem nebo elektronickou značkou (založenou na kvalifikovaném systémovém certifikátu, vydaném akreditovaným poskytovatelem certifikačních služeb). Zákon samozřejmě vyjímá některé druhy písemností z možnosti konverze kvůli tomu, že u nich by něco takového nemělo smysl. Z "papírových" písemností jde například o různé průkazy (občanské, řidičské, zbrojní atd.), cestovní pasy, vkladní knížky, šeky, směnky, losy, sázenky apod. Určitá omezení se pochopitelně týkají i elektronických písemností převáděných v opačném směru. Konvertována například nemůže být písemnost, u které "nesedí" její elektronický podpis či značka (například kvůli pozměnění obsahu, kvůli zneplatněnému certifikátu v době podpisu atd.).

Předmětem "elektronické legalizace" je elektronický podpis, který žadatel o legalizaci uznává za svůj a tuto skutečnost stvrzuje ten, kdo legalizaci provádí. Jde tedy o elektronickou obdobu situace, kdy notář stvrzuje to, že někdo prohlásí konkrétní podpis "na papíře" za svůj vlastnoruční podpis. Řeší se tím tedy skutečnost, kdy některé agendy ze zákona vyžadují od žadatele "úředně ověřený podpis" na předkládaných písemnostech, což dosud implikuje nutnost předkládat potřebné písemnosti pouze v listinné podobě.

Poplatky za provedení autorizované konverze dokumentů jsou definovány zákonem č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů, kde v části první jsou uvedeny změny ve správních poplatcích následovně:

- Provedení autorizované konverze dokumentů do elektronické podoby za každou i započatou stránku konvertované listiny – 30,-Kč
- Provedení autorizované konverze dokumentů do listinné podoby za každou i započatou stránku konvertované listiny – 30,-Kč
- Opětovné vydání přístupových údajů k datové schránce – 200,-Kč

Zde popisovaný zákon by měl především zrovnoprávnit listinnou formu dokumentu s elektronickou a v neposlední řadě postavit Informační a komunikační technologie 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 bude již z velké části uskutečňována elektronicky.

4 Bezpečnostní standardy státní správy

Při nasazování nejrůznějších kryptografických funkcí je třeba si nejdříve definovat, co zabezpečovací technologie na bázi kryptografie mohou a co nemohou dělat. Systémy na bázi kryptografie poskytují dostatečné zabezpečení, jestliže jsou správně používány v rámci schopností a omezení kryptografických technologií. Celková síla zabezpečovacích systémů závisí na mnoha faktorech, jako jsou vhodnost technologie, odpovídající zabezpečovací procedury a procesy, a jak dobře lidé tyto procedury, procesy a technologie používají. Jinak řečeno: zabezpečení je tak dobré, jaký je nejslabší článek v celém zabezpečovacím systému.

Můžeme použít nejlepší dostupnou zabezpečovací technologii, ale všechna zabezpečovací snažení budou zmařena, jestliže někdo (vetřelec nebo některý zaměstnanec) může snadno vstupovat do kanceláří a získávat cenné soukromé informace, které byly vytištěny v podobě nešifrovaného textu na tiskárně.

Úroveň zabezpečení ve veřejné správě je určena hodnotou informací, kterou je třeba chránit, náklady, které jsou potřebné na implementaci požadované úrovně zabezpečení a příslušnou legislativou. Při definování bezpečnostních standardů a posuzování úrovně zabezpečení dat jsem vycházel ze zkušeností, které jsem získal při testování a následné praktické realizaci metod asymetrické kryptografie používané u přihlašování a autentifikace zaměstnanců do systému v rezortu Ministerstva financí České republiky

4.1 Definice základních pojmů

Nejdříve definujme základní pojmy a techniky, které budou následně použity v dalších částech práce a jejichž správná interpretace je pro další výklad nezbytná.

4.1.1 Principy asymetrické kryptografie

Základním principem asymetrické kryptografie je použití dvojice klíčů - soukromého a veřejného klíče, kterou každý zúčastněný uživatel či služba vlastní a spravuje. Soukromý klíč se používá pro vytváření elektronických podpisů, které lze následně

pomocí odpovídajícího veřejného klíče ověřit a zkontrolovat tak, že data skutečně pocházejí od majitele dvojice klíčů, a že nebyla nijak modifikována při přenosu.

Naopak pomocí veřejného klíče je možné zašifrovat data tak, že je lze dešifrovat pouze pomocí odpovídajícího soukromého klíče a je tak zaručeno, že je může přečíst opravdu pouze určený adresát, tj. majitel dotyčného páru klíčů. Soukromý klíč je tedy určen pouze pro použití svým majitelem, který jej musí držet v tajnosti a veřejný klíč je naproti tomu distribuován v rámci celé komunity a je volně k dispozici komukoliv, kdo má zájem navázat bezpečné spojení s majitelem tohoto klíče. Veřejné klíče se nejčastěji distribuují ve formě certifikátů veřejného klíče vydávaných certifikačními autoritami. Certifikáty obsahují identifikaci majitele klíče a další informace, které jsou důležité pro komunikaci, jako je doba platnosti klíče, adresa seznamu revokovaných certifikátů či emailová adresa uživatele.

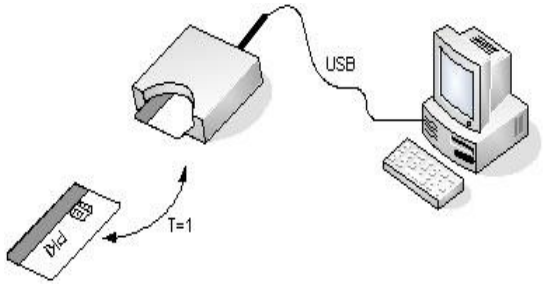
Jedním ze základních problémů se kterými se asymetrická kryptografie potýká je správa soukromých klíčů. Používané klíče představují velmi dlouhé řetězce znaků a na rozdíl od hesel si je člověk nemůže zapamatovat. Musí být proto uloženy v nějaké elektronické podobě tak, aby je mohla přečíst aplikace, kterou uživatel používá.

Pro bezpečné ukládání soukromých klíčů existuje několik alternativ, které se liší ve způsobu práce s nimi i v zabezpečení, které uloženým klíčům poskytují. Nejjednodušší možností je použít nějaký typ vyjímatelného média, jako je např. disketa, CD-ROM nebo populární *USB flash disk*, na které se soukromý klíč uloží místo pevného disku. Po dobu práce je médium s klíčem zapojeno do počítače a aplikace s klíčem pracují stejně, jako by byl přímo na pevném disku počítače, tj. přistupují k souboru na výměnném médiu. Po ukončení práce uživatel vyjme médium z počítače a klíč tak není v počítači nadále dostupný a nemůže se stát předmětem útoku. Tento postup je sice jednoduchý, ale neposkytuje žádnou ochranu pro klíč v okamžiku, kdy je médium s klíčem připojeno k počítači. Navíc se zvyšuje riziko prozrazení klíče, protože médium je přenosné a může se ztratit nebo být odcizeno. Naopak výhodou tohoto přístupu je fakt, že jej lze začít používat okamžitě a nejsou potřeba žádné změny v aplikacích.

Další možností je použití *čipových karet* a příbuzných technologií, které obsahují jak chráněný prostor, do kterého lze uložit soukromý klíč s certifikátem, tak i samostatný procesor, který je schopen s těmito klíči pracovat a provádět s nimi základní kryptografické operace. Karta je k počítači připojena pomocí čtečky zapojené přes USB nebo sériový port, pomocí které komunikují aplikace s kartou. Aplikace tak nepoužívají přímo soukromý klíč, ale předávají kartě data, která jsou zpracována procesorem na tokenu a výsledek je vrácen zpět aplikaci. Klíč tak nikdy neopustí kartu a není jej možné nijak zkopírovat.

Karty Smart Card jsou velikosti kreditních karet a obsahují desku s integrovanými obvody[14], mohou být použity pro uložení certifikátů a soukromých klíčů nebo pro realizaci kryptografických operací veřejným klíčem, jako je ověření totožnosti, elektronické podepisování, případně výměny klíčů.

Navíc karty Smart Card používají namísto hesla tzv. PIN[15]. Karta Smart Card je chráněna proti zneužití tímto PINem, který je znám pouze majiteli karty Smart Card. Při použití uživatel vloží kartu do čtečky, která je připojena k počítači, a když je vyzván, zadá PIN. PIN nabízí dokonalejší ochranu než standardní síťová hesla, která cestují napříč sítí a jsou předmětem hrubých nebo slovníkových útoků. Síla hesla závisí na jeho délce, jak dobře je chráněno a jak obtížné je heslo uhodnout.



Obrázek 5 – Použití karty Smart Card[16]

[14] ICC - Integrated Circuid Card

[15] PIN - Personal Identifications Numbers

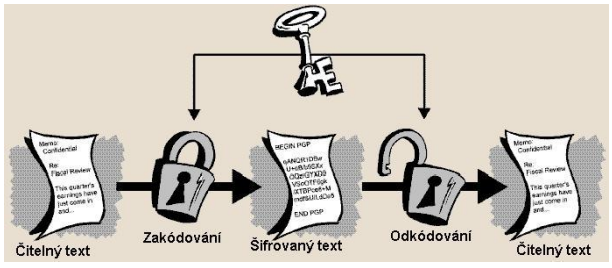
[16] Karty a čtečky, ze dne 12. 1. 2007; přístup z Internetu: URL: http:\\www.cryptoplus.cz

Naopak PINy nikdy necestují po síti a nemohou být elektronicky detekovány. Navíc útoky nebo hrubé útoky (hledání klíče, kde útočník zkouší početné kombinace PINů při pokusech uhodnout PIN) mohou být uskutečněny pouze někým, kdo fyzicky kartu Smart Card vlastní. A karty Smart Card se zablokují již po několika málo neúspěšných pokusech uhodnout PIN.

Vedle čipových karet s čtečkami také existují čipové tokeny připojitelné do USB, které kombinují funkcionalitu karty a čtečky v jednom kusu hardware. Vzhledem se podobají USB flash diskům, ale vnitřní architektura je totožná s čipovými kartami, tj. obsahují vlastní procesor a není možné přistupovat přímo k citlivým datům na tokenu. Výhodou tokenů je jejich vyšší mobilita, protože není potřeba s sebou nosit kartu i čtečku. Další výhodou je jejich tvar, protože vzhledem k jejich malé velikosti je lze připojit např. ke svazku klíčů, takže se snižuje riziko, že zůstanou zapomenuté v počítači.

4.1.2 Symetrické šifry

Pro šifrování i dešifrování dat se používá jeden šifrovací klíč sdílený mezi odesílatelem a příjemcem. Hlavní výhodou symetrických algoritmů je jejich rychlost.



Obrázek 6 – Symetrické šifrování[17]

17 Bezpečné šifrování, ze dne 19. 6. 2008; přístup z Internetu: URL: http:\\www.cryptosafe.cz

Symetrické šifrování je časově nenáročné. Problémem je bezpečná distribuce sdíleného klíče a potřeba vysokého počtu klíčů za předpokladu, že každá dvojice na Internetu chce uskutečňovat bezpečnou komunikaci. Ve chvíli, kdy dojde k prozrazení klíče byť jen jednou zúčastněnou osobou, jsou všechny jím zašifrované informace prozrazeny[18].

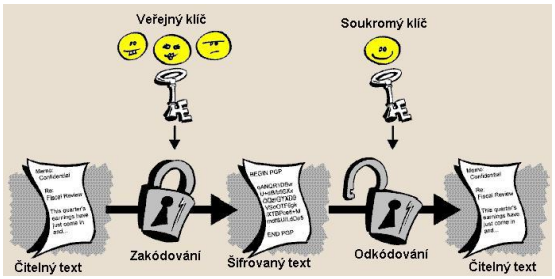
Nejrozšířenějším šifrovacími algoritmy byl DES používající šifrovací klíč délky 56 bitů. Dnes se však považuje za nedostatečný. Z algoritmu DES byl odvozen v současnosti používaný algoritmus 3DES s klíčem 112 bitů. Dále se často používají algoritmy s délkou klíče 128 bitů (IDEA, RC2, RC4). Na obzoru je využívání algoritmu AES s délkou klíče 128, 192, nebo 256 bitů. Jedná se o blokové šifry, data se šifrují/dešifrují po blocích dlouhých zpravidla 8B. I když útočník nevidí do šifrovaného textu, tak by mohl hypoteticky útočit tak, že by zaměnil pořadí zašifrovaných bloků. Tomu se šifry brání vázáním po sobě následujících bloků. Hovoříme o tzv. módu šifry, který zajišťuje, že nelze snadno přehazovat jednotlivé šifrované bloky. Často používanými módy jsou CBC či ECB. Šifrovací algoritmus s konkrétním módem se pak značí např. takto: DES-CBC, DES-ECB, IDEA-EB.

4.1.3 Asymetrické šifry

Pro šifrovací operace se používá tzv. klíčový pár. Jeden klíč pro šifrování a druhý pro dešifrování. U elektronického podpisu mluvíme o veřejném a soukromém klíči. Základní vlastností šifrování na bázi asymetrických šifrovacích algoritmů je skutečnost, že je relativně jednoduché za využití veřejného klíče šifrovat text, ale na základě znalosti veřejného klíče a veřejným klíčem šifrované zprávy je velice obtížné získat původní zprávu. Nejznámějším šifrovacím algoritmem je RSA, kde délka šifrovacích klíčů, která se ještě považuje za bezpečnou, je alespoň 2048 bitů. Algoritmus RSA používá klíče, které jsou o řád delší než klíče, které se používají u symetrických šifer.

18 DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: Bezpečnost. Praha. 2003.

To je důvodem, proč je šifrování asymetrickou šifrou výrazně pomalejší než šifrování symetrickou šifrou.

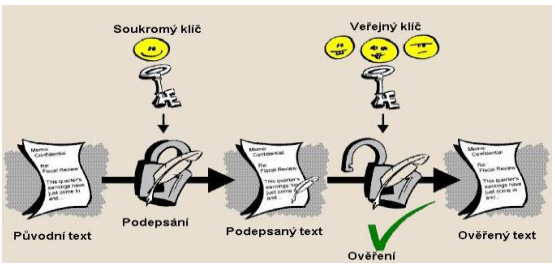


Obrázek 7 – Asymetrické šifrování[19]

Dnes se často mluví o algoritmu ECC (eliptické křivky). Z bezpečnostního hlediska odpovídá 1024 bitů dlouhému klíči RSA 160 bitů dlouhý klíč ECC. Dalším asymetrickým algoritmem je algoritmus DH (Diffie-Hellmanův), který hojně využívá protokol Ipsec[20].

4.1.4 Elektronický (digitální) podpis

Velkou výhodou asymetrického kódování je možnost vytváření tzv. *digitálních podpisů.* Digitální podpisy dávají příjemci možnost ověřit si, od koho dokument pochází a zda je pravý. Digitální podpis slouží ke stejnému účelu jako podpis psaný rukou, až na to, že na rozdíl od digitálního podpisu lze rukou psaný podpis napodobit.



Obrázek 8 – Digitální podpis[6]

---

[19] Šifrování, ze dne 19. 6. 2008; přístup z Internetu: URL: http:\\www.cryptosafe.cz

[20] Microsoft Windows Server Team, členové Microsoft MVP a partneři. *Microsoft Windows Server 2003 : Resource Kit.* Praha. 2004.

4.1.5 Zaručený elektronický podpis

ZAREP – Datové zprávy opatřené zaručeným elektronickým podpisem, které přijímá "Společné technické zařízení správců daně", musí být vytvořeny dle formátu PKCS#7 verze 1.5 (RFC 2315). PKCS#7 objekt musí být ve formátu DER (ITU-T Recommendation X.690).

Obsah PKCS#7 objektu, reprezentujícího datovou zprávu opatřenou zaručeným elektronickým podpisem, musí splňovat následující podmínky:

- musí být typu "signedData"
- musí obsahovat podepisovaná data (není přípustná reference)
- musí obsahovat certifikát podepisujícího (vložený)
- musí obsahovat právě jeden elektronický podpis

Při příjmu datové zprávy opatřené zaručeným elektronickým podpisem se kromě kryptografických kontrol platnosti podpisu datové zprávy kontroluje také následující:

- certifikát podepisujícího musí být vydán akreditovaným poskytovatelem certifikačních služeb, (přehled udělených akreditací zveřejňuje dle zákona Ministerstvo informatiky)
- certifikát podepisujícího musí obsahovat bezvýznamový identifikátor klienta MPSV.

4.1.6 Hash – kontrolní součet

Hash je jednocestná funkce[21] , která nám z libovolně dlouhého textu vyrobí krátký řetězec konstantní délky. Výsledný řetězec (hash) přesně charakterizuje původní text. To znamená, že při jakékoliv změně původního textu dostaneme výrazně jiný výsledek[22]. Typická velikost výsledného textu je 16B (algoritmus MD-5) nebo 20 B (algoritmus SHA-1).

---

[21] Jednocestné funkce jsou ty, které nejsou výpočetně náročné. Avšak výpočetně velice náročné je k výsledku nalézt původní text. Klasickou jednocestnou funkcí je např. manželství. Je jednoduché se oženit, ale často velice obtížné se rozvést.

[22] HATCH, Brian , LEE, James , KURTZ, George . *Hacking bez tajemství: Linux* . Praha. 2000.

V oblasti digitálních podpisů se hashovací funkce obvykle používají při asymetrickém šifrování, přesněji digitálním podepisování soukromým klíčem. Namísto původní zprávy o desítkách nebo stovkách megabytů se však nejprve vytvoří mnohem menší otisk takovéhoto souboru a odesílatel podepíše pouze několik desítek vzniklých bitů, tzn. podepisujeme pouze podstatně „kratší“ otisk původní zprávy.

4.1.7 Kvalifikovaná certifikační autorita

Certifikační autorita představuje objekt, který vydává digitální certifikáty k použití ostatním zúčastněným. Jde vlastně o jistou formu notářského úřadu, figurujícího mezi komunikujícími stranami, o které by se dalo říci, že spojuje veřejný klíč s uživatelem a ozřejmuje jeho autenticitu. Mezi certifikační autoritou a klientem je sepisována smlouva, která jednoznačně definuje pravidla užívání, odvolávání a generování digitálních certifikátů.

Základním dokumentem, kterým se certifikační autorita řídí, je certifikační politika. Certifikační politiky je možné najít přímo na webových stránkách příslušné certifikační autority. Zákon č. 297/2000 Sb., o elektronickém podpisu, stanovuje řadu požadavků a náležitostí, které musí poskytovatel certifikačních služeb splňovat. Například ručí do stanovené výše za případné škody vzniklé vlastním pochybením, má omezené možnosti dalšího podnikání atp.

Nedílnou součástí každé certifikační autority je minimálně jedna podřízená registrační autorita. Podřízenou registrační autoritu si můžeme představit jako kancelář certifikační autority, která od zákazníků přijímá žádosti o vydání certifikátu a ověřuje jejich totožnost. Jedna registrační autorita může spadat vždy pouze pod jednu certifikační autoritu.

Mezi nejdůležitější povinnosti majitele certifikátu patří, oznámit v případě nutnosti autoritě prozrazení (diskreditaci) jeho soukromého klíče. Ta poté musí „neprodleně a bez zbytečných odkladů“ certifikát zneplatnit jeho zařazením do seznamu

zneplatněných certifikátů[23]. Pokud si následně kdokoliv pomocí CRL ověřuje platnost certifikátu, zjistí, že ten je odvolaný a digitálnímu podpisu tedy nelze důvěřovat.

4.1.8 Kvalifikovaný certifikát

Kvalifikovaný certifikát jednoznačně identifikuje odesílatele. Jedná se o datovou strukturu (řetězec bitů), která je uložená ve standardním, mezinárodně platném formátu, pomocí které se zveřejňují údaje o uživateli a zejména uživatelův veřejný šifrovací klíč (v případě RSA šifer). Pro certifikáty se používá mezinárodní norma X.509, která jednoznačně popisuje strukturu certifikátu.

Obrázek 9 - Kvalifikovaný certifikát

Kvalifikovaný certifikát je elektronicky podepsán (ověřen) akreditovanou certifikační autoritou. Z certifikátu je možné získat veřejný šifrovací klíč uživatele, který je možné použít k prokazování totožnosti uživatele. V případě, že certifikát obsahuje šifrovací klíč určený také k šifrování dat, pak je možné i tento klíč z certifikátu použít k šifrování dat odesílaných uživateli.

[23] CRL - CertificateRevocation List

Pokud tedy chce podnikatel, ať už fyzická nebo právnická osoba, komunikovat s úřady elektronicky a podepisovat se zaručeným elektronickým podpisem, musí získat kvalifikovaný certifikát od akreditované certifikační společnosti. Akreditaci provádělo Ministerstvo informatiky, po jeho zrušení příslušná agenda přešla na Ministerstvo vnitra. Akreditované společnosti jsou v Česku zatím pouze tři: První certifikační autorita, Česká pošta a e-Identity.

Kvalifikovaný certifikát pak musí podle zákona obsahovat mimo jiné informace o poskytovateli certifikátu, jméno podepisující osoby, data pro ověřování podpisu, číslo certifikátu či počátek a konec jeho platnosti. V případě potřeby je možné nechat platný certifikát zneplatnit. Databáze platných i neplatných certifikátů mají pro ověření certifikační společnosti na svých internetových stránkách.

4.1.9 Datová schránka

Datová schránka je elektronické úložiště, které slouží k doručování dokumentů orgánů veřejné moci či k provádění úkonů vůči veřejné moci. Všechny datové schránky budou umístěny v rámci jednoho informačního systému, nejedná se tedy v případě komunikace mezi datovými schránkami o zasílání (necestuje žádný mail), ale spíše o vkládání zpráv do konkrétní datové schránky. Proto zákon počítá se zaručeným doručením a zavádí institut vyzvednuté zásilky, který říká, že každá zásilka vložená do datových schránek je považována za vyzvednutou po 10 dnech od jejího doručení, a to i v případě, že si ji adresát nevyzvedl. To je zásadní moment, který výrazně urychlí řadu řízení, neboť doposud se čekalo, zda si adresát vyzvedl známou proužkovou obálku nebo ne, zda se nachází na konkrétní adrese, či nikoli. Z toho důvodu bude mít každý jednu konkrétní adresu pro doručování (datové schránky jsou od 1.7.2009 povinné pro veřejnou správu a právnické osoby, fyzické a fyzické podnikající osoby je zřízení dobrovolné).

4.1.10 Daňová informační schránka

Daňovou informační schránku si zřizuje daňový subjekt v rámci elektronické aplikace EPO (Elektronické daňové podání). Slouží pro komunikaci mezi daňovým

poplatníkem a daňovou správou a obsahuje informace z daňového řízení a informace o stavu osobního daňového účtu.

Přístup k těmto informacím je umožněn pouze fyzické osobě, která je daňovým subjektem nebo která je oprávněna jménem daňového subjektu, popřípadě za daňový subjekt jednat. Ke zřízení informační schránky je třeba vlastnit kvalifikovaný certifikát.

4.2 Bezpečnostní model rezortu ministerstva financí

Problematikou bezpečnosti dat a zabezpečené komunikace po síti jsem se začal vážně zabývat již v roce 2000, kdy jsme na Finančním ředitelství v Hradci Králové vytvořili řešitelský tým, který pracoval na projektu přechodu z architektury Windows NT4 Server na doménový model s architekturou Server Windows 2003, což nám dnes umožňuje pracovat s mnohem vyšší úrovní zabezpečení, než jsme kdy mohli dosáhnout s technologií serverů Windows NT4.

S přechodem na serverovou architekturu Windows 2003 se výrazně rozšířily možnosti zabezpečení jak při ověřování klientů a řízení přístupu k síťovým prostředkům, tak i v procesu komunikace mezi daňovými subjekty a jednotlivými rezorty státní správy, kde jedním z určujících prvků zabezpečené elektronické komunikace je plošné využívání certifikátů pro podepisování a šifrování zabezpečené zprávy.

Aby bylo možné efektivně pracovat a aktualizovat databázi zaměstnanců rezortu, bylo nutné, současně se zaváděním operačního systému Windows 2003 Server na jednotlivých finančních úřadech (dále jen FÚ), započít se stavbou a konfigurací centrálního MIIS serveru, což je vlastně LDAP server s rozšířenou funkčností, který pracuje s daty zaměstnanců, které jsou uloženy v centrálním personálním systému a zprostředkovává jejich provázání se stěžejními aplikacemi daňové správy a samozřejmě také synchronizuje tyto údaje s adresářovými službami Active Directory, včetně automatické instalace a aktualizace uživatelských certifikátů z interního úřadu Certifikační autority MFČR.

Tímto způsobem by se nám podařilo automatizovat celý životní cyklus zaměstnance od jeho založení v personálním systému, synchronizace s centrálním MIIS serverem až po vytvoření odpovídajícího účtu Active Directory na příslušném FÚ včetně vygenerování interního zaměstnaneckého certifikátu. Propojení dat personálního systému s aplikacemi, které jsou v Rezortu využívány pro správu daní a poplatků, umožňuje definovat aktuální přístupová práva do jednotlivých úloh dle pracovního zařazení zaměstnance, přičemž autentifikace probíhá na základě certifikátu, který má každý zaměstnanec uložen na své kartě Smart Card.

4.2.1 Používání čipových karet Smart Card

Jak jsem se již v předchozí kapitole zmiňoval, bezprostředně po přechodu na OS Windows 2003 Server se započalo s testováním a následným nasazením čipových karet jako standardního způsobu přihlašování k přidělenému PC a tedy i do celého systému rezortu. Zde bych chtěl upozornit, že MFČR má vybudovanou vlastní, zabezpečenou síť FINet, uvnitř které využívá služeb interního certifikačního úřadu, jehož působnost je samozřejmě pouze uvnitř sítě. Tento úřad zajišťuje služby ověření totožnosti zaměstnance a následné vystavení certifikátu jakož i obnovení certifikátu před koncem platnosti, nesplňuje však podmínky kvalifikovaného certifikátu vydaného akreditovanými poskytovateli dle příslušných ustanovení zákona o elektronickém podpisu.

V době, kdy jsem psal tuto práci, probíhalo testování exportu a automatické synchronizace databáze personálního systému ministerstva financí do Active Directory a certifikačního úřadu. Ve finále by již nebylo třeba do Active Directory manuálně nahrávat či generovat žádosti o nové certifikáty. Vše by se odvíjelo od data započetí, případně ukončení zaměstnaneckého poměru v personálním systému.

Z výše uvedeného je zřejmé, že pro jednoznačné definování platnosti zaměstnaneckého certifikátu Rezortu bylo nutné definovat pouze jediný zdroj dat, ze kterého by se přebíraly informace o zaměstnancích další zúčastněné instituce, ať zaměstnanecká certifikační autorita, databáze active directory či další aplikace, kde je přístup vázán na přístupová práva, která jsou závislá na zaměstnaneckém poměru pracovníka. Jako stále aktuální a tedy nejvhodnější se jeví databáze personálního

systému Rezortu. Samozřejmě, je nutné řadu aplikací upravit či zcela přepracovat, jelikož jednotlivé komponenty rezortu se vyvíjely v různých časových obdobích, kdy personální data nebyla ještě zcela synchronizována a dostupná po celém rezortu a bylo nutno volit jiné, alternativní způsoby ověřování zaměstnanců.

Komplexní využívání databáze personálního systému je zcela jistě myšlenka správná, v praxi se ale objevila i mnohá úskalí. K narušení správné funkce například stačí, aby příslušný FÚ nenahlásil včas nástup nového zaměstnance. Personální oddělení nevyplní včas zaměstnaneckou kartu pracovníka, nevygeneruje se žádost o zaměstnanecký certifikát rezortu, nevytvoří se účet v Active Directory a samozřejmě v den nástupu pracovníka nebude k dispozici ani čipová karta opravňující ke vstupu zaměstnance na pracoviště. Aby k tomuto nedocházelo je nutné vytvořit organizační a technické předpoklady, definované i formou vnitřních předpisů, které by tuto nestandardní situaci řešily. Jednou z možností je uchovávat na jednotlivých lokalitách několik čipových karet s omezenými právy a platností, popřípadě ve zcela výjimečných případech umožnit podle jasně definovaných pravidel přístup správci informačního systému do procesu vytváření příslušných oprávnění a generování přístupových účtů. Tyto akce je však třeba pečlivě monitorovat, protože zde je právě prostor pro realizace potenciálních bezpečnostních útoků[24].

Je třeba si uvědomit, že přechod na ověřování uživatelů pomocí čipových karet s sebou přináší i mnohá úskalí. Cena jedné čipové karty se pohybuje kolem 1200,-Kč, ke každému PC je třeba nakoupit čtecí zařízení a v případě, že se čipové karty používají i v docházkovém systému, je třeba na jednotlivé FÚ instalovat také docházkové čtecí zařízení a terminály. Náklady na jeden úřad se tak pohybují kolem několika desítek tisíc Kč (dle velikosti FÚ), z čehož vyplívá, že vybavit všechny lokality čipovými kartami a čtecím zařízením je nákladná a dlouhodobá záležitost.

Pokud má čipová karta sloužit pro identifikaci vstupu zaměstnance na pracoviště, pro přihlašování do systému, případně pro podepisování a šifrování dokumentů, je třeba,

---

[24] Microsoft Corporation Inc., Windows 2003 Server Resource Kit

aby ji zaměstnanci měli neustále pod kontrolou. Problém však nastane, když ji zaměstnanec zapomene doma nebo se čipová karta častým používáním znehodnotí. V takovém případě pracovník není schopen registrovat svůj příchod na pracoviště, systém ho nevpustí do budovy a samozřejmě nemá žádnou možnost přihlášení do systému. Problém se patřičně vyhrotí v případě, že se čipová karta používá i k objednávání a odběru obědů v závodním stravování. V takovém případě je nutno řešit věc okamžitě, protože nemožnost odebrání stravy bez náhrady se kupodivu přičte na vrub samotnému používání čipových karet, vlastní zapomnětlivost pracovníka se v takovém případě nijak zvlášť neřeší.

Ve všech zde popsaných případech je nutný ruční zásah správce systému do přístupových oprávnění příslušných aplikací, přičemž hlavní důraz je kladen na rychlost zneplatnění zaměstnaneckého certifikátu a je-li to nutné, na vydání karty nové.

Existuje však ještě další, velice závažný bezpečnostní problém, spojený s užíváním čipových karet. Zaměstnanci karty sice použijí pro přihlášení do systému při příchodu do zaměstnání, kartu však při krátkodobém opuštění pracoviště nechávají ve čtecím zařízení. Zde přichází do úvahy jediná možnost nápravy a to ve formě finančního postihu takového zaměstnance a deklarací příslušných ustanovení ve vnitřních předpisech, že se jedná o hrubé porušení pracovních povinností.

V této souvislosti je velice zajímavé zjištění, že problém se zapomínáním karty ve čtecím zařízení se pronikavě zlepšil po zpřístupnění webového portálu personálního oddělení, kde má každý aktuálně přihlášený zaměstnanec možnost prohlížet své osobní údaje včetně výpisů z platebních karet. Skutečnost, že při zanechání čipové karty ve čtečce si může kolega přečíst osobní údaje „zapomnětlivého“ zaměstnance problém z větší části odstranila spolehlivěji, než hrozba finančního postihu či riziko zneužití citlivých dat poplatníků.

V zásadě lze ale říci, že přes počáteční odmítavý postoj zaměstnanců Rezortu, se používání čipových karet Smart Card stalo běžnou součástí pracovní náplně na testovacích FÚ a předpokládá se postupné nasazení v celém Rezortu.

4.2.2 Náklady spojené s přechodem na Windows 2003

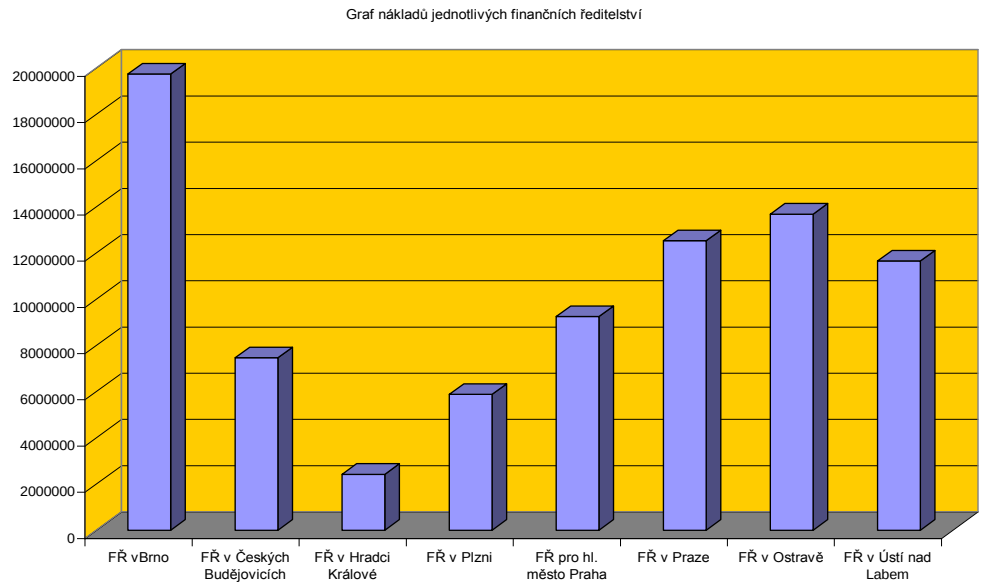
Snaha o zvyšování bezpečnosti a s tím související nutnost modernizace operačních systémů a hardwarového vybavení serverů i pracovních stanic je finančně nákladná záležitost. S náklady na modernizaci operačních systémů je třeba počítat průběžně, protože licenční politika Microsoftu nás poměrně nekompromisně nutí k nákupu nových operačních systémů i s tím souvisejícího programového vybavení. Podpora jedné verze operačního systému je garantována 3 roky po ukončení prodeje, takže se dá říct, že zakoupený software je třeba modernizovat v průměru každých 5-7 let. Nákup nového programového vybavení samozřejmě přináší větší hardwarové nároky, což znamená současný nákup nových počítačů a serverů.

Kupříkladu, zde zmiňovaný přechod resortu MFČR z používaných serverů Windows NT4 na Servery Windows 2003 si vyžádal náklady ve výši 82 600 000,-Kč. V této částce je zahrnut upgrage operačního systému, Exchange Serveru a SQL Serveru. Jedná se pouze o minimum nákladů, další náklady na zálohovací software, síťové prvky či pracovní stanice nejsou do prvotního rozpočtu vůbec započítány. V následující tabulce jsou náklady pro přechod na Server Windows 2003 pro 220 lokalit rezortu ministerstva financí:

Lokality	*Celkem za OS*	*Celkem za Exchange*	*Celkem za SQL*	*Celkem za Hardware*
FŘ vBrno	4 297 857	6 667 482	887 887	7 898 000
FŘ v Č.	1 574 861	2 208 495	221 972	3 460 000
FŘ v Hradci Králové	1 036 995	112 154	332 958	938 000
FŘ v Plzni	922 627	2 147 899	228 512	2 584 000
FŘ pro hl. město Praha	2 413 404	3 559 571	388 450	2 888 000
FŘ v Praze	2 575 886	3 616 109	610 422	5 732 000
FŘ v Ostravě	3 009 376	4 604 467	443 943	5 626 000
FŘ v Ústí nad Labem	2 451 834	3 535 130	443 943	5 224 000

Tabulka 1- Náklady rezortu MFČR

Z grafu rozdělení nákladů je patrné, že FŘ v Hradci Králové se již na připravovaný přechod na nový operační systém připravovalo a nutné počáteční náklady byly potom mnohem nižší.



Obrázek 10 – Graf nákladů[25]

Přechodem na vyšší verzi systému Windows Server byly vytvořeny podmínky pro změnu způsobu přihlašování zaměstnanců resortu státní správy. Používání karet Smart Card i přes počáteční problémy je dnes standardem pro bezpečné přihlašování do většiny aplikací státní správy. Karty představují bezpečné úložiště pro zaměstnanecké certifikáty pracovníků státní správy a nabízejí možnost uložit případně i další certifikát, který mohou vybraní pracovníci využívat k zabezpečené komunikaci mezi jednotlivými orgány státní správy.

[25] Portál České daňové správy, URL: http://cds.mfcr.cz

5 Bezpečnost dat při komunikaci mezi úřady státní správy a samosprávy

Rozvoj e-Governmentu a využívání zabezpečené elektronické komunikace mezi orgány státní správy bylo v podstatě umožněno až zrovnoprávněním klasických listinných dokumentů s dokumenty v elektronické podobě. Tato situace nastala schválením zákona o elektronickém podpisu[26], který vychází ze Směrnice o zásadách společenství pro elektronické podpisy ze dne 13.12.1999, vydané Evropským parlamentem.

Cílem tohoto zákona je stanovit podmínky pro závaznou elektronickou komunikaci mezi dotčenými subjekty, tj. definovat pojem zaručeného elektronického podpisu na základě kvalifikovaného certifikátu vydaného akreditovaným poskytovatelem. Dnes již tedy můžeme platně elektronicky podepisovat kupní smlouvy či smlouvy o dílo (§ 34 až § 51 občanského zákoníku[27]) nebo můžeme učinit podání podle Správního řádu, ZSDP, Občanského soudního řádu[28] či Trestního řádu[29]. Dá se říci, že se zaručeným elektronickým podpisem neuspějeme pouze v případě, kdy zákon výslovně stanoví, že dokument musí být vlastnoručně podepsán nebo je platnost dokumentu přímo závislá na dodržení písemné formy.

Bohužel, elektronický podpis se dodnes masivně nerozšířil a do budoucna je ochota k jeho používání poměrně nízká. Po vydání výše uvedeného zákona se počítalo s tím, že občan bude komunikovat se státní správou a podepisovat svoje e-maily elektronickým podpisem, ale státní správa směrem k občanům a dalším organizacím zůstává dosud převážně při svém zaběhnutém způsobu práce. Svědčí o tom stále nízká znalost získání tohoto nástroje elektronické komunikace, minimální je pak z hlediska populace jeho aplikace v praxi.

---

[26] Zákon č. 486/2004 Sb., o elektronickém podpisu

[27] Zákon č. 40/1964 sb., Občanský zákoník, ve znění pozdějších předpisů

[28] Zákon č. 99/1963 Sb., Občanský soudní řád, ve znění pozdějších předpisů

[29] Zákon č. 141/1961 Sb., Trestní řád, ve znění pozdějších předpisů

Zcela zásadní přelom v bezpečném fungování veřejné správy, představuje schválení zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Tento zákon zavádí pojem datové schrány, přičemž tato datová úložiště budou umístěna v rámci jednoho informačního systému. Nejedná se tedy o zasílání, ale spíše o vkládání datových zpráv do datových schránek, které neopustí zmiňovaný informační systém. Velice důležité je, že zákon počítá se zaručeným doručením a zavádí institut vyzvednuté zásilky, který říká, že každá zásilka do datových schránek je považována za vyzvednutou po 10 ti dnech od jejího doručení a to i v případě, že si ji adresát nevyzvedl. To je zásadní moment, který výrazně urychlí řadu řízení, neboť doposud se čekalo, zda se adresát nachází na konkrétní adrese a doporučenou zásilku si vyzvedne či nikoliv.

V zákoně se dále zavádí pojem autorizované konverze dokumentů, čímž se rozumí převedení dokumentu do elektronické podoby a naopak. Dokument, který vznikl autorizovanou konverzí, má stejnou právní váhu jako jeho vzor. V praxi to tedy znamená, že již nebude nutné předkládat orgánům dokumenty osobně, případně poštou, ale bude možné je zaslat v elektronické podobě do datové schránky dané instituce.

5.1 Základní podmínky bezpečné elektronické komunikace

Než začneme hovořit o jednotlivých aspektech bezpečné elektronické komunikace v rámci e-Governmentu, je nutné definovat základní podmínky a nastavení, která je třeba provést, a bez kterých by takováto komunikace nebyla možná.

5.1.1 Spolehlivé a stabilní připojení k Internetu

Základním předpokladem pro využití nabízených možností komunikace je přístup k internetu a jeho aktivní využívání. Tato podmínka je dnes již splněna na všech stupních veřejné správy, i když samozřejmě pro plné využívání všech možností on-line komunikace bude případně potřebné zásadně povýšit rychlost komunikačních kanálů

5.1.2 Standardní a aktualizovaný operační systém

Veřejná správa využívá v převážné většině operační systém *Windows 2000 a vyšší*, internetový prohlížeč Internet Explorer minimálně ve verzi 6.0 a k elektronické poštovní komunikaci používá poštovního klienta minimálně verze Outlook 2000 nebo klienta Outlook Expres. Bohužel, málo se provádí pravidelná aktualizace operačních systémů či kancelářských balíků Office. Zajímavé možnosti, které výrazně ušetří náklady na administraci při prováděných aktualizacích, nabízí produkt WSUS (Windows Server Update Services). Před vlastním nasazením produktu je však třeba splnit následující předpoklad - jednotlivé stanice musí mít instalován legální verzi OS minimálně verze Windows 2000 SP4. Pokud tuto podmínku nesplníme, nebude nám automatická aktualizace systému fungovat.

Výhody pravidelného spouštění produktu WSUS jsou zřejmé – budeme mít automaticky staženy a nainstalovány známe bezpečnostní záplaty našeho operačního systému, aktualizují se nám nejnovější kořenové certifikáty, které jsou potřebně pro bezpečnou elektronickou komunikaci a samozřejmě se nám budou také instalovat všechny aktualizace, které byly pro náš systém vydány.

Na druhou stranu, nové aktualizace poměrně výrazně zasahují do samotné konstrukce jádra systému, takže může dojít k výraznému zpomalení práce u původně docela svižného počítače. Je to způsobené tím, že instalované aktualizace kladou vyšší nároky na hardware počítače a tak jsme vlastně nepřímo nuceni počítače v poměrně krátkých intervalech modernizovat.

5.1.3 Vlastnictví kvalifikovaného certifikátu

O kvalifikovaném certifikátu a elektronickém podpisu se toho v posledních několika letech napsalo a namluvilo opravdu mnoho. Stále se však setkáváme s případy, kdy jsou základní informace podávány poněkud „zkresleně“, takže v nich méně znalý uživatel může mít „trošičku zmatek“. Přibližme si nyní problematiku elektronického podpisu ve vazbě na e-Government srozumitelnou formou jak z teoretické, tak i z praktické stránky.

Využívání elektronického podpisu bylo fakticky umožněno zákonem č. 227/2000 Sb., o elektronickém podpisu, jehož schválením byly mimo jiné vytvořeny podmínky pro závaznou elektronickou komunikaci mezi dotčenými subjekty a také byl definován pojem zaručeného elektronického podpisu na základě kvalifikovaného certifikátu. Není cílem této práce zabíhat příliš do oblasti zákonů a práva z oblasti elektronického podpisu, nicméně se však zastavme u znění §11 zmiňovaného zákona[30]:

V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb. To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám (zákon č. 227/2000 Sb.).

Faktem je, že abychom tuto zákonnou podmínku splnili, můžeme si nechat vystavit certifikát pouze u kvalifikovaných poskytovatelů certifikačních služeb, které splňují akreditaci Odboru elektronického podpisu Ministerstva informatiky (dnes Ministerstva vnitra). V současné době jsou v Česku tři akreditované společnosti, které výše uvedenou podmínku splňují:

- Česká pošta s.p., http://qca.postsignum.cz/
- e Identity, a.s., http://www.eidentity.cz
- První certifikační autorita, a.s., http://www.ica.cz

Podmínky pro získání kvalifikovaného certifikátu jsou u všech tří kvalifikovaných autorit v zásadě stejné, rozdílná je pouze cena pořízení kvalifikovaného certifikátu. Certifikát platí vždy jeden rok, a poté je ho třeba periodicky obnovovat, přičemž je nutné opakovaně hradit příslušný poplatek. Cena kvalifikovaných certifikátů není bohužel státem nijak regulovaná, je tedy u jednotlivých certifikačních autorit rozdílná.

Česká pošta s.p. (http://qca.postsignum.cz/)

- Doba platnosti 12 měsíců (365 dní)
- Použití 1024 nebo 2048 bitového kryptografického klíče
- Základní cena: 190,-Kč včetně DPH

e Identity, a.s. (http://www.eidentity.cz)

- Doba platnosti 12 měsíců (365 dní)

[30] Zákon č. 227/2000 Sb., o elektronickém podpisu ve znění pozdějších předpisů

- Použití 1024 bitového kryptografického klíče
- Základní cena: 470,-Kč včetně DPH

První certifikační autorita, a.s. (http://www.ica.cz)

- Doba platnosti 12 měsíců (365 dní)
- Použití 1024 bitového kryptografického klíče
- Základní cena: 495,-Kč včetně DPH

Každý kvalifikovaný certifikát má z bezpečnostních důvodů omezenou platnost (v našem případě 365 dní). Před skončením platnosti je nutné požádat o vydání nového kvalifikovaného certifikátu. Tento proces je podstatně jednodušší než proces vydání prvního kvalifikovaného certifikátu a nevyžaduje již nutně osobní návštěvu pracoviště certifikační autority. O prodloužení platnosti můžeme požádat e-mailem, který musíme podepsat, v té době ještě platným, certifikátem.

V případě prozrazení klíčů vlastníka certifikátu je nutné podat žádost o mimořádné zneplatnění certifikátu. Žádost o zneplatnění certifikátu podává zaměstnanec či OSVČ, které byl certifikát vydán. Zneplatnění se provádí na základě hesla pro zneplatnění, které se zadává do písemné žádosti o certifikát a nachází se také na protokolu o vydání certifikátu. Se znalostí hesla pro zneplatnění můžete požádat o zneplatnění certifikátu telefonicky nebo e-mailem. Zneplatnění certifikátu bez znalosti hesla je také možné, ale musíte se osobně dostavit na pracoviště certifikační autority.

Veškeré postupy tvorby žádosti o kvalifikovaný certifikát a jeho instalace jsou velice pěkně popsány na webových stránkách příslušných certifikačních autorit. Uvádím zde pouze několik hlavních problémů,se kterými jsem se setkal na různých setkáních spojených s problematikou bezpečné komunikace s orgány veřejné správy.

a) Při žádosti o certifikát je třeba definovat zákaznickou skupinu. Na základě této volby jsou nám následně žadateli předkládány příslušné formuláře, které jsou pro každou skupinu zákazníků mírně odlišné. Při rozhodování o příslušnosti k výše uvedeným skupinám je třeba tedy uvážit, co má být z kvalifikovaného certifikátu patrné, např. vazba zaměstnance na organizaci nebo vlastnictví IČO u osoby samostatně výdělečně činné. Z hlediska komunikace s veřejnou správou jsou

však všechny tři uvedené skupiny rovnocenné! Pozor! Z typu pořízeného kvalifikovaného certifikátu nelze v žádném případě usuzovat, jaké máme pověření k úkonům vůči orgánům veřejné správy. Tuto problematiku je nutno řešit přímo u odpovědného orgánu veřejné správy.

b) Bezvýznamný identifikátor Ministerstva práce a sociálních věcí (IK MPSV) je používán pro jednoznačnou identifikaci osoby, a nelze z něho vyčíst datum narození ani pohlaví. O zapsání tohoto údaje do kvalifikovaného certifikátu však musíme speciálně akreditovanou certifikační autoritu požádat. Pokud tento údaj v žádosti nezaškrtneme, IK MPSV nám nebude do certifikátu uveden! *Takovýto certifikát však nemůžeme použít při komunikaci s orgány veřejné správy*.

V případě, že chceme elektronicky komunikovat s veřejnou správou, je nutné dodržovat tyto zásady:

- počítač nevystavovat žádným experimentům, omezit stahování informací z nedůvěryhodných zdrojů
- mít instalován antivirový program, v lepším případě instalovat na PC firewal
- provozovat pouze legálně zakoupenou kopii operačního systému Windows
- provádět pravidelné aktualizace systému, případně využívat WSUS
- vzhledem k rychlému stárnutí počítačové techniky pravidelně investovat do obnovy hardware i software počítače
- mít vystaven kvalifikovaný certifikát u akreditované certifikační autority, přičemž v žádosti je třeba výslovně uvést, aby náš zaručený elektronický podpis obsahoval IK MPSV.

V zásadě se dá říci, že bez vlastnictví kvalifikovaného certifikátu je nutné podání provedené elektronicky vždy následně potvrdit osobní návštěvou příslušného orgánu veřejné správy. Efektivita takového úkonu je tedy velice nízká, tento způsob komunikace je možné využít například pro dodržení termínů pro různá podání. Stanovený termín vůči veřejnému orgánu tedy dodržíme, ale příslušnou instituci musíme následně ještě osobně navštívit, abychom potvrdili, že jsme úkon vůči orgánu veřejné správy provedli opravdu my a nikdo jiný.

5.2 Možnosti zabezpečené komunikace mezi orgány veřejné správy

V současné době máme k dispozici několik způsobů elektronické komunikace, přičemž předpokládáme, že uživatel splňuje podmínky, které jsme definovali v předchozí kapitole.

5.2.1 Zaslání datové zprávy na elektronickou adresu podatelny

Ze zákona o elektronickém podpisu[31] je zřejmé, že orgán veřejné moci by měl mít pro příjem a odesílání datové zprávy elektronickou podatelnu. Podrobné informace přináší Vyhláška o elektronických podatelnách[32], kde je v §2 definováno Přijetí a doručení datové zprávy: *Nestanoví-li tato vyhláška jinak, je přijatá datová zpráva považována za doručenou orgánu veřejné moci, pokud je dostupná elektronické podatelně provozované podle zvláštního právního předpisu (* Vyhláška č. 496/2004 Sb.).

Zvláštní předpis nás odkazuje na Nařízení vlády[33], kde nacházíme v § 1 další informace k elektronickým podatelnám - *Orgány veřejné moci provozují jednu nebo více elektronických podatelen; to se považuje za splněné rovněž v případě, kdy orgán veřejné moci dohodne s jiným orgánem veřejné moci, že bude přijímat a odesílat datové zprávy prostřednictvím jím provozované elektronické podatelny (*Nařízení vlády č. 495/2004 Sb.).

Z výše uvedeného je zřejmé, že každý orgán veřejné správy musí mít veřejně dostupnou podatelnu, bohužel, většina těchto podatelen orgánů není vybavena odpovídajícím technickým zařízením, které by umožňovalo vystavení časového razítka k došlé datové zprávě. Není tedy možné hodnověrným způsobem dokázat, v kterém časovém okamžiku datová zpráva dorazila na podatelnu příslušného úřadu. Podatelny nejsou také schopny plnit nároky Spisového a skartačního řádu, vznikají problémy s dlouhodobým ukládáním datových zpráv, které jsou opatřené zaručeným elektronickým podpisem (elektronickou značkou). Veškerá úřední elektronická

[31] Zákon č. 227/2000 Sb., o elektronickém podpisu ve znění pozdějších předpisů

[32] Vyhláška č. 496/2004 Sb., o elektronických podatelnách

[33] Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon o elektronickém podpisu

komunikace by měla probíhat přes veřejně přístupné podatelny, zasílání datových zpráv přímo na úředníky veřejné zprávy je legislativně a často i technicky nemožné.

5.2.2 Zasílání datových správ na portály orgánů veřejné správy

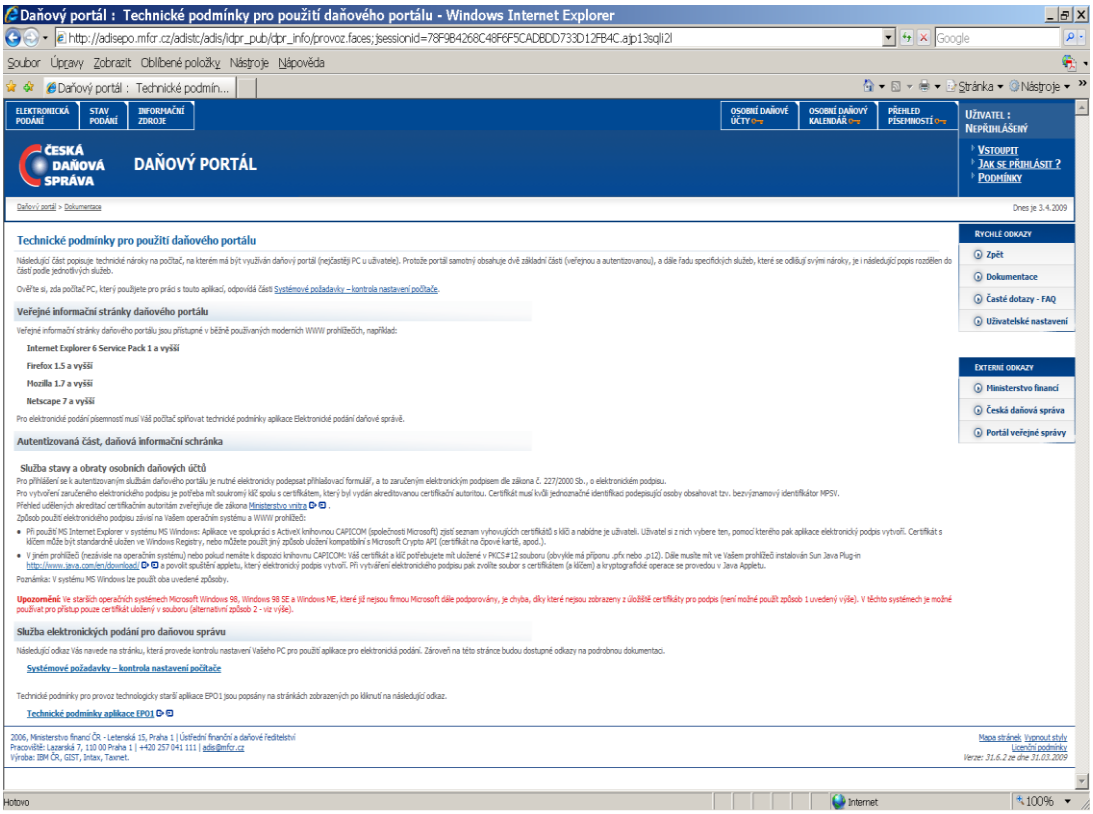
Některé orgány veřejné správy řešily špatnou situaci v technickém zabezpečení jednotlivých podatelen vytvořením vlastních portálů s jednotnou rezortní podatelnou. Tyto portály umožňují nejen plnou obousměrnou komunikaci, ale centrální podatelna umožňuje reagovat na podání zasláním doručenky s přesným údajem o čase podání a navíc datovou zprávu uloží do archivu v souladu se Spisovým a skartačním řádem.

Jako příklad použiji Portál České daňové správy, kde mají daňové subjekty možnost podat elektronicky daňové přiznání, zjišťovat důležité informace spojené s daňovým řízením a samozřejmě posílat datové zprávy, které jsou následně směrovány místně příslušnému správci daně. Směrování veškeré elektronické komunikace na jednotné zařízení správce daně je upraveno metodickým pokynem[34], kde jsme informováni, že doručit datovou zprávu opatřenou zaručeným elektronickým podpisem (ZAREP) lze pouze na adresu společného technického zařízení správce daně, které je pro ČDS elektronickou podatelnou ve smyslu Vyhlášky o elektronických podatelnách a je zveřejněna na úřední desce. Pouze tato podatelna dokáže tuto zprávu správně zpracovat a přiložit k ní nezpochybnitelný údaj o čase doručení (časové razítko).

Bohužel, ani komunikace s portály veřejné správy není zcela bez problémů. Každý portál předpokládá určitá specifická nastavení klientského, která musíme na stánkách příslušného úřadu veřejné správy nastudovat a funkčnost otestovat.

Podívejme se například na portál daňové správy, kde je umístěna internetová aplikace EPO – Daňová přiznání elektronicky (http://cds.mfcr.cz).

[34] Pokyn č. D-252 Ministerstva financí České republiky



Obrázek 11 - Portál České daňové správy

Již na úvodní stránce jsme upozorněni, že pokud neprovádíme pravidelně Windows Update, konkrétně aktualizaci kořenových certifikátů, aplikace nám pravděpodobně nebude fungovat správně. Opět platí, že všechny potřebné informace jsou vždy na příslušných internetových stránkách k dispozici, problém však je dané informace vyhledat a správně aplikovat. Informace o nutnosti instalace certifikátů jsou v tomto případě přímo na úvodní stránce aplikace EPO. Aplikace EPO však umožňuje klientům provést kontrolu programového vybavení počítače, takže problémy se spouštěním aplikace se omezí na minimum. Přesto však není spuštění aplikace EPO zcela jednoduchá a bez problémů.

Vlastní příprava počítače pro zabezpečenou obousměrnou elektronickou komunikaci s portály veřejné správy je časově i technicky věc poměrně náročná, ale získáváme tak nástroj, který nám umožní provádět úkony v rámci e-Governmentu rychle, efektivně mimo pracovní dobu a bez dalších poplatků.

5.2.3 Zasílání datových zpráv prostřednictvím datových schránek

Komunikace prostřednictvím datové schránky přenese několik zásadních výhod. Odpadne poměrně složité nastavování klientského PC, které je nutné pro správnou funkčnost portálů veřejné správy. K vlastnímu přihlášení do datové schránky nepotřebuje uživatel vlastnit kvalifikovaný certifikát, stačí znalost přihlašovacího identifikátoru a hesla. Zaručený podpis je nutné použít pouze v případech, kdy je nutné zaslat dokument opatřený ověřeným podpisem vlastníka. Dokument opatřený takovýmto elektronickým podpisem si potom adresát může dát případně zkonvertovat zpět do listinné podoby. Konverze se však provádí pouze na kontaktních místech veřejné správy (Czech POINT), kde je možno dokumenty za poplatek vytisknout nebo naopak převést do datové zprávy.

Abychom však mohli komunikovat prostřednictvím datové schránky, musíme si nejdříve tuto schránku zřídit, přičemž:

- Datová schránka je povinná pro právnické osoby zřízené zákonem, orgány veřejné moci a pro právnické osoby zapsané v obchodním rejstříku. Ostatní osoby mohou datovou schránku dobrovolně bezplatně získat na základě žádosti. Samotná aktivace schránky je zdarma
- Vyplněnou žádost je možno donést osobně na kontaktní místo veřejné správy (Czech POINT), nebo zaslat elektronickou poštou. Zde je samozřejmě nutné přiložit platný kvalifikovaný elektronický podpis.

Datová schránka slouží pouze k přijímání a posílání úředních (elektronických) dopisů mezi vlastníkem schránky a orgány veřejné moci. Nejedná se tedy o email! Do e-mailové schránky je možné zasílat pouze oznámení, že v datové schránce je nová datová zpráva.

Jak tedy bude probíhat komunikace prostřednictvím datové schránky?

Nejdříve bude nutné vybrat adresáta, kterému je datová zpráva určena. Nebude existovat žádný oficiální seznam datových schránek, systém ale při zadávání adresáta on-line zjistí, zda příslušná osoba má datovou schránku. Pokud adresát nemá v daném okamžiku datovou schránku zřízenu, dokument bude nutno vytisknout a odeslat normální poštou. Tímto způsoben se z velké části odbourá papírová korespondence

a v důsledku institutu doručení zásilky fikcí, kdy až na výjimky každá zásilka dodaná do datové schránky je po stanovené lhůtě považována za doručenou do vlastních rukou, se výrazně urychlí jednotlivá řízení.

Je však zřejmé, že na úřadech dojde postupně k velkému nárůstu elektronických dokumentů – originálů, ke kterým neexistuje papírová předloha. Tyto dokumenty bude potřeba uchovávat v souladu se spisovým a skartačním řádem, přičemž musí být zachována jejich jednoznačnost a právní prokazatelnost. Datové schránky nefungují jako úložiště, zprávy jsou po 90 dnech po doručení vymazány. Bude tedy nutné zavést na úřadech elektronickou spisovou službu, která bude komplexně zajišťovat komunikaci s Informačním systémem datových schránek (ISDS), bude podporovat konverzi dokumentů a umožní práci s elektronickými podpisy a časovými razítky.

Dále je třeba si uvědomit, že elektronická spisová služba „udrží“ dokument maximálně do doby skartačního řízení, ale potom již musí být uložen někde jinde, to znamená, že je třeba ho archivovat. A opět musíme zajistit jeho právní a ekonomickou validitu, protože dokument nebude mít papírový ekvivalent. Znamená to tedy vytvořit elektronické spisovny, které budou schopny zabezpečit služby pro střednědobé uložení dokumentů. Vzhledem k tomu, že každý právnický subjekt bude mít pouze jednu schránku, bude nutno zajistit také vnitřní třídění a rozesílání dokumentů na podřízené organizační jednotky. To nebude jednoduché, obzvláště v případech, kdy zprávy nebudou adresovány konkrétní osobě čo odboru, ale budou zasílány na základě určitého zákona či pouze s číslem jednacím. Takové datové zprávy bude nutno nejdříve otevřít a teprve podle obsahu předat příslušnému úředníkovi ke zpracování.

5.3 Informační systémy v procesu e-Governmentu

E-Government je ve své podstatě chápán jako zrychlení a zefektivnění komunikace občanů, podnikatelských subjektů a neziskových organizací s orgány veřejné správy, tj. samosprávy i státní správy. Hlavní úlohu mají v tomto procesu informační systémy, které se významně podílejí na budování a zabezpečení veřejné správy především v těchto oblastech:

- Komunikace s veřejností

- Komunikace mezi úřady veřejné správy

5.3.1 Komunikace s veřejností

Orgány veřejné správy i samosprávy poskytují dnes více či méně úspěšně informace na svých webovských stránkách. Zveřejňují základní informace o úřadu, informace o historii i současnosti města, o rozhodnutích samosprávy, případně fungují jako zpravodajský servis o kultuře, sportu, podnikatelských subjektech, ubytování atd. Nezřídka navíc přinášejí návody, jak komunikovat s úřadem, či jak postupovat v úředních záležitostech. Výhody jsou zřejmé, je možno získat velké množství informací, které jsou často aktualizovány a archivovány. Bezpečnostní rizika naopak přináší velké množství webových stránek a tedy i velké množství datových zdrojů. Informace jsou často nepřehledné, orientace pro občana je složitá a hlavně, zatím je tato komunikace většinou pouze jednosměrná od veřejné správy k občanovi. Obousměrnou komunikaci dnes poskytují pouze některé portály veřejné správy, například Portál České daňové správy Ministertva financí České republiky. Ovšem u úkonů, které jsou na magistrátech a městských úřadech nejčastější (např. vyřizování občanských průkazů, cestovních pasů, řidičských průkazů, evidence vozidel, stavební povolení a ohlašování staveb, sociální dávky), tuto variantu občané zatím nemají.

Celá oblast komunikace s veřejností je klíčovou úlohou veřejné správy. Úspěšně zvládnutá a efektivní komunikace představuje nezbytný předpoklad úspěšné veřejné správy. V současné době se intenzivně rozšiřuje spektrum služeb, které se budou moci nabídnout občanům. Pro využití moderních technologií se nabízí celá řada oblastí, které řeší především velká města – např. systémy veřejné dopravy, parkovací systémy, knihovny, návštěvy divadel, muzeí, dalších kulturních a sportovních zařízení. Právě takovéto projekty, pracovně označené jako e-city, jsou vhodným místem pro spolupráci samosprávy a podnikatelských subjektů.

5.3.2 Komunikace mezi úřady veřejné správy

Je zřejmé, že bez kvalitního informačního systému v podstatě nelze úspěšně řešit úkoly samosprávy či veřejné správy. Je třeba si navzájem předávat mnohem více

informací a zkušeností o jednotlivých platformách či aplikacích, a to jak pozitivních tak i negativních. Jen tak se podaří vyřešit problémy, které řeší jednotlivá města v oblasti informačních technologií.

Například velké mezery doposud existují v oblasti komunikace mezi úřady veřejné správy. Veřejná správa v podstatě ví o občanech vše, ale stále dokola je nutí, aby dodávali pro jejich rozhodnutí stanoviska a potvrzení jiných úřadů. Dnes místo informací a dokumentů obíhá občan či podnikatel, ale cílový stav musí být opačný. Současný vývoj e-Governmentu, který předchází zásadní politická rozhodnutí, však uvedené problémy již bude schopen řešit.

6 Závěr

Bezpečnost dat a elektronické komunikace v rámci e-Governmentu s sebou přináší mnoho problémů, o kterých je třeba diskutovat a následně je řešit. Problémy spojené s tématem bezpečnosti, používání čipových karet, či elektronické komunikace a používání datových schránek, jsou shrnuty v následující závěrečné části diplomové práce.

Úroveň zabezpečení dat a elektronické komunikace v rámci jednotlivých orgánů státní správy se neustále zvyšuje, probíhá proces centralizace a vizualizace výpočetních systémů, výrazně se redukuje počet serverů na jednotlivých úřadech státní správy a naopak se posiluje kapacita linek, aby bylo možné sdílené aplikace provozovat po síti. Uvažuje se dokonce o výrazné redukci počtu úřadů státní správy. Tato opatření jsou spojená s postupnou centralizací databází a tvorbou jednotných datových skladů. Centralizací se podstatně snižují nároky na administraci, snižuje se počet redundantních a duplicitních dat, ale úměrně s tím se podstatně zvyšují nároky na zabezpečení, protože pokud by v takovém případě došlo k bezpečnostnímu incidentu, bude rozsah škod úměrně vyšší.

S nastupující centralizací státní správy bylo nutno zpřísnit nároky na zabezpečení dat, přičemž navrhovaný standard využívá metod asymetrické kryptografie. K zajištění požadované úrovně bezpečnosti bylo nutné nejdříve v jednotlivých rezortech státní správy aktualizovat výpočetní systémy takovým způsobem, aby umožňovaly používat kvalifikované zaměstnanecké certifikáty jak pro autentizaci uživatelů, tak pro zajištění bezpečnosti uložených dat. Jako bezpečné úložiště zaměstnaneckých certifikátů byly následně zvoleny čipové karty, které se staly všeobecně používaným bezpečnostním standardem a využívají se dnes pro přihlašování do interních systémů státní správy a samozřejmě také k zabezpečené elektronické komunikaci v rámci e-Governmentu. Čipové karty jsou také často provázány s dalšími podpůrnými systémy, které se v jednotlivých rezortech státní správy využívají. Jedná se například o elektronické docházkové či stravovací systémy, systémy požární ochrany, případně zabezpečovací

systémy, které ke své identifikaci využívají pouze vnitřní (bezkontaktní) čísla čipových karet a vlastní uživatelský certifikát, který je uložen v kontaktní části karty (čipu), ke své činnosti nepotřebují.

Čipové karty však mají poměrně krátkou životnost a výrobci vyvíjejí neustále nové typy karet, bohužel bez zpětné kompatibility s původními čtecími zařízeními. Je tedy nutné neustále investovat do nových typů těchto zařízení; například za posledních pět let provozování čipových karet v rezortu Ministerstva financí České republiky bylo nutno již 3krát tyto karty a příslušná čtecí zařízení obměnit právě v souvislosti s ukončením výroby starých karet a nekompatibilitou nových čipových karet s původním čtecím zařízením. Přitom náklady na jednu čipovou kartu s integrovaným čipem činí cca 1200,-Kč na zaměstnance a jedno čtecí zařízení okolo 8000,-Kč! Docházkové terminály jsou samozřejmě finančně ještě nákladnější. Na základě těchto zjištění by bylo jistě vhodnější využívat čipové karty pouze v souvislosti s autentifikací a bezpečnou komunikací uživatelů a pro ověřování přístupu k podpůrným systémům státní správy využívat například identifikace založené na biometrice. Pořizovací náklady takovýchto čtecích zařízení jsou sice o něco vyšší, kolem 25000,-Kč na jedno čtecí zařízení, ale vzhledem k tomu, že biometrické znaky zaměstnance se v čase nemění, ušetřily by se ve výsledku náklady na hardware, software a také na administrativu spojenou s instalací nových zařízení.

Problém s kompatibilitou čipových karet je patrný i v souvislosti s novelou zákona o občanských průkazech, která přináší možnost pořízení elektronického občanského průkazu s čipem, na který si vlastník může uložit kvalifikovaný certifikát. Tato varianta e-OP je za poplatek 500,-Kč. Využitelnost tohoto řešení je však podle dostupných informací poměrně malá, certifikát uložený na e-OP bude možno samozřejmě přečíst na preferovaných místech Czech Pointu (asistované místo výkonu veřejné správy), ale všude jinde bude uživatel muset mít k počítači připojenu speciální čtečku elektronického občanského průkazu.

Zcela nové možnosti a formy elektronické komunikace vůči orgánům veřejné moci přináší schválení zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Obrovské zjednodušení tento zákon rozhodně přinese v oblasti doručování. Při doručení do datové schránky bude dokument označen časovým

razítkem, čímž bude jasně definován okamžik doručení. Tato informace je velice důležitá a často rozhodující pro určení dalšího postupu při vyřizování doručené a na ní navazujících písemností. Údaj časového razítka souvisí úzce s fikcí doručení, která je pevně stanovena na 10 dnů. Orgánům veřejné správy tato zákonná úprava zcela jistě usnadní řešení problémů, které dosud vznikají v souvislosti s často nesnadným doručováním úředních dokumentů. Na druhou stranu, fyzické podnikající osoby, budou z výše uvedeného důvodu zřízení schránky důkladně zvažovat, a to i v případě, že zřízení i provoz datové schránky je s výjimkou orgánů veřejné moci zdarma.

Zavádění datových schránek však s sebou přineslo i řadu nejasností, které se nepodařilo zatím zcela odstranit. Vzhledem k tomu, že k datu odevzdání diplomové práce nebyly zatím zveřejněny prováděcí vyhlášky k zákonu, není zcela jasné, jak a zda vůbec budou s datovými schránkami provázány portálové aplikace, které v současnosti umožňují občanům obousměrnou elektronickou komunikaci s orgány státní správy.

Například využívání aplikace EPO, která je provozovaná ministerstvem financí, bude po zavedení datových schránek výrazně omezeno. Přitom aplikace „elektronické daňové přiznání“ je uživatelsky přívětivě zpracovaná webová aplikace, která umožňuje elektronickou komunikaci daňových subjektů se správci daně. Vývoj této aplikace byl zcela jistě finančně i organizačně náročný a díky ní může dnes daňový poplatník s využitím kvalifikovaného certifikátu podat daňové přiznání bez nutnosti návštěvy finančního úřadu.

Se schválením zákona č. 300/2008 Sb. a zákona č. 301/2008 Sb. bude samozřejmě možno využívat datové schránky pro podávání daňových přiznání, v tomto případě se však poplatník, podle současného výkladu zákona, navíc nebude muset prokazovat svým zaručeným elektronickým podpisem. V datových schránkách není také zatím připravena žádná podpora pro vyplňování daňových přiznání; u aplikace EPO však veškeré finanční i logické kontroly prováděl za poplatníka program. Aplikace EPO má ještě jednu podstatnou výhodu (zejména pro správce daně) - veškeré datové zprávy, které poplatník zašle přes webovou aplikaci EPO, jsou ihned automaticky integrovány do systému ADIS (Automatizovaný daňový a informační systém). Datové schránky bohužel zatím nejsou s vnitřním systémem správce daně nijak svázány a hrozí tedy

nebezpečí, že daňová přiznání zaslaná elektronicky přes EPO, bude nutno správcem daně znovu pracně zadávat do aplikace ADIS na finančním úřadě.

Přihlašování do datových schránek bude probíhat pomocí jednoznačného identifikátoru a hesla (PINu). K autentizaci oprávněné osoby se tedy nebude využívat metod asymetrické kryptografie, což je zcela jistě určitý ústupek v úrovni bezpečnosti. Riziko spojené s tímto způsobem přihlašování ale pravděpodobně vyváží jednoduchost navrhovaného řešení a navíc toto řešení eliminuje problémy, které jsou s používáním kvalifikovaného certifikátu spojené (nutnost zakoupení kvalifikovaného certifikátu, pravidelná obnova, atd.).

Je všeobecně známým faktem, že se úřady státní správy po zavedení ustanovení zákona č. 300/2008 Sb., neobejdou bez kvalitní spisové služby, která musí být provázána na ISDS. Je třeba se vyvarovat situace, kdy mezi datovými schránkami sice bude komunikace probíhat elektronicky, ale dokumenty budou následně u adresáta - orgánu státní správy vytištěny a uvnitř úřadu již budou postupovat standardně ve své listinné podobě. Aby elektronická komunikace byla opravdu efektivní, musí probíhat elektronicky v celém svém rozsahu, zasílaná datová zpráva by tedy měla dorazit ve své elektronické formě až ke svému finálnímu příjemci, tzn. ke konkrétnímu pracovníkovi státní správy. Je opravdu nutné omezit provoz listinných dokumentů uvnitř úřadů veřejné správy, protože každá konverze dokumentu je na úkor efektivity a představuje práci navíc. Pro ověření původnosti elektronického dokumentu se předpokládá využití zaručeného elektronického podpisu, přičemž kvalifikovaný certifikát a soukromý klíč zaměstnance je uložen na čipové kartě příslušného pracovníka.

Diplomová práce „Rozvoj e-Governmentu typu G2G“ se svým zaměřením snaží najít odpovědi na otázky, které odrážejí hlavní cíle práce definované v úvodu:

Jaká je úroveň a možnosti využívání kvalifikovaných certifikátů ve státní správě?

Na základě údajů, které byly získány studiem dostupných informačních zdrojů, a které vyplívají z praktických poznatků o bezpečnosti, je zřejmé, že kvalifikované certifikáty se dnes využívají prakticky v celé státní správě. Jednotlivé orgány státní správy však zatím nevyužívají stejné úložiště certifikátů, nejčastěji se však používá

čipová karta Smart Card. Výhodou tohoto řešení je dostatečná mobilita, ke kartě však uživatel potřebuje také čtečku čipových karet. Nevýhodou je poměrně nízká životnost čipových karet a problémy se zpětnou kompatabilitou ve vazbě na používaná čtecí zařízení. Druhým nejčastějším způsobem je ukládání certifikátů a soukromých klíčů na lokální disk uživatele. Tato varianta je sice výrazně levnější, pro širší nasazení ve státní správě je však nevhodná. Využívání certifikátů je v tomto případě omezeno pouze na počítač uživatele a není tedy možné efektivně provádět centrální správu počítačů.

Pracovníkovi státní správy kvalifikovaný certifikát umožňuje tedy nejen bezpečnou autentifikaci do interních systémů, ale umožňuje mu také jednoznačně identifikovat zasílaný elektronický dokument, což je důležité zejména v dnešní době, kdy se v souvislosti se zákonem č. 300/2008 Sb., zavádí povinná elektronická komunikace pro orgány veřejné moci a listinná forma komunikace se tím v blízké době výrazně omezí.

Jaké jsou hlavní změny v elektronické komunikaci v souvislosti s přijetím zákona č. 300/2008 Sb.?

Orgány veřejné moci budou ze zákona povinny od 1.7.2009 využívat k elektronické komunikaci datové schránky, a to jak mezi sebou navzájem, tak ke komunikaci s právnickými či fyzickými osobami, které mají datové schránky zřízeny. Další výraznou změnu přináší zavedení autorizované konverze dokumentů, neboli převod dokumentů z listinné podoby do podoby elektronické (a naopak) spojený s ověřením shody vstupu a výstupu a připojením ověřovací doložky. Důležitá je ta skutečnost, že výstup z autorizované konverze, má stejné právní účinky jako běžně ověřená kopie listinného dokumentu, což je pro rozvoj e-Governmentu věc zcela zásadního významu. Na základě studia dostupné literatury a hlavně mých osobních zkušeností z pilotního provozu datových schránek, se objevily i některé problémy, na jejichž odstranění se průběžně pracuje. Aby elektronická veřejná správa byla opravdu efektivní, je nutná intenzivnější spolupráce všech složek státní správy, bude nutné provázat dnes fungující webové aplikace jednotlivých rezortů státní správy se systémem datových schránek nebo se minimálně snažit využít těch modulů, které se již v praxi osvědčily a jejichž zrušení by efektivitu e-Governmentu mohlo spíše poškodit.

7 Seznam použité literatury

7.1 Publikace

- MICROSOFT Windows Server Team, členové Microsoft MVP a partneři. *Microsoft Windows Server 2003 : Resource Kit*. Přel. Kocan Marek, Kocanová Pavla. 1. vyd. Praha : Computer Press, 2004. 4624 s. ISBN 80-7226-951-2.
- DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP*: Bezpečnost. 2. aktualiz. vyd. Praha : Computer Press, 2003. 571 s. ISBN 80-7226-849-X.
- HATCH, Brian , LEE, James , KURTZ, George . *Hacking bez tajemství: Linux* . Přel. Kocan Marek, Kocanová Pavla. 1. vyd. Praha : Computer Press, 2000. 660 s. ISBN 8072268694.
- MATES, Pavel, SMEJKAL, Vladimír. *E-Government v českém právu*. 1. vyd. Praha : Linde, 2006. 244 s. Praktické právnické příručky. ISBN 80-7201-614-8.
- DOSEDĚL Tomáš, *Počítačová bezpečnost a ochrana dat*. 1. vyd. Praha: Computer Press, 2004, 200 s. ISBN 80-251-0106-1
- DOSTÁLEK Libor, Vohnoutová Marta, *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu* 1. vyd. Praha: Computet Press, 2006, 535 s. ISBN 80-251-0828-7
- Štědroň Bohumír, *Úvod do e-Governmentu-právní a technický průvodce* 1. vyd. Praha: Úřad vlády ČR, 2007, 213 s. ISSN 1212-5075

7.2 Právní předpisy

- Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu
- Pokyn č. D-252 Ministerstva financí České republiky, č.j. 471/14664/2003
- Zákon č. 40/1964 Sb., Občanský zákoník, ve znění pozdějších předpisů
- Zákon č. 99/1963 Sb., Občanský soudní řád, ve znění pozdějších předpisů
- Zákon č. 141/1961 Sb., Trestní řád, ve znění pozdějších předpisů
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů

- Zákon č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- Zákon č.486/2004 Sb. (227/2000 Sb.) Úplné znění zákona č.227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn.
- Vyhláška č.366/2001 Sb., k Zákonu o elektronickém podpisu. č.227/2000 Sb. - Vyhláška Úřadu pro ochranu osobních údajů ze dne 3. října 2001 o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu).
- 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. (dne 13.2.2009 jej ve třetím čtení schválila Poslanecká sněmovna Parlamentu ČR)
- Vyhláška č. 496/2004 Sb. o elektronických podatelnách
- Zákon 480/2008 Sb., kterým se mění zákon č. 274/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o Policii České republiky, zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu), ve znění pozdějších předpisů, a zákon č. 141/1961 Sb., o trestním řízení soudním (Trestní řád), ve znění pozdějších předpisů
- Zákon č.300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č.301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů

7.3 Internetové zdroje

- **Bezpečné šifrování**, ze dne 19.11.2008

  T-Soft, Informační systémy na zakázku

  Přístup z Internetu: URL: http: //www.cryptosafe.cz

- **Elektronická podání,** citace 20.1.2009
  Česká daňová správa, Praha, Ministerstvo financí České republiky

  Přístup z Internetu: URL: http: //cds.mfcr.cz

- **Bilanční dokument,** citace 14.1.2008
  eStat, Efektivní stát

  Přístup z Internetu: URL: www.eStat.cz

- **PostSignum QCA,** citace 15.1.2009
  Praha, Česká pošta,
  Přístup z Internetu: URL: http://postsignum.cz
- E-Government, citace 6.9.2008
  Professional Computing
  Přístup z Internetu: URL: www.procomputing.cz
- **Hašovací funkce, principy, příklady a kolize**
  Vlastimil Klíma, citace 19.12.2008
  Přístup z Internetu: URL: http://www.cryptofest.cz
- **Karty a čtečky**, citace 12. 12. 2008
  Čipové karty Crypto Plus
  Přístup z Internetu: URL: http: //www.cryptoplus.cz
- **Karty Smart Card,** citace 21.1.2008

  Microsoft TechNet, Česká republika,
  Přístup z Internetu: URL: http://www.microsoft.com/technet

- **Problematika bezpečnosti**, citace 30.8.2008

  Svět sítí, Praha

  Přístup z Internetu: URL: http://www.svetsiti.cz

Bibliografické citace byly zpracovány podle citační normy ČSN ISO 690 (010197) Bibliografické citace. Obsah, forma a struktura a dále podle materiálů Studijního a informačního centra České zemědělské univerzity v Praze.

8 Přílohy

8.1 Příloha č. 1 – seznam obrázků

8.2 Příloha č. 2 - zákon č. 227/2000 Sb.: znění § 11- - § 15

§ 11

V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

§ 12

Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,
b) obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,
c) jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,
d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,
e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,
f) zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,
g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,
h) počátek a konec platnosti kvalifikovaného certifikátu,

i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,

j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(2) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

§ 13
Povinnosti akreditovaného poskytovatele certifikačních služeb při ukončení činnosti

(1) Akreditovaný poskytovatel certifikačních služeb musí záměr ukončit svou činnost ohlásit Úřadu nejméně 3 měsíce před plánovaným datem ukončení činnosti a musí vynaložit veškeré možné úsilí na to, aby platné kvalifikované certifikáty byly převzaty jiným akreditovaným poskytovatelem certifikačních služeb. Akreditovaný poskytovatel certifikačních služeb dále musí prokazatelně informovat každou podepisující osobu, které poskytuje své certifikační služby, o svém záměru ukončit svoji činnost nejméně 2 měsíce předem.

(2) Nemůže-li akreditovaný poskytovatel certifikačních služeb zajistit, aby platné kvalifikované certifikáty převzal jiný akreditovaný poskytovatel certifikačních služeb, je povinen na to včas Úřad upozornit. V takovém případě Úřad převezme evidenci vydaných kvalifikovaných certifikátů a oznámí to dotčeným podepisujícím osobám.

(3) Ustanovení odstavců 1 a 2 se použijí přiměřeně také v případě, když akreditovaný poskytovatel certifikačních služeb zanikne, zemře nebo přestane vykonávat svoji činnost, aniž splní ohlašovací povinnost podle odstavce 1.

§ 14
Opatření k nápravě

(1) Zjistí-li Úřad, že akreditovaný poskytovatel certifikačních služeb nebo poskytovatel certifikačních služeb vydávající kvalifikované certifikáty porušuje povinnosti stanovené tímto zákonem, uloží mu, aby ve stanovené lhůtě sjednal nápravu, a případně určí, jaká opatření k odstranění nedostatků je tento poskytovatel certifikačních služeb povinen přijmout.

(2) V případě, že se akreditovaný poskytovatel certifikačních služeb dopustí závažnějšího porušení povinností stanovených tímto zákonem nebo ve stanovené lhůtě neodstraní nedostatky zjištěné Úřadem, je Úřad oprávněn mu udělenou akreditaci odejmout.

(3) Rozhodne-li Úřad o odnětí akreditace, může ukončit současně platnost kvalifikovaných certifikátů vydaných poskytovatelem certifikačních služeb v době platnosti akreditace.

§ 15
Zrušení kvalifikovaného certifikátu

(1) Úřad může nařídit poskytovateli certifikačních služeb jako předběžné opatření[7)] zneplatnění kvalifikovaného certifikátu podepisující osoby, pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán, nebo pokud byl vydán na základě nepravdivých údajů. Nařízení o zneplatnění kvalifikovaného certifikátu může být vydáno také v případě, kdy bylo zjištěno, že podepisující osoba používá prostředek pro vytváření podpisu, který vykazuje bezpečnostní nedostatky, které by umožnily padělání zaručených elektronických podpisů nebo změnu podepisovaných údajů.

(2) Seznam certifikátů podle § 6 odst. 1 písm. g) musí obsahovat přesný časový údaj, od kdy byl certifikát zneplatněn. Zneplatněné certifikáty není povoleno opětovně zprovoznit a používat.

8.3 Příloha č. 3- zákon č. 300/2008 Sb.

ZÁKON č. 300/2008 Sb.
ze dne 17. července 2008
o elektronických úkonech a autorizované konverzi dokumentů

Parlament se usnesl na tomto zákoně České republiky:

§ 1
Předmět úpravy

(1) Tento zákon upravuje

a) elektronické úkony státních orgánů, orgánů územních samosprávných celků, Pozemkového fondu České republiky a jiných státních fondů, zdravotních pojišťoven, Českého rozhlasu, České televize, samosprávných komor zřízených zákonem, notářů a soudních exekutorů (dále jen „orgán veřejné moci“) vůči fyzickým osobám a právnickým osobám, elektronické úkony fyzických osob a právnických osob vůči orgánům veřejné moci a elektronické úkony mezi orgány veřejné moci navzájem prostřednictvím datových schránek,

b) informační systém datových schránek,

c) autorizovanou konverzi dokumentů[1)] (dále jen „konverze“).

(2) Tento zákon se nevztahuje na dokumenty, které obsahují utajované informace[2)].

§ 2
Datová schránka

(1) Datová schránka je elektronické úložiště, které je určeno k

a) doručování orgány veřejné moci,

b) provádění úkonů vůči orgánům veřejné moci.

(2) Datové schránky zřizuje a spravuje Ministerstvo vnitra (dále jen „ministerstvo“).

§ 3
Datová schránka fyzické osoby

(1) Datovou schránku fyzické osoby zřídí ministerstvo bezplatně na žádost fyzické osobě, která je plně způsobilá k právním úkonům, do 3 pracovních dnů ode dne podání žádosti.
(2) Fyzická osoba má nárok na zřízení jedné datové schránky fyzické osoby.
(3) Náležitosti žádosti o zřízení datové schránky fyzické osoby jsou

a) jméno, popřípadě jména, příjmení, jejich případné změny,

b) rodné příjmení,

c) den, měsíc a rok narození,

d) místo a okres narození; pokud se fyzická osoba narodila v cizině, místo narození a stát, na jehož území se narodila,

e) státní občanství, není-li fyzická osoba státním občanem České republiky.

(4) Žádost o zřízení datové schránky fyzické osoby musí obsahovat úředně ověřený podpis fyzické osoby.
(5) Splňuje-li žádost o zřízení datové schránky fyzické osoby požadavky stanovené v odstavcích 3 a 4, zřídí ministerstvo datovou schránku fyzické osoby, jinak fyzickou osobu po předchozí marné výzvě k odstranění nedostatků žádosti vyrozumí o tom, že datovou schránku fyzické osoby nelze zřídit. Má-li již fyzická osoba zřízenu datovou schránku fyzické osoby nebo není-li plně způsobilá k právním úkonům, ministerstvo ji vyrozumí, že datovou schránku fyzické osoby nelze zřídit.

§ 4
Datová schránka podnikající fyzické osoby

(1) Datovou schránku podnikající fyzické osoby zřídí ministerstvo bezplatně na žádost této osoby do 3 pracovních dnů ode dne podání žádosti.
(2) Podnikající fyzická osoba má nárok na zřízení jedné datové schránky podnikající fyzické osoby.
(3) Datovou schránku podnikající fyzické osoby zřídí ministerstvo bezplatně advokátu, daňovému poradci a insolvenčnímu správci bezodkladně poté, co obdrží informaci o jejich zapsání do zákonem stanovené evidence. Ustanovení odstavce 2 se použije pro advokáty, daňové poradce a insolvenční správce obdobně.

(4) Náležitosti žádosti o zřízení datové schránky podnikající fyzické osoby jsou

a) jméno, popřípadě jména, a příjmení, popřípadě obchodní firma,

b) rodné příjmení,

c) den, měsíc a rok narození,

d) místo a okres narození; pokud se podnikající fyzická osoba narodila v cizině, místo narození a stát, na jehož území se narodila,

e) státní občanství, není-li podnikající fyzická osoba státním občanem České republiky,

f) identifikační číslo ekonomického subjektu, bylo-li přiděleno,

g) místo podnikání, popřípadě sídlo.

(5) Žádost o zřízení datové schránky podnikající fyzické osoby musí obsahovat úředně ověřený podpis podnikající fyzické osoby.

(6) Splňuje-li žádost o zřízení datové schránky podnikající fyzické osoby požadavky stanovené v odstavcích 4 a 5, zřídí ministerstvo datovou schránku podnikající fyzické osoby, jinak podnikající fyzickou osobu po předchozí marné výzvě k odstranění nedostatků žádosti vyrozumí o tom, že datovou schránku podnikající fyzické osoby nelze zřídit. Má-li již podnikající fyzická osoba zřízenu datovou schránku podnikající fyzické osoby, ministerstvo ji vyrozumí, že datovou schránku podnikající fyzické osoby nelze zřídit.

§ 5
Datová schránka právnické osoby

(1) Datovou schránku právnické osoby zřídí ministerstvo bezplatně právnické osobě zřízené zákonem, právnické osobě zapsané v obchodním rejstříku a organizační složce podniku zahraniční právnické osoby zapsané v obchodním rejstříku, a to v případě právnické osoby zřízené zákonem bezodkladně po jejím vzniku, v případě právnické osoby zapsané v obchodním rejstříku a organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku bezodkladně poté, co obdrží informaci o jejím zapsání do obchodního rejstříku.

(2) Právnické osobě, která není uvedena v odstavci 1, zřídí ministerstvo datovou schránku právnické osoby bezplatně na žádost této osoby do 3 pracovních dnů ode dne podání žádosti.

(3) Právnická osoba má nárok na zřízení jedné datové schránky právnické osoby.

(4) Náležitosti žádosti o zřízení datové schránky právnické osoby jsou

a) název nebo obchodní firma,

b) identifikační číslo ekonomického subjektu, a nebylo-li přiděleno, registrační číslo, evidenční číslo nebo jiný obdobný údaj, byl-li přidělen,

c) adresa sídla,

d) jméno, popřípadě jména, příjmení, datum narození a adresa pobytu osoby oprávněné jednat jménem právnické osoby,

e) stát registrace nebo evidence právnické osoby.

(5) Žádost o zřízení datové schránky právnické osoby musí obsahovat úředně ověřený podpis osoby oprávněné jednat jménem právnické osoby.

(6) Splňuje-li žádost o zřízení datové schránky právnické osoby požadavky stanovené v odstavcích 4 a 5, zřídí ministerstvo datovou schránku právnické osoby, jinak právnickou osobu po předchozí marné výzvě k odstranění nedostatků žádosti vyrozumí o tom, že datovou schránku právnické osoby nelze zřídit. Má-li již právnická osoba zřízenu datovou schránku právnické osoby, ministerstvo ji vyrozumí, že datovou schránku právnické osoby nelze zřídit.

§ 6
Datová schránka orgánu veřejné moci

(1) Datovou schránku orgánu veřejné moci zřídí ministerstvo bezodkladně po jejich vzniku, v případě notářů a soudních exekutorů bezodkladně poté, co obdrží informaci o jejich zapsání do zákonem stanovené evidence.

(2) Orgánu veřejné moci se zřizuje pouze datová schránka orgánu veřejné moci.

(3) K identifikaci datové schránky orgánu veřejné moci slouží identifikátor datové schránky orgánu veřejné moci.

§ 7
Zvláštní ustanovení o datových schránkách orgánů územních samosprávných celků

(1) Pro orgány územního samosprávného celku se zřizuje jedna datová schránka orgánu veřejné moci.
(2) Pro orgány městské části hlavního města Prahy se zřizuje jedna datová schránka orgánu veřejné moci. Pro orgány městské části nebo městského obvodu územně členěného statutárního města se zřizuje jedna datová schránka orgánu veřejné moci.
(3) Pro účely tohoto zákona se za vedoucího orgánu veřejné moci považuje hejtman kraje, primátor hlavního města Prahy, starosta obce, starosta městské části hlavního města Prahy a starosta městské části nebo městského obvodu územně členěného statutárního města.

§ 8
Osoby oprávněné k přístupu do datové schránky

(1) K přístupu do datové schránky fyzické osoby je oprávněna fyzická osoba, pro niž byla datová schránka zřízena.
(2) K přístupu do datové schránky podnikající fyzické osoby je oprávněna podnikající fyzická osoba, pro niž byla datová schránka zřízena.
(3) K přístupu do datové schránky právnické osoby je oprávněn statutární orgán právnické osoby, člen statutárního orgánu právnické osoby nebo vedoucí organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro něž byla datová schránka zřízena.
(4) K přístupu do datové schránky orgánu veřejné moci je oprávněn vedoucí orgánu veřejné moci, pro něhož byla datová schránka zřízena.
(5) Není-li dále stanoveno jinak, pouze osoby uvedené v odstavcích 1 až 4 jsou oprávněny činit úkony uvedené v § 11 odst. 4 a 6. Rozsah přístupu osob uvedených v odstavcích 1 až 4 do datové schránky zahrnuje i přístup k dokumentům určeným do vlastních rukou adresáta.
(6) K přístupu do datové schránky je dále oprávněna pověřená osoba, kterou je

a) u datové schránky fyzické osoby a datové schránky podnikající fyzické osoby fyzická osoba pověřená osobou, pro niž byla datová schránka zřízena, a to v rozsahu jí stanoveném,
b) u datové schránky právnické osoby fyzická osoba pověřená statutárním orgánem právnické osoby nebo vedoucím organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro něž byla datová schránka zřízena, a to v rozsahu jimi stanoveném,
c) u datové schránky orgánu veřejné moci fyzická osoba určená vedoucím orgánu veřejné moci, pro který byla datová schránka zřízena, a to v rozsahu jím stanoveném.

(7) Osoby uvedené v odstavcích 1 až 4 mohou určit, že úkony, které jsou jim podle tohoto zákona vyhrazeny ve vztahu k pověřeným osobám a k ministerstvu, může činit fyzická osoba k tomu určená (dále jen „administrátor“).
(8) Pověřená osoba je oprávněna k přístupu k dokumentům určeným do vlastních rukou adresáta pouze, stanoví-li tak osoba uvedená v odstavcích 1 až 4 nebo administrátor.
(9) Osoby oprávněné k přístupu do datové schránky jsou povinny

a) využívat datovou schránku způsobem, který neohrožuje bezpečnost informačního systému datových schránek,
b) uvědomit neprodleně ministerstvo o tom, že hrozí nebezpečí zneužití datové schránky; pověřená osoba uvědomí rovněž toho, kdo ji určil pověřenou osobou.

§ 9
Přístupové údaje

(1) Osoba oprávněná k přístupu do datové schránky se do ní přihlašuje prostřednictvím přístupových údajů.
(2) Osoba oprávněná k přístupu do datové schránky je povinna zacházet s přístupovými údaji tak, aby nemohlo dojít k jejich zneužití.
(3) Přihlášení podle odstavce 1 zajišťuje ministerstvo prostřednictvím jím vydaných přístupových údajů nebo elektronických prostředků anebo prostřednictvím elektronických prostředků třetích osob. Náležitosti přístupových údajů a elektronické prostředky k přihlášení stanoví ministerstvo vyhláškou. Ustanovení o přístupových údajích se použijí obdobně i pro elektronické prostředky podle věty první.
(4) Ministerstvo stanoví vyhláškou technické podmínky a bezpečnostní zásady přístupu do datové schránky.

§ 10
Zpřístupnění datové schránky

(1) Ministerstvo zašle do vlastních rukou přístupové údaje k datové schránce osobě uvedené v § 8 odst. 1 až 4, případně administrátorovi, bezodkladně po zřízení datové schránky.
(2) Datová schránka je zpřístupněna prvním přihlášením osoby uvedené v § 8 odst. 1 až 4 nebo administrátora, nejpozději však patnáctým dnem po dni doručení přístupových údajů těmto osobám.
(3) Na žádost osoby uvedené v § 8 odst. 1 až 4 nebo administrátora zašle ministerstvo přístupové údaje k datové schránce pověřené osobě do vlastních rukou, případně administrátorovi, jinak se zasílají osobě uvedené v § 8 odst. 1 až 4.

§ 11
Znepřístupnění datové schránky

(1) Ministerstvo znepřístupní datovou schránku fyzické osoby a podnikající fyzické osoby, a to případně i zpětně, ke dni

a) úmrtí osoby, pro niž byla datová schránka zřízena,
b) uvedenému v rozhodnutí soudu o prohlášení za mrtvého jako den úmrtí této osoby,
c) nabytí právní moci rozhodnutí o zbavení nebo omezení způsobilosti této osoby k právním úkonům,
d) kdy byla tato osoba omezena na osobní svobodě z důvodu vzetí do vazby, výkonu trestu odnětí svobody, výkonu zabezpečovací detence, ochranného léčení nebo ochrany zdraví lidu.

(2) Ministerstvo znepřístupní datovou schránku podnikající fyzické osoby a právnické osoby, a to případně i zpětně, ke dni jejího výmazu ze zákonem stanovené evidence.
(3) Ministerstvo znepřístupní datovou schránku právnické osoby zřízené zákonem a datovou schránku orgánu veřejné moci dnem jejich zrušení, a jde-li o notáře nebo soudního exekutora, ke dni zániku funkce, a to případně i zpětně.
(4) Ministerstvo znepřístupní datovou schránku fyzické osoby, podnikající fyzické osoby a právnické osoby rovněž na žádost osoby, jíž byla datová schránka zřízena, nebo administrátora, jde-li o datovou schránku, kterou ministerstvo zřizuje na žádost.
(5) Datová schránka je znepřístupněna nejpozději třetím pracovním dnem následujícím po dni podání žádosti podle odstavce 4.
(6) Znepřístupněnou datovou schránku fyzické osoby, podnikající fyzické osoby nebo právnické osoby ministerstvo zpřístupní na žádost osoby, jíž byla datová schránka zřízena, nebo administrátora do 3 pracovních dnů od podání žádosti. Byla-li datová schránka na žádost znepřístupněna dvakrát za poslední rok, lze ji zpřístupnit nejdříve uplynutím 1 roku od jejího posledního znepřístupnění.

§ 12
Zneplatnění přístupových údajů

(1) Ministerstvo zneplatní přístupové údaje osoby oprávněné k přístupu do datové schránky neprodleně po jejím oznámení, zejména při ztrátě či odcizení přístupových údajů, a současně zašle této osobě do vlastních rukou nové přístupové údaje.
(2) Ministerstvo zneplatní přístupové údaje pověřené osobě v případě zrušení pověření podle § 8 odst. 6 neprodleně po oznámení osoby uvedené v § 8 odst. 1 až 4 nebo administrátora a o této skutečnosti informuje pověřenou osobu, jejíž údaje znepřístupnilo, i osobu, která o znepřístupnění požádala.
(3) Ministerstvo zneplatní přístupové údaje statutárnímu orgánu právnické osoby nebo jeho členu, přestane-li být statutárním orgánem právnické osoby nebo jeho členem, vedoucímu organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, přestane-li být vedoucím organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, a vedoucímu orgánu veřejné moci, přestane-li být vedoucím orgánu veřejné moci, neprodleně po oznámení této skutečnosti novým statutárním orgánem právnické osoby nebo jeho členem, novým vedoucím organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, novým vedoucím orgánu veřejné moci nebo administrátorem. Ministerstvo současně zašle novému statutárnímu orgánu právnické osoby nebo jeho členu, novému vedoucímu organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, novému vedoucímu orgánu veřejné moci, případně administrátorovi nové přístupové údaje do vlastních rukou.
(4) Jsou-li osobě oprávněné k přístupu do datové schránky zaslány přístupové údaje podle odstavce 1 opětovně během 3 let (dále jen „opětovné vydání přístupových údajů“), ministerstvo vybírá správní poplatek stanovený jiným právním předpisem[3)].

§ 13
Zrušení datové schránky

Ministerstvo zruší

a) datovou schránku fyzické osoby po uplynutí 3 let ode dne úmrtí fyzické osoby, případně dne, který je v rozhodnutí soudu o prohlášení za mrtvého uveden jako den úmrtí,

b) datovou schránku podnikající fyzické osoby po uplynutí 3 let ode dne výmazu podnikající fyzické osoby ze zákonem stanovené evidence,

c) datovou schránku právnické osoby po uplynutí 3 let ode dne zániku právnické osoby nebo organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, které nemají právního nástupce, případně ode dne jejich výmazu ze zákonem stanovené evidence,

d) datovou schránku orgánu veřejné moci po uplynutí 3 let ode dne po jeho zrušení.

§ 14
Informační systém datových schránek

(1) Informační systém datových schránek je informačním systémem veřejné správy[4)], který obsahuje informace o datových schránkách a jejich uživatelích.

(2) Správcem informačního systému datových schránek je ministerstvo. Provozovatelem informačního systému datových schránek je držitel poštovní licence. Odměna držiteli poštovní licence za provozování informačního systému datových schránek se stanoví podle cenových předpisů[5)].

(3) V informačním systému datových schránek se vedou tyto informace o datových schránkách:

a) identifikátor datové schránky (dále jen „identifikátor“),

b) datum zřízení, zpřístupnění, znepřístupnění a zrušení datové schránky s uvedením hodiny, minuty a sekundy,

c) datum přihlášení osoby oprávněné k přístupu do datové schránky do této datové schránky s uvedením hodiny, minuty a sekundy a údaj identifikující tuto osobu,

d) datum odeslání dokumentu nebo provedení úkonu z datové schránky s uvedením hodiny, minuty a sekundy a údaj identifikující osobu, která odeslání dokumentu nebo úkon provedla,

e) jméno, popřípadě jména, příjmení, datum a místo narození, adresa místa trvalého pobytu nebo jiného pobytu na území České republiky anebo adresa bydliště mimo území České republiky fyzické osoby, pro niž byla zřízena datová schránka,

f) jméno, popřípadě jména, a příjmení, popřípadě obchodní firma podnikající fyzické osoby, pro niž byla zřízena datová schránka, datum a místo jejího narození, adresa místa trvalého pobytu u občanů České republiky, místo, kde má povolení k pobytu nebo k trvalému pobytu v České republice, včetně uvedení adresy, a adresa bydliště v cizině, jde-li o cizince, adresa bydliště v členském státě Evropské unie, ve kterém je usazen, jde-li o státního příslušníka členského státu Evropské unie, který nemá povolení k pobytu nebo k trvalému pobytu v České republice, místo podnikání a identifikační číslo ekonomického subjektu, bylo-li přiděleno,

g) obchodní firma nebo název právnické osoby, pro niž byla zřízena datová schránka, sídlo a identifikační číslo ekonomického subjektu, bylo-li přiděleno,

h) název a sídlo organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro kterou byla zřízena datová schránka,

i) název orgánu veřejné moci, pro nějž byla zřízena datová schránka, sídlo a identifikační číslo ekonomického subjektu, bylo-li přiděleno,

j) jméno, popřípadě jména, příjmení, datum narození, adresa místa trvalého pobytu nebo jiného pobytu na území České republiky anebo adresa bydliště mimo území České republiky osoby oprávněné k přístupu do datové schránky, přístupové údaje, rozsah přístupu a datum vzniku a zániku oprávnění k přístupu do datové schránky s uvedením hodiny, minuty a sekundy,

k) jméno, popřípadě jména, příjmení, datum narození, adresa místa trvalého pobytu nebo jiného pobytu na území České republiky anebo adresa bydliště mimo území České republiky administrátora a datum vzniku a zániku určení administrátorem s uvedením hodiny, minuty a sekundy,

l) elektronická adresa nebo obdobný údaj pro vyrozumění o dodání datové zprávy do datové schránky, popřípadě kontaktní adresa, na niž má být adresátu doručováno; seznam kontaktních adres, u nichž

byl dán souhlas k jejich zveřejnění, vede ministerstvo způsobem umožňujícím dálkový přístup,

m) datum a čas událostí spojených s provozem informačního systému datových schránek.

(4) Údaje uvedené v odstavci 3 jsou neveřejné a nelze je poskytnout jiným osobám, s výjimkou kontaktní adresy, na niž má být adresátu doručováno, byl-li dán souhlas k jejímu zveřejnění. Ministerstvo umožní orgánům veřejné moci identifikovat datovou schránku tak, aby do ní mohlo být doručováno.

(5) Správce a provozovatel informačního systému datových schránek zajišťuje náležitá opatření v oblasti bezpečnosti informačního systému datových schránek.

(6) Správce ani provozovatel informačního systému datových schránek nejsou oprávněni k přístupu do datových schránek jiných subjektů.

§ 15
Využití informačního systému evidence obyvatel a součinnost

(1) Ministerstvo za účelem správy informačního systému datových schránek využívá tyto údaje vedené v informačním systému evidence obyvatel:

a) u státních občanů České republiky
   1. jméno, popřípadě jména, příjmení, případně jejich změna, rodné příjmení,
   2. datum narození,
   3. místo a okres narození; u občana, který se narodil v cizině, místo a stát, na jehož území se narodil,
   4. rodné číslo a jeho změny,
   5. adresa místa trvalého pobytu,
   6. zbavení nebo omezení způsobilosti k právním úkonům,
   7. datum úmrtí,
   8. den, který byl v rozhodnutí soudu o prohlášení za mrtvého uveden jako den úmrtí,

b) u cizinců, o nichž jsou vedeny údaje v informačním systému evidence obyvatel,
   1. jméno, popřípadě jména, příjmení, případně jejich změna, rodné příjmení,
   2. datum narození,
   3. místo a stát, na jehož území se narodil,
   4. rodné číslo a jeho změny,
   5. státní občanství,
   6. adresa místa pobytu,
   7. zbavení nebo omezení způsobilosti k právním úkonům,
   8. datum úmrtí,
   9. den, který byl v rozhodnutí soudu o prohlášení za mrtvého uveden jako den úmrtí.

(2) Ministerstvo spravedlnosti bezodkladně informuje ministerstvo o zápisu osoby do seznamu insolvenčních správců, o údajích vedených o osobě v seznamu insolvenčních správců nezbytně nutných pro zřízení datové schránky a jejich změnách a o výmazu osoby ze seznamu insolvenčních správců.

(3) Soud určený k vedení obchodního rejstříku bezodkladně informuje ministerstvo o zápisu právnické osoby nebo organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku do obchodního rejstříku, o údajích vedených o právnické osobě nebo organizační složce podniku zahraniční právnické osoby zapsané v obchodním rejstříku nezbytně nutných pro zřízení datové schránky, jejich statutárních orgánech a změnách těchto údajů a o výmazu právnické osoby nebo organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku z obchodního rejstříku.

(4) Česká advokátní komora bezodkladně informuje ministerstvo o zápisu osoby do seznamu advokátů, o údajích vedených o osobě v seznamu advokátů nezbytně nutných pro zřízení datové schránky a jejich změnách a o výmazu osoby ze seznamu advokátů.

(5) Notářská komora České republiky bezodkladně informuje ministerstvo o zápisu osoby do evidence notářů, o údajích vedených o osobě v evidenci notářů nezbytně nutných pro zřízení datové schránky a jejich změnách a o výmazu osoby z evidence notářů.
(6) Exekutorská komora České republiky bezodkladně informuje ministerstvo o zápisu osoby do seznamu soudních exekutorů, o údajích vedených o osobě v seznamu soudních exekutorů nezbytně nutných pro zřízení datové schránky a jejich změnách a o výmazu osoby ze seznamu soudních exekutorů.
(7) Komora daňových poradců České republiky bezodkladně informuje ministerstvo o zápisu osoby do seznamu daňových poradců, o údajích vedených o osobě v seznamu daňových poradců nezbytně nutných pro zřízení datové schránky a jejich změnách a o výmazu osoby ze seznamu daňových poradců.
(8) Správní orgán vedoucí evidenci podnikajících fyzických osob bezodkladně informuje ministerstvo o výmazu podnikající fyzické osoby z této evidence.

§ 16

Věznice nebo vazební věznice bezodkladně informuje ministerstvo o vzetí fyzické osoby do vazby nebo o nástupu fyzické osoby do výkonu trestu odnětí svobody. Detenční ústav bezodkladně informuje ministerstvo o nástupu fyzické osoby do výkonu zabezpečovací detence. Soud bezodkladně informuje ministerstvo o vykonatelném rozhodnutí, jímž se fyzická osoba omezuje na osobní svobodě z důvodu ochranného léčení nebo ochrany zdraví lidu.

§ 17

Doručování dokumentů orgánů veřejné moci prostřednictvím datové schránky

(1) Umožňuje-li to povaha dokumentu, orgán veřejné moci jej doručuje jinému orgánu veřejné moci prostřednictvím datové schránky, pokud se nedoručuje na místě. Umožňuje-li to povaha dokumentu a má-li fyzická osoba, podnikající fyzická osoba nebo právnická osoba zpřístupněnu svou datovou schránku, orgán veřejné moci doručuje dokument této osobě prostřednictvím datové schránky, pokud se nedoručuje veřejnou vyhláškou nebo na místě. Doručuje-li se způsobem podle tohoto zákona, ustanovení jiných právních předpisů upravující způsob doručení se nepoužijí.
(2) Připouštějí-li jiné právní předpisy doručování prostřednictvím datových schránek, pořadí způsobů doručování stanovené těmito právními předpisy zůstává ustanovením odstavce 1 nedotčeno.
(3) Dokument, který byl dodán do datové schránky, je doručen okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k dodanému dokumentu.
(4) Nepřihlásí-li se do datové schránky osoba podle odstavce 3 ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručený posledním dnem této lhůty; to neplatí, vylučuje-li jiný právní předpis náhradní doručení[6].
(5) Osoba, pro niž byla datová schránka zřízena, může za podmínek stanovených jiným právním předpisem[7] žádat o určení neúčinnosti doručení podle odstavce 4.
(6) Doručení dokumentu podle odstavce 3 nebo 4 má stejné právní účinky jako doručení do vlastních rukou.
(7) Doručování mezi orgány veřejné moci prostřednictvím datové schránky se nepoužije, pokud je z bezpečnostních důvodů mezi těmito orgány zavedena jiná forma elektronické komunikace.

§ 18

Provádění úkonů vůči orgánům veřejné moci prostřednictvím datové schránky

(1) Fyzická osoba, podnikající fyzická osoba a právnická osoba může provádět úkon vůči orgánu veřejné moci, má-li zpřístupněnu svou datovou schránku a umožňuje-li to povaha tohoto úkonu, prostřednictvím datové schránky.
(2) Úkon učiněný osobou uvedenou v § 8 odst. 1 až 4 nebo pověřenou osobou, pokud k tomu byla pověřena, prostřednictvím datové schránky má stejné účinky jako úkon učiněný písemně a podepsaný, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob.

§ 19

Datová zpráva

(1) Dokumenty orgánů veřejné moci doručované prostřednictvím datové schránky a úkony prováděné vůči orgánům veřejné moci prostřednictvím datové schránky mají formu datové zprávy.
(2) Je-li dokument nebo úkon určen do vlastních rukou adresáta, vyznačí tuto skutečnost odesilatel v datové zprávě.

§ 20
Působnost ministerstva

(1) Ministerstvo

a) zajistí připojení kvalifikovaného časového razítka k datové zprávě odeslané z datové schránky,

b) dodá datovou zprávu odeslanou z datové schránky do datové schránky osoby, která je odesílatelem označena jako adresát,

c) oznámí odesílateli, že datová zpráva, kterou odeslal, byla dodána do datové schránky adresáta, a toto oznámení označí elektronickou značkou ministerstva založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále jen „uznávaná elektronická značka“),

d) vyrozumí adresáta o dodání datové zprávy do jeho datové schránky na jím zvolenou elektronickou adresu nebo jiný technický prostředek pro vyrozumění; adresát je v tomto případě povinen uhradit náklady, které ministerstvu v souvislosti s vyrozuměním vznikly, s výjimkou, bylo-li vyrozumění učiněno na adresátem zvolenou elektronickou adresu,

e) oznámí odesílateli, že datová zpráva, kterou odeslal do datové schránky adresáta, byla doručena, a toto oznámení označí uznávanou elektronickou značkou ministerstva,

f) oznámí odesílateli, že datová schránka, do které odeslal datovou zprávu, neexistuje,

g) oznámí odesílateli, že datová schránka, do které odeslal datovou zprávu, je znepřístupněna, a to i zpětně,

h) oznámí odesílateli, že datová schránka, do které odeslal datovou zprávu, byla zrušena,

i) vede evidenci o datu a času událostí podle tohoto odstavce včetně identifikace datové zprávy, odesílatele a adresáta.

(2) Ministerstvo je oprávněno datovou zprávu zničit, pokud u ní zjistí výskyt chybného formátu nebo počítačového programu, které jsou způsobilé přivodit škodu na informačním systému datových schránek nebo na informacích v tomto informačním systému. O zničení datové zprávy ministerstvo neprodleně vyrozumí odesílatele.

(3) Obsah datové zprávy a všech jejích částí musí být uzpůsoben tak, aby se s ním bylo možné seznámit a dále jej zpracovávat bez zvláštních technických znalostí a způsobem umožňujícím práci s ním i osobám se zdravotním postižením prostřednictvím speciálních technických pomůcek. Ministerstvo zveřejní přípustné formáty datových zpráv a seznam možných technických prostředků pro vyrozumění o dodání datové zprávy do datové schránky v provozní dokumentaci informačního systému datových schránek.

§ 21
Identifikátor datové schránky

K identifikaci datové schránky slouží identifikátor. Identifikátor není zaměnitelný s žádným jiným identifikátorem využívaným orgány veřejné moci. Způsob tvorby identifikátoru stanoví ministerstvo vyhláškou.

§ 22
Konverze

(1) Konverzí se rozumí

a) úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky, nebo

b) úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky.

(2) Dokument, který provedením konverze vznikl (dále jen „výstup“), má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením výstup vznikl (dále jen „vstup“).

(3) Má-li být podle jiného právního předpisu předložen dokument v listinné podobě správnímu orgánu, nebo soudu anebo jinému státnímu orgánu, zejména aby byl užit jako podklad pro vydání rozhodnutí, je tato povinnost splněna předložením jeho výstupu.

§ 23
Subjekty provádějící konverzi

(1) Konverzi na žádost provádějí kontaktní místa veřejné správy[4)].

(2) Konverzi z moci úřední provádějí orgány veřejné moci pro výkon své působnosti.

§ 24
Postup při provádění konverze

(1) Při konverzi do dokumentu v listinné podobě subjekt provádějící konverzi

a) ověří platnost kvalifikovaného časového razítka vstupu[8)],

b) ověří, že kvalifikovaný certifikát[8)] vydaný akreditovaným poskytovatelem certifikačních služeb, na němž je založen zaručený elektronický podpis[8)], kterým je podepsán vstup, nebo kvalifikovaný systémový certifikát[8)] vydaný akreditovaným poskytovatelem certifikačních služeb, na němž je založena elektronická značka[8)], kterou je označen vstup, nebyly před okamžikem uvedeným v kvalifikovaném časovém razítku zneplatněny,

c) ověří platnost zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále jen „uznávaný elektronický podpis“) nebo platnost uznávané elektronické značky.

(2) Bezodkladně poté, kdy subjekt provádějící konverzi ověří shodu výstupu se vstupem a shoduje-li se výstup se vstupem, připojí k výstupu ověřovací doložku.

(3) Při konverzi do dokumentu obsaženého v datové zprávě opatří subjekt, který konverzi provedl, výstup svou uznávanou elektronickou značkou nebo uznávaným elektronickým podpisem osoby, která konverzi provedla, a zajistí, aby byl výstup opatřen kvalifikovaným časovým razítkem.

(4) Technické náležitosti provádění konverze, vstupu a výstupu stanoví ministerstvo vyhláškou.

(5) Konverze se neprovádí

a) je-li dokument v jiné než v listinné podobě či v podobě datové zprávy,

b) jde-li o dokument v listinné podobě, jehož jedinečnost nelze konverzí nahradit, zejména o občanský průkaz, cestovní doklad, zbrojní průkaz, řidičský průkaz, vojenskou knížku, služební průkaz, průkaz o povolení k pobytu cizince, rybářský lístek, lovecký lístek nebo jiný průkaz, vkladní knížku, šek, směnku nebo jiný cenný papír, los, sázenku, geometrický plán, rysy a technické kresby,

c) jsou-li v dokumentu v listinné podobě změny, doplňky, vsuvky nebo škrty, které by mohly zeslabit jeho věrohodnost,

d) není-li z dokumentu v listinné podobě patrné, zda se jedná o:

   1. prvopis,
   2. vidimovaný dokument,
   3. opis nebo kopii pořízenou ze spisu, nebo
   4. stejnopis písemného vyhotovení rozhodnutí anebo výroku rozhodnutí vydaného podle jiného právního předpisu,

e) je-li dokument v listinné podobě opatřen plastickým textem nebo otiskem plastického razítka,

f) jedná-li se o výstup z konverze,

g) v případě provedení konverze na žádost, nebylo-li k dokumentu obsaženém v datové zprávě připojeno kvalifikované časové razítko,

h) v případě provedení konverze na žádost, nebyl-li dokument obsažený v datové zprávě podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou toho, kdo dokument vydal nebo vytvořil,

i) byl-li dokument obsažený v datové zprávě podepsán uznávaným elektronickým podpisem oprávněné osoby nebo označen uznávanou elektronickou značkou toho, kdo příslušnou datovou zprávu vydal nebo vytvořil, a nebyla-li shledána shoda tohoto dokumentu s výstupem,

j) jde-li o dokument obsažený v datové zprávě, který nelze konvertovat do listinné podoby, například o zvukový nebo audiovizuální záznam,

k) pokud dokument obsažený v datové zprávě nesplňuje technické náležitosti podle odstavce 4.

(6) Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy.

§ 25
Ověřovací doložka

(1) Ověřovací doložka konverze do dokumentu obsaženého v datové zprávě je součástí výstupu a obsahuje

a) název subjektu, který konverzi provedl,

b) pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí,

c) údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu,

d) údaj o tom, z kolika listů se skládá vstup,

e) údaj o tom, zda vstup obsahuje vodoznak, reliéfní tisk nebo embossing, suchou pečeť nebo reliéfní ražbu, opticky variabilní prvek nebo jiný zajišťovací prvek,

f) datum vyhotovení ověřovací doložky,

g) jméno, případně jména, a příjmení osoby, která konverzi provedla.

(2) Ověřovací doložka konverze do dokumentu v listinné podobě je součástí výstupu a obsahuje

a) název subjektu, který konverzi provedl,

b) pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí,

c) údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu,

d) údaj o tom, z kolika listů se skládá výstup,

e) datum vyhotovení ověřovací doložky,

f) údaj o tom, zda byl vstup podepsán platným uznávaným elektronickým podpisem nebo označen platnou uznávanou elektronickou značkou, číslo kvalifikovaného certifikátu, na němž je uznávaný elektronický podpis založen, nebo číslo kvalifikovaného systémového certifikátu, na němž je uznávaná elektronická značka založena, a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydal,

g) datum a čas uvedené v kvalifikovaném časovém razítku, číslo kvalifikovaného časového razítka a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal,

h) otisk úředního razítka, jméno, popřípadě jména, příjmení a podpis osoby, která konverzi provedla.

§ 26
Evidence provedených konverzí

(1) Subjekt provádějící konverzi vede evidenci provedených konverzí. Záznam v evidenci obsahuje tyto údaje:

a) pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí,

b) datum provedení konverze,

c) konkrétní označení vstupu a datum jeho sepsání, je-li datum ve vstupu obsaženo,

d) údaj o uhrazení správního poplatku nebo odměny notáře (uvedení čísla dokladu, kterým byl uhrazen) nebo údaj o osvobození od správního poplatku s odkazem na právní předpis.

(2) Údaje podle odstavce 1 jsou v evidenci provedených konverzí uchovávány po dobu 10 let od provedení konverze.

Společná, přechodná a závěrečná ustanovení

§ 27

(1) Žádosti a oznámení podle tohoto zákona lze podat rovněž prostřednictvím kontaktního místa veřejné správy.

(2) Úředně ověřený podpis žádosti podle § 3 odst. 4, § 4 odst. 5 a § 5 odst. 5 se nevyžaduje, je-li žádost podepsána před zaměstnancem státu zařazeným v ministerstvu nebo zaměstnancem zařazeným v kontaktním místu veřejné správy anebo je-li podepsána zaručeným elektronickým podpisem, který je založen na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

(3) Učiní-li osoba oprávněná k přístupu do datové schránky oznámení podle § 12 odst. 1 prostřednictvím kontaktního místa veřejné správy, obdrží nové přístupové údaje na počkání.

§ 28

Příjem žádostí nebo oznámení podle § 27 odst. 1 a vydávání přístupových údajů podle § 12 odst. 1 s výjimkou opětovného vydání přístupových údajů je bezplatné.

§ 29

(1) Vedou-li orgány veřejné moci spisovou službu elektronicky, činí tak způsobem umožňujícím doručování dokumentů a provádění úkonů prostřednictvím datové schránky, ledaže je z bezpečnostních důvodů nezbytné vést spisovou službu odděleně.
(2) Zřizují-li orgány veřejné moci elektronickou podatelnu, elektronická podatelna umožňuje doručování dokumentů a provádění úkonů prostřednictvím datové schránky.

§ 30

(1) Konverzi na žádost provádí u držitele poštovní licence a Hospodářské komory České republiky zaměstnanec, který složil zkoušku.
(2) Obsahem zkoušky je ověření znalostí tohoto zákona, vybraných ustanovení právních předpisů týkajících se správních poplatků a správního řádu a schopnosti jejich aplikace.
(3) Provádění zkoušky zabezpečuje ministerstvo.
(4) Složení zkoušky se prokazuje osvědčením o vykonání zkoušky. Vzor osvědčení stanoví ministerstvo prováděcím právním předpisem.
(5) Neuspěl-li zaměstnanec při zkoušce, může zkoušku dvakrát opakovat. Opakovanou zkoušku je možno vykonat nejdříve za 60 dnů a nejpozději do 90 dnů ode dne konání zkoušky, při níž zaměstnanec neuspěl.

§ 31

Přechodná ustanovení

(1) Ministerstvo zřídí datovou schránku subjektům uvedeným v § 4 odst. 3, § 5 odst. 1 a § 6 odst. 1 s výjimkou advokáta a daňového poradce do 90 dnů ode dne nabytí účinnosti tohoto zákona.
(2) Subjekty uvedené v § 15 odst. 2 až 9 zašlou ministerstvu do 30 dnů ode dne nabytí účinnosti tohoto zákona údaje nezbytně nutné pro zřízení datové schránky vedené o osobách v evidencích uvedených v § 15 odst. 2 až 9 ke dni nabytí účinnosti tohoto zákona.
(3) Ministerstvo zřídí advokátu a daňovému poradci datovou schránku podnikající fyzické osoby prvním dnem prvního kalendářního měsíce třetího roku po dni nabytí účinnosti tohoto zákona. Tím není dotčeno právo advokáta a daňového poradce na zřízení datové schránky podnikající fyzické osoby na žádost.

§ 32

Účinnost

Tento zákon nabývá účinnosti dnem 1. července 2009.