Využití technologie elektronického podpisu a prostředí Datových schránek ve STÁTNÍ TISKÁRNĚ CENIN, státní podnik

Use of electronic signature technology and the environment of data boxes in the STÁTNÍ TISKÁRNA CENIN, státní podnik

Bc. Tomáš Bánský

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

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

Jméno a příjmení:	**Bc. Tomáš Bánský**
Osobní číslo:	**A12337**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Využití technologie elektronického podpisu a prostředí Datových schránek ve STÁTNÍ TISKÁRNĚ CENIN, státní podnik**
Téma anglicky:	**The Use of Electronic Signature Technology and Data Box Environments in the State-run STÁTNÍ TISKÁRNĚ CENIN Organisation**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Analyzujte možnosti využití elektronického podpisu ve specifickém prostředí.**
3. **Navrhněte způsoby využití elektronického podpisu a Datových schránek pro komunikaci s orgány veřejné moci.**
4. **Ověřte navržené postupy v praxi.**
5. **Proveďte diskusi ke zvolenému řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **PETERKA, Jiří. Báječný svět elektronického podpisu. Praha: CZ.NIC, c2011, 430 s. CZ.NIC. ISBN 978-80-904248-3-8.**
2. **SMEJKAL, Vladimír. Jak na datové schránky: praktický manuál pro každého. Praha: Linde Praha, 2012. ISBN 80-861-3180-7.**
3. **ŠPAČEK, David. eGovernment: cíle, trendy a přístupy k jeho hodnocení. Vyd. 1. V Praze: C.H. Beck, 2012. Beckova edice ekonomie. ISBN 978-807-4002-618.**
4. **LIDINSKÝ, Vít. eGovernment bezpečně. 1. vyd. Praha: Grada, 2008, 145 s. ISBN 978-80-247-2462-1.**
5. **BUDIŠ, Petr. Datové schránky: fungování, doručování, bezpečnost, návody. 1. vyd. Olomouc: ANAG, 2010. ISBN 80-726-3617-0.**
6. **LAPÁČEK, Jiří. Jak na datovou schránku a elektronickou komunikaci s úřady. 1. vyd. Brno: Computer Press, 2012, 197 s. ISBN 978-80-251-3680-5.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Abstrakt česky

Tato práce je zaměřena na problematiku využití elektronického podpisu a prostředí datových schránek ke komunikaci s orgány veřejné moci. Nejdříve představuje důvody zavedení datových schránek jako prvku eGovernmentu, jejich základní popis a účel použití pro občana, živnostníka a právnickou osobu. Vysvětluje princip elektronického podepisování a uvádí způsoby získání kvalifikovaného certifikátu. V závěru hodnotí tuto službu z pohledu běžného uživatele a zmiňuje její výhody a nevýhody.

Klíčová slova:

elektronický podpis, datové schránky, eGovernment, certifikát, certifikační autorita

ABSTRACT

Abstrakt ve světovém jazyce

This work is focused on the use of electronic signature and surroundings data boxes for communication with public authorities. It first presents the reasons for the introduction of data boxes as an element of eGovernment, their basic characteristics and the intended use for the citizen, entrepreneur and legal person. It explains the principle of an electronic signature and provides ways to get a qualified certificate. In conclusion, my thesis evaluates the service from the perspective of the common user and discusses its advantages and disadvantages.

Keywords:

electronic signature, data boxes, eGovernment, certificate, certification authority

Poděkování, motto

Chtěl bych tímto poděkovat panu doc. Mgr. Romanu Jaškovi, Ph.D., za metodické vedení, cenné rady a připomínky při vytváření této diplomové práce.

Prohlašuji, že

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

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Každý jedinec je již od svého narození součástí informační společnosti. Stává se totiž zdrojem i adresátem informací. Během svého života informace získává, vyhodnocuje, shromažďuje a používá pro rozhodování. Aby byl ve svém životě a rozhodování úspěšný, potřebuje získat informace kvalitní, spolehlivé, aktuální a hlavně rychle.

Společně s obrovským rozvojem výpočetní techniky a informačních a komunikačních technologií dochází ke stále většímu využívání digitálního zpracování a přenosu informací. Za přímé účasti politických struktur je ve všech vyspělých zemích budována Politika informační společnosti, jejímž cílem je například zlepšení kvality života občanů nebo zkvalitnění služeb.

Jedním z hlavních nástrojů budování informační společnosti je eGovernment. Cílem eGovernmentu je rychlejší, spolehlivější a levnější poskytování služeb veřejnosti s využitím modernizace veřejné správy. Ve své práci krátce popisuji historické události, které měly podstatný vliv na budování eGovernmentu v České republice, a reakci na budování informačních systémů veřejné správy. Dále postupy při zavádění čtyř základních etap eGovernmentu symbolizujících tento proces jako živý organismus v podobě panáčka eGONa.

V další části popisuji legislativní a technickou přípravu, které předcházely vzniku datových schránek. Definuji jednoznačný účel použití datových schránek, jejich základní rozdělení podle typu uživatelů a způsoby jejich zřízení.

V poslední kapitole se věnuji problematice elektronického podpisu. Okolnostem, které vedly k jeho vzniku, potřebám jeho zavedení do právních řádů České republiky, až po přijetí zákona o elektronickém podpisu. Dále pak uvádím jeho přesnou definici, základní vlastnosti, které zajišťuje, a princip jeho používání.

K elektronickému podpisu neodmyslitelně patří certifikát vydaný akreditovanou certifikační autoritou. Jaké jsou druhy certifikátů, k čemu slouží a jak se tvoří, charakterizuji v závěru teoretické části.

Praktická část mé práce je zaměřena na skutečné využití elektronického podpisu a prostředí datových schránek ve specifickém prostředí výrobního podniku. Nejdříve nabízím teoretické možnosti využití elektronického podpisu a vzápětí podrobně analyzuji jeho reálné používání v oblasti administrativy, poskytování služeb i v oblasti výroby.

Zřízení datových schránek bylo STC dáno zákonem, povinnosti z tohoto právního předpisu vyplývající popisuje další část práce.

Poté jsem se zaměřil na vyhodnocení stavu využívání služby datových schránek pro odesílání datových zpráv orgánům veřejné moci v porovnání s běžnými poštovními službami za uplynulé období.

Nakonec jsem specifikoval možnosti a rozdíly využívání přístupu k datové schránce pomocí webového rozhraní a spisové služby. Popsal rozdíly v oprávnění osob, které k datové schránce přistupují, a představil trend dalšího využívání služeb datových schránek na základě množství odeslaných datových zpráv.

V závěru práce jsem shrnul projekt eGovernmentu, ekonomický přínos zavedení datových schránek a nastínil možný rozvoj potenciálu informačního systému datových schránek. A uvedl vlastní názor na využívání elektronického podpisu a datových schránek z pohledu běžného uživatele.

I. TEORETICKÁ ČÁST

1 VZNIK DATOVÝCH SCHRÁNEK

Ostrý provoz datových schránek byl v České republice spuštěn dne 1. července 2009, kdy nabyl účinnosti zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Tento zákon přinesl zásadní změnu v komunikaci mezi úřady navzájem a mezi úřady a občanem. Využívání informačního systému datových schránek se totiž dotýká velkého množství subjektů, obchodních společností, úřadů, ale i běžných lidí. [1] Jejich zavedení se ovšem neprovedlo ze dne na den, ale předcházela mu celá řada kroků.

1.1 Politika informační společnosti

Prvním z nich bylo zavedení Politiky informační společnosti. Charakteristickými rysy informační společnosti, tj. společnosti, která se ve stále větší míře opírá o shromažďování, uchovávání, využívání a předávání informací, jsou:

- podstatné využívání digitálního zpracovávání, uchovávání a přenosu informací,
- využívání moderních informačních technologií a digitální komunikace,
- přímá účast politických struktur na určení koncepce jejího budování, stanovení jejích postupných cílů a zásad jejich dosažení, včetně vytvoření právní, finanční a společenské podpory realizace této koncepce.

Jedná se tedy o kvalitní komunikaci s daty v digitalizované podobě předurčenými k co nejširšímu spektru využití. Rychlost a obsahová hodnota informací ovlivňuje chování jedince například v oblasti ekonomických aktivit, dopravy, bezpečnosti, veřejného zdraví, nebo životního prostředí a stala se významnou tržní aktivitou.

Klíčovým faktorem pro rozvoj společnosti a její hospodářský růst je vybudování komunikační infrastruktury. Toto vybudování závisí nejen na technologickém výzkumu, dosažitelnosti a zajištění finančních zdrojů, ale i na přijetí právních aktů, týkajících se zajištění bezpečnosti a uživatelské jednotnosti.

Politika informační společnosti tedy představuje soubor procesů a pro ně charakteristických metod a nástrojů, na jejichž základě, resp. s jejichž pomocí je budována informační společnost a prosazovány její zájmy a cíle (např. zlepšení konkurenceschopnosti, zlepšení kvality života občanů, zkvalitnění služeb). [1]

1.2 e-Government

Jedním z hlavních nástrojů budování informační společnosti je e-Government. Hodně se o něm mluví i píše, až by se mohlo zdát, že v České republice zdomácněl. Ale představují si všichni pod tímto pojmem to samé? Můžeme konstatovat, že ne. Pro jednoho jsou to elektronické výpisy z rejstříků vedených státem, pro druhého používání internetu orgány veřejné moci. Najít tu správnou definici, která by vystihovala rozsah eGovernmentu, není totiž jednoduché. Definice na stránkách Ministerstva vnitra nám podle Budiše a Hřebíkové popisuje obsah tohoto pojmu v obecné rovině takto: „eGovernment představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům“. [1] Lidinský uvádí vlastní definici v širším smyslu: „eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb“. [3] A Smejkal doplňuje, že obecných definic je mnoho, a každá se zaměřuje na některý z typických aspektů eGovernmentu, např.:

- „Efektivní a výkonné veřejné služby a informační a komunikační technologie umožňující občanům plně se podílet na životě společensky a kulturně tvůrčích komunit včetně demokratického procesu“ (podle EU[1]).
- „Použití elektronických komunikací, zejména pak internetu jako nástroje pro dosažení lepší správy“ (podle OECD[2]). [5]

Oblast působnosti eGovernmentu se rozděluje na tři skupiny:

- Government-to-Citizen (G2C), komunikace mezi úřady státní správy a občanem;
- Government-to-Business (G2B), komunikace mezi úřady státní správy a podnikateli, obchodními společnostmi;
- Government-to-Government (G2G), komunikace mezi úřady navzájem.

[1] EU – Evropská unie
[2] OECD – angl. Organisation for Economic Co-operation and Development – Organizace pro hospodářskou spolupráci a rozvoj

eGovernment je tedy způsob, jak umožnit komunikaci s institucemi státní a veřejné správy v elektronické podobě a elektronizaci veškerých procesů s tím souvisejících, například doručování dokumentů, vedení spisové služby v elektronických systémech nebo tvorba předpisů a jejich publikace. Jeho cílem je především usnadnit tuto komunikaci mezi úřady a veřejností, vytvořit její jednoznačné postupy a zajistit požadovanou míru informovanosti za pomoci využití moderních komunikačních technologií a platné legislativy.

Mezi největší výhody elektronizace státní správy patří:

- rychlost a kvalita služeb občanům a obchodním společnostem,
- jednoduchost, uživatelská přívětivost,
- „úřední hodiny“ pro podání 24 hodin denně, 7 dní v týdnu,
- finanční úspory,
- transparentnost procesů a rozhodování. [1]

1.3 Vládní strategie

eGovernment nelze v plném rozsahu spustit ke konkrétnímu datu jediným rozhodnutím, zákonem, nařízením, či zavedením nové technologie. Procesy spojené s eGovernmentem tvoří komplikovaný a neustále se měnící celek. Stanovení jednoznačné koncepce budování informační společnosti představuje uplatňování moderních informačních a komunikačních technologií do většiny pracovních činností, se zaměřením na jejich vývoj a účinnější využití. S cílem minimalizace případných negativních dopadů.

Již v roce 1994 vycházela Česká republika při vytváření těchto zásad z dokumentů Evropské unie, a to zejména z Akčního plánu Evropské komise „Cesta Evropy k informační společnosti“. Dalším podkladem byly závěry přijaté na konferenci „Informační společnost přibližující administrativu občanům“, která se konala ve Vídni v roce 1998.

Prvním oficiálním dokumentem pro budování informační společnosti v ČR byla „Státní informační politika – cesta k informační společnosti“, který byl vydán jako usnesení vlády v roce 1999. Jednalo se o první ucelenou koncepci státu v oblasti budování tzv. informační společnosti. Zároveň v něm bylo konstatováno, že pro rozvoj informační společnosti v České republice chybí legislativní zázemí, které by se zabývalo oblastí elektronického obchodu, elektronického podpisu a používání dokumentů v elektronické podobě. Jedním z prioritních úkolů bylo uzákonit elektronický podpis a dát dokumentům v elektronické

podobě stejnou právní váhu jako dokumentům klasickým. Tato strategie proto byla zaměřena na tři realizační oblasti, informatizaci veřejné správy, která byla prioritní, informační gramotnost a elektronický obchod.

Ve stejném roce byla přijata „Koncepce budování informačních systémů veřejné správy“, jejímž hlavním cílem bylo zvýšení efektivnosti a důvěryhodnosti veřejné správy, zvýšení její uživatelské přívětivosti vůči fyzickým osobám a zpřehlednění jejích postupů. Dále pak zajištění rozvoje ekonomického prostředí, omezení byrokracie a časové zátěže účastníků jednotlivých řízení.

Pro reálné uplatnění těchto strategických dokumentů byly vytvářeny legislativní podmínky, jejichž přijetím bylo dosaženo slučitelnosti právního řádu České republiky s právem Evropské unie, a to zejména:

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
- zákon č. 29/2000 Sb., o poštovních službách,
- zákon č. 101/2000 Sb., o ochraně osobních údajů,
- zákon č. 227/2000 Sb., o elektronickém podpisu,
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- vyhláška č. 496/2004 Sb., o elektronických podatelnách,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě,
- zákon č. 127/2005 Sb., o elektronických komunikacích,
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Za klíčový dokument lze považovat usnesení vlády z roku 2006, kterým vláda vzala na vědomí dosavadní vývoj budování eGovernmentu v České republice a současně schválila „Soubor opatření pro urychlení rozvoje eGovernmentu v České republice“. Tímto usnesením byla vytvořena státní zakázka na vybudování univerzálních kontaktních míst občanů s úřady – Českého podacího ověřovacího informačního národního terminálu – „Czech POINT“.

Výše uvedené dokumenty jsou pouhým výčtem milníků v budování informační společnosti v České republice a mým cílem bylo ukázat, že se ze strany státu jedná o promyšlený dlouhodobý projektový záměr, podléhající projektové analýze a projektovému řízení, v rámci měnících se aplikačních podmínek.

1.4 Informační systémy veřejné správy

Informační systémy veřejné správy (ISVS) jsou informační systémy, které jsou definovány zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů. V § 3 odstavci 1 tohoto zákona jsou ISVS vymezeny jako „soubor informačních systémů, které slouží pro výkon veřejné správy“. [3]

I pro pracovníky Ministerstva informatiky, gestora předpisu, bylo mnohdy velmi obtížné odpovědět na otázku, zda určitý informační systém je ISVS, nebo ne.

Po novelizaci zákona o ISVS počátkem roku 2006 byla orgánům veřejné správy dána povinnost vytvořit a vydat informační koncepci. Tedy dokument, v němž budou uvedeny dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných ISVS, obecné principy pořizování, vytváření a provozování ISVS. Při vytváření informační koncepce jsou orgány veřejné správy postaveny před zásadní úkol identifikovat informační systémy veřejné správy, u kterých vykonávají úlohu správce ve smyslu zákona o ISVS.

Počátkem roku 2007 proto vznikl metodický pokyn „Co je a co není ISVS“. Tento metodický pokyn má sloužit pracovníkům orgánů veřejné správy i společností, které se zabývají vývojem informačních systémů pro orgány veřejné správy či dodávají služby v této oblasti, aby mohli snáze určit, zda je určitý informační systém informačním systémem veřejné správy ve smyslu zákona o ISVS. Na konkrétních příkladech vysvětluje, jaký informační systém je podle zákona o ISVS informačním systémem veřejné správy, a vysvětluje, jak přistupovat k popisu ISVS v informační koncepci.

Proč je rozdíl mezi informačním systémem a ISVS tak důležitý? Pokud je konkrétní informační systém definován jako ISVS, musí se řídit zákonem č. 365/2000 Sb., a zde je rozdíl v dokumentaci, komunikaci a správě informačního systému.

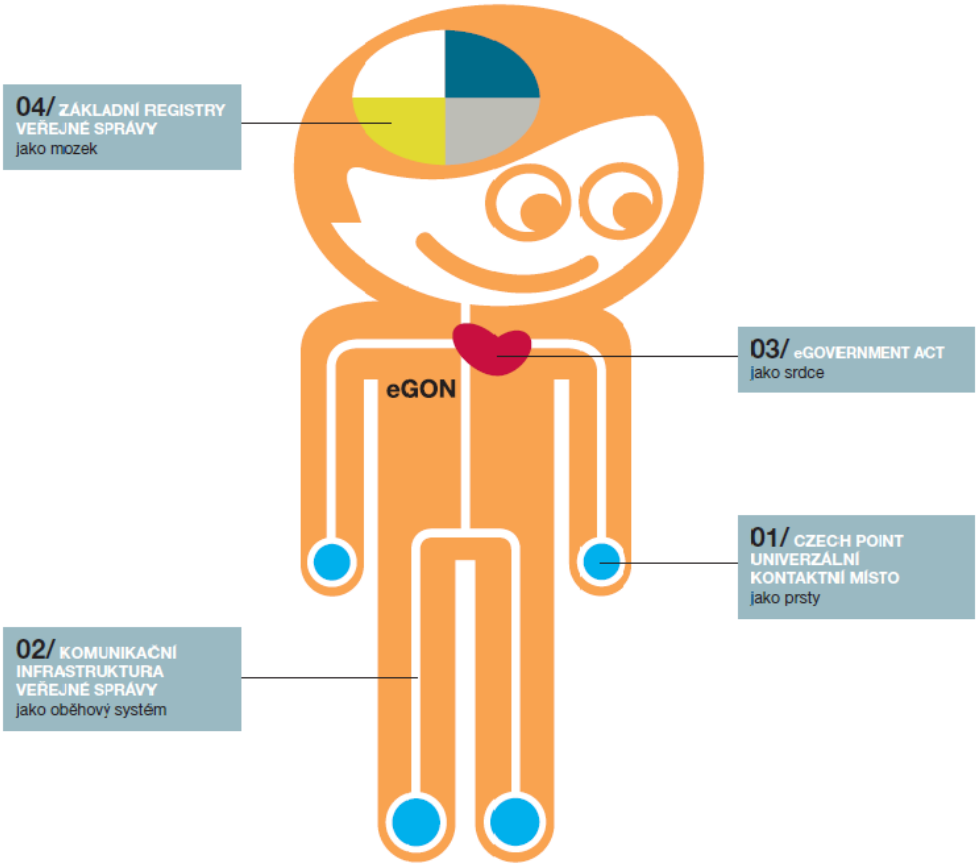
Za ISVS můžeme u orgánů veřejné správy označit následující informační systémy:

- informační systém, o kterém zákon (který stanovuje požadavky na vznik informačního systému) stanoví, že se jedná o ISVS podle zákona č. 365/200 Sb. (například § 137 odst. 1 zákona č. 262/2006 Sb., zákoník práce),
- informační systém, který je zákonem označen jako registr, rejstřík nebo evidence (například § 21 zákona č. 76/2002 Sb., o integrované prevenci, omezování znečišťování, o integrovaném registru znečišťování),

- informační systém, u kterého je v zákoně uvedeno, že se jedná o ISVS, ale odkaz na zákon č. 365/2000 Sb. není uveden (například § 419 odst. 1 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení),
- informační systém, který je zákonem stanoven bez označení, že se jedná o ISVS (například § 4 odst. 1 písm. i) a j) zákona č. 365/2000 Sb.),
- informační systémy, které nejsou upraveny zákonem, ale prostřednictvím nichž orgán veřejné správy vykonává svěřené činnosti (např. informační systém o poplatcích za psy, pokud je tento informační systém provozován obcí, která tuto činnost vykonává ze zákona č. 565/1990 Sb., o místních poplatcích). [3]

1.5 Panáček eGON

Jako symbol eGovernmentu byl zvolen oranžový panáček eGON, pomocí něhož lze jednoduše vysvětlit, jak eGovernment funguje. V přeneseném významu je to živý organismus, ve kterém vše souvisí se vším, a fungování jednotlivých částí se navzájem podmiňuje. Existenci a životní funkce eGONa zajišťují čtyři základní symboly – prsty, oběhová soustava, srdce a mozek. Prsty ucítí podnět, vyšlou signál do mozku, ten informaci vyhodnotí, správný orgán rozhodne a zpětně prsty informuje o tom, co mají udělat. Informace se přenáší přímo, bez slepých cest, bez křižovatek a bez zbytečných průtahů.



Obr. 1. eGON jako živý organismus (převzato z [9])

1.5.1 Prsty

Czech POINT znamená Český Podací Ověřovací Informační Národní Terminál. Czech POINTY představují eGONovy prsty, které zajišťují snadný kontakt občanů s veřejnou správou. Jedná se o kontaktní místo veřejné správy, poskytující občanům zejména ověřené údaje vedené v centrálních registrech, jako jsou rejstřík trestů, obchodní rejstřík nebo registr živnostenského podnikání. Nově zde zájemci o veřejnou zakázku dostanou výpis k prokázání kvalifikace a také výpisy z bodového registru řidičů. Jejich cílem je zrychlit a zpřístupnit služby občanům zprostředkováním snadné komunikace se státem prostřednictvím jednoho univerzálního místa a redukce přílišné byrokracie mezi občanem a veřejnou správou.

Postupně je vytvářena rozsáhlá a snadno dostupná síť poboček Czech POINTů, která odbourává někdejší zdlouhavé cestování po úřadech a sjednocuje různá vyřizování na jedno místo. Czech POINTy jsou dostupné na obecních a městských úřadech, na pobočkách České pošty, na pobočkách Hospodářské komory ČR, na českých

zastupitelstvích v zahraniční, u vybraných notářů, nebo prostřednictvím e-shopu na www.czechpoint.cz. Do budoucna se připravuje úprava služeb, aby byly přístupné nejen na pobočkách Czech POINTů, ale prostřednictvím internetu kdekoli, kde je občan právě potřebuje.

1.5.2 Oběhová soustava

Komunikační infrastruktura veřejné správy – KIVS – je oběhový systém eGONa, zabezpečuje propojení sítí a systémů dílčích institucí do společného prostředí. Vytváří jednotnou komunikační infrastrukturu pro elektronické úřadování a znamená rychlejší a efektivnější přístup k informacím pro ty, kteří k tomu mají oprávnění.

Poskytuje bezpečné místo komunikace orgánů veřejné správy navzájem a bezpečnou komunikaci s občany. Komunikují přes něj Czech POINTy s orgány veřejné správy a také jednotlivé orgány veřejné správy s registry. Jeho realizací se vytvořila jednotná datová síť, která poskytuje bezpečné připojení a vysoký standard nabízených služeb. Navíc se odstranil monopol na poskytování datových služeb, protože kromě Telefónicy O2 se zapojili i operátoři GTS Novera a konsorcium T-Systems a ČD Telematika.

Přínosem komunikační infrastruktury veřejné správy je zefektivnění služeb a také výrazné úspory. Již za dva roky od své realizace přinesl systém úspory v hodnotě více než 250 milionů Kč. Úspory jsou k dispozici uživatelům systému, kteří je mohou využít pro investice do informačních systémů, a získat tak kvalitnější nebo rychlejší připojení, a tím pádem i zlevnění služeb díky konkurenčnímu prostředí.

Novým a nejdůležitějším elektronickým prvkem celé komunikační infrastruktury je Centrální místo služeb (CMS). Je to jediné místo výměny dat mezi jednotlivými informačními systémy veřejné správy. CMS také umožňuje propojení internetu ke specifickým neveřejným sítím, např. sítím EU, a také je to jediné logické místo propojení jednotlivých operátorů telekomunikačních infrastruktur poskytujících služby pro KIVS. [21]

1.5.3 Srdce

eGONovo srdce, které ho přivádí k životu, představuje Zákon o elektronických úkonech a autorizované konverzi dokumentů (zákon č. 300/2008 Sb.). Tento zákon je nazýván jako zákon o eGovernmentu nebo eGovernment Act.

Pomocí tří základních pilířů:

- zavedení datových schránek,
- zrovnoprávnění elektronických a papírových dokumentů,
- povinnost institucí komunikovat elektronicky

zajistil vytvoření optimálních podmínek pro elektronickou komunikaci mezi úřady a občany i mezi úřady samotnými.

Klíčový institut pro provádění elektronických úkonů, tedy pro komunikaci s orgány veřejné moci, představují datové schránky, jejichž informační systém zabezpečuje doručení úředních zpráv v elektronické podobě. Druhým klíčovým prvkem zákona o elektronických úkonech je autorizovaná konverze dokumentů, tedy převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo převedení dokumentu obsaženého v datové zprávě do listinného a zároveň ověření shody jejich obsahu a připojení ověřovací doložky. [21]

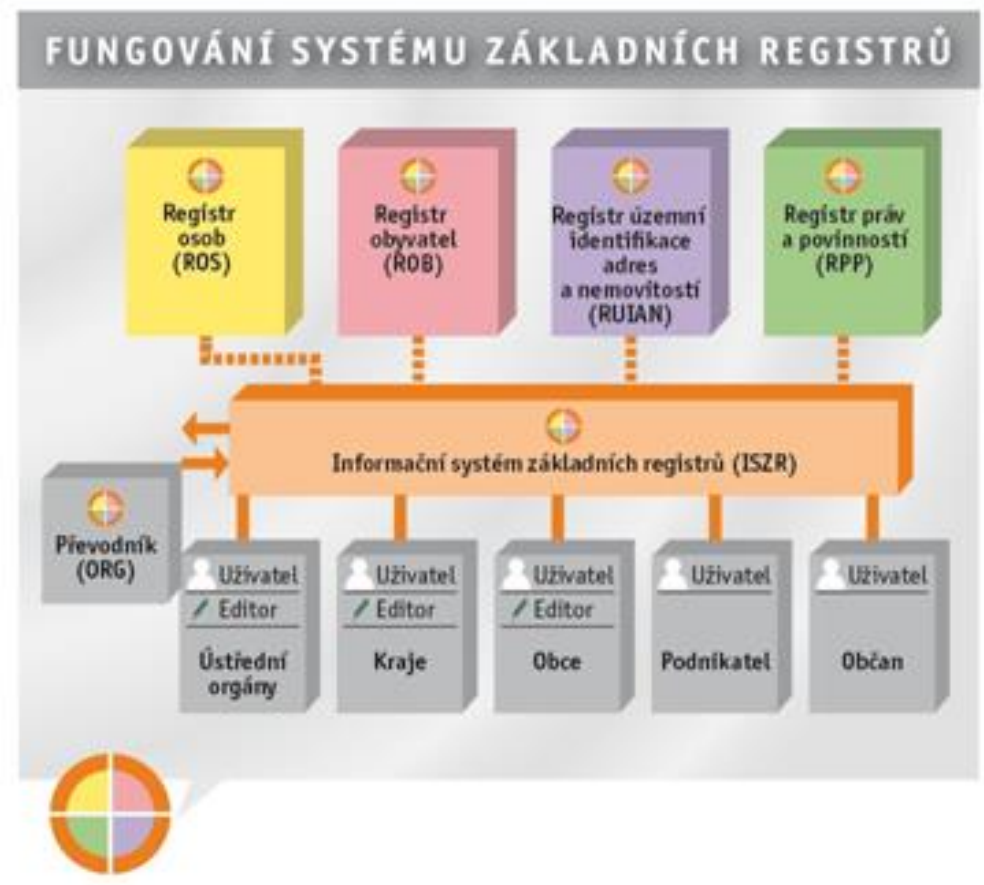
1.5.4 Mozek

Základní registry symbolizují eGONův mozek, bez něj by celé fungování eGovernmentu nebylo efektivní. Vytvořením centrálních registrů veřejné správy se vyřešily dosavadní potíže související s nejednotností, multiplicitou a neaktuálností klíčových databází. Zásadním prvkem v systému základních registrů je tzv. referenční údaj. Ve své podstatě jde o údaj, který je přebírán ze systému základních registrů a v příslušných agendách se využívá jako údaj zaručený, platný a aktuální, bez nutnosti jeho ověření. Došlo tak k odstranění roztříštěnosti velkého množství databází, které spravovala každá instituce samostatně, a data v nich byla často chybná. Úřady jsou povinny využívat právě data ze základních registrů, a nikoli je vyžadovat po občanovi. V principu tak stačí jedna změna v registru, například při změně jména nebo adresy, která se promítne i v ostatních registrech.

Registry zajišťují ochranu osobních údajů tím, že data nejsou spojena se jménem osoby, které patří. Patřičnou osobu identifikuje číselný kód, tzv. agendový identifikátor. Díky tomuto opatření není možné data z jednotlivých registrů neoprávněně propojit. Důležitým prvkem pro ochranu osobních údajů v systému je převodník identifikátorů fyzických osob - tzv. ORG. Tato instituce spadá pod Úřad pro ochranu osobních údajů a jako jediná dokáže přepočítávat agendové identifikátory z jednoho registru pro druhý. Už tedy není možné díky znalosti rodného čísla získat o tomto obyvateli informace prakticky z každého informačního systému veřejné správy, jak tomu bylo dosud.

Zásadním krokem k fungování systému základních registrů bylo přijetí zákona č. 111/2009 Sb., o základních registrech, a zákona č. 227/2009 Sb. na počátku roku 2009. Základní registry jsou celkem čtyři:

- Registr osob – ROS – obsahující údaje o právnických osobách, podnikajících fyzických osobách, orgánech veřejné moci i o nekomerčních subjektech, jako jsou občanská sdružení a církve.
- Registr obyvatel – ROB – obsahující základní údaje o občanech a cizincích s povolením k pobytu, mezi tyto údaje patří: jméno a příjmení, datum a místo narození a úmrtí a státní občanství.
- Registr práv a povinností – RPP – obsahující referenční údaje o působnosti orgánů veřejné moci, mj. oprávnění k přístupu k jednotlivým údajům, informace o změnách provedených v těchto údajích apod. Slouží jako garance bezpečné správy dat občanů a subjektů vedených v jednotlivých registrech.
- Registr územní identifikace, adres a nemovitostí – RÚIAN – spravující údaje o základních územních a správních prvcích.



Obr. 2. Systém základních registrů (převzato z [19])

Všechny čtyři základní registry fungují v rámci informačního systému základních registrů, tzv. ISZR, jehož správu zajišťuje státní úřad (Správa základních registrů).

2 DATOVÉ SCHRÁNKY V ČR

V České republice se o vizi datových schránek začalo uvažovat již v roce 2005. Koncept datových schránek byl otevřeně diskutován na politické i odborné úrovni. Mezi roky 2006 – 2008 vzniklo několik návrhů zákonné úpravy datových schránek. V roce 2008 byl přijat klíčový zákon o elektronických úkonech a autorizované konverzi dokumentů. Systém datových schránek byl spuštěn v roce 2009 a od té doby probíhá jeho neustálý rozvoj.

2.1 Legislativní příprava

Myšlenka datových schránek vznikla na půdě iniciativy eStát v letech 2005 a 2006 jako jeden z pilířů odvážné vize efektivního státu. V roce 2006 byly datové schránky zařazeny jako jeden z klíčových pilířů ucelené strategie eGON MVČR, která stanovila jasné priority rozvoje eGovernmentu v České republice. Dílčími pilíři eGONa byly základní registry, kontaktní místa Czech POINT a komunikační infrastruktura veřejné správy. eGON jako celek byl veřejnosti představen v roce 2007.

Již v roce 2006 byl zpracován a zveřejněn první návrh zákona „o elektronizaci některých procesních úkonů v oblasti orgánů veřejné moci“ (tzv. „e-Government Act“). Návrh zákona se pokoušel upravit autorizovanou konverzi písemností, tzv. legalizaci elektronického podpisu, jednoznačné určení fyzické osoby při elektronické komunikaci (tzv. osobní číslo) a zaváděl institut elektronické přepážky a datových schránek coby nástroje pro komunikaci mezi orgány veřejné moci vůči právnickým a fyzickým osobám a mezi orgány veřejné moci navzájem.

V letech 2006 – 2008 probíhala odborná i politická diskuse o způsobu realizace datových schránek a způsobu jejich legislativní úpravy, a to i v širším kontextu dalších připravovaných projektů eGON, zejména projektu základních registrů a projektu kontaktních míst Czech POINT. Během této doby vzniklo několik zásadně přepracovaných verzí připravovaného zákona. Společně s precizováním a zeštíhlováním navrhovaného zákona se postupně upravoval i jeho název.

Finální znění zákona bylo přijato Poslaneckou sněmovnou 17.7.2008 jako zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Zákon definoval především základní principy a procesy datových schránek, povinnosti a práva uživatelů a provozovatele systému a zavedl institut autorizované konverze, který umožnil hladké propojení elektronického a papírového způsobu zpracování dokumentů.

2.2 Technická příprava

Základní otázkou technické realizace datových schránek byla volba modelu financování informačního systému datových schránek. Nabízely se dvě možnosti, model založený na poskytování služeb nebo model investiční. Nakonec byl vybrán model poskytování služeb a stát na sebe převzal počáteční investici a všechna rizika. Služba je placena poplatkem za jednotlivé transakce, podle toho, jak je systém využíván. V tomto případě za jednu zaslanou zprávu.

Ministerstvo vnitra je podle zákona správcem informačního systému datových schránek, určuje účel a prostředky zpracování informací a odpovídá za informační systém datových schránek (ISDS). Provozovatelem informačního systému datových schránek je přímo ze zákona stanovena Česká pošta, s. p., národní držitel poštovní licence.

Ministerstvo vnitra podepsalo v roce 2008 memorandum o spolupráci se sedmi významnými výrobci elektronických spisových služeb, aby pomohli při přípravě technické části prováděcí vyhlášky k zákonu č. 300/2008 Sb. a vytvořili technickou specifikaci pro otevřenou komunikaci spisové služby a systému datových schránek. Do července roku 2010 přistoupilo k memorandu dalších více než 50 výrobců a dodavatelů informačních systémů.

Pilotní ověřovací provoz informačního systému datových schránek byl na vybraných úřadech a organizacích spuštěn dne 1. května 2009. Od 1. června 2009 bylo pomocí otevřeného rozhraní pro uživatele ISDS spuštěno veřejné testování systému. Do ostrého provozu byl systém datových schránek, za značného zájmu médií, spuštěn dne 1. července 2009.

2.3 Účel datových schránek

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, nám v § 2 odst. 1 definuje datovou schránku takto:

„Datová schránka je elektronické úložiště, které je určeno k

a) doručování orgány veřejné moci,
b) provádění úkonů vůči orgánům veřejné moci,
c) dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.

Datová schránka je tedy určena zejména k doručování a provádění úkonů vůči orgánům veřejné moci a také k dodávání dokumentů soukromých osob. Zákon nám v úvodu definuje orgány veřejné moci jako státní orgány, orgány územních samosprávných celků, státních fondů, zdravotních pojišťoven, Českého rozhlasu, České televize, samosprávných komor zřízených zákonem, notářů a soudních exekutorů. Z pohledu uživatele lze datovou schránku přirovnat k běžné e-mailové schránce. Rozdíl je ovšem v tom, že u datové schránky je garantována důvěryhodnost a integrita doručovaných zpráv.

2.3.1 Datové zprávy

Dokumenty doručované prostřednictvím datových schránek mají formu datových zpráv. To znamená elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích používaných při zpracování a přenosu dat elektronickou formou. Datová zpráva se skládá z obálky, která obsahuje údaje o odesílateli a příjemci a další potřebné informace, například požadavek na doručení „do vlastních rukou“. Druhou část datové zprávy tvoří obsah datové zprávy. Je to vlastní dokument, který se přikládá ve formě jedné nebo více příloh. Vlastní obsah datových zpráv je neveřejný. Velikost datové zprávy je omezena na maximální velikost 10 MB. Za doručení datové zprávy je považován okamžik přihlášení oprávněné osoby do schránky. Odesílatel dostane informaci o doručení zprávy, nepřístupnosti schránky, nebo její neexistenci.

2.3.2 Datové formáty

Datový formát je způsob kódování záznamu (dokumentu), který zajišťuje uložení dokumentu nebo jeho části (částí) pro účely zpracování výpočetní technikou a jeho znázornění. [1]

Podporovány jsou následující formáty:

- PDF[3] a PDF / A (Portable Document Format) jsou nejspíš nejběžnější. Jedná se typicky o převážně textové dokumenty, ačkoliv PDF může obsahovat i formuláře, audio, video, 3D objekty a dokonce i programový kód. PDF / A je jeho varianta určená pro dlouhodobou archivaci.

[3] PDF – angl. Portable Document Format – přenosný formát dokumentu

- DOC, DOCX, RTF a ODT jsou formáty pro převážně textové dokumenty, podporované kancelářskými balíky jako Microsoft Office, OpenOffice.org nebo Libre Office.
- XLS, XLSX a ODS jsou formáty týchž balíků pro tabulková data.
- PPT, PPTX a ODP jsou formáty týchž balíků pro prezentace.
- Prostý text (TXT).
- Přiložit můžete i obrázky, ve formátech JPEG, GIF, PNG a TIFF.
- Zvukové záznamy ve formátech WAV, MP2 a MP3.
- Videa ve formátech MPEG-1 a MPEG-2.
- XML[4], k němuž vyhláška dodává, že musí odpovídat schématu vyhlášenému příjemcem zprávy, což je podmínka v praxi nekontrolovatelná. Typicky se bude nicméně jednat například o data vyexportovaná z nějakého specializovaného programu.
- FO z ZFO, což jsou formáty programu Software602 Form Filler, například uložená celá zpráva z datové schránky.
- Webové stránky ve formátu HTML[5].
- ISDOC a ISDOCX, což je poněkud zvláštní a v praxi nepříliš rozšířený národní formát pro zasílání účetních dokladů.
- EDI, což je podstatně rozšířenější mezinárodní standard pro totéž.
- No a konečně širokou škálu formátů, které se používají pro technické a mapové výkresy, jako DWG (AutoCad), DGN (MicroStation), SHP, DBF, SHX, PRJ, QIX, SBX (ESRI) a GML, GFS, XSD (Geography Markup Language definovaný OGC). [5]

Pokud se odesílatel pokusí poslat pomocí datové schránky datovou zprávu jiného formátu, než je uvedeno, nebo její velikost přesáhne uvedených 10 MB, je povinností správce informačního systému datových schránek tuto zprávu nepřijmout.

2.4 Typy datových schránek

Podle subjektů, jimž jsou zřizovány, rozlišujeme čtyři základní typy datových schránek:

[4] XML – angl. eXtensible Markup Language – rozšiřitelný značkovací jazyk
[5] HTML – HyperText Markup Language – značkovací jazyk pro hypertext

- Datová schránka fyzické osoby (FO)
- Datová schránka podnikající fyzické osoby (PFO)
- Datová schránka právnické osoby (PO)
- Datová schránka orgánu veřejné moci (OVM)

Počet datových schránek je pro jednotlivé subjekty omezen. Fyzická osoba má nárok pouze na jednu datovou schránku fyzické osoby. Podnikající fyzická osoba může disponovat datovou schránkou fyzické osoby i podnikající fyzické osoby. Každá právnická osoba může disponovat pouze jednou datovou schránkou. Každý OVM může mít pouze jednu datovou schránku. Více datových schránek si mohou zřídit pouze orgány územních samosprávných celků.

2.4.1 Zřizování datové schránky

Správcem a provozovatelem informačního systému datových schránek je Česká pošta. Ta také přijímá žádosti o jejich zřízení. O zřízení datové schránky může zažádat každý, pro fyzické osoby, většinu podnikajících fyzických osob a část právnických osob je však tento krok nepovinný. Datové schránky je možno zřídit dvojím způsobem, na žádost a ze zákona.

Datová schránka FO je zřizována ministerstvem bezúplatně na žádost fyzické osobě, která je plně způsobilá k právním úkonům, do 3 pracovních dnů ode dne podání žádosti.

Datovou schránku PFO zřídí ministerstvo podnikající fyzické osobě bezúplatně na žádost této osoby do 3 pracovních dnů ode dne podání žádosti. Advokátu, daňovému poradci a insolvenčnímu správci ji zřizuje ministerstvo bezodkladně poté, co obdrží informaci o jejich zapsání do zákonem stanovené evidence. Ministerstvo však 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.

Datovou schránku PO zřídí ministerstvo bezúplatně 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. 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.

Datovou schránku OVM zřídí ministerstvo bezodkladně po jejich vzniku, v případě notářů a soudních exekutorů bezodkladně poté, co obdrží informaci o jejich zapsání do zákonem stanovené evidence. K přístupu do datové schránky orgánu veřejné moci je oprávněn vedoucí orgánu veřejné moci, pro něhož byla datová schránka zřízena. [17]

2.4.2 Zpřístupnění datové schránky

Přijímat a odesílat datové zprávy prostřednictvím datové schránky je možné pouze, pokud je zpřístupněna. Přístupové údaje k datové schránce zašle Ministerstvo vnitra, v obálce se žlutým pruhem, do vlastních rukou oprávněné osobě bezodkladně po zřízení datové schránky. Oprávněnou osobou je buď fyzická osoba, podnikající fyzická osoba, statutární orgán právnické osoby, nebo vedoucí orgánu veřejné moci.

V rámci tohoto postupu platí doručení přístupových údajů prostřednictvím fikce. Datová schránka je zpřístupněna prvním přihlášením oprávněné osoby nebo automaticky patnáctým dnem od doručení přístupových údajů, bez ohledu zda se do ní uživatel přihlásil. Datová schránka se zpřístupní vždy patnáctý den bez ohledu na to, zda je to pracovní den, sobota, neděle, nebo svátek. Tímto dnem je datová schránka zpřístupněna a mohou do ní být zasílány zprávy.

2.4.3 Znepřístupnění datové schránky

Datovou schránku fyzické osoby nebo podnikající fyzické osoby znepřístupní Ministerstvo vnitra na základě úmrtí, omezení způsobilosti k právním úkonům, či omezení osobní svobody. Ostatní datové schránky se znepřístupní v případě zániku daného subjektu, nebo rušení jeho funkce. Znepřístupnění schránky se provede ke dni, kdy došlo k události, jež je důvodem znepřístupnění.

Pokud byla datová schránka zřízena na základě žádosti, je možné ji také na základě žádosti znepřístupnit. Datová schránka zřízená ze zákona takovou možnost nemá.

2.4.4 Zrušení datové schránky

Zrušení datové schránky musí vždy předcházet její znepřístupnění.

Ministerstvo vnitra 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. [17]

Existují ale případy, kdy znepřístupněná schránka nemůže být zrušena. A to, pokud bude mít zaniklá právnická osoba právního nástupce. Pak by měl správce informačního systému datových schránek umožnit právnímu nástupci zaniklé právnické osoby přístup k obsahu její datové schránky. Dále zákon neumožňuje zrušení datové schránky znepřístupněné na žádost.

3 ELEKTRONICKÝ PODPIS

Elektronický podpis je jedním z hlavních nástrojů identifikace a autentizace fyzických osob v prostředí internetu. Postupně stále více právních předpisů umožňuje jeho používání v oblasti orgánů veřejné správy, a to jak při komunikaci mezi úřady navzájem, tak i při komunikaci občanů s jednotlivými úřady. [12]

3.1 Krátká historie vzniku

Vůbec prvním legislativním dokumentem o elektronickém podpisu ve světě je „Utah Digital Signature Act“, který stát Utah přijal již 27. února 1995. Evropská unie se touto problematikou začala zabývat v dubnu 1997, kdy potřebovala právní úpravu k zajištění bezpečnosti a důvěryhodnosti elektronické komunikace pro fungování elektronického obchodu. Výsledkem byla Směrnice Evropského parlamentu a Rady 1999/93/ES[6] o zásadách Společenství pro elektronické podpisy. Jejím cílem bylo usnadnit používání elektronických podpisů, stanovit jejich právní účinky a podmínky ověřovacích služeb. Zároveň stanovila členským státům lhůtu do 19. července 2001, aby tyto požadavky transponovaly do svých právních řádů. Česká republika přijala v roce 2000 zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), a stala se tak v pořadí třetí zemí, kde začal platit zákon o elektronickém podpisu.

3.1.1 Definice elektronického podpisu

Zákon o elektronickém podpisu definuje elektronický podpis v § 2 písm. a) jako:

„údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“. [20]

Vyšší formou elektronického podpisu je zaručený elektronický podpis, který je v § 2 písm. b) zmiňovaného zákona definován jako:

„elektronický podpis, který splňuje následující požadavky

1. je jednoznačně spojen s podepisující osobou,

[6] ES – Evropské společenství

2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat“. [20]

3.2 Vlastnosti elektronického podpisu

Elektronický podpis totiž ve své podstatě není ničím jiným než (hodně velkým) číslem. Dokonce tak velkým, že by nebylo až tak šikovné ho psát jako binární číslo (jako posloupnost jedniček a nul). Takže pokud je někdy třeba ho zapsat tak, aby to bylo alespoň nějak srozumitelné pro člověka, využívá se k tomu nějaká efektivnější reprezentace (kódování) tak, aby se vystačilo s méně znaky. Příkladem takového znázornění elektronického podpisu může být následující řetězec:

„IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthba4Blrcnjaqbc
KgNv+a5kr4537y8RCd+RHm75yYh5xxA1ojELwNhhb7cltrp2V7LlOnAelws
4S87UX80cLBtBcN6AACf11qymC2h+Rb2j5SU+rmXWru+=QFMx“

Pokud vás tento řetězec poněkud vystrašil, pak nezoufejte, v praxi nebudete s elektronickým podpisem pracovat v takovéto podobě (jako s číslem). Tak s ním pracují programy, které elektronický podpis na elektronickém dokumentu ověřují, a výsledek svého ověření dokážou svým uživatelům zobrazit v mnohem uživatelsky příjemnější (a také obsažnější) podobě. [4]

Pokud je zajištěna správná implementace technologií spojených s využitím elektronického podpisu, můžeme říci, že elektronický podpis zajišťuje vysokou míru bezpečnosti z pohledu integrity přenášených informací a neodmítnutelnosti odpovědnosti komunikujících stran za odeslání, případně doručení dokumentu. Využití certifikátů a kryptografických metod zajišťuje navíc i důvěrnost přenášených dat.

3.2.1 Integrita přenášených informací

Integrita znamená stav, kdy jsou přečtená data totožná s daty uloženými. To znamená zajištění, že se dokument v průběhu zpracování a přenosu nezměnil. Jediný spolehlivý způsob, jak toho dosáhnout, je aplikace kryptografických mechanismů. Tyto mechanismy v případě elektronického podpisu nebo datové schránky nezajišťují neporušitelnost integrity, tedy neznemožňují provedení úpravy přenášených dat. Jsou ale schopny provést následnou detekci případné změny datového obsahu, tedy zjistit, že se dokument změnil.

3.2.2 Neodmítnutelnost odpovědnosti

S tímto pojmem jsou spojovány termíny autentizace a autorizace. Autentizace je proces ověření proklamované identity osoby přistupující do informačního systému. Základní úroveň autentizace je prezentována uživatelským jménem a bezpečnostním heslem. I když bývají požadavky informačních systémů na bezpečnostní heslo přísné, minimální délka osm znaků, minimálně jedno velké písmeno, jedno malé písmeno, jedna číslice, případně speciální znak, představuje tento způsob nejnižší únosnou míru bezpečnosti, a není proto odborníky doporučován.

Autorizace je proces zjišťování, zda je osoba přistupující do informačního systému oprávněna provádět požadovaný úkon. Znamená tedy schválení, umožnění přístupu či provedení konkrétní operace danou osobou.

Neodmítnutelnost odpovědnosti je vlastně vyšší forma autentizace. Autentizací identifikujeme přistupující osobu v daném okamžiku, ale neodmítnutelností odpovědnosti je možné tuto identifikaci prokázat i následně. Standardně je používán buď zaručený elektronický podpis, nebo elektronická značka. Technologie elektronických značek je prakticky stejná jako technologie elektronického podpisu. Jediný rozdíl je v právních důsledcích jejich užití. Pokud je zpráva opatřena zaručeným elektronickým podpisem, má se za to, že se podepisující osoba s obsahem zprávy před jejím podepsáním seznámila. Elektronickou značkou jsou však zprávy označovány automatizovaně, tedy bez ověření obsahu. Připojením zaručeného elektronického podpisu odesílatele ke zprávě je splněn požadavek neodmítnutelnosti odpovědnosti, protože jeho identita ve vztahu k datové zprávě může být jednoznačně ověřena, jak požaduje zákon.

3.2.3 Důvěrnost přenášených dat

Doručování dokumentů prostřednictvím informačních systémů musí splňovat princip neporušitelnosti listovního tajemství. V čl. 13 Listiny základních práv a svobod je stanoveno:

„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením“. [7]

Dokument doručený poštovní službou v zalepené a nepoškozené obálce poskytuje vysokou garanci důvěrnosti dokumentu po celou cestu od odesílatele k příjemci. Důvěrnost informačních systémů je nejčastěji definována jako zajištění, že informace jsou přístupné

nebo sděleny pouze těm, kteří jsou k tomu oprávněni. Informační systém musí zabezpečit, že neautorizované subjekty nebudou mít možnost přístupu k citlivým informacím. Zabezpečuje to šifrováním komunikace, za použití aktuálních a běžně užívaných technologií. Podobně jako v aplikacích elektronického bankovnictví je takto zajištěna důvěrnost zpráv před potenciálním útokem zvenčí.

3.3 Kryptografie

Pro zabezpečení elektronického podpisu je v současnosti využívána kombinace dvou kryptografických metod, a to asymetrické kryptografie a tzv. hashovací funkce.

3.3.1 Asymetrické šifrování

Asymetrické šifrování je založeno na dvojici klíčů. Tuto dvojici klíčů si vygeneruje uživatel pomocí některého z běžně dostupných softwarových produktů, a stává se tak jejich jediným majitelem. Princip spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Jeden z nich, takzvaný privátní klíč, je s maximální bezpečností ukrýván majitelem (čipová karta, USB[7] token…), zatímco druhý klíč je zveřejněn – veřejný klíč. Veřejný klíč je následně využíván pro ověřování elektronického podpisu.

3.3.2 Hashovací funkce

Funkce hash je matematická funkce (resp. algoritmus) pro převod vstupních dat do (relativně) malého čísla. Její vlastnosti umožňují její použití v aplikacích zabezpečení informací, jako například autentizace nebo zaručení integrity zprávy. Výstupem hashovací funkce je otisk, výtah či hash (česky též někdy jako haš).

Mezi hlavní vlastnosti této funkce patří:

- jakékoliv množství vstupních dat poskytuje stejně dlouhý výstup (otisk),
- malou změnou vstupních dat dosáhneme velké změny na výstupu (tj. výsledný otisk se od původního zásadně na první pohled liší),

[7] USB – angl. Universal Serial Bus – univerzální sériová sběrnice, moderní způsob připojení periferií k počítači

- z hashe je prakticky nemožné rekonstruovat původní text zprávy (což je rozdíl oproti klasickému šifrování).

Ještě v roce 2009 se i v oblasti elektronického podpisu nejčastěji používala hašovací funkce SHA[8]-1. Ta vytváří otisky (hashe) o velikosti 160 bitů.

Od počátku roku 2010 je doporučeno používat propracovanější hašovací funkce z rodiny SHA-2, které již pracují s většími otisky: velikosti 224, 256, 384, nebo 512 bitů. [4]

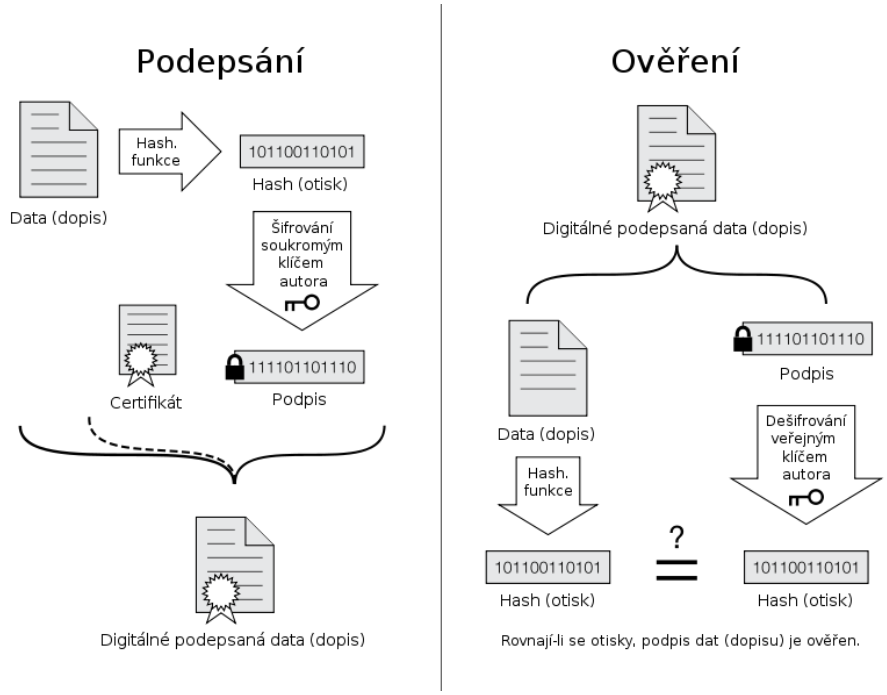
V praxi je vysoce nepravděpodobné, že dvěma různým zprávám odpovídá stejný hash, proto lze pomocí hashe identifikovat právě jednu zprávu (ověřit její správnost).

3.4 Princip elektronického podpisu

Nejprve je vypočten otisk, tzv. hash dokumentu, což je datový řetězec o určité pevné délce, který jednoznačně charakterizuje obsah dokumentu. Výsledný hash je poté zašifrován autorovým privátním klíčem (tj. utajeným klíčem), čímž vznikne elektronický podpis, který spolu s původním obsahem dokumentu tvoří elektronicky podepsaný dokument.

Při ověření podpisu příjemce dokumentu nejprve znovu vypočte hash zprávy. Poté pomocí veřejného klíče autora podpisu dešifruje obsah elektronického podpisu a výsledek porovná s vypočteným hashem zprávy. Pokud jsou obě hodnoty hashe stejné, je podpis z matematického hlediska platný. V tuto chvíli však není možné považovat platný elektronický podpis za důvěryhodný, protože není jisté, kdo je majitelem veřejného klíče, pomocí kterého došlo k matematickému ověření podpisu. K tomu slouží takzvaný certifikát, vydaný a elektronicky podepsaný uznávanou certifikační autoritou, který potvrzuje platnost veřejného klíče podepisujícího.

[8] SHA – angl. Secure Hash Algorithm – je rozšířená hašovací funkce, která vytváří ze vstupních dat výstup (otisk) fixní délky



Obr. 3. Elektronický podpis (převzato z [10]).

3.5 Certifikační autorita a certifikáty

Certifikační autorita je subjekt, který vydává digitální certifikáty a zajišťuje jejich správu, včetně vydávání seznamů zneplatněných certifikátů. Při vzájemné komunikaci dvou subjektů vystupuje jako třetí nezávislý subjekt. Musí být důvěryhodný pro uživatele certifikačních služeb, kterým vydává certifikáty. Musí být ale také důvěryhodný pro osoby, které se spoléhají na podpisy, s nimiž jsou tyto certifikáty spojeny. Svojí autoritou potvrzuje prostřednictvím jím vydaného certifikátu pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. Na základě principu přenosu důvěry tak můžeme důvěřovat údajům uvedeným v digitálním certifikátu za předpokladu, že důvěřujeme samotné certifikační autoritě.

Ministerstvo vnitra vykonává povinnosti stanovené zákonem č. 227/2000 Sb., o elektronickém podpisu, a stanovuje požadavky podle vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. Zpracovává také návrhy právních předpisů týkajících se elektronického podpisu a v jeho působnosti je rovněž zajištění mezinárodní spolupráce v této oblasti a plnění úkolů plynoucích z členství ČR v mezinárodních organizacích.

Ministerstvo vnitra zveřejňuje v souladu s § 9 odst. 2 písm. e) zákona č. 227/2000 Sb. přehled udělených akreditací. Ministerstvo vnitra udělilo akreditaci k působení jako

akreditovaný poskytovatel certifikačních služeb v tabulce uvedeným subjektům na základě:

- splnění všech podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona č. 227/2000 Sb. (zákon o elektronickém podpisu);
- splnění podmínek, požadavků a postupů stanovených vyhláškou č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb);
- ověření kvalifikovaných systémových certifikátů Ministerstvem vnitra podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu. [9]

V současné době jsou v České republice tři akreditovaní poskytovatelé certifikačních služeb, kterých může zájemce o získání certifikátu využít.

Tab. 1. Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich služeb (převzato z [15])

Poř. číslo	Poskytovatelé certifikačních služeb	Kvalifikované služby	Zahájení vydávání
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	03/2002 02/2006 02/2006
2.	Česká pošta, s. p., identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	09/2005 04/2005 07/2009
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	08/2005 08/2005 08/2010

Odbor Hlavního architekta eGovernment, 1.8.2012

3.6 Rozdělení certifikátů

Nejzákladnější rozdělení certifikátů z hlediska použití je na certifikáty kvalifikované a komerční.

Kvalifikované certifikáty jsou nedílnou součástí bezpečné komunikace občanů se státní správou a samosprávou. Dále si pak můžeme vybrat mezi osobním kvalifikovaným certifikátem, který identifikuje konkrétní osobu, a systémovým kvalifikovaným certifikátem, který lze přirovnat k razítku organizace.

Komerční certifikáty nabízejí řešení pro bezpečné přihlašování nebo posílání zašifrovaných e-mailů. Stejně jako u kvalifikovaných certifikátů je dále rozdělujeme na osobní komerční certifikáty a systémové komerční certifikáty. Osobní je určen pro konkrétní osoby a může například zvýšit bezpečnost přihlášení do datové schránky. Systémový je určen pro technická zařízení, jako například aplikace na serverech, a může být využit při řešení spisové služby nebo zabezpečení komunikace mezi servery.

3.6.1 Kvalifikovaný certifikát

Kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb splňuje všechny aktuální požadavky dané legislativou, zejména zákonem o elektronickém podpisu (zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů v aktuálním znění). Kvalifikovaný certifikát je standardizován také v rámci Evropské unie (Směrnice Evropského parlamentu a Rady 1999/93/ES). [11] Certifikáty jsou vydávány s platností na jeden rok.

Kvalifikované certifikáty nám umožňují zejména:

- elektronicky archivovat dokumenty,
- elektronicky podávat daňové přiznání,
- odesílat datové zprávy, pokud vaše společnost má více jednatelů,
- komunikovat s Českou správou sociálního zabezpečení,
- využívat elektronické formuláře a e-podatelny,
- pracovat s e-tržišti.

Osobní kvalifikovaný certifikát je naprosto nezbytný při odesílání zpráv z datové schránky u společností s více jednateli nebo ze schránek orgánů veřejné moci. Dále k vytváření elektronického podpisu, ověřování elektronických podpisů a zajištění nepopiratelnosti. Od ledna 2012 je možné nechat si nahrát kvalifikovaný certifikát do elektronického občanského průkazu - eOP vybaveného kontaktním čipem.

Systémové kvalifikované certifikáty lze používat pro:

- vytváření elektronické značky

- ověřování elektronických značek
- bezpečné ověřování elektronických značek
- zajištění nepopiratelnosti (vazba mezi dokumentem a subjektem vytvářející elektronickou značku)

Elektronickou značku je možno vytvářet automatizovaně bez součinnosti konkrétní fyzické osoby. Příkladem jsou např. elektronická fakturace, hromadné zasílání e-mailů, doručenek e-podatelny apod.

Použití kvalifikovaného certifikátu je podle platné legislativy omezeno pouze pro elektronický podpis. Pro další úkony, jako je například šifrování přenášených zpráv nebo zabezpečení vlastního webového serveru, potřebujeme jiný komerční certifikát.

3.6.2 Komerční certifikát

Svoji významnou úlohu má komerční certifikát především tam, kde nelze s ohledem na platnou legislativu využít kvalifikované certifikáty. Nejčastěji se používá mezi komerčními subjekty jako nástroj pro bezpečnou komunikaci, pro přihlášení do datové schránky nebo pro bezpečný přístup do aplikací. Jejich nejčastější použití má podobu zaměstnaneckých certifikátů, jejichž účelem je zajištění interní bezpečné komunikace mezi zaměstnanci, případně pro realizaci vzdáleného přístupu zaměstnanců k firemním datovým zdrojům.

V současné době mají komerční certifikáty použití zejména pro šifrování a autentizaci. Jedná se především o neanonymní přístup na webové servery a předávání šifrovaných dat jak e-mailovou poštou, tak prostřednictvím webových formulářů. Komerční certifikáty jsou vydávány s platností na jeden rok.

3.7 Tvorba certifikátu

Postup pro získání certifikátu se liší pro orgány veřejné moci, firmy a organizace, podnikatele a pro fyzické osoby, ale dá se shrnout zhruba do šesti kroků.

1. Generování klíčů – zpravidla přímo na stránkách certifikační autority si žadatel sám na svém PC[9] spustí automatickou nebo poloautomatickou proceduru, pomocí které vygeneruje dvojici klíčů.

[9] PC – angl. Personal Computer – osobní počítač

2. Příprava identifikačních dat a žádosti o certifikát – žadatel o certifikát si podle požadavků certifikační autority připraví dokumenty nutné pro vydání certifikátu. Je to například:
    - občanský průkaz nebo cestovní pas,
    - další doklad totožnosti (karta zdravotní pojišťovny, cestovní pas, řidičský průkaz),
    - doložení existence společnosti (originál nebo úředně ověřená kopie živnostenského listu, zřizovací listiny, úplné obchodní jméno, identifikační číslo (je-li přiřazeno), adresa sídla, jméno osoby/osob, oprávněné/oprávněných k zastupování (statutárních zástupců), a způsob, jakým za právnickou osobu jednají a podepisují),
    - potvrzení o zaměstnaneckém poměru (potvrzení musí být opatřeno podpisem osoby s právem jednání za příslušného zaměstnavatele; na dokumentu se vždy uvádí jméno, příjmení a funkce oprávněné osoby – statutárního zástupce).
3. Předání žádosti o certifikát certifikační autoritě – pro vydání prvotního certifikátu je nutná osobní návštěva registrační autority. Jsou to kontaktní místa certifikační autority pro styk s veřejností. Bývají oddělena od centrálního systému z důvodu zajištění vyšší bezpečnosti, ale především pro vytvoření kontaktních míst v co nejvíce lokalitách, aby se zvýšila dostupnost poskytovaných služeb.
4. Ověření informací – certifikační autorita provede kontrolu předložených dokladů a ověří si informace z dostupných registrů a ostatních datových zdrojů, že je možné žadateli certifikát vydat.
5. Tvorba certifikátu – registrační autorita pošle žádost o certifikát do centrálního systému certifikační autority, kde dojde k vytvoření digitálního dokumentu příslušného datového formátu. Ten je následně podepsán privátním klíčem certifikační autority a odeslán zpět na registrační autoritu.
6. Předání certifikátu – certifikát je žadateli předán na paměťovém médiu, zaslán e-mailem a případně zveřejněn. Zveřejněním lze zjistit informace o jeho platnosti a stavu, což zvyšuje jeho důvěryhodnost. Naopak nezveřejnění poskytuje pouze minimální ochranu proti zneužití.

3.8 Časová razítka

Zákon o elektronickém podpisu nám v § 2 písm. r) definuje kvalifikované časové razítko takto:

„datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem“. [1]

Časové razítko je podobně jako elektronický podpis kontrolním otiskem dokumentu. Na rozdíl od elektronického podpisu z něj však zpětně nezjistíme, kdo dokument podepsal, ale kdy byl podepsán. Tedy kdy k němu bylo časové razítko připojeno. Tento čas není odvozen ze systémového času PC uživatele, ale z údajů hodin provozovaných certifikační autoritou, které jsou neustále synchronizovány s několika atomovými hodinami v různých částech světa.

Připojuje se tedy k dokumentům jako nezpochybnitelný důkaz, že v daném čase a v dané podobě existovaly. Spojení důvěryhodného a zpětně ověřitelného časového údaje a konkrétních dat je nepostradatelné zejména pro účely prokazatelnosti, kdy dokument vznikl, kdy byl přijat a kdy byl podepsán. Protože každý podpisový certifikát dříve či později ztratí platnost, může majitel dokumentu pomocí časového razítka prokázat, že elektronický podpis byl v době připojení k dokumentu platný.

Pokud chceme k dokumentům připojovat kvalifikované časové razítko, máme dvě možnosti. Můžeme získávat razítka přímo od akreditované certifikační autority, jako je třeba Time Stamp Authority. Budeme ovšem muset investovat do technického propojení a cena razítka se bude odvíjet od počtu spotřebovaných razítek za určité časové období. Nebo můžeme získávat razítka v rámci služby SecuStamp, která poskytuje razítka od české akreditované autority PostSignum, která jsou právně uznávaná v rámci celé Evropské unie. K jejich pořízení není zapotřebí uzavírat smlouvu, ani řešit otázku propojení. Můžeme koupit balík razítek a spotřebovávat je postupně podle potřeby, bez časového limitu jejich použitelnosti.

II. PRAKTICKÁ ČÁST

4 ELEKTRONICKÝ PODPIS VE SPECIFICKÉM PROSTŘEDÍ

STÁTNÍ TISKÁRNA CENIN, státní podnik, (STC) používá při svých činnostech několik druhů certifikátů. Jsou to kvalifikované certifikáty QC, kvalifikované systémové certifikáty QSC, komerční certifikáty SC a serverové certifikáty SS. Jako dodavatele si STC zvolila akreditovanou certifikační autoritu První certifikační autorita, a. s., (I.CA), se kterou uzavřela smlouvu.

4.1 Možnosti získání certifikátu

Postup pro získání certifikátu v sobě zahrnuje požadavky Certifikační politiky akreditované certifikační autority a požadavky vnitropodnikové dokumentace STC.

Pokud zaměstnanci z titulu své pracovní funkce nebo pro plnění svých pracovních povinností vyplývá potřeba používat kvalifikovaný nebo komerční certifikát, musí nejdříve vnitřním sdělením zažádat příslušného nadřízeného zaměstnance o schválení jeho pořízení.

Po schválení své žádosti může přistoupit k vlastnímu získání certifikátu. První certifikační autorita, a. s., nabízí na svých internetových stránkách www.ica.cz komerční a kvalifikované certifikáty s možností výběru úložiště certifikátu. Ve variantě „STANDARD“ jsou certifikát a příslušná data pro vytváření elektronického podpisu umístěny v PC. Žádost o certifikát je tedy nutné generovat na PC žadatele. Po vytvoření žádosti je doporučeno provést zálohu soukromého klíče. Ve variantě „KOMFORT“ je součástí služby čipová karta nebo USB token, jako bezpečné úložiště pro data potřebná pro vytvoření elektronického podpisu a certifikátu. Pokud si žadatel na vytvoření žádosti sám netroufá, může navštívit registrační autoritu v místě sídla společnosti. Tam mu po předložení potřebných dokumentů operátor žádost o certifikát vygeneruje a data mu na čipovou kartu uloží.

Žádost o certifikát je možné vytvořit dvěma způsoby, prostřednictvím online formuláře uvedeného na webových stránkách nebo prostřednictvím offline aplikace I.CA NewCert, kterou je možno nainstalovat také z webových stránek I.CA. V obou případech je nutné tvořit žádost o certifikát na tom PC, na kterém bude certifikát následně používán. V STC je ve většině případů žádost tvořena online s certifikátem uloženým v PC uživatele.

4.2 Generování žádosti online

Po kliknutí na tlačítko „Žádost o certifikát“ dojde nejdříve k otestování, zda PC žadatele splňuje požadavky na bezproblémové vytvoření žádosti o certifikát. Testuje se například verze operačního systému, typ a verze prohlížeče, nebo podpora Java Runtime Environment (JRE). Po úspěšném ukončení testu je kliknutím na tlačítko zahájena vlastní tvorba žádosti o certifikát.

Při vyplňování žádosti jsou žlutě označena pole povinná a je nutné je vyplnit. Ostatní pole jsou nepovinná, ale pokud jsou vyplněna, je nutno tyto údaje doložit. Pro úspěšné dokončení tvorby žádosti máme k dispozici průvodce. Pokud jsme vše vyplnili správně, je žádost uložena na serveru certifikační autority a přijata ke zpracování. Informační systém I.CA automaticky vygeneruje zprávu a odešle ji e-mailem na adresu žadatele. Ve zprávě je uvedena informace o uložení žádosti, výzva k osobní návštěvě registrační autority pro vydání certifikátu a ID[10] uložené žádosti. Přílohou e-mailu je vlastní žádost o certifikát. Lhůta pro osobní vyzvednutí certifikátu je 30 dní, poté bude žádost z informačního systému automaticky smazána.

4.3 Návštěva registrační autority

Pro vydání prvotního certifikátu je nutná osobní návštěva registrační autority. Při návštěvě registrační autority jsou pro vydání certifikátu potřeba požadované dokumenty a žádost o certifikát. Zaměstnanec je povinen pro vydání certifikátu předložit:

- občanský průkaz,
- další doklad totožnosti (karta zdravotní pojišťovny, cestovní pas, řidičský průkaz),
- potvrzení o zaměstnaneckém poměru dle vzoru.

STC je společností zapsanou v Obchodním rejstříku ČR a tento dokument je k dispozici v elektronické podobě na internetových stránkách Ministerstva spravedlnosti. Žadatel proto nemusí předkládat výpis, je možné jej pořídit přímo na registrační autoritě I.CA. V případě, že by si zaměstnanec nevyzvedával svůj certifikát sám, ale byl zastupován určenou osobou, musí tato osoba kromě výše uvedených dokumentů u registrační autority doložit:

[10] ID – identifikátor

- občanský průkaz zmocněnce
- další doklad totožnosti zmocněnce
- doklad prokazující právo jednat jako zmocněnec – plnou moc
- originály občanského průkazu nebo cestovního pasu, protože v ČR nelze pořizovat ověřené kopie osobních dokladů, případně úředně ověřené kopie druhého dokladu totožnosti žadatele o certifikát (zmocnitele)
- další dokumenty dle typu certifikátu.

Po vygenerování žádosti má žadatel o certifikát dvě možnosti, jak pokračovat v získání certifikátu. První z nich je postupovat, jak bylo popsáno výše, a dostavit se s potřebnými dokumenty na vybranou registrační autoritu. Druhou možností je navštívit vlastní „pobočku“ registrační autority přímo v STC.

4.4 Registrační autorita STC

V roce 2006 společně s přípravou výrobního projektu Cestovní doklady s biometrickými prvky (CDBP) došlo po vzájemné dohodě mezi STC a I.CA ke vzniku registrační autority přímo ve výrobním závodě, kde probíhá výroba dokladů. Byl vytvořen dokument, který jasně definuje pravidla pro registrační autoritu STC a stanovuje podmínky podání a vyřízení žádosti o kvalifikovaný certifikát.

V STC byl vybrán zaměstnanec, který byl proškolen a stal se operátorem registrační autority. Do jeho počítače mu byla technikem První certifikační autority, a. s., nainstalována softwarová aplikace „icara“, která mu umožňuje vyřizovat žádosti o kvalifikované i komerční certifikáty. Jako nový hardware mu byl připojen terminál pro autentizaci k této aplikaci pomocí PIN[11] kódu zaměstnance a čtečka čipových karet. Pro vyřízení certifikátu smí tento zaměstnanec potřebné dokumenty podepisovat a orazítkovat razítkem První certifikační autority, a. s.

4.4.1 Tvorba certifikátu

Tvorba certifikátu na registrační autoritě STC probíhá v několika krocích:

[11] PIN – angl. Personal Identification Number – osobní identifikační číslo

1. Nejdříve zaměstnanec, který žádá o certifikát, přepošle e-mailem žádost o certifikát, kterou obdržel od informačního systému I.CA, na e-mail operátora RA[12] a domluví se s ním na termínu návštěvy.
2. Operátor RA načte žádost do aplikace a ověří platnost předložených dokladů. Potom provede kontrolu údajů v žádosti a doplní číslo občanského průkazu, druhého dokladu, případně další potřebné údaje.
3. Dalším krokem je systémem prováděná rekapitulace vyplněných údajů, tedy jestli jsou vyplněna všechna povinná pole.
4. V případě, že je výsledek provedených kontrol pozitivní, okopíruje operátor RA obě strany obou dokladů totožnosti a vytvoří dokument „Protokol o podání žádosti o vydání certifikátu I.CA“. Součástí dokumentu je heslo pro zneplatnění certifikátu, prohlášení žadatele, že zachází s daty pro vytváření elektronických podpisů s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití, a ve většině případů nesouhlas se zveřejněním certifikátu. Protokol je vytištěn ve dvou provedeních, první je pro žadatele s viditelným heslem pro zneplatnění certifikátu, druhý je pro operátora RA a má toto heslo zakryto hvězdičkami. Svým podpisem žadatel stvrzuje, že zkontroloval správnost uvedených údajů a souhlasí se shromažďováním osobních údajů (kopie osobních dokladů) dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Pokud žadatel odmítne tento protokol podepsat, je operátor RA povinen proces vydávání certifikátu ukončit a kopie osobních dokladů vrátit žadateli.
5. Po podpisu protokolu žadatelem i operátorem RA je žádost odeslána do centrálního systému certifikační autority. V online režimu je možné při čekání na odpověď sledovat ruční kontrolu jednotlivých položek operátorem certifikační autority.
6. Pokud je vše vyplněno správně a kontrola je v pořádku, operátor certifikační autority vytvoří certifikát. Odešle ho na e-mail uvedený v žádosti a potvrdí operátorovi RA předání certifikátu.
7. Po předání certifikátu žadateli vytiskne operátor RA „Smlouvu o vydání a používání certifikátu“ mezi I.CA, zastoupenou na základě plné moci operátorem RA, na straně jedné a žadatelem, tedy zaměstnancem, na straně druhé. Smlouva

[12] RA – registrační autorita

obsahuje údaje o tom, pro koho je certifikát určen, otisk certifikátu, datum vzniku a ukončení platnosti certifikátu, registrační číslo žádosti a popisuje práva a povinnosti majitele certifikátu a záruky ze strany I.CA. Je vytištěna ve dvou vyhotoveních a po podepsání oběma stranami je jedno předáno majiteli certifikátu.

8. Zbývá poslední krok celého procesu získávání certifikátu – uložit nový certifikát. Zaměstnancům administrativy, pokud v žádosti uvedli svoji e-mailovou adresu, byl certifikát odeslán e-mailem společně s pokyny pro jeho instalaci. Pro zaměstnance výroby dokladů je certifikát operátorem RA uložen na čipovou kartu a předán do vlastních rukou.

Celý proces tvorby certifikátu zabere operátorovi RA asi deset minut, včetně online kontroly operátorem centrálního systému certifikační autority. To je velmi krátká doba v porovnání s nutností navštívit RA mimo STC. Příkladem z praxe je událost, kdy operátorovi personalizace dokladů skončila platnost certifikátu uprostřed výrobní dávky. Došlo k přerušení výroby a situaci bylo potřeba rychle vyřešit. Operátor RA vytvořil certifikát nový a výroba mohla za patnáct minut po výpadku dále pokračovat.

4.4.2 Archivace žádostí

Zákon o elektronickém podpisu ukládá kvalifikovanému poskytovateli certifikačních služeb povinnost uchovávat informace a dokumentaci související s poskytovanými kvalifikovanými certifikačními službami po dobu nejméně 10 let. Každá žádost o službu má přiděleno jedinečné číslo. Všechny doklady jsou shromažďovány vždy k určitému číslu, a dokumentují tak postup od klientovy žádosti o vydání certifikátu až po předání certifikátu, včetně všech předložených dokladů nebo jejich kopií a potvrzení operátora RA. Souhrn těchto dokumentů tvoří takzvaný protokol. Protokoly musí být uchovány na bezpečném místě, například v trezoru. Operátor RA nese přímou odpovědnost za jejich ztrátu nebo zneužití.

Protokoly se ukládají na RA podle identifikačních čísel žádostí a jednou ročně se předávají zástupci I.CA k archivaci. O jejich předání se vytvoří zápis, který obsahuje zejména:

- období, za které se protokoly vydávají
- interval čísel žádostí
- celkový počet protokolů
- datum předání a jména předávajícího a přebírajícího.

Tento zápis je vyhotoven ve dvou kopiích a podepsán oběma stranami. V případě potřeby mohou být protokoly využity jako podklady pro ověření účetních položek v daném období.

5 MOŽNOSTI VYUŽITÍ ELEKTRONICKÉHO PODPISU

Zaručený elektronický podpis, tedy kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát, lze využít například při komunikaci s orgány veřejné správy výhradně v případech, že tak stanoví příslušný právní předpis. Komerční certifikáty využívají komerční subjekty pro komunikaci s jinými subjekty, které jsou zpravidla klienty jejich služeb, např. banky. S využitím webového rozhraní lze provozovat řadu autorizovaných služeb. Prostřednictvím certifikátů lze také zajistit bezpečný přístup v několika úrovních. S využitím technologie elektronického podpisu (PKI[13]) lze realizovat komplexní informační systémy k zabezpečení externí i interní komunikace.

5.1 Obecné možnosti použití elektronického podpisu

Zaručený elektronický podpis lze ve veřejné správě použít:

- při zasílání datové zprávy prostřednictvím datových schránek
- při zasílání elektronických podání úřadům prostřednictvím e-podatelen
- při podávání daňových přiznání prostřednictvím aplikace EPO (daňový portál)
- při zasílání dokumentů České správě sociálního zabezpečení
- při zasílání dokumentů v rámci projektu e-Customs – bezpapírové celní prostředí napříč celou Evropou (NCTS – elektronická komunikace mezi deklaranty, Celní správou ČR a zeměmi EU a ESVO[14], eDovoz, vývoz)
- při žádostech o dotace EU podávaných prostřednictvím aplikace eAccount CzechInvest
- při žádostech o výpisy z rejstříku trestů
- při podávání hlášení prostřednictvím ISPOP (Integrovaný systém plnění ohlašovacích povinností), tj. ohlašovacích povinností z oblasti životního prostředí
- při vyřizování jednotlivých agend na Magistrátu hl. m. Prahy a na úřadech městských částí prostřednictvím portálu praha.eu
- při odesílání jednotných registračních formulářů (JRF) pro podání živnostenskému rejstříku
- při podávání návrhů na zápis nebo změnu zapsaných údajů do obchodního rejstříku

[13] PKI – angl. Public Key Infrastructure – struktura veřejných klíčů
[14] ESVO – Evropské sdružení volného obchodu

- při odesílání formulářů resortu MPSV[15]
- při elektronickém podávání přihlášek Úřadu průmyslového vlastnictví
- při odesílání formulářů prostřednictvím Portálu farmáře – Ministerstvo zemědělství
- při elektronické komunikaci s VZP[16]

Dále se zaručený elektronický podpis využívá v komerční sféře, například:

- při obchodování na trhu s elektřinou a plynem
  - ČEPS[17], a. s., prostřednictvím elektronického portálu Damas
  - Operátor trhu (OTE, a. s.)
  - Organizátor krátkodobého trhu s elektřinou (OKTE, a. s., portál ISOT[18], ISZO[19])
- při elektronické komunikaci se zdravotními pojišťovnami
- pro komunikaci s ČNB[20] (cenné papíry)

Obecně lze zaručený elektronický podpis použít:

- při ukládání dokumentů v systémech elektronické spisové služby a v elektronických archivech (PDF)
- při zasílání elektronických faktur, dodacích listů a jiných účetních dokladů
- při podepisování e-mailových zpráv [14]

5.2 Možnosti využití elektronického podpisu v STC

V STC je používán elektronický podpis například na podepisování a šifrování e-mailů, pro přihlašování k různým portálům a ke komunikaci s úřady.

5.2.1 Mzdová účtárna

Mzdová účtárna používá softwarovou aplikaci s kvalifikovaným elektronickým podpisem ve svých počítačích pro komunikaci s okresní správou sociálního zabezpečení. V současné době je možnost používat čtyři elektronické formuláře:

[15] MPSV – Ministerstvo práce a sociálních věcí
[16] VZP – Všeobecná zdravotní pojišťovna
[17] ČEPS – Česká přenosová soustava
[18] ISOT – Informační systém organizátora trhu
[19] ISZO – Informační systém zúčtování odchylek
[20] ČNB – Česká národní banka

- evidenční list důchodového pojištění,
- příloha k žádosti o nemocenské, ošetřovné, pomoc v mateřství,
- přehled odvodů na sociální pojištění,
- přihlášky/odhlášky sociálního pojištění/zdravotního pojištění.

Zejména v případě evidenčního listu se jedná o výraznou úsporu času zaměstnanců a nákladů podniku. Do roku 2003 měl totiž každý zaměstnanec svoji vlastní kartu a potřebné údaje se do ní každý rok připisovaly na psacím stroji. Potom účetní musely karty vzít a odnést na okresní správu sociálního zabezpečení. Od roku 2004 se postup změnil, a každý zaměstnanec měl svoji kartu, do které se zapisovaly údaje jen za jeden rok. Pro zjednodušení práce byl vytvořen formulář a data se doplňovala elektronicky v počítači. Použití výpočetní techniky sice zrychlilo vyplňování formulářů, ale stejně bylo nutné je vytisknout a odnést.

Zavedením elektronického podpisu se práce ještě více zrychlila a zjednodušila. Softwarová aplikace v sobě obsahuje příslušný elektronický formulář, který navíc kontroluje nesprávně vyplněné nebo nevyplněné údaje. Jediným kliknutím je možno odeslat hlášení za všech cca 530 zaměstnanců, bez potřeby posílání papírové verze, nebo osobní návštěvy na pobočce správy.

5.2.2 Materiálně technické zásobování

Dalšími útvary, které využívají kvalifikovaný certifikát i komerční certifikát, jsou materiálně technické zásobování a útvar technického rozvoje. Oběma slouží elektronický podpis ke komunikaci s celním úřadem. Dříve se žádost o proclení zboží vypsala do předepsaného formuláře, vytiskla a odnesla na celní úřad ke kontrole a k projednání. Při výskytu nějaké chyby se v lepším případě mohla provést oprava na místě a clo vyřídit. Nebo se zaměstnanec musel vrátit zpět do kanceláře, žádost přepsat a znovu se dostavit ke kontrole údajů.

V dnešní době se formulář vyplňuje elektronicky, potom se komerčním certifikátem zašifruje, kvalifikovaným certifikátem podepíše a odešle ke kontrole. Z celního úřadu přijde odpověď, zda jsou vyplněné údaje v pořádku, nebo ne. Pokud je ve formuláři chyba, zaměstnanec ji opraví, a znovu ho odešle ke kontrole. Když je formulář vyplněn správně, zaměstnanec jej vytiskne a odnese ho na celní úřad k vyřízení. Bez osobní návštěvy celního úřadu se to sice neobejde, ale člověk má jistotu, že se věc vyřídí napoprvé a nebude se muset opakovaně vracet.

Elektronická komunikace je podepsána z důvodu jednoznačné identifikace odesílatele a šifrována jako ochrana proti zneužití dat v případě odchycení nebo nedoručení zprávy.

Materiálně technické zásobování má ve své správě i vozový park STC. Jednou ročně se posílají finančnímu úřadu údaje pro výpočet silniční daně. Její výše je stanovena na základě počtu vozidel, jejich druhu – osobní, nákladní, a obsahu motoru.

5.2.3 Útvar veřejných zakázek

Útvaru veřejných zakázek slouží elektronický podpis k podepisování e-mailové komunikace a k přístupu do systému Věstník veřejných zakázek. Tento portál je součástí informačního systému o veřejných zakázkách, jehož správcem je Ministerstvo pro místní rozvoj. Věstník veřejných zakázek je jednotným místem pro uveřejňování základních informací o veřejných zakázkách, které jsou zadávány v souladu se zákonem č. 137/2006 Sb., o veřejných zakázkách. Elektronický podpis je nutný pro odeslání oznámení (formuláře) elektronickou cestou. Elektronicky podepsaný e-mail se používá pro zasílání dodatečných informací k veřejné zakázce případným zájemcům o výběrové řízení.

Součástí výběrového řízení může být i elektronická aukce. Do ní se musí případní zájemci přihlásit, a pak mohou ve stanoveném časovém limitu přímo online ovlivňovat cenu soutěžené zakázky. Každá provedená změna musí být potvrzena elektronickým podpisem, aby bylo zajištěno, že tuto změnu provedla pouze oprávněná osoba.

Do budoucna se chystá jedna podstatná změna, a to nový systém elektronizace postupu zadávání zakázek. Dodavatelé pak budou mít možnost elektronicky podepisovat své nabídky, aniž by je museli posílat zadavateli v papírové podobě.

5.2.4 Obchodní oddělení

Elektronický podpis využívají i někteří obchodní zástupci. Po absolvování krátkého školení a získání kvalifikovaného certifikátu se mohou přihlásit na elektronická tržiště veřejné správy. Příkladem takového tržiště může být Gemin nebo TENDERMARKET.

Gemin je první elektronické tržiště nové generace v České republice. Představuje jednoduchý, efektivní a transparentní elektronický nástroj pro obchodování veřejného sektoru s komerčními subjekty. Přihlášený uživatel má přístup do systému a může elektronicky zadávat veřejné zakázky nebo se účastnit veřejných zakázek a také sledovat poptávky ve svém oboru.

TENDERMARKET je plně elektronický systém, kde všechny úkony v zadávacím, resp. výběrovém řízení provádí zadavatel i dodavatel v elektronické podobě. Na věstníku elektronického tržiště TENDERMARKET jsou uveřejňovány veřejné zakázky jednotlivých zadavatelů. Dodavatelé k nim mohou přistupovat a komunikovat se zadavateli.

Obchodní zástupci vyhledávají na těchto tržištích ve vypsaných veřejných zakázkách nabídky ve svém oboru pomocí klíčových slov, jako například polygrafie, tisk apod. Pokud mají o nějakou zakázku zájem, mohou se přihlásit a pokusit se ji získat.

5.2.5 Datové schránky

Kvalifikovaný certifikát potřebují i zaměstnanci, kteří mají přístup k datovým schránkám pro komunikaci s orgány veřejné moci nebo komerčními subjekty. Jedná se tedy o oprávněnou osobu, pověřenou osobu a administrátora. S tím je spojena i agenda spisové služby a archivnictví, která je státním podnikům dána jako povinnost.

5.2.6 Service Desk

Service Desk je primárním centrálním bodem pro kontakt se všemi uživateli smluvního zákazníka. Služba je poskytována modelem jediného kontaktního místa (SPOC – Single Point of Contact). SPOC je možné kontaktovat všemi možnými způsoby, prioritně prostřednictvím webového rozhraní, dále telefonicky, mailem nebo přímo ze zákaznické aplikace či systému.

Jsou zde zaznamenávány a spravovány veškeré incidenty, servisní požadavky, události a je rozhraním pro všechny ostatní procesy a činnosti provozu služeb. Z pohledu uživatele jde o kontaktní místo, kde může hlásit problémy a požadavky a kde mu budou poskytnuty relevantní a přesné informace k daným případům.

Operátor požadavek nebo incident zpracovává a předává relevantním řešitelům a zajišťuje veškerou komunikaci s uživatelem. Díky vysoké odborné znalosti a bohatým zkušenostem dosahuje tato služba vysoké efektivnosti řešení. Celkem 75 – 80 % veškerých případů se daří vyřešit ihned na první úrovni, tzn. během prvního kontaktu uživatele s operátorem.

Tato skutečnost významně ovlivňuje nákladovou složku obou stran. Snižují se náklady za servisní výjezdy k takovým případům, které lze se zákazníkem vyřešit formou telefonických rad a konzultací. Navíc se filtrují běžné a často se opakující incidenty či uživatelské dotazy už pomocí první úrovně podpory. To snižuje vytíženost pracovníků

technické podpory, kteří se díky tomu mohou věnovat jiným a komplikovanějším servisním případům stejného nebo jiného zákazníka.

Service Desk Národního datového centra STÁTNÍ TISKÁRNY CENIN, státní podnik, používá kvalifikovaný systémový certifikát pro komunikaci se zákazníky. Certifikát není spojen s jednotlivými operátory, ale s celým systémem Service Desk. Zákazník má tedy pomocí certifikátu zaručeno, že s ním skutečně komunikuje systém, který má.

5.2.7 Výroba osobních dokladů

Asi nejzajímavějším je používání kvalifikovaných a komerčních certifikátů při výrobě osobních dokladů. Podle nařízení Rady EU byly všechny členské státy EU povinny zavést první biometrické prvky (obličej) do nově vydávaných cestovních dokladů do konce srpna 2006 a další biometrické prvky (otisky prstů) do konce února 2008. Tyto biometrické charakteristiky jsou používány pro ověřování autenticity pasů a víz a také pro ověřování identity držitele pasu.

Biometrické systémy jsou aplikace biometrických technologií, které umožňují automatickou identifikaci nebo autentizaci/verifikaci určité fyzické osoby. Každý druh biometrie se zakládá ve větší či menší míře na příslušném biometrickém prvku, který je:

- univerzální - biometrický prvek existuje u všech osob,
- jedinečný - biometrický prvek musí každou osobu odlišovat,
- stálý - každá fyzická osoba si v průběhu času biometrický prvek trvale uchovává.

Rozlišují se dvě hlavní kategorie:

- Postupy založené na fyzických a fyziologických aspektech, které měří fyziologické vlastnosti fyzické osoby, tzv. stabilní data. Mezi ně patří například otisk prstu, rozpoznávání duhovky, analýza sítnice, rozpoznávání obličeje nebo rozpoznávání hlasu.
- Postupy založené na rysech chování, které měří chování osoby, tzv. dynamická data. Jedná se o verifikaci vlastnoručního podpisu nebo analýzu stisku tlačítek.

Rychlý technický rozvoj a zvýšené riziko narušení bezpečnosti vedly k vytvoření nového trendu. Většina biometrických systémů pracuje tak, že kombinují různé biometrické znaky fyzické osoby s jinými technologiemi identifikace nebo autentizace.

Shromažďování biometrických dat se provádí za použití senzoru specifického pro každý typ biometrického znaku. Jen v tomto okamžiku jsou současně přítomny „hrubé“ údaje,

výběrové a ochranné algoritmy (kryptografie, hašování atd.) a šablony. Hrubé údaje představují informaci, kterou lze považovat za „citlivý údaj“, a proto je nutné biometrické údaje zpracovávat jako údaje citlivé.

Biometrický systém vybírá z biometrických dat rysy specifické pro jednotlivce, aby pak vytvořil tzv. „šablonu“. Tato šablona je strukturovanou redukcí biometrického obrazu a zaznamenává biometrické měření jednotlivce, tzv. biometrické prvky.

Žadatel o ePas se osobně dostaví na kontaktní místo na obci s rozšířenou působností (v místě trvalého pobytu) se stanovenými doklady. Po kontrole doložených skutečností proti datům ze systému evidence obyvatel a evidence cestovních dokladů pořídí úředník fotografii žadatele. Potom vytiskne ze systému žádost s potřebnými daty, včetně fotografie, a vyzve žadatele k podpisu do příslušného místa žádosti (systém automaticky podpis graficky snímá pro následné použití při výrobě ePasu). Data jsou zašifrována veřejným klíčem serverového certifikátu STC a následně elektronicky podepsána úředníkem, který žádost zpracoval, a elektronicky odeslána do centra, papírová žádost zůstává na obci.

Data přijatá z jednotlivých kontaktních míst jsou v centrále shromážděna podle data přijetí žádosti a je ověřen podpis úředníků z podacích míst. Potom jsou jako celek nahrána na datová média, digitálně podepsána serverovým certifikátem centrálního systému, a ještě navíc podepsána úředníkem, který nosič vytvořil. Takto zabezpečená data jsou předána do centrální výrobny dokladů. Dvojí podepisování je z důvodu zvýšení bezpečnosti přenášených dat a zároveň to zabraňuje tomu, aby si úředník nechal vyrobit doklady bez oprávnění a žádosti.

Takto přijatá datová média musí nejdříve administrátoři dat ověřit. Ověřuje se oprávnění a platnost podpisu úředníka i podpisu centrálního systému. Pomocí privátního klíče serverového certifikátu STC jsou zašifrovaná data rozšifrována a poté rozdělena do výrobních dávek ke zpracování. Data jsou ve výrobě zpracovávána v systému hvězdicové sítě a komunikace je šifrována proti odposlechu na úrovni operačního systému.

Operátoři personalizační linky, výstupní kontroly i expedice s pomocí komerčního certifikátu spouští aplikaci personalizace osobních dokladů. Certifikát je vždy platný pro celou výrobní proceduru, ale administrátoři nastaví v systému konkrétním osobám konkrétní práva přístupu. To znamená, že výstupní kontrola nemůže spustit personalizační stroj, nebo že expedice nemůže provádět výstupní kontrolu. Prakticky je tím zajištěno, že se na výrobě jedné dávky podílí několik zaměstnanců v různých odděleních. Při předávání

výrobních dávek mezi jednotlivými zpracujícími celky dochází vždy ke stoprocentním přepočtům, a tím ke kontrole úplnosti předávaných dávek.

Společně s vyrobenými doklady se do centrálního systému vrací i zpracovaná data. Na výstupní nosič jsou zašifrovány veřejným serverovým certifikátem centrálního systému jednotlivé okresy a celý balík je podepsán veřejným serverovým certifikátem STC. Celý nosič je pak ještě elektronicky podepsán pověřenou osobou STC a předán zákazníkovi. Ověřování v centrálním systému probíhá analogicky s postupem ověřování administrátory v STC.

Po zpracování dat a vyrobení ePasu s biometrickými údaji v centrální výrobně je pas odeslán zpět na obec. Při převzetí ePasu si občan může zkontrolovat funkčnost čipu a v něm uložená data a musí podepsat poučení, že dodrží stanovené podmínky pro nakládání s ePasem (dostává pasovou knížku včetně elektronického zařízení).

5.3 Zhodnocení využití elektronického podpisu

Elektronický podpis, kvalifikovaný certifikát a komerční certifikát k STC neoddělitelně patří. Jejich možnosti využívá ke své práci velké množství zaměstnanců, ať již z povinnosti vůči jiným subjektům, nebo ke zjednodušení vlastní práce. K některým činnostem, jako je obsluha výroby dokladů, jsou dokonce životní nutností. Za rok 2013 je v STC evidováno celkem 63 vydaných a platných certifikátů.

6 DATOVÉ SCHRÁNKY V STC

Datové schránky byly STC povinně zřízeny ze zákona v roce 2009, jako právnické osobě zapsané v obchodním rejstříku. Přístup do datových schránek může mít několik různých uživatelů, s různou úrovní oprávnění, podle toho, jak její vlastník zvolí. Existují celkem tři typy uživatelských účtů:

- oprávněná osoba,
- administrátor
- a pověřená osoba.

Oprávněná osoba je v našem případě statutární zástupce, tedy generální ředitel. Je to vlastně neomezený vládce datové schránky. Může vykonávat veškeré úkony a umožnit dalším osobám přístup k datové schránce. Jeho práva mu nemůže nikdo odebrat. Administrátorem byl určen vedoucí podnikové kontroly a pověřenou osobou zaměstnanec centrální spisovny. Tomuto způsobu nastavení přístupových práv se říká dvoustupňová delegace.

Zákon nařizoval orgánům veřejné moci doručovat dokumenty pomocí datových schránek jiným orgánům veřejné moci, právnickým osobám, fyzickým podnikajícím osobám jako povinnost a fyzickým osobám, pokud ji mají zřízenou. Posílat dokumenty orgánům veřejné moci však bylo pouze dobrovolné a v STC zpočátku také nevyužívané.

Doručování fyzickými osobami, fyzickými podnikajícími osobami a právnickými osobami mezi sebou nebylo ze začátku možné. Umožňovala to až novela zákona od 1.1.2010.

6.1 Spisová služba v STC

Ještě dříve než byly v České republice zavedeny datové schránky, vyplývala podle § 3, odst. 1, písmena e) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů ve znění pozdějších předpisů, Státní tiskárně cenin povinnost vést od 1.1.2006 archiv a spisovou službu. Zákon umožňoval státním podnikům vést spisovou službu v listinné nebo elektronické podobě a možnost volby nechával na nich. V novelizaci tohoto zákona z května 2009 (zákon č. 190/2009) vyplývala nově povinnost vést spisovou službu v elektronické podobě. Pro STC to však nebyla žádná překážka, neboť si zvolila možnost vést elektronickou spisovou službu již v roce 2006.

6.1.1 Zákon o archivnictví a spisové službě

Tento zákon upravuje zejména povinnost uchovávat dokumenty a umožnit výběr archiválií, jejich evidenci a ochranu. Skartační řízení, tedy postup, při kterém se vyřazují dokumenty, jimž uplynuly skartační lhůty a jež jsou nadále nepotřebné pro činnost původce. Práva a povinnosti vlastníků archiválií, využívání archiválií, zpracování osobních údajů pro účely archivnictví, práva a povinnosti zřizovatelů archivů, spisovou službu a správní delikty.

Při vedení spisové služby je povinností určených původců zajistit příjem, označování, evidenci a rozdělování dokumentů. U dokumentů v digitální podobě zajistit příjem, alespoň v datových formátech stanovených jako výstupní datové formáty nebo formáty dokumentů, které jsou výstupem z autorizované konverze dokumentů obsažených v datové zprávě.

Doručené i vytvořené dokumenty se v den, kdy byly doručeny nebo vytvořeny, opatří jednoznačným identifikátorem. Jednoznačný identifikátor je označení dokumentu zajišťující jeho nezaměnitelnost a musí být s dokumentem spojen. Dokumenty opatřené jednoznačným identifikátorem se evidují v evidenci dokumentů. Samostatnou funkční částí evidence dokumentů může být jmenný rejstřík určený pro vyhledávání, ověřování a automatické zpracovávání údajů o adresách odesílatelů a adresátech dokumentů evidovaných v této evidenci.

Při vyřizování dokumentů se všechny dokumenty týkající se téže věci spojí ve spis. Dokumenty v analogové podobě se vzájemně spojí fyzicky, dokumenty v digitální podobě se vzájemně spojí prostřednictvím metadat, vzájemné spojení dokumentu v analogové podobě a dokumentu v digitální podobě se činí pomocí odkazů. Dokumenty podepisuje statutární orgán nebo jiná osoba oprávněná za něj jednat anebo osoba, která k tomu byla statutárním orgánem pověřena.

Po vyřízení věci se spis uzavře. Uzavřením spisu se rozumí kompletace všech dokumentů patřících do spisu, kontrola a doplnění údajů před uložením do spisovny a převedení dokumentů v digitální podobě do výstupního datového formátu a jejich opatření metadaty podle národního standardu. Z uzavřeného spisu nesmějí být vyjímány jednotlivé dokumenty, ale je možno ho připojit k jinému spisu, pokud neuplynula jeho skartační lhůta.

Do vlastních rukou adresáta se odesílají dokumenty, u nichž je nutno, aby doručení bylo doloženo. Doklad stvrzující, že dokument byl doručen nebo že poštovní zásilka obsahující dokument byla dodána, včetně časového údaje, kdy se tak stalo, se po vrácení připojí k příslušnému dokumentu nebo vloží do příslušného spisu.

Všechny vyřízené spisy a jiné dokumenty jsou po dobu trvání skartační lhůty uloženy ve spisovně nebo ve správním archivu. Prostory pro ukládání dokumentů musí být zajištěny proti vstupu nepovolané osoby. Dokumenty se ukládají podle spisového a skartačního plánu zpravidla ihned po jejich vyřízení.

V případě zániku určeného původce převezme spisovnu nebo správní archiv jeho právní nástupce, zřizovatel nebo ten, na něhož přechází působnost zaniklého určeného původce.

6.2 Analýza používání elektronické spisové služby v STC

Podobnost úkonů prováděných při vedení elektronické spisové služby s úkony při používání datových schránek je velmi vysoká. To vedlo v roce 2011 k rozhodnutí vedení podniku nahradit tehdejší elektronickou spisovou službu novým systémem, který by umožňoval propojení s datovou schránkou. Cílem bylo vybrat spisovou službu, která by splňovala nejen legislativní požadavky na SSL[21], ale i požadavky na veškeré řízení a oběh dokladů, DMS[22] a řízení dokumentů a řízení záznamů podle požadavků systému managementu jakosti a evidence projektových dokumentací podle motta: „obíhat budou dokumenty, nikoliv lidé“.

Tomuto, z dnešního pohledu správnému rozhodnutí předcházelo několik kroků. Nejdříve byla provedena SWOT analýza používání spisové služby v STC. Název analýzy vychází z počátečních písmen anglických slov Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti) a Threats (hrozby), které reprezentují 4 oblasti zájmu spojené s určitým projektem nebo záměrem. Základ metody spočívá v klasifikaci a ohodnocení jednotlivých faktorů. Vzájemnou interakcí faktorů silných a slabých stránek na jedné straně vůči příležitostem a nebezpečím na straně druhé lze získat nové kvalitativní informace, které charakterizují a hodnotí úroveň jejich vzájemného střetu.

[21] SSL – spisová služba
[22] DMS – angl. Document management system – systém pro správu dokumentů

Silné stránky

- ucelené řešení administrativního informačního systému
- přehledná evidence dokumentů od vzniku po archivaci a skartaci
- vyhledávání dokumentů v centrální databázi, která umožňuje odpovídající manažerské pohledy a přispívá ke zkvalitnění řídicího procesu
- řízení toků dokumentů, sledování jejich pohybu a sledování osobní odpovědnosti jednotlivých zaměstnanců
- snadné vyhledání konkrétního zaměstnance, který má dokument právě v držení
- vyhledávání dokumentu v každé fázi rozpracování, včetně archivovaných dokumentů
- automatizace kancelářských činností
- možnost sdíleného přístupu k dokumentu
- splnění legislativních požadavků na vedení SSL
- rychlost předání elektronického dokumentu (vnitřní dokumenty mohou chodit pouze elektronicky)
- spolehlivost – elektronický dokument se nemůže ztratit, je garantováno doručení
- prokazatelnost – kdo, komu, kdy
- možnost elektronického podepisování, na interní dokumenty stačí interní certifikáty
- možnost konverze dokumentů do PDF
- pravidelné zálohování
- interní školitel SSL

Slabé stránky

- před spuštěním SSL nebyla provedena komplexní analýza vzniku a oběhu dokumentů
- nechuť používat SSL a DS[23]
- nedostatečné využití SSL, evidence dokumentů je prováděna v dalších databázích STC
- nedostatečná kontrola činností v rámci výkonu SSL vedoucími organizačních celků
- nárůst objemu dat v datovém úložišti, potřeba dostatečné diskové kapacity

[23] DS – datové schránky

- nedostatečná uživatelská přívětivost SW[24]
- nedostatečná podpora vrcholového managementu v prosazení používání spisové služby.

Příležitosti

- možnost hromadného schvalování a podepisování elektronických dokumentů
- možnost odesílat většinu dokumentů datovou schránkou
- řízený oběh elektronických dokumentů
- rozšíření přístupů do eSSL[25]
- větší operativnost v odesílání elektronického dokumentu přímo zpracovatelem dokumentu do DS přes eSSL
- vytvoření garantovaného úložiště elektronických dokumentů
- změna metodiky, interních norem – sjednotit různé evidence do jednotné SSL, zařadit do šablon v SSL formuláře
- nižší stupeň podpory ze strany poskytovatelů SSL.

Hrozby

- zabezpečení datové schránky
- dokazování autenticity elektronických dokumentů i po delší době
- dlouhodobé uchovávání elektronických dokumentů
- lidský faktor
- legislativní změny.

Potom byla provedena analýza používání elektronické SSL se zaměřením na odchozí poštu. Touto analýzou bylo zjištěno, že v roce 2010 bylo z STC odesláno celkem 3 022 dokumentů. Z toho bylo orgánům veřejné moci odesláno 836 dokumentů. Pokud by tyto dokumenty vůči OVM byly odeslány prostřednictvím datové schránky, úspora nákladů na poštovném by činila nejméně 20 894,- Kč, viz tabulka.

[24] SW – angl. SoftWare – programové vybavení
[25] eSSL – elektronická spisová služba

Tab. 2. Přehled odchozí pošty za rok 2010

2010	celkem odesláno	z toho faktur vlastních	ostatní dopisy	z toho OVM	cena za 1 ks (Kč)	cena celkem (Kč)
obyčejný dopis	242	2	240	72	10	720
doporučený dopis	2287	1668	619	628	26	16 328
s dodejkou	117	0	117	119	32	3 808
s dodejkou do vlastních rukou	15	0	15	1	38	38
obyčejný balík	0	0	0	0	0	0
doporučený balík	139	1	138	1	0	0
kurýr	8	0	8	0	0	0
fax	2	0	2	1	0	0
datová schránka	10	0	10	10	0	0
e-mail	22	0	22	0	0	0
osobní doručení	180	97	83	4	0	0
	3022	**1768**	**1254**	**836**		**20 894**

Nejméně znamená, že bylo počítáno na každý 1 ks dopisu s nejnižší sazbou, tzn. dopis do 50 g. Dále zde nejsou zahrnuty náklady na papír, obálky, tonery. Další úsporu by přineslo elektronické odesílání faktur.

Nakonec bylo provedeno vyhodnocení odeslaných a přijatých dokumentů jednotlivými uživateli za rok 2010. Na základě tohoto vyhodnocení bylo navrženo odebrání licencí některým z nich. Důvody pro odebrání byly dva. Prvním důvodem bylo, že skupina uživatelů měla tak nízký objem dokumentů, které zpracovávají přes elektronickou SSL, že je jednodušší, aby tyto úkony za ně řešily sekretariáty. Druhým důvodem bylo, že skupina uživatelů se spisovou službou pravděpodobně vůbec nepracuje, protože nepřebírá dokumenty i elektronicky. Nepřebrané dokumenty v eSSL zůstávaly neuloženy ve vzduchoprázdnu, a nebyly tak v podacím deníku uzavřeny.

Na základě provedených analýz a vyhodnocení byly navrženy tři varianty řešení. Nakonec zvítězila varianta pořídit od společnosti CNS, a. s., novou verzi programu Spisová služba ELISA.

6.3 Spisová služba Elisa

ELISA znamená elektronický informační systém spisových agend. Tento program slouží ke sledování oběhu dokumentů v organizaci od jejich příchodu do systému (profil dokumentu) přes jejich zpracování (historie dokumentu, lhůty vyřízení, zařazení do spisu) až po jejich archivaci a skartaci.

ELISA je novou technologickou verzí původního informačního systému Spisová služba spol. CNS, a. s., která byla uživateli využívána v rutinním provozu již od roku 1998. ELISA tak navazuje a využívá rozsáhlé znalosti správy dokumentů z předchozí verze Spisové služby. Zárukou kvality SSL jsou získané certifikáty a atestace od atestačního střediska EQUICA, které je pověřeno k výkonu atestací Ministerstvem vnitra ČR.

Tento nástroj umožňuje efektivněji evidovat, ukládat, vyhledávat dokumenty, a to dokumenty papírové nebo dokumenty, které byly přijaty v elektronické podobě, včetně datových schránek. Navíc posílá upozornění na e-mail uživatele o novém dokumentu k převzetí či k odeslání. A umožňuje přístup k dokumentům odkudkoliv. Uživatel v programu pracuje v prostředí svého internetového prohlížeče.

6.4 Práce s datovou schránkou

Existují v zásadě čtyři způsoby, jak můžeme s datovou schránkou pracovat:

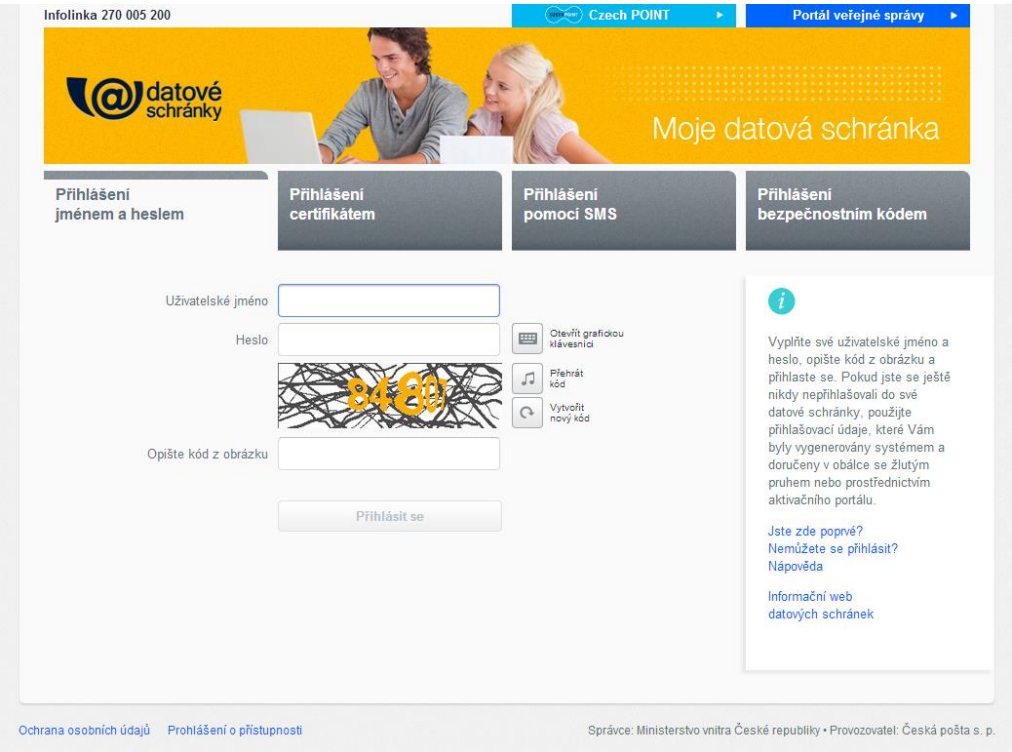
- prostřednictvím webového prohlížeče (browseru),
- prostřednictvím speciálního programu,
- prostřednictvím spisové služby,
- přeposíláním zpráv na e-mail.

Každý z těchto přístupů má své výhody a nevýhody. [5]

6.4.1 Webový prohlížeč

Použití webového prohlížeče je nejpoužívanějším způsobem práce s datovou schránkou. Důvodem je skutečnost, že prohlížeče jako například Internet Explorer, Mozilla Firefox nebo Google Chrome jsou dnes součástí každého počítače a uživatelé jsou na práci s nimi

zvyklí. V STC tento způsob práce s datovou schránkou používá oprávněná osoba – generální ředitel a administrátor – vedoucí podnikové kontroly.



Obr. 4. Přihlašovací obrazovka (převzato z [8])

Jediným místem pro přihlášení do Portálu datových schránek pomocí internetových stránek je adresa http://www.mojedatovaschranka.cz/. Portál nabízí čtyři různé způsoby přihlašování. U nás se používá základní způsob přihlášení jménem a heslem.

Nejprve je třeba vyplnit pole Uživatelské jméno, což je náhodně vygenerovaný řetězec písmen a číslic o délce 6-12 znaků, přičemž nezáleží na tom, zda se zadávají velká, nebo malá písmena. Někdy si ho uživatelé pletou s Identifikátorem datové schránky. Je to také alfanumerický řetězec, například „hqe39ah“, který se ovšem v procesu přihlašování nepoužívá. Je nezměnitelný a slouží výhradně k identifikaci naší schránky v systému.

Dále je třeba vyplnit Heslo. Jeho délka je 8-32 znaků, musí obsahovat nejméně jedno velké písmeno, nejméně jedno malé písmeno a nejméně jednu číslici. Heslo se dá kdykoliv libovolně změnit. Zadat se dá přímo z klávesnice, nebo pomocí myši přes virtuální klávesnici, která se zobrazí pokaždé v jiné velikosti a na jiném místě obrazovky. Platnost hesla je nastavena na 90 dní, poté musí být změněno. Na základě zpětné vazby od

uživatelů, kteří tuto povinnost kritizovali jako obtěžující, umožnil správce systému změnu hesla vypnout. Zbývá do posledního pole opsat číselný kód z obrázku (CAPTCHA) a přihlásit se.

Pro zvýšení bezpečnosti přihlášení k datové schránce je možno použít dodatečnou autentizační metodu přihlášení:

- komerčním certifikátem,
- bezpečnostním kódem,
- SMS[26] kódem.

Certifikát musí být uložen pouze na čipové kartě, jeho platnost je omezena a navíc je třeba koupit čtečku karet.

Bezpečnostní kód je jednorázové heslo, které lze použít pouze k jedinému přihlášení, a potom je bezcenné. Hesla jsou generována speciálním nástrojem, hardwarovým nebo softwarovým tokenem.

SMS kód je opět jednorázové heslo, které je ovšem generováno systémem a formou krátké textové zprávy je zasláno po síti operátora do mobilního telefonu uživatele.

Výhodou používání webového rozhraní je jeho snadná a bezplatná dostupnost. Dále pak možnost využití všech nástrojů, které datové schránky nabízejí.

Nevýhodou jsou bezpečnostní rizika možnosti různých útoků, jako je například podvržení cílové adresy. Omezená uživatelská přívětivost systému vyplývající z běhu prohlížeče. Nutnost manuálně řešit archivaci, protože datové zprávy jsou po 90 dnech od doručení smazány, takže si uživatel musí zaplatit za službu Datový trezor, nebo nechat provést konverzi dokumentů pro jejich trvalé uložení.

Oprávněná osoba v STC s datovými schránkami prakticky nepracuje, ale jenom ona má právo jmenovat administrátora a pověřenou osobu. Administrátor se přes webové rozhraní přihlašuje také pouze ve výjimečných případech. Jeho možnosti jsou pro nakládání s dokumenty pro potřeby STC tímto způsobem totiž výrazně omezeny. Kromě svých běžných práv však může vytvářet a rušit další pověřené osoby a nastavovat jejich oprávnění.

---

[26] SMS – angl. Short message service – systém krátkých zpráv

6.4.2 Speciální program

Další možností pro práci s datovou schránkou je použití speciálního programu, jako je například Datovka nebo Manažer datových schránek. Těchto programů je dnes velké množství, zadarmo i placené, kvalitní i méně kvalitní. Jedno mají ale společné, běží na našem počítači a pro komunikaci se systémem datových schránek používají speciální rozhraní API[27]. Práce s nimi je výrazně pohodlnější než při používání webového prohlížeče. Zvyšuje se i bezpečnost, protože se snižuje možnost napadení prohlížeče phishingovými útoky. Výhodou je i skutečnost, že tyto programy vytváří vlastní databázi přijatých a odeslaných zpráv, kterou ukládají na pevný disk počítače. Zprávy tedy nezmizí, ale jsou automaticky archivovány.

6.4.3 Spisová služba

Třetí možností, kterou využívá i STC, je napojení datové schránky na spisovou službu. Jak bylo popsáno výše, spisová služba ELISA používaná v STC umožňuje komplexní řešení pro práci s tištěnými i elektronickými dokumenty. Určeným zaměstnancům byla zakoupena licence k používání a nainstalován program do jejich počítače. K přihlášení do spisové služby je třeba zadat přihlašovací jméno a heslo, které se musí měnit každých 90 dní. Každý uživatel systému má přidělena uživatelská práva, přiřazeno funkční místo a může být v rámci programu definován do tzv. konfiguračních skupin. Navíc k jednotlivým dokumentům pak může volit úroveň přístupu ostatních uživatelů programu. Spisová služba podporuje označování PDF dokumentů elektronickými podpisy a využívá certifikáty umístěné přímo v úložišti certifikátů v PC.

Právo přijímat a odesílat datové zprávy za celou STC mají pomocí spisové služby jenom dva zaměstnanci. Jsou to podle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, pověřené osoby. Dva jsou z toho důvodu, aby byla zajištěna jejich zastupitelnost v případě nemoci, dovolené apod. Oprávněná osoba tedy přijme datovou zprávu z datové schránky, zaeviduje ji jako doručený dokument a v rámci spisové služby ho přepošle tomu uživateli, kterému patří.

Odesílání datových zpráv je prováděno analogicky. Zaměstnanec vytvoří dokument, zaeviduje ho do spisové služby a přepošle oprávněné osobě k vyřízení. Oprávněná osoba

[27] API – angl. Application Programming Interface – programové rozhraní aplikace

provede autorizovanou konverzi originálu dokumentu. Tedy úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě. Zpravidla uložením do formátu PDF a podepíše ho elektronickým podpisem. Potom ho uloží jako přílohu datové zprávy a odešle do datové schránky příjemce. O úspěšném odeslání následně informuje původce dokumentu.

6.4.4 E-mailové zprávy

Poslední možností je přeposílání zpráv z datové schránky do e-mailu. Využívání takové služby s sebou však přináší celou řadu rizik. Musíme totiž sdělit své přístupové údaje třetí osobě, která pak vlastně jedná naším jménem, ale bez naší kontroly. Doručování e-mailových zpráv je navíc nespolehlivé a není nijak chráněno. Zpráva může být odposlechnuta při síťové komunikaci, nebo si ji může přečíst správce některého z poštovních serverů. Může být cestou modifikována, aniž by se to dalo zjistit. Chybou nebo výpadkem serveru může zpráva dorazit se zpožděním, nebo vůbec ne. Nemůžeme ověřit, že odesílatelem je skutečně ten, kdo se za něj vydává.

6.5 Zhodnocení služby datových schránek

Za zhruba pět let používání datových schránek v STC se dá říci, že se jejich používání pro odesílání datových zpráv zlepšuje. Jak uvádí následující tabulka, počet odeslaných datových zpráv byl v roce 2013 více než desetkrát vyšší než v roce 2010. Počet odeslaných zpráv za čtyři měsíce roku 2014 je vyšší než počet odeslaných datových zpráv za celý rok 2012.

Tab. 3. Přehled doručených a odeslaných DZ

rok	**doručené DZ**	**odeslané DZ**
2010	85	12
2011	136	18
2012	226	49
2013	284	123
2014 (k 28.4.)	108	56

Pro zaměstnance už nejsou datové schránky žádnou nevyzkoušenou novinkou. Díky tomu, že informační systém datových schránek je provozován nepřetržitě v režimu 24 x 7, mohou

odeslat datovou zprávu kdykoliv s jistotou, že bude každá datová zpráva do informačního systému datových schránek doručena. Porozuměli také pěti hlavním výhodám datových schránek:

1. garance doručení
2. rychlost
3. nemožnost nahlížet do obsahu datové zprávy
4. odstranění nezastižitelnosti adresáta
5. přístup do datových schránek kdykoliv a odkudkoliv v České republice

Vzhledem k tomu, že odesílání datových zpráv je bezplatné, jsou datové schránky i výraznou finanční úsporou pro podnik.

V současné době je vedením STC zvažována možnost zakoupit balíček pro odesílání datových zpráv právnickým a podnikajícím fyzickým osobám. Možností je buď platit paušál, nebo si předplatit kredit a čerpat z něj za každou odeslanou zprávu. Tím by se zvýšilo využití datových schránek pro odesílání již výše zmíněných faktur, zásilek do vlastních rukou, ale i obyčejné pošty.

ZÁVĚR

Před několika lety bylo v České republice zahájeno budování eGovernmentu. Úspěšně se podařilo realizovat řadu projektů, jako je Czech POINT, Komunikační infrastruktura veřejné správy, základní registry nebo datové schránky. Tyto projekty přispívají k odbourávání zbytečné byrokratické zátěže, ke zvýšení efektivity veřejné správy a tím ke konkurenceschopnosti celé země.

Datové schránky představují největší změnu ve způsobu doručování za posledních sto let. Měly by být přínosem pro širokou veřejnost i pro orgány státní správy. Myšlenka vytvořit informační systém a elektronické úložiště, které by umožňovaly bezproblémovou komunikaci mezi občanem, živnostníkem, nebo právnickou osobou na straně jedné a orgány veřejné moci na straně druhé, je velmi pokroková. Cílem datových schránek bylo, že by se veškeré dokumenty, které musely být doručovány doporučeně, všechny žádosti a povolení, která musel člověk přinést, nebo vyzvednout na úřadě osobně, mohly dát vyřídit z pohodlí domova, nebo kanceláře prakticky z jakéhokoliv počítače.

Zavedením datových schránek do praxe se potvrdilo, že jde o úžasnou inovaci a zefektivnění procesů ve veřejné správě. Statistiky uvádějí, že ke konci dubna 2014 bylo zřízeno více než 587 000 datových schránek a počet odeslaných zpráv přesáhl 188 milionů. Nejvíce viditelný je přínos ekonomický. Při porovnání nákladů na jednu datovou zprávu oproti tradiční listovní zásilce bylo vypočteno, že za dobu používání datových schránek v letech 2009 – 2013 vytvořily i po odpočtu výdajů na provoz ISDS přínos ve výši 3 546 mil. Kč.

Potenciál datových schránek je však třeba dále rozvíjet. Nabízí se řada možností, k čemu se dají datové schránky využívat. Zejména přenos strukturovaných informací, přístup do datových schránek pro fyzické osoby přes elektronické bankovnictví, automatizovaná konverze příchozí papírové dokumentace nebo elektronické volby.

Nesmíme však zapomínat na otázky bezpečnosti a ochrany soukromí. Je systém zabezpečen, aby nemohl být zneužit? Nemohou se moje dokumenty někde ztratit? Nemůže někdo zneužít moje osobní údaje? Jak vyplývá z informačních materiálů poskytovaných správcem a provozovatelem datových schránek, něco takového by se nemělo stát. Zabezpečení systému ovlivňuje v první řadě sám uživatel, svým bezpečným chováním – opatrností, aktualizací operačního systému, používáním antivirových programů, nebo používáním bezpečných hesel. Bezpečnost ISDS je garantována také provozovatelem,

který používá jako ochranný prvek šifrovanou komunikaci a zaručuje doručení, důvěrnost a průkaznost zpráv i uživatelů.

Využití elektronického podpisu ve státním i soukromém sektoru jako hlavního nástroje identifikace a autentizace osob v prostředí internetu je dnes nepopiratelné. Jeho získání a používání je celkem jednoduchou záležitostí a ve spojení s vhodnou aplikací přináší mnoho výhod a zjednodušení. A to nejen v případě komunikace se státní správou nebo při řízení výrobních procesů, ale ve všech případech, kdy potřebujeme zajistit důvěrnost informací, integritu a neodmítnutelnost odpovědnosti.

Praktické využívání elektronického podpisu a prostředí datových schránek je pro STÁTNÍ TISKÁRNU CENIN, státní podnik, velkým přínosem. Nejen že zaměstnancům usnadňuje jejich práci a podniku šetří náklady, ale je důležité i pro zlepšení komunikačních možností mezi firmou a zákazníkem.

ZÁVĚR V ANGLIČTINĚ

A few years ago the implementation of eGovernment began in the Czech Republic. A number of projects have been successfully implemented, such as Czech POINT, Communication infrastructure of public administration, basic registers or data boxes. These projects contribute to the reduction of unnecessary red tape, they increase the efficiency of public administration and the competitiveness of the whole country.

Data boxes represent the biggest change in the method of delivery in the last hundred years. They should be of benefit to the general public and to government. The idea of an information system and an electronic repository that would enable seamless communication between citizens, entrepreneurs or legal persons on one hand and public authorities on the other, is very progressive. The goal of data boxes was that all the documents that had to be delivered by registered post, all applications and permits that had to be brought or picked up at an office in person, could be received within the comfort of your home or office from virtually any computer.

The introduction of data boxes in practice confirmed that this is an amazing innovation and streamlining processes in public administration. Statistics show that by the end of April 2014 more than 587,000 data boxes had been set up and the number of sent messages exceeded 188 million. The most visible benefit is economic. When comparing to the cost of a data message over traditional means, it has been calculated that for the period of use of data boxes in the years 2009 – 2013 after deducting expenses of running ISDS, the savings were in the amount of CZK 3,546 million.

The potential of data boxes, however, should be further developed. There are many possibilities for potential data box use. In particular, the transfer of structured information, access to data boxes for individuals through electronic banking, automated conversion of incoming paper-based or electronic options.

But we must not forget the issues of security and privacy. Is it a security system that could be misused? Can´t they lose my documents somewhere? Can´t someone misuse my personal information? As is clear from the informational material provided by managers and operators of data boxes, something like that should not happen. The security of the system is determined primarily by the user, their safe behavior - caution, operating system updates, using antivirus programs, and using secure passwords. ISDS Safety is also guaranteed by the operator, which is used as a protective element that provides encrypted

communication and delivery, and ensures the confidentiality and relevance of messages and users.

The use of electronic signatures in the public and private sector as the main tool for identification and authentication of persons on the Internet today is unavoidable. Its acquisition and use is a quite simple matter and in conjunction with a suitable application provides many benefits and great convenience. And it does so, not only in matters of communication with the civil administration or the management of production processes, but in all matters where we need to ensure the confidentiality, integrity and accountability.

The practical use of electronic signatures and environment of data boxes is of great benefit for the State Printing Works of Securities, state enterprise. Not only does it facilitate the employees in their work and help the company to save costs, but it is also vital in improving the possibilities for communication between the company and its customers.

SEZNAM POUŽITÉ LITERATURY

[1] BUDIŠ, Petr a Iva HŘEBÍKOVÁ. *Datové schránky: fungování, doručování, bezpečnost, návody*. 1. vyd. Olomouc: ANAG, 2010, 287 p. ISBN 80-726-3617-0.

[2] LAPÁČEK, Jiří. *Jak na datovou schránku a elektronickou komunikaci s úřady*. 1. vyd. Brno: Computer Press, 2012, 197 s. ISBN 978-80-251-3680-5.

[3] LIDINSKÝ, Vít, Ivana ŠVARCOVÁ, Petr BUDIŠ, Zbyněk LOEBL a Barbora PROCHÁZKOVÁ. *EGovernment bezpečně*. 1. vyd. Praha: Grada, 2008, 145 s. ISBN 978-80-247-2462-1.

[4] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-809-0424-838.

[5] SMEJKAL, Vladimír a Michal Altair VALÁŠEK. *Jak na datové schránky: praktický manuál pro každého*. Praha: Linde, 2012, 197 s. ISBN 978-808-6131-801.

[6] ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. Vyd. 1. V Praze: C.H. Beck, 2012, xix, 258 s. Beckova edice ekonomie. ISBN 978-807-4002-618.

[7] Česká republika. Listina základních práv a svobod. In: *2/1993*. 1992. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=40453&fulltext=&nr=2~2F1993&part=&name=&rpp=15#local-content

[8] *Datové schránky* [online]. 2014 [cit. 2014-05-21]. Dostupné z: https://www.mojedatovaschranka.cz/as/login?uri=https://www.mojedatovaschranka.cz/portal/ISDS/&status=NCOO

[9] EGON jako symbol eGovernmentu - moderního, přátelského a efektivního úřadu - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. © 2014 [cit. 2014-05-21]. Dostupné z: http://www.mvcr.cz/clanek/egon-jako-symbol-egovernmentu-moderniho-pratelskeho-a-efektivniho-uradu-252052.aspx

[10] Elektronický podpis – Wikipedie. In: *Wikipedie, otevřená encyklopedie* [online]. 2001-2014 [cit. 2014-05-21]. Dostupné z: http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis

[11] *I.CA | Komerční a kvalifikované certifikáty* [online]. 2014 [cit. 2014-05-21]. Dostupné z: https://www.ica.cz/Certifikaty

[12] Informace k používání elektronického podpisu - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. © 2014 [cit. 2014-05-21]. Dostupné z: http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx

[13] *Komerční certifikáty | Certifikační autorita PostSignum* [online]. © 2010 [cit. 2014-05-21]. Dostupné z: http://www.postsignum.cz/komercni_certifikaty.html

[14] *První certifikační autorita a.s.* [online]. 2014 [cit. 2014-05-21]. Dostupné z: http://www.ica.cz/Elektronicky-podpis

[15] Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. © 2014 [cit. 2014-05-21]. Dostupné z: http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx

[16] *SecuStamp - Software602* [online]. © 2009-2014 [cit. 2014-05-21]. Dostupné z: https://www.secustamp.eu/cz

[17] *Slovník pojmů | Datové schránky* [online]. © 2011 [cit. 2014-05-21]. Dostupné z: http://www.datoveschranky.info/cz/o-datovych-schrankach/slovnik-pojmu-id34696/

[18] *Správa základních registrů* [online]. © 2010 – 2014 [cit. 2014-05-21]. Dostupné z: http://www.szrcr.cz

[19] Základní registry veřejné správy - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. © 2014 [cit. 2014-05-21]. Dostupné z: http://www.mvcr.cz/clanek/zakladni-registry-zakladni-registry-verejne-spravy.aspx

[20] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In: *227/2000*. 2000. Dostupné z: http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx

[21] Zákon o eGovernmentu - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. © 2014 [cit. 2014-05-21]. Dostupné z: http://www.mvcr.cz/clanek/ega-cili-zakon-o-egovernmentu.aspx

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CDBP	cestovní doklady s biometrickými prvky
CMS	centrální místo služeb
ČD	České dráhy
ČEPS	Česká přenosová soustava
ČNB	Česká národní banka
ČR	Česká republika
DMS	angl. Document management system – systém pro správu dokumentů
DS	datová schránka
DZ	datová zpráva
eOP	elektronický občanský průkaz
ES	Evropské společenství
eSSL	elektronická spisová služba
EU	Evropská unie
FO	fyzická osoba
HTML	angl. HyperText Markup Language – značkovací jazyk pro hypertext
I.CA	První certifikační autorita, a. s.
ISDS	Informační systém datových schránek
ISOT	Informační systém organizátora trhu
ISVS	Informační systémy veřejné správy
ISZO	Informační systém zúčtování odchylek
ISZR	Informační systém základních registrů
JRE	Java Runtime Environment
KIVS	Komunikační infrastruktura veřejné správy
MB	megabajt
MPSV	Ministerstvo práce a sociálních věcí

MVČR	Ministerstvo vnitra České republiky
OECD	angl. Organisation for Economic Co-operation and Development – Organizace pro hospodářskou spolupráci a rozvoj
OKTE	Organizátor krátkodobého trhu s elektřinou
OVM	orgány veřejné moci
PC	angl. Personal Computer – osobní počítač
PDF	angl. Portable Document Format – přenosný formát dokumentu
PFO	podnikající fyzická osoba
PIN	angl. Personal Identification Number – osobní identifikační číslo
PKI	angl. Public Key Infrastructure – infrastruktura veřejných klíčů
PO	právnická osoba
RA	registrační autorita
s. p.	státní podnik
Sb.	sbírky
SHA	SHA (Secure Hash Algorithm) je rozšířená hašovací funkce, která vytváří ze vstupních dat výstup (otisk) fixní délky.
SPOC	angl. Single Point of Contact – jedno kontaktní místo
SSL	spisová služba
STC	STÁTNÍ TISKÁRNA CENIN, státní podnik
SWOT	angl. Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti) a Threats (hrozby)
TXT	prostý text
USB	angl. Universal Serial Bus – univerzální sériová sběrnice, moderní způsob připojení periferií k počítači
VZP	Všeobecná zdravotní pojišťovna
XML	eXtensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK