VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

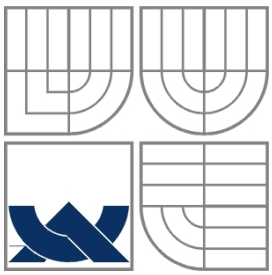
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

MODUL PRO KOMUNIKACI S PORTÁLEM ČESKÉ DAŇOVÉ SPRÁVY

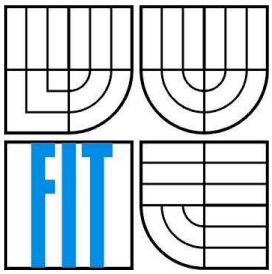
BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE JAN HAVLENA
AUTHOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

MODUL PRO KOMUNIKACI S PORTÁLEM ČESKÉ DAŇOVÉ SPRÁVY

MODULE FOR ELECTRONIC COMMUNICATION WITH THE CZECH TAX ADMINISTRATION

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

JAN HAVLENA

VEDOUCÍ PRÁCE
SUPERVISOR

ING. BOHUSLAV KŘENA, PH.D.

BRNO 2008

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav inteligentních systémů Akademický rok 2007/2008

Zadání bakalářské práce

Řešitel: **Havlena Jan**
Obor: Informační technologie
Téma: **Modul pro komunikaci s portálem České daňové správy**
Kategorie: Databáze

Pokyny:

1. Získejte a analyzujte požadavky zadavatele (Organizační kancelář, s.r.o.) na modul pro komunikaci mezi ekonomickým informačním systémem WinFas a portálem České daňové správy (ČDS).
2. Seznamte se s technologiemi používanými pro komunkaci s portálem ČDS, zejména s protokolem HTTPS, jazykem XML a s mechanizmem elektronického podpisu.
3. Na základě požadavků navrhněte modul pro komunikaci mezi IS WinFas s portálem ČDS.
4. Modul implementujte a otestujte.
5. Zhodnoťte dosažené výsledky a diskutujte možnosti dalšího vývoje.

Literatura:

- W3C. Extensible Markup Language (XML) [online]. Poslední změna 2007-05-08. Dostupné na URL: http://www.w3.org/XML/
- Network Working Group. Request for Comments 2818: HTTP over TLS [online]. Poslední změna: květen 2000. Dostupné na URL: http://www.ietf.org/rfc/rfc2818.txt

Při obhajobě semestrální části projektu je požadováno:

- První tři body zadání.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Křena Bohuslav, Ing., Ph.D.**, UITS FIT VUT
Datum zadání: 1. listopadu 2007
Datum odevzdání: 14. května 2008

L.S.

doc. Dr. Ing. Petr Hanáček
vedoucí ústavu

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami

1. Pan

Jméno a příjmení: **Jan Havlena**
Id studenta: 79009
Bytem: Nížkov 48, 592 12 Nížkov
Narozen: 31. 03. 1986, Nové Město na Moravě
(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta informačních technologií
se sídlem Božetěchova 2/1, 612 66 Brno, IČO 00216305
jejímž jménem jedná na základě písemného pověření děkanem fakulty:

.....
(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
bakalářská práce

Název VŠKP: Modul pro komunikaci s portálem České daňové správy
Vedoucí/školitel VŠKP: Křena Bohuslav, Ing., Ph.D.
Ústav: Ústav inteligentních systémů
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:

tištěné formě počet exemplářů: 1
elektronické formě počet exemplářů: 2 (1 ve skladu dokumentů, 1 na CD)

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizování výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti:
   - ☐ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

.....	.....
Nabyvatel	Autor

Abstrakt

Bakalářská práce „Modul pro komunikaci s portálem České daňové správy“ má za cíl vytvoření modulu pro komunikaci s portálem České daňové správy (ČDS) a implementování jedno pilotní elektronické podání přiznání na tento úřad. Zabývá se legislativou a postupy při elektronickém podání na úřady. Jsou v ní rozebrány používané technologie: základní údaje o jazyku XML, postup zhotovení elektronického podpisu, popis certifikátu, certifikačních autorit a komunikace HTTPS. Dále popisuje postup návrhu, implementace modulu pro komunikaci ČDS a problémy, na něž bylo naraženo při implementaci.

Klíčová slova

Elektronická komunikace, elektronické podání, protokol pro komunikaci s PVS, mechanizmus elektronického podpisu, certifikát, certifikační autority, jazyk XML, protokol HTTPS

Abstract

Bachelor thesis „Module for Electronic Communication with the Czech Tax Administration“ has aim at the creation of module for electronic communication with the Czech Tax Administration (CTA) and implementation of one pilot electronic declaration of taxes for this office. It deals with legislation and methods used for declaring tax. It analyzes the used technologies: XML, methods of creation of digital signatures, signed certificate, certificate authority and HTTPS communication. Next, it describes procedure of layout, implementation of module for communication with CTA and problems solved during the implementation.

Keywords

Electronic communication, electronic filing, protocol for communication with PVS, mechanism of electronic signature, certificate, certification authority, language XML, protocol HTTPS

Citace

Jan Havlena: Modul pro komunikaci s portálem České daňové správy, bakalářská práce, Brno, FIT VUT v Brně, 2008.

Modul pro komunikaci s portálem České daňové správy

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Bohuslava Křeny, Ph.D. Další informace mi poskytli zaměstnanci Organizační kanceláře, s.r.o. Ing. Filip Linsbauer, Ing. Jiří Koukal a Ing. Bohdan Čuhel.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Jan Havlena
5. května 2008

Poděkování

Tímto bych chtěl poděkovat vedoucímu své bakalářské práce Ing. Bohuslavu Křenovi, Ph.D za jeho hodnotné rady a připomínky k vypracování této práce. Chci také poděkovat společnosti Organizační kancelář, s.r.o. za zadání práce a za odborné rady při jejím vypracování. Konkrétně pracovníkům Ing. Filipu Linsbauerovi, Ing. Jiřímu Koukalovi a Ing. Bohdanu Čuhelovi.

Obsah

1 Úvod ... 3
1.1 Zadavatel Organizační kancelář s.r.o. ... 3
1.2 Struktura písemné práce ... 4
2 Analýza a specifikace požadavků ... 5
2.1 Specifikace modulu firmou ... 5
2.2 Analýza IS WinFAS ... 5
2.3 Model případu užití ... 6
3 Použité technologie ... 7
3.1 Jazyk XML ... 7
3.2 Mechanizmus elektronického podpisu ... 8
3.2.1 Technologie používané při tvorbě elektronického podpisu ... 8
3.2.2 Vytvoření a ověření elektronického podpisu ... 9
3.3 HTTPS ... 10
4 Elektronické podání ... 11
4.1 Komunikace s PVS ... 12
4.1.1 Podací a dotazovací protokol ... 12
4.1.2 Typy zpráv ... 14
4.1.3 Hlavičky protokolu http ... 18
4.1.4 Definice zpráv ... 18
4.1.5 Testovací větev PVS ... 18
4.2 Komunikace s ČDS ... 19
4.2.1 Funkce systému ... 20
4.2.2 GovTalk zpráva SUBMISSION_REQUEST ... 20
5 Návrh řešení modulu ... 23
5.1 Architektura modulu ... 24
5.1.1 Část odeslání podání ... 24
5.1.2 Část kontroly stavu podání ... 25
5.1.3 Dotaz na stav podání na ČDS ... 25
5.2 Implementační rozvržení modulu ... 26
5.3 Uložení dat ... 26
5.3.1 Entity databáze ... 26
5.4 Uživatelské rozhraní ... 28
6 Implementace ... 29
6.1 Použité vývojové prostředky ... 29

6.2 Implementace tříd 29
6.2.1 Knihovna aplikační d1098 29
6.2.2 Knihovna bs0510 30
6.2.3 Knihovna bd0070 31
6.2.4 SQL dotazy 32
6.2.5 Implementace šifrovacích a podepisovacích funkcí 32
6.3 Problémy při implementaci 32
7 Závěr 33
Literatura 34
Seznam příloh 35
Příloha 1 36
Manuál pro odeslání DPH z WinFASu 36

1 Úvod

V současné době, kdy neuvěřitelným tempem přibývá možností internetu, se stává elektronická komunikace běžně využívanou službou. Do této komunikace patří také dnes již standardně podporované služby elektronického podání písemností. Zvyšuje se obliba a využití elektronické komunikace mezi fyzickými nebo právnickými osobami a úřady České republiky. Tento jev je způsoben zejména jednoduchostí a snadností jeho použití, čímž se velice urychlují administrativní úkony firem, které tyto služby využívají. Proto tyto firmy požadují, aby v informačních systémech, které využívají pro správu svých dat, byla tato komunikace součástí.

Ze stejného důvodu vznikl požadavek společnosti Organizační kancelář s.r.o. ve Žďáře nad Sázavou na vytvoření komunikačního modulu, pro jí vyvíjený a distribuovaný informační systém WinFAS, což je předmětem této bakalářské práce. Prostřednictvím tohoto modulu budou mít možnost jeho uživatelé elektronicky podávat různé typy přiznání na úřad České daňové správy.

1.1 Zadavatel Organizační kancelář s.r.o.

Organizační kancelář s.r.o. je společnost s dlouhou tradicí. Je následníkem Aplikační skupiny, která vznikala v roce 1979 na Okresní zemědělské správě. Aplikační skupina měla na starosti výpočetní techniku na všech zemědělských podnicích okresu Žďár nad Sázavou. Zajišťovala dodání techniky, školení, organizační zajištění sběru dat i distribuci výstupních sestav. V té době probíhalo zpracování dat na sálovém počítači EC1033 v Brně. Podniky měly pouze možnost vlastního předzpracování dat na 8-bitových počítačích MIDO-16. Právě programy pro tyto 8-bitové počítače vytvářela na míru Aplikační skupina. V roce 1990 přešly všechny tyto agendy na platformu PC. Od tohoto přechodu si podniky všechna data zpracovávaly samy na svých PC. Tento program se jmenoval ASŘ ZpoK.

Po zrušení Aplikačních skupin vznikla Organizační kancelář, s.r.o. ve Žďáře nad Sázavou. Založili ji bývalí pracovníci Aplikačních skupin. ASŘ ZpoK neumožňoval zpracování více firem, a proto v roce 1992 začala tato společnost vyvíjet a svým zákazníkům dodávat vlastní informační systém FAS pod prostředím DOS. Ten byl rozšířen o další funkčnost, a tak začal být využíván i nezemědělskými zákazníky. Což vedlo opět k rozšíření o další agendy.

Další zlom vývoje informačního systému firmou Organizační kancelář s.r.o. byl způsoben přechodem osobních počítačů na platformu Windows. Pro tuto platformu začal být vyvíjen následník informačního systému FAS. Ten byl pojmenován WinFAS a na trh byl uveden v roce 2001. Pro vývoje systému v prostředí Windows byly vybrány nástroje společnosti Sybase. Databáze je realizována pomoci SQL Anywhere a klientská část systému je naprogramována v prostředí PowerBuilder. S počátečním rozběhem pomohla dnes již největší česká SW společnost Unicorn, a.s.

Informační systém WinFAS je komplexní, účetní, ekonomický a informační systém. Obsahuje také řadu dalších modulů, které jsou spolu propojeny. Jako například moduly řízení zásob, pozemky, zvířata, majetek, výroba, doprava a další. Společnost také poskytuje službu vývoje informačního systému na zakázku.

1.2 Struktura písemné práce

Písemná práce je rozdělena do sedmi hlavních oddílů. Obsahem první části je zasazení řešené problematiky do širšího kontextu, seznámení se zadavatelem projektu, stručný popis struktury technické zprávy a obsahu jednotlivých kapitol.

Druhá část obsahuje specifikaci požadavků Organizační kanceláře s.r.o. na vyvíjený modul komunikace s portálem České daňové správy. Dále jsou zde analyzovány a získány potřebné informace o IS WinFAS, pro který je modul vyvíjen, a sestaven model případu užití.

Následující třetí část obsahuje podrobnější seznámení s technologiemi použitými při komunikaci, konkrétně jazykem XML, mechanizmem elektronického podpisu a komunikačním protokolem HTTPS. Ve čtvrté je stručně popsán princip elektronického podání na úřady, se kterými se bude v tomto případě komunikovat. Dále analyzuje mechanizmy používané při komunikaci s Portálem veřejné správy a Českou daňovou správou.

Pátá část se zaobírá vlastním návrhem modulu. Konkrétně jeho architekturou, implementačním rozvržením, uložením dat v databázi a uživatelským rozhraním. V šesté je popsána implementace, prostředky k ní využité a problémy, se kterými jsem se při implementaci setkal.

Sedmá závěrečná kapitola shrnuje celou práci. Zabývá se zhodnocením dosažených výsledků, přínosů pro řešitele a další možnosti vývoje a využití modulu pro komunikaci s Českou daňovou správou.

2 Analýza a specifikace požadavků

V této kapitole budou analyzovány a specifikovány požadavky zadávající firmy na modul, analyzován informační systém WinFAS, pro který je modul určen, a sestaven modul případu užití.

2.1 Specifikace modulu firmou

Organizační kancelář s.r.o. zadala požadavek na vytvoření modulu pro jí vyvíjený a distribuovaný informační systém WinFAS. Modul bude zprostředkovávat komunikaci WinFASu s portálem České daňové správy. Jeho pomocí budou mít možnost klienti, kteří informační systém používají, podávat elektronická přiznání na Českou daňovou správu. Pro splnění podmínek zadání stačí realizovat pilotní implementaci podání jednoho vybraného typu daňového přiznání. Modul ovšem musí být navržen a implementován s důrazem na rozšiřitelnost o další typy daňových přiznání.

2.2 Analýza IS WinFAS

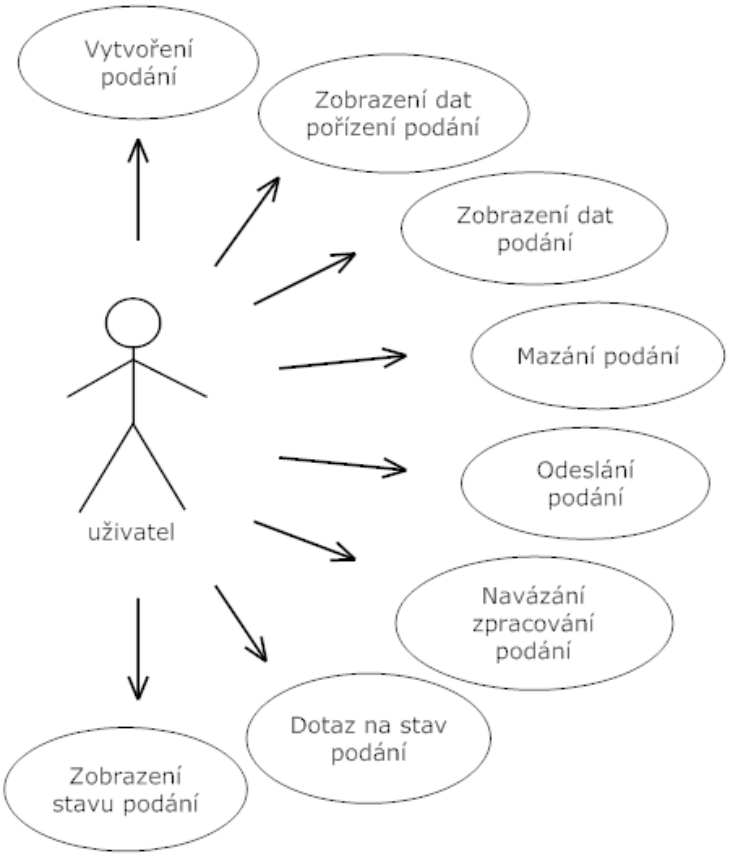
Nejprve bylo třeba důkladně prozkoumat funkční mechanizmy informačního systému WinFAS. Zadání stanovilo podmínku zhotovení implementace podání jednoho pilotního přiznání na portál České daňové správy.

Pro odeslání bylo přednostně zvoleno podání daně z přidané hodnoty. K tomuto výběru vedl jeden hlavní důvod. Informační systém obsahuje modul účetnictví, který využívá převážná většina firem používající tento software. V tomto modulu uživatelé všechna data potřebná pro výpočty a zhotovení daně z přidané hodnoty zaznamenávají. IS obsahuje také mechanizmus pro výpočet dat daňového přiznání. Na něj navazuje možnost tisku přiznání do formuláře daňového přiznání. Klienti tohoto mechanizmu s tiskem přiznání hojně využívají. Elektronický způsob podání písemností na úřady České republiky se stává standardem, a proto od klientů vznikl požadavek o doplnění této možnosti podání do informačního systému WinFAS. Některé firmy již elektronicky přiznání daně z přidané hodnoty podávají. Využívají pro to aplikaci Elektronické podání pro daňovou správu dostupnou na stránkách České daňové správy. Za zdroj zde vyplňovaných dat jim slouží tištěná podoba podání z IS WinFAS. Aplikace nabízí více možností pro práci s daty přiznání. Je to nejen samotné odeslání přiznání, ale i ukládání a kontrola dat přiznání v XML podobě, kterou vyžaduje pro elektronické přijetí ČDS. Těchto možností bude výhodné využít při konstruování a ověřování správnosti sestavování těla elektronické zprávy odesílané na ČDS. V tomto kroku analýzy bylo tedy rozhodnuto o pilotním přiznání, které bude implementovat modul. Data budou získávána z mechanizmu pro výpočet dat přiznání sloužícího pro papírový tisk přiznání daně z přidané hodnoty.

Další vlastností modulu, na níž zadavatel Organizační kancelář klade důraz, je obecná využitelnost mechanizmů modulu a možnost jeho snadného rozšíření o další daňová přiznání. Při analýze byla zjištěna skutečnost, že se v systému WinFAS nachází elektronické odesílání na Českou správu sociálního zabezpečení. Odeslání je realizováno prostřednictvím Portálu veřejné správy. Zadavatel preferuje odeslání na Českou daňovou správu také jeho prostřednictvím. Řešení tímto způsobem je výhodné pro jeho obecnost. Uživatelé budou mít takto možnost kontrolovat a obsluhovat všechna podání z jednoho místa. Mechanizmus podání na Českou správu sociálního zabezpečení však nelze obecně použít i pro odeslání na Českou daňovou správu. Také proto chce zadavatel, aby část mechanizmu odeslání na Portál veřejné správy byla obecně použitelná pro jakékoli odeslání na PVS, a byla používána i odesíláním na Českou správu sociálního zabezpečení.

2.3 Model případu užití

V předcházející části bylo specifikováno pilotní podání přiznání na ČDS. Jedná se o přiznání z daně z přidané hodnoty. Uživatelé budou mít při využívání podání přiznání daně z přidané hodnoty možnost provádět různé úkony zobrazené na obrázku 2.1 modelu případu užití.



Obrázek 2.1 model případů užití

3 Použité technologie

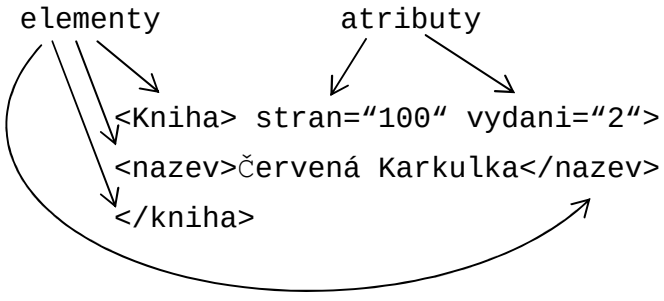
Pro komunikaci s portálem České daňové správy je použito různých technologií. Nejdůležitější z nich jsou jazyk XML, mechanizmus elektronického podpisu a protokol HTTPS. S těmito technologiemi se podrobněji seznámíme v této části textu.

3.1 Jazyk XML

Informace k této podkapitole jsem čerpal z [10]. Jazyk XML je jednoduchý a velmi účinný pro ukládání, zpracování a šíření informací. Je tedy používán hlavně pro výměnu dat mezi aplikacemi a pro vytváření, uchovávání a publikování dokumentů.

XML je zkratkou anglického *Extensible Markup Language* a jedná se o označení jednoduchého textového formátu vzniklého především z jazyka SGML. Některé vlastnosti zdědil také z HTML. Je to jazyk otevřený. Není majetkem žádného samostatného komerčního subjektu. Vyvinut a standardizován byl konsorciem W3C.

Dokument XML má logickou a fyzickou strukturu. Obsahuje specifické instrukce, nazývané tagy (značky). Logická struktura rozděluje dokument do pojmenovaných jednotek a podjednotek, nazývaných elementy. Ty jsou tvořeny počátečním a koncovým tagem spolu s daty mezi nimi. Tímto způsobem XML identifikuje jednotlivé objekty. Hierarchie dokumentu je utvářena sestavením elementů. Element obsahující ve svých vnitřních datech jiný element je mu nadřazen. Každý element musí být vždy úplně vnořen do jiného elementu, není možné, aby zasahoval do více elementů stejné úrovně. Element může kromě svého jména obsahovat ještě další informace. Tato metadata specifikující například jeho obsah či vlastnosti jsou ukládána v atributech. Element může obsahovat více atributů, a proto má každý atribut své jméno.



Obrázek 4.1 příklad XML

Fyzická struktura umožňuje pojmenovat a uložit samostatné části dokumentu, zvané entity, někdy i v dalších datových souborech, aby mohly být tyto informace opakovaně použity a aby bylo možné vkládat odkazy na data neodpovídající standardu XML.

XML je ve skutečnosti metajazyk, což znamená, že je to jazyk, který je používán k popisu dalších jazyků. Neexistuje předdefinovaný seznam elementů. XML poskytuje naprostou svobodu při využívání prvků, jejichž jména mají pro danou aplikaci smysl. Zmatku v pojmenování elementů je však možné zamezit díky mechanizmu, jehož pomocí se předdefinují elementy, které mohou být používány v dané třídě dokumentu. DTD (Document Type Definition) definuje povolené prvky a kontrolující analyzátor porovnává pravidla DTD s příslušným dokumentem, aby určil, zda dokument těmto pravidlům neodporuje.

3.2 Mechanizmus elektronického podpisu

V dnešní době je třeba při mnoha úkonech provozovaných prostřednictvím internetu dbát na bezpečnost. Z toho důvodu je používán mechanizmus elektronického podpisu. V úřední sféře se rozrůstá počet úkonů využívajících elektronického podpisu. Jedná se jak o komunikaci fyzických osob s úřady veřejné správy, tak i komunikaci mezi úřady navzájem.

Česká legislativa vyžaduje použití zaručeného elektronického podpisu, který zaručuje integritu a autentizaci podepsaných dat. Pro jeho vytvoření je třeba kvalifikovaný certifikát. K jeho vydání jsou v České republice v současné době akreditování tři poskytovatelé certifikačních služeb. Jsou to První certifikační autorita, a. s., Česká pošta, s. p. a eIdentity a. s. Ti také potvrzují autentičnost vydaných certifikátů. Takto získaný certifikát je poté použit v mechanizmu elektronického podpisu[1].

3.2.1 Technologie používané při tvorbě elektronického podpisu

Tvorba elektronického podpisu úzce souvisí s šifrováním zpráv a vytvářením jejich hash pomocí hash funkcí. Informace k další části této podkapitole jsem čerpal z [8,9].

Šifrování je používáno pro zabezpečení dat proti přečtení třetí osobou. Šifrování se dělí na symetrické a asymetrické. Symetrické používá pro zašifrování i dešifrování stejný klíč. Jeho výhodou je použití pouze jediného klíče, což se však při jeho vyzrazení stává jeho nevýhodou, protože jsou takto zašifrovaná data odkryta. Mezi algoritmy symetrického šifrování patři např. DES a IDEA.

Oproti tomu asymetrické používá pro šifrování dvou klíčů. Jeden z nich je soukromý a druhý veřejný. Při nejčastěji používaném způsobu generování klíče pomocí speciálního počítačového programu jde o jeden klíč, který se později „rozdělí“ na dvě části. Mezi těmito klíči je přesně definovaný matematický vztah. Soukromý klíč je určen pouze pro jeho majitele a ten si ho musí co nejlépe chránit proti odcizení. Veřejný klíč je poskytovaný všem. Data (zprávu) zašifrovanou jedním z dvojice klíčů lze rozšifrovat pouze druhým z tohoto páru a naopak. Pokud je tedy úspěšně

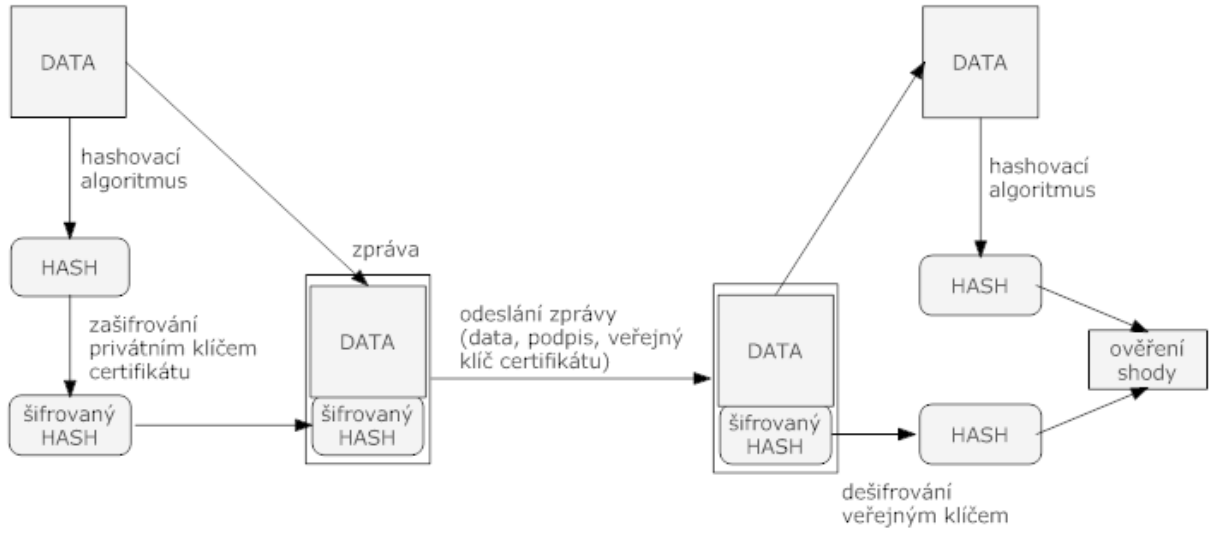
rozšifrována zpráva veřejným klíčem, je zaručeno, že byla zhotovena pomocí soukromého klíče. Dá se předpokládat, že byla zpráva sestavena majitelem soukromého klíče (pokud nebyl zcizen či zfalšován). Mezi asymetrické šifrovací algoritmy patří např. RSA a SHA.

Hash je otisk dat (zprávy). Ten je vytvořen hashovacím algoritmem, do kterého vstupují data, a jehož výstupem je jejich hash. Jedná se o speciální matematickou funkci, která z libovolně velkých dat generuje výstup pevné délky. Funkce je sestavena, tak aby byla co nejmenší pravděpodobnost vygenerování stejného hash pro různé datové vstupy. Další její důležitou vlastností je velká obtížnost sestavení inverzní funkce, kterou by šla získat zdrojová data z jejich hash. Mezi hashovací algoritmy patří SHA-1 a MD5.

3.2.2 Vytvoření a ověření elektronického podpisu

Při podepisování dat je nejprve vygenerován jejich hash. Tento hash je poté zašifrován pomocí asymetrického algoritmu privátním klíčem, který je součástí osobního certifikátu podpisatele. Čímž vznikl šifrovaný hash tedy podpis. Při odesílání jsou k podpisu přidána původní data a veřejný klíč certifikátu podpisatele. Takto vzniklá zpráva je odeslána [8].

Příjemce ze zprávy vyjme její zašifrovaný hash. Ten pomocí veřejného klíče certifikátu, obsaženého ve zprávě, dešifruje. Poté zhotoví stejným algoritmem jako odesilatel vlastní hash z dat zprávy a ten porovná s hashem získaným při dešifrování. Pokud se hashe shodují je potvrzena integrita dat. Data tedy byla odeslána osobou, která vlastní veřejný klíč (pokud nebyl zcizen či zfalšován) [8].

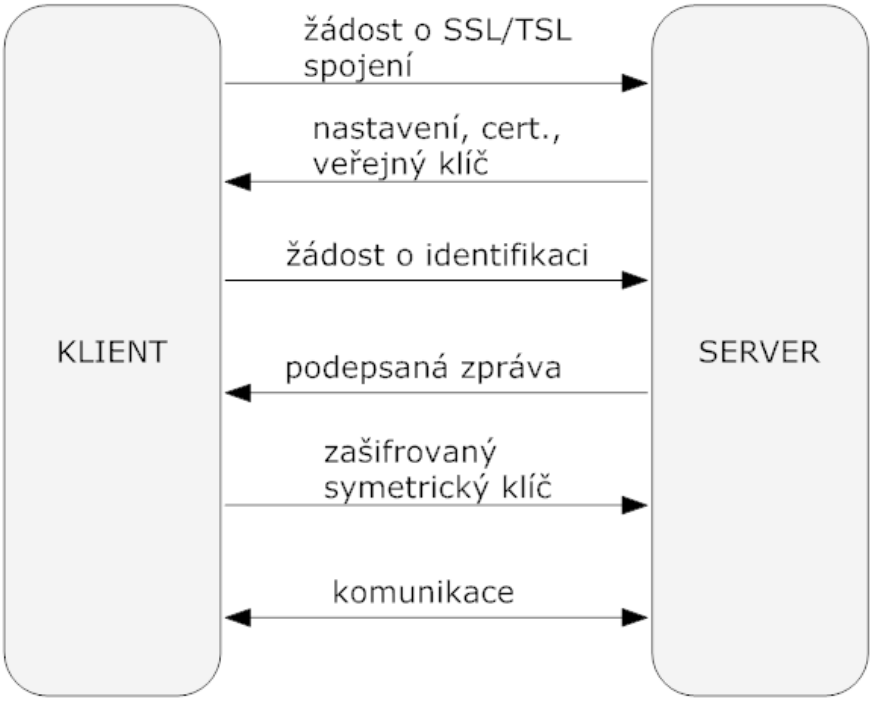


Obrázek 4.2 Vytvoření a ověření elektronického podpisu [8]

3.3 HTTPS

HTTPS je nadstavbou komunikačního protokolu HTTP. Protokol HTTPS zajišťuje větší bezpečnost při přenosech. Data jsou zabezpečena proti odposlouchávání a podvržení. Bezpečnost protokolu tkví ve formátu dat, která jsou přenášena. Již se nepřenáší data ve formátu prostého textu, ale jsou šifrována pomocí SSL nebo TLS technologií. Přenos nadále probíhá prostřednictvím protokolu HTTP [8].

Technologie SSL a TLS jsou založeny na principu navázání bezpečného spojení pomocí certifikátu, který musí vlastnit server. Klient požádá o inicializaci spojení s použitím SSL nebo TLS. Server obratem zašle klientovi nastavení SSL/TSL, svůj certifikát a veřejný klíč. Klient požádá server, aby se identifikoval. Server zašle klientovi podepsanou zprávu. Z níž klient ověří pomocí dříve obdrženého certifikátu jeho identitu. Poté vygeneruje náhodný šifrovací klíč. Ten zašifruje pomocí získaného veřejného klíče a zašle ho serveru. Zprávu s tímto klíčem může dešifrovat pouze server svým privátním klíčem, čímž je zamezeno jeho odhalení další stranou. Server ho tedy ze zprávy získá. Další komunikace mezi klientem a serverem probíhá pomocí symetricky šifrovaných zpráv prostřednictvím tohoto klíče [8].

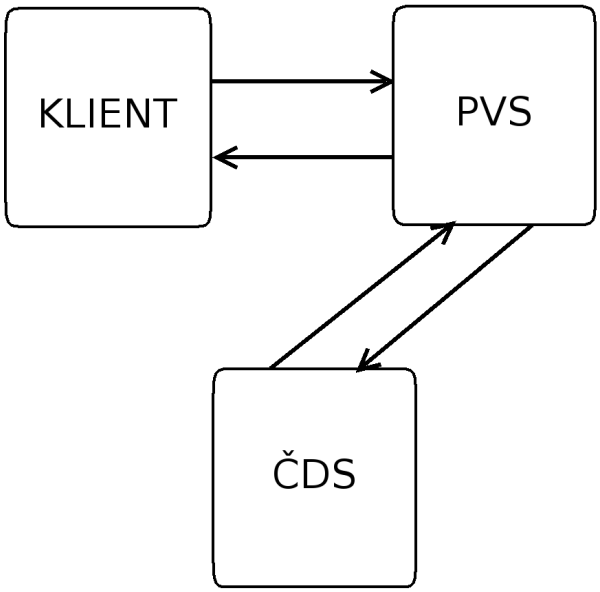


Obrázek 4.3 Navázání HTTPS spojení [8]

4 Elektronické podání

Elektronické podání je obdobou klasického podání v podobě papírového tiskopisu na příslušnou podatelnu příslušného úřadu. Elektronické podání se však, jak již je z názvu patrné, odehrává elektronickou formou.

V současné době již většina státních orgánů umožňuje právnickým i fyzickým osobám elektronickou komunikaci. Tato komunikace zahrnuje i elektronická podání. Jak již vyplynulo ze zadání, bude se v tomto případě komunikovat s Českou daňovou správou.



Obrázek 4.1 komunikace s ČDS prostřednictvím PVS

Základní agendu České daňové správy (ČDS) tvoří správa daní. Jedná se o daň z příjmů fyzických osob, daň z příjmů právnických osob, daň z přidané hodnoty, daň silniční, daň z nemovitostí, daň z převodu nemovitostí, daň dědická a daň darovací. Česká daňová správa tyto daně přijímá a zpracovává. Ministerstvo financí v souladu s platnou legislativou připravilo pro daňové subjekty možnost podávat daňové přiznání a další písemnosti i v elektronické podobě. Podání lze uskutečnit na disketě nebo více využívanou možností prostřednictvím internetu. Podání po internetu lze uskutečnit jako podání s datovou zprávou opatřenou zaručeným elektronickým podpisem nebo jako podání s datovou zprávou neopatřenou zaručeným elektronickým podpisem. V případě podání s datovou zprávou neopatřenou zaručeným elektronickým podpisem se ještě vyžaduje podání v písemné podobě, tj. doručení počítačové sestavy správci daně (e-tiskopis) [1,7].

Další možností je využít podání na ČDS prostřednictvím Portálu veřejné správy (PVS) (obr. 4.1), který zprostředkovává veškerá elektronická podání poskytovaná veřejnou správou České republiky. Portál veřejné správy poskytuje službu prostředníka mezi uživateli elektronického podání a příslušnou organizací veřejné správy. Součástí portálu je aplikace Podání sloužící pro registraci uživatelů, kteří chtějí využívat elektronické služby poskytované veřejnou správou České republiky. Po registraci je možno zasílat a přijímat formuláře z úřadů veřejné správy s využitím identifikátoru uživatele nebo s užitím digitálního certifikátu. Komunikace s příslušnou organizací veřejné správy může dále probíhat prostřednictvím webových formulářů, které mohou být umístěny na příslušných webových stránkách úřadu veřejné správy nebo prostřednictvím aplikací jiných dodavatelů (např. účetní a mzdové programy) [2].

Pro jednotlivé orgány veřejné správy jsou vyhotoveny krátké dokumentace obsahující základní informace potřebné pro zhotovení komunikačních modulů externích aplikací. Nejsou však zcela dostačující pro pochopení celé problematiky komunikace, a proto byla pro vývojáře založena diskusní skupina Podpora vývojářů https://bezpecne.dev.gov.cz/diskuze/. Zde je možno dohledat další informace potřebné pro vývoj komunikačního modulu.

4.1 Komunikace s PVS

Informace k této podkapitole jsem čerpal z [4]. Komunikace s Portálem veřejné správy je zprostředkována prostřednictvím aplikace Elektronická podání, kterou portál provozuje. Funguje jako bod pro veškeré elektronické transakce mezi jednotlivci, firmami nebo jejich zástupci a úřady veřejné správy. Aplikace Elektronická podání zajišťuje předání elektronických písemností portálu příslušného úřadu veřejné správy. Zajišťuje také zpětné doručování odpovědí úřadů na jim předané elektronické písemnosti.

4.1.1 Podací a dotazovací protokol

Podací a dotazovací protokol definuje způsob komunikace mezi klientskou aplikací a aplikací Elektronická podání. Je založen na schématu pod názvem GovTalk. Představuje mechanizmus podávání dokumentů určených pro systémy úřadů veřejné správy přes aplikace Elektronická podání. Také definuje způsob komunikace při zjišťování stavu a místa cyklu, ve kterém se podání nachází.

Odesílané dokumenty jsou podávány nejlépe ve formátu XML (eXtensible Markup Language) prostřednictvím protokolu HTTP (Hypertext Transport Protocol) nebo alternativně ve formátu HTML (Hyper Text Markup Language). Dále se budeme zabývat pouze definicemi zasílaných zpráv v nativním formátu XML.

4.1.1.1 Konstrukce protokolu

Protokol je navržen tak, aby implementoval konečné cíle zákazníků a aby zabezpečoval integritu při jakémkoli neočekávaném chování klienta (klientské aplikace) nebo rozhraní rezortu (portálu úřadu). Postup při zpracování dokumentu Portálu veřejné správy je následující:

1. Zkontroluje se formát a data příchozí zprávy.
2. Jsou zkontrolovány přihlašovací údaje.
3. Nastala-li z nějakého důvodu chyba (špatné přihlašovací nebo jiné údaje) je odeslána chybová zpráva.
4. Pokud vše proběhlo bez chyby, je klientovi zpět odesláno CorrelationID (identifikátor transakce), pomocí něhož je na podání odkazováno v další komunikaci.
5. Část zprávy určené konkrétnímu úřadu je tomuto úřadu zaslána.
6. Systém úřadu veřejné správy data zpracuje a zprávu o stavu zašle aplikaci Elektronická podání PVS.
7. Aplikace Elektronická podání zprávu přijme a uloží k příslušnému podání.
8. Klientovi je odpovídáno na dotaz stavu podání podle uložených dat.
9. Po ukončení komunikace týkající se příslušného podání jsou všechna data s ním spjata smazána.

4.1.1.2 URL adresa pro odesílání

Aktuální adresou pro komunikaci s aplikací Elektronické podání Portálu veřejné správy je:

https://bezpecne.podani.gov.cz/submission

4.1.1.3 Kódování, formát

Kódování všech dokumentů předávaných metodou HTTP POST musí být ve znakové sadě UTF-8. Elementy v dokumentu XML musí být v pořadí odpovídajícím pořadí elementů definované schématem. Pokud není uvedeno jinak, je třeba rozlišovat mezi použitím malých a velkých písmen. Protokol je case sensitive.

4.1.1.4 Struktura zpráv

Všechny zprávy přijímané aplikací Elektronická podání musí být formátu schématu GovTalk. Zprávy vlastního odeslání dat obsahují jeden kořenový element pro přenášení dat podání. Struktura obsahu tohoto elementu se liší podle dokumentu odesílaného touto zprávou a je definován příslušným úřadem, kterému je určen.

I další zprávy používané při komunikaci obsahují jeden kořenový element. V těchto případech nese informace o stavu podání. Samotná aplikace Elektronická podání tento element ignoruje, protože slouží pouze jako prostředník, pro ni jsou důležité pouze hodnoty hlavičky GovTalk.

4.1.2 Typy zpráv

Zprávy zasílané při komunikaci se rozdělují do dvou skupin podle strany, kterou je zpráva generována. Zprávy jsou ve tvaru schématu GovTalk. Obálka každé z těchto zpráv obsahuje elementy Qualifier a Class. Těmito elementy je určen typ zprávy.

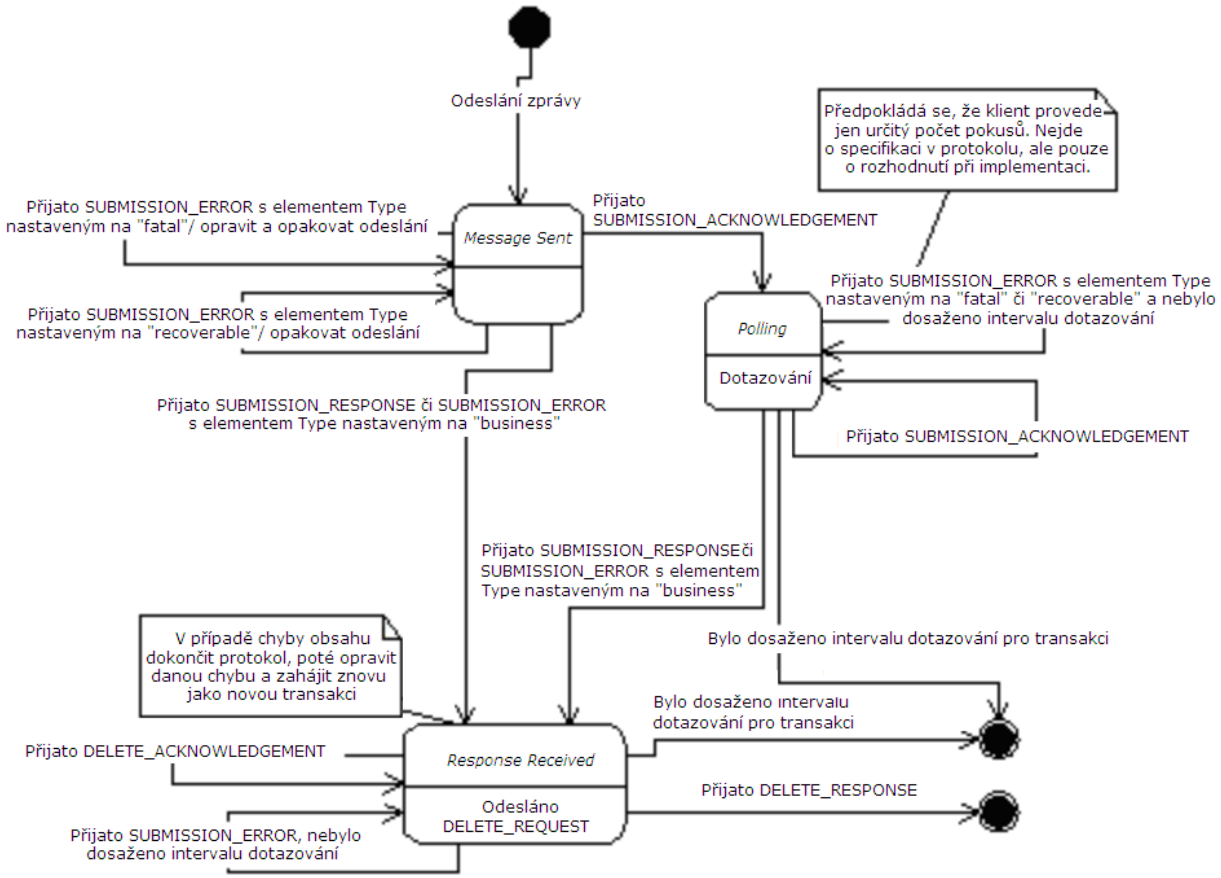
Zprávy generované klientskou aplikací:

- SUBMISSION_REQUEST
- SUBMISSION_POLL
- DATA_REQUEST
- DELETE_REQUEST

Zprávy generované aplikaci Elektronická podání:

- SUBMISSION_ACKNOWLEDGEMENT
- SUBMISSION_ERROR
- SUBMISSION_RESPONSE
- DATA_RESPONSE
- DELETE_RESPONSE
- DELETE_ACKNOWLEDGEMENT

Zprávy musí být definovány podle určitých pravidel. Definice, význam a posloupnost těchto zpráv je popsána dále.



Obrázek 4.2 stavové schéma protokolu [4]

4.1.2.1 Podání

Průběh podání je znázorněn stavovým protokolem na obrázku 4.2. Podání vlastních dat dokumentu je uskutečněno zprávou SUBMISSION_REQUEST. Tato zpráva je vygenerována a odeslána klientskou aplikací na PVS. Zde je zpracována aplikací Elektronická podání, která na ni může odpovědět třemi způsoby.

Nejčastěji odpovídá zprávou SUBMISSION_ACKNOWLEDGEMENT, kterou aplikace Elektronická podání zasílá v případě, kdy podání dosud nezpracovala. Je třeba pokračovat v dotazování do chvíle, kdy přijde od aplikace Elektronická podání odpověď SUBMISSION_ERROR nebo SUBMISSION_RESPONSE. Zpráva SUBMISSION_ERROR je zaslána v případě, že zpráva SUBMISSION_REQUEST obsahovala chyby. Zprávou SUBMISSION_RESPONSE je odpovídáno v případě, kdy je zpracování vlastního podání dokončeno bez chyb, datová část zprávy byla předána příslušnému úřadu veřejné správy. Poté musí klientská aplikace odeslat zprávu DELETE_REQUEST jako žádost o odstranění původní zprávy. Aplikace na ni odpoví DELETE_RESPONSE což znamená, že byla komunikace ukončena a všechna data s ní spojená byla smazána.

Odesílání podání může skončit čtyřmi různými výsledky. Jedná se o podání dokončené v pořádku, podání skončilo chybou, která nelze být odstraněna, podání ukončené chybou či chybami, které lze odstranit, a podání, které obsahuje chyby ve vlastních datech. Tyto případy budou podrobněji rozepsány dále.

Protokol také umožňuje klientovi kontrolní výpis podání zpracovávaných pod jeho jménem aplikací Elektronická podání. Jedná se o komunikaci prostřednictvím zpráv DATA_REQUEST vytvořenou a zaslanou klientem a DATA_RESPONSE navrácenou zpět aplikací Elektronická podání. Tato možnost vznikla z důvodu kontroly doručení podání dokumentu. Komunikace přes internet je uskutečňována prostřednictvím protokolů HTTP/HTTPS, ty však nezaručují doručení odesílaných zpráv.

4.1.2.2 Úspěšné podání

Cyklus úspěšného podání probíhá v těchto krocích:

1. Klientskou aplikací je sestavena zpráva SUBMISSION_REQUEST s daty nového podání a je zaslána aplikaci Elektronická podání PVS.
2. Aplikace Elektronická podání je však zaneprázdněná. Podání nezpracovává okamžitě, a proto odesílá zprávu SUBMISSION_ACKNOWLEDGEMENT. Ta klienta informuje, že zpráva nebyla aplikací dosud zpracována ani předána dále příslušnému úřadu veřejné správy. Zpráva obsahuje identifikátor podání CorrelationID, jehož prostřednictvím se dále na podání dotazuje klientská aplikace.
3. Po vyčkání určitého časového intervalu zasílá klientská aplikace zprávu pro zjištění stavu podání SUBMISSION_POLL.
4. Podání nebylo stále aplikací Elektronická podání zpracováno, a proto je klientské aplikaci odpovězeno zprávou SUBMISSION_ACKNOWLEDGEMENT.
5. Za další časový interval zasílá klientská aplikace opět zprávu pro dotaz stavu podání SUBMISSION_POLL.
6. Nyní již bylo podání aplikací Elektronická podání zpracováno, o čemž je informována klientská aplikace zprávou SUBMISSION_RESPONSE.
7. Klientská aplikace zašle požadavek pro ukončení komunikace a smazání původní zprávy DELETE_REQUEST.
8. Aplikace Elektronická podání je však zaneprázdněna a nemůže tento požadavek zpracovat, tak zasílá DELETE_ACKNOWLEDGEMENT.
9. Po určitém časovém intervalu zašle klientská aplikace opět zprávu DELETE_REQUEST.
10. Nyní již je zpracována, komunikace je ukončena a všechna její data jsou ze systému vymazána, zpět je zaslána o tom informující zpráva DELETE_RESPONSE.

Opakující se části komunikace, konkrétně kroky 3, 4 a 8, 9 se v komunikačním cyklu vyskytovat nemusejí nebo mohou být zastoupeny i vícekrát. Množství jejich výskytu je závislé na rychlosti vyřízení zpráv, tedy na aktuální zaneprázdněnosti aplikace Elektronická podání.

4.1.2.3 Podání s neodstranitelnou chybou

Jedná se o podání obsahující chyby ve zprávě zasílaných klientskou aplikací. Aplikace Elektronická podání na ně odpovídá zprávou SUBMISSION_ERROR s hodnotou Error/Type fatal a jedná se o neodstranitelnou chybu. Pokud je takto odpovězeno na zprávu SUBMISSION_REQUEST, jsou chyby způsobeny například zapomenutými či chybně zadanými elementy v obálce GovTalk. Chyby je třeba odstranit a celé zaslání podání opakovat znovu.

Pokud byla klientskou aplikací přijata zpráva SUBMISSION_ERROR v pokročilé části cyklu podání, je třeba pokračovat v dotazování s identifikátorem CorrelationID, získaným v počáteční odpovědi SUBMISSION_ACKNOWLEDGEMENT nebo SUBMISSION_RESPONSE.

4.1.2.4 Podání s odstranitelnou chybou

Při elektronickém podání mohou vzniknout chyby v důsledku zahlcení čí přetížení systému. Klientskou aplikací je vrácena zpráva SUBMISSION_ERROR s hodnotou Error/Type recoverable. V těchto případech se jedná o chyby odstranitelné a dočasné. Klient musí pokračovat v cyklu znovu odesláním poslední zprávy.

4.1.2.5 Podání s chybnými vnitřními daty

Další typ chyby je vyvolán odesláním podání s chybným obsahem. Může se jednat například o vynechání některého z jeho elementů nebo zadání špatné hodnoty. Aplikace Elektronická podání zasílá zprávu SUBMISSION_ERROR s hodnotou Error/Type business. V tomto případě je třeba dokončit cyklus až po přijetí zprávy DATA_RESPONSE a opakovat odeslání s opravenými daty znovu.

4.1.2.6 Stavy protokolu

Při komunikaci mezi klientem a aplikací Elektronická podání se dostáváme prostřednictvím zasílání a přijímání zpráv do pěti základních stavů cyklu podání:

- *Submission (Podání)*

  Tento stav nastává při zahájení komunikace mezi klientem a aplikací Elektronická podání a odesláním zprávy SUBMISSION_REQUEST.
- *Polling (Dotazování)*

  Do tohoto stavu se podání dostává obdržením zprávy SUBMISSION_ACKNOWLEDGEMENT. Klient nadále pokračuje odesíláním zprávy SUBMISSION_POLL, dokud nedostane odpověď SUBMISSION_RESPONSE.

- *Response Received (Přijata odpověď)*
  Obdržením zprávy SUBMISSION_RESPONSE se cyklus dostává do tohoto stavu.
- *Delete Response (Uzavření transakce)*
  Nastává po odeslání zprávy DELETE_REQUEST klientem na aplikace Elektronická podání, která žádá o ukončení cyklu podání a odstranění všech informací s tímto podáním souvisejícím.
- *Error State (Chybový stav)*
  Do stavu se dostává po obdržení jakékoli chybové zprávy.

4.1.3 Hlavičky protokolu http

Dokumenty je do aplikace Elektronická podání možné podávat ve třech formátech, jsou to XML, HTML a text. Umožňuje to element Transformation v hlavičce GovTalk. Od skutečnosti, že jsou data podávána v různých formátech, jsou úřady veřejné správy zcela odstíněny prostřednictvím aplikace Elektronická podání, která tato data zpracuje a teprve poté odešle příslušnému úřadu. Odesílání podání, které jsou ve formátu XML, je realizováno prostřednictvím HTTP POST. Hlavička Content-type protokolu HTTP musí být nastavena na hodnotu text/xml. Aplikace Elektronická podání tuto hodnotu požaduje, jestliže je element Transformation nastaven na XML.

4.1.4 Definice zpráv

Zprávy odesílané klientem aplikací Elektronická podání musí mít podle definovaných schémat předepsaný tvar a obsah. Také zprávy zasílané aplikací Elektronická podání musí těmto definovaným schématům odpovídat.

Při podávání aplikace Elektronická podání kontroluje zprávy podle schémat. Pokud je nalezena chyba, při srovnávání zprávy s předdefinovanými schématy, je zpět zaslána odpověď SUBMISSION_ERROR. V této chybové zprávě jsou označeny chybové bloky tím způsobem, že jsou naplněny hodnotou UndefinedClass.

Definice těchto schémat jsou podrobně popsány ve vývojářských dokumentech dostupných na stránkách Podpora vývojářů https://bezpecne.dev.gov.cz/diskuze/ Portálu veřejné správy [3].

4.1.5 Testovací větev PVS

Informace o testovací větvi PVS jsou čerpány z literatury [5]. Při vývoji aplikací určených pro komunikaci s PVS konkrétně jeho aplikací Elektronická podání je třeba testovat jejich správnou funkčnost. To však nelze ostrým odesíláním dokumentů. Z tohoto důvodu existuje testovací větev Portálu veřejné správy. Vznikla fyzickým rozdělením transakční části PVS na dva technologické celky, ostrý a testovací.

Ostré provozní prostředí transakční části je určeno pro reálné zasílání podání. Je navrženo pro maximální dostupnost, propustnost a spolehlivost. Aby nebylo ostré prostředí ovlivňováno

testovacím, například při velkém zatížení testovací části, jsou všechny komponenty aplikace transakční části zdvojeny.

Testovací prostředí transakční části je určeno pro testování a vývoj aplikací. Toto prostředí je přesnou kopií ostré větve. Přesto však nezaručuje redundanci jednotlivých komponent a stálou propustnost systému. Celé testovací prostředí je zapojené do struktury GovNetu a je připojeno na testovací DIS servery, které jsou umístěny u připojených orgánů veřejné správy. Testovací podání tedy prochází celý cyklus a jeho obsah je odesílán na testovací servery jednotlivých úřadů veřejné správy. Tím pádem po úspěšném otestování aplikace pouze stačí její odesílání přesměrovat na ostrou větev.

Testovací prostředí se také používá při implementaci nových služeb. Ty jsou vždy nejdříve zavedeny v testovací větvi, kde se ladí a testují. Po jejich odladění jsou teprve přeneseny do ostrého prostředí.

V testovacím prostředí nejsou vyloučeny krátkodobé výpadky. Jsou způsobeny jak skutečností, že testovací větev není provozována v plně stabilním prostředí, tak tím, že jsou na ni testovány nové služby spojené s implementačními prácemi.

Pro komunikaci na testovací větvi se stejně jako na ostré používá SSL komunikace. Jsou pro ni však využívány jiné certifikáty, určené pouze pro testovací větev. Před jejím využíváním je třeba tyto certifikáty nainstalovat.

Před navázáním komunikace s testovací větví se je třeba stejně jako na ostré větvi registrovat na Portálu veřejné správy. Registruje se pod příslušnou službou. Registrace probíhá pro testovací větev na stránkách http://www.dev.gov.cz .

Testovací větev transakční části je dostupná na adrese: http://www.dev.gov.cz
Testovací podávání se uskutečňuje na adrese: https://bezpecne.dev.gov.cz/submission

4.2 Komunikace s ČDS

Informace o komunikaci s ČDS byli získány z [3,6]. Tato část se zabývá komunikací s ČDS, konkrétně vytvořením elektronického zasílání formulářů daňové správy prostřednictvím transakční části PVS, na které byla za účelem poskytnutí elektronických služeb Ministerstva financí zřízena služba „*Daňová správa – elektronická podání*“. Tato služba je na Portál veřejné správy napojena stejným způsobem jako další služby tímto portálem poskytované a má zatím jedinou implementovanou transakci s identifikátorem MF_DS_EDP (obsah elementu CLASS v GovTalk obálce).

4.2.1 Funkce systému

Systém zpracování dat pro službu „*Daňová správa – elektronická podání*“ plní následující funkce:

- Přijetí elektronického podání a potvrzení doručení od transakčního jádra PVS
- Kontrola správnosti obálky a rozšifrování zprávy
- Doručení rozšifrované zprávy do elektronické podatelny Ústředního finančního a daňového ředitelství (ÚFDŘ)
- Podpora rozšiřujících funkcí (dotaz na stav zpracování, testovací režim apod.)
- Zaslání výsledku zpracování od elektronické podatelny zpět do transakčního jádra PVS

4.2.2 GovTalk zpráva SUBMISSION_REQUEST

Pro odeslání dat podání na portál ČDS prostřednictvím PVS aplikace Elektronická podání je používána zpráva SUBMISSION_REQUEST. Příklad její struktura s obálky PVS je na obrázku 4.3.

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
        <Class>MF_DS_EDP</Class>
            <Qualifier>request</Qualifier>
            <Function>submit</Function>
            <TransactionID />
            <AuditID />
            <CorrelationID />
            <ResponseEndPoint />
            <Transformation>XML</Transformation>
        </MessageDetails>
      <SenderDetails>
            <IDAuthentication/>
      </SenderDetails>
    </Header>
    <GovTalkDetails>
        <Keys/>
    </GovTalkDetails>
    <Body>
        <Message version="1.0" xmlns="http://adis.mfcr.cz/adis/submission">
            <Header>
                <Vendor productName="VENDOR01" version="1.0" />
            </Header>
            <Body encrypted="yes" contentEncoding="gzip" onlyTest="yes"
function="submit" email="ufdr@neurodot.com" >
                MIICEAYJKoZIhvcNAQcDoIICATCCAf0CAQAxgc
                YwgcMCAQAwbTBfMQswCQYDVQQG TlpA +Pjhkg==
            </Body>
        </Message>
    </Body>
</GovTalkMessage>
```

Obrázek 4.3 příklad zprávy SUBMISSION_REQUEST [6]

4.2.2.1 Údaje GovTalk obálky

Údaj v obálce ***GovTalkMessage/Header/MessageDetails/Class*** je vždy nastaven na hodnotu MF_DS_EDP, která identifikuje podání pro ČDS.

Atribut ***GovTalkMessage/GovTalkDetails/Keys/Key@Type*** může nabývat dvou hodnot. ***bday*** při použití služby pod účtem občana nebo jeho zástupce a DIČ, pokud je služba použita organizací nebo jejím zástupcem.

Do element ***GovTalkMessage/GovTalkDetails/Keys/Key*** jsou zadávány ve správném tvaru přihlašovací údaje osoby nebo společnosti, které byly získány při registraci k příslušné službě PVS.

4.2.2.2 Popis prvků obálky datové věty

Prvky obálky datové věty se rozdělují na povinné a nepovinné. Mezi povinné prvky patří:

- ***Message*** identifikující dokument v rámci UFDŘ (interní obálky). Pro elektronická podání je kvalifikována jmenným prostorem **http://adis.mfcr.cz/adis/submission.**
- ***version*** značící použitou verzi obálky a struktury datové věty určené pro UFDŘ. Hodnota současné verze je 1.0.
- ***Header*** je hlavička obálky pro DIS server.
- ***Verdon*** nese informace o produktu, který tento dokument vygeneroval. Informace jsou uvedeny v jeho atributech ***productName****="název produktu"* a ***version****="verze produktu"*.
- ***Body*** obsahuje vlastní zašifrovaná data uložená ve formátu base64.
- ***Encrypted*** označuje zda je datová věta zašifrována. V současné verzi (1.0) je šifrování povinné, a tedy encrypted musí být nastaveno na hodnotu „*yes*“.
- ***contentEncoding*** označuje, zda je obsah (datová věta) zašifrována v komprimované formě nebo v čisté formě. Atribut může nabývat hodnot „*gzip*“ a „*raw*“.

Nepovinné prvky jsou následující:

- ***onlyTest*** označuje, zda se jedná o podání v testovacím režimu. Pokud se jedná o tento režim, musí být atribut přítomný a jeho hodnota nastavena „*yes*“. V jiném případě se o podání v testovacím režimu nejedná.
- ***Email*** je určen pro zadání e-mailové adresy. Pokud je zadána, jsou na ni posílány informace o stavu zpracování podání.
- ***Function*** může nabývat dvou hodnot „***submit“*** nebo „***poll“***. Pokud je naplněn hodnotou „*submit*“ nebo není uveden, jedná se o vlastní podání. V případě kdy nabývá hodnoty „*poll*“, jde o dotaz na stav podání na ČDS.

4.2.2.3 Vlastní elektronické podání

Atribut ***Function*** nacházející se ***v GovTalkMessage/Body/Message/Body/@function*** má hodnotu „*submit*“. Obsahem datové věty jsou potom data elektronického podání a jedná se o vlastní podání.

Tyto data musí být chráněny proti vnějším zásahům a musí být zaručena identifikace odesílatele. V současné verzi jsou povoleny pouze datové zprávy v tzv. formě „ZAREP“ – „Zaručený elektronický podpis“. To znamená, že datová věta musí být opatřena elektronickým podpisem vytvořeného kvalifikovaným certifikátem (tzv. „attach“ forma – data jsou součástí podpisu). Po tom co jsou opatřena tímto podpisem, je nutné je ještě zašifrovat pomocí šifrovacího certifikátu vydaného PVS.

Zpráva sestavená podle výše popsaných pravidel s takto sestaveným obsahem datové věty je připravena pro odeslání na PVS. Jedná se o vlastní podání na úřad Daňové správy prostřednictvím PVS.

4.2.2.4 Dotaz na stav podání na ČDS

Odeslání na ČDS může být ukončeno potvrzením přijetí podaných dat na ČDS. V tomto bodě vlastní odeslání končí. ČDS však poskytuje rozšířenou funkci dotazování na stav zpracování podání na ČDS. Při odesílání dotazu na stav je založena vždy nová transakce. Odesílání probíhá obdobně jako při vlastním podání. Liší se však obsah datové věty.

Atribut ***Function*** nacházející se v ***GovTalkMessage/Body/Message/Body/@function*** má hodnotu „***poll***“ a obsah elementu „***Body***“ je následující struktura. Tato struktura musí být, jako všechny struktury v „***Body***“, před vložením do obálky zašifrována.

```
<PollRequest xmlns="http://adis.mfcr.cz/adis/poll">
        <SubmNumber>564654</SubmNumber>
        <Password>*****</Password>
</PollRequest>
```

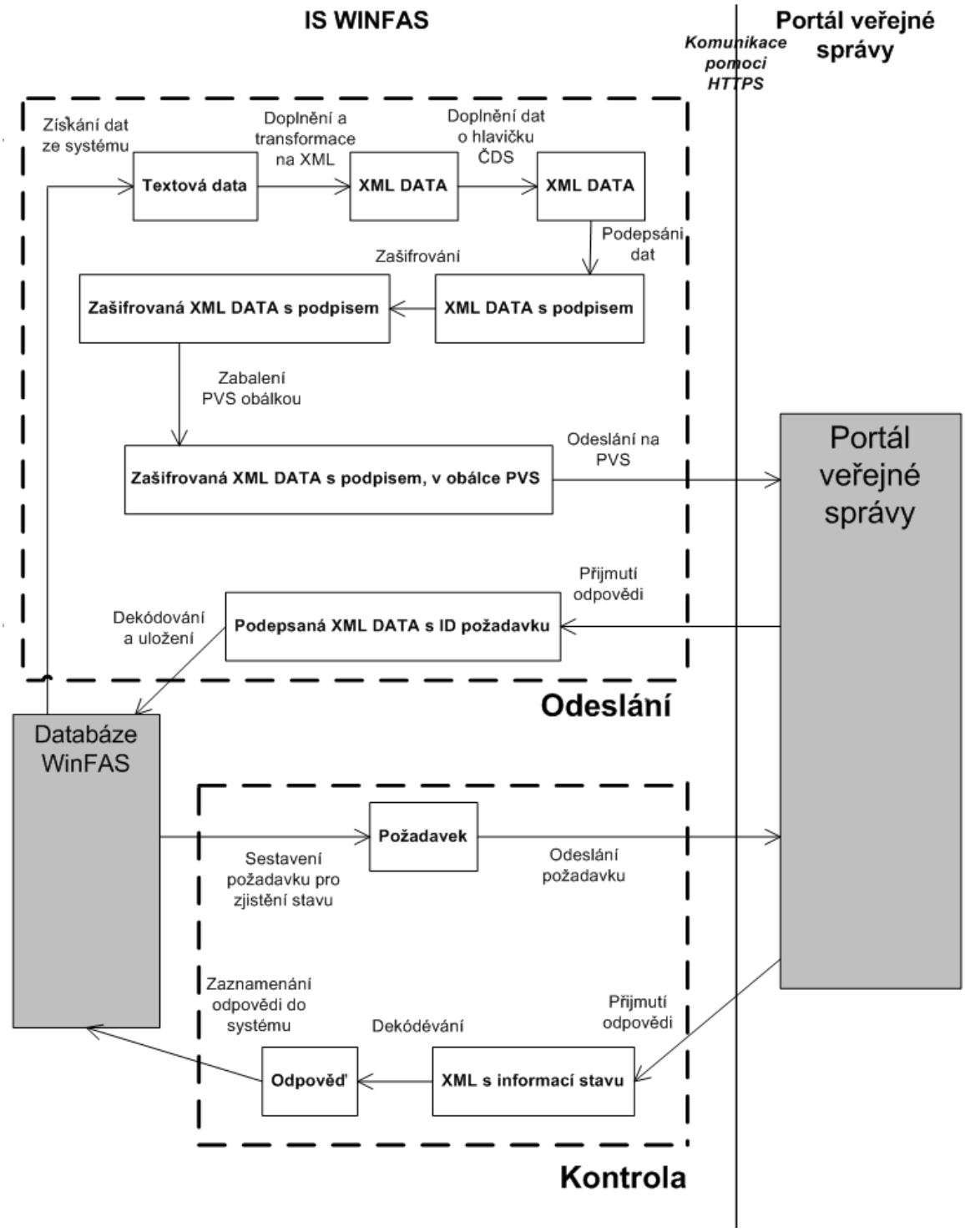
Obrázek 4.4 příklad obsahu elementu „Body“ [6]

Struktura obsahuje elementy „*SubmNumber*“ a „*Password*“. Obsahem „*SubmNumber*“ je číslo podání získano z tzv. doručenky předchozího úspěšného podání. „*Password*“ je naplněn heslem pro zjištění stavu také získaném z doručenky předchozího úspěšného podání.

Celý cyklus odeslání proběhne stejně jako odeslání vlastního podání. Na konci cyklu je klientské aplikaci doručena zpráva obsahující informace stavu podání na ČDS. Tento dotaz je možné posílat vícekrát. Odpověď se bude měnit podle stavu podání na ČDS.

5 Návrh řešení modulu

V předchozí části byly zanalyzovány všechny požadavky a vlastnosti modulu. Způsob vytváření zpráv a komunikace mezi modulem a aplikací Elektronická podání Portálu veřejné správy. Dalším krokem je návrh mechanizmu modulu.



Obrázek 5.1 Architektura modulu

5.1 Architektura modulu

Architektura modulu se skládá z části odeslání a části kontroly. V této části jsou dále rozloženy do jednotlivých kroků, které uvnitř nich probíhají. Architektura modulu je znázorněna na obrázku 5.1.

5.1.1 Část odeslání podání

V této části se získají odesílaná data. Z nich je dále sestavena zpráva stanoveného tvaru, která je odeslána na Portál veřejné správy.

5.1.1.1 Získání a transformace dat

Jako zdroj dat bude použit stávající mechanizmus výpočtu používaný pro tiskový výstup přiznání daně z přidané hodnoty. Tento mechanizmus získává data ze systému WinFAS a to přímo nebo výpočty. Získaná data jsou však pro potřeby elektronického podání neúplná. Dalším nedostatkem těchto dat je jejich formát, protože jsou v textové podobě používaná na přiznání písemné podoby.

Data je tedy třeba doplnit. Zbývající část bude získána z IS WinFAS a přímo z uživatelského vstupu. Dalším krokem bude jejich transformace do formátu stanoveného a používaného v odesílané zprávě. Takto upravená data jsou sestavena do zprávy ve tvaru XML a zabalena do obálky úřadu, pro který jsou určena. Definice XML zpráva, formát jejího obsahu a obálky je stanovena příslušným úřadem v tomto případě tedy Českou daňovou správou.

5.1.1.2 Podpis a šifrování

Sestavená datová část zprávy pro ČDS je třeba zabezpečit. Nejprve se data podepíší podpisovým certifikátem osoby pověřené pro odeslání daňového přiznání. K podpisu se přidají podepisovaná data a tento celek se dále šifruje prostřednictvím certifikátu ČDS.

Pro šifrování a podepisování bude použita již ve WinFASu naimplementovaná třída, která se používá pro šifrování a podepisování dat odesílaných na Českou správu sociálního zabezpečení.

5.1.1.3 Zabalení zprávy

Takto vzniklá šifrovaná data je třeba zabalit do obálky České daňové správy a poté do obálky PVS. Obálky jsou formátu XML.

Obálka České daňové správy je pro každý úřad veřejné správy specifická. Obsahuje informace o formátu dat v ní uložené, jméno aplikace, která zprávu vytvořila, informační email, případně další popsané v analýze.

Stavba obálky Portálu veřejné správy je shodná pro podání na všechny úřady veřejné správy, pro které PVS zprostředkovává komunikaci. Obálka je v tvaru jazyka XML a obsahuje informace určené výhradně pro PVS. Podle těchto informací PVS identifikuje zprávu, jejího odesilatele a úřad veřejné správy, pro který je zpráva určena.

5.1.1.4 Odeslání zprávy

Pokud je zpráva na příslušný úřad úspěšně sestavena, následuje její odeslání na Portál veřejné správy. Pro odesílání je třeba použít zabezpečené předávání dat prostřednictvím internetu. Komunikace s PVS je předepsána pomocí HTTPS protokolu.

5.1.1.5 Přijmutí a uložení odpovědi

V dalším kroku je obdržena odpověď z PVS, která nese informace, zda proběhlo přijetí podání na PVS v pořádku a identifikátor podání, popřípadě chybové hlášení. Data z ní získaná musí být zaznamenána do systému, aby je bylo možno použít v další části kontroly stavu podání.

5.1.2 Část kontroly stavu podání

5.1.2.1 Odeslání a přijetí odpovědi

Při kontrole stavu je nejdříve třeba sestavit zprávu dotazu. Její tvar je definován PVS. Jejím hlavním obsahem je identifikační číslo podání, na které je dotazováno. Tato zpráva je odeslána na Portál veřejné správy.

Zpět je obdržena odpověď, která obsahuje část s informacemi o stavu podání ve tvaru XML. Odpověď je zpracována a zaznamenána do systému. Podle výsledku bude vybrán následující krok. Postup komunikace je popsán výše v kapitole analýzy.

5.1.2.2 Cyklus tázání

V analýze bylo zjištěno, že kontrolu stavu bude třeba s největší pravděpodobností provádět vícekrát, protože vyřízení podání aplikací Elektronická podání nebude okamžité. Proto tuto kontrolu budeme provádět v cyklu do doby, kdy nebude podání vyřízeno nebo do určitého počtu kontrol. Pro případ, kdy bude dotazování ukončeno a nebude zjištěno, že podání je uzavřeno, je třeba v cyklu dotazování navázat a pokračovat dále.

5.1.3 Dotaz na stav podání na ČDS

Dotaz na stav podání na České daňové správě bude probíhat téměř shodně jako odeslání podání s daty DPH. Jedná se o nové podání, které využívá stejného mechanizmu jako vlastní odeslání přiznání. Pouze obsah datové části a příznak v obálce ČDS jsou pozměněny podle údajů získaných v analýze.

5.2 Implementační rozvržení modulu

Výše popsaným rozdělením do dvou částí byly popsány jednotlivé kroky odeslání a kontroly stavu podání, vlastní implementace se však bude lišit. Je třeba vzít v úvahu v zadání kladený důraz na rozšiřitelnost a obecnou použitelnost, proto bude modul koncipován do **části komunikace s aplikací Elektronická podání PVS** a **části získání a sestavení vlastních dat podání.**

Část získání a sestavení vlastních dat podání nejprve získá data ze systému. Poté je sestaví do tvaru vyžadovaného úřadem. Sestavená data budou uložena v jedné tabulce společně s dalšími daty zadanými při jejich vytváření. Zde budou také sestaveny metody pro volání úkonů z části komunikace s aplikací Elektronická podání PVS.

Operace spojené s odesíláním a kontrolou stavu podání budou implementovány v částí odeslání komunikace s aplikací Elektronická podání. Data s touto komunikací spojená budou ukládána do dalších samostatných tabulek.

5.3 Uložení dat

Datový model se skládá ze dvou částí. Toto je zapříčiněno vlastností IS WinFAS, který používá dvě databáze. Tzv. fifor, což je firemní část, tuto databázi má každá firma vlastní a tzv. sysor, systémová databáze, která je pro všechny firemní databáze na jenom PC nebo serveru společná.

5.3.1 Entity databáze

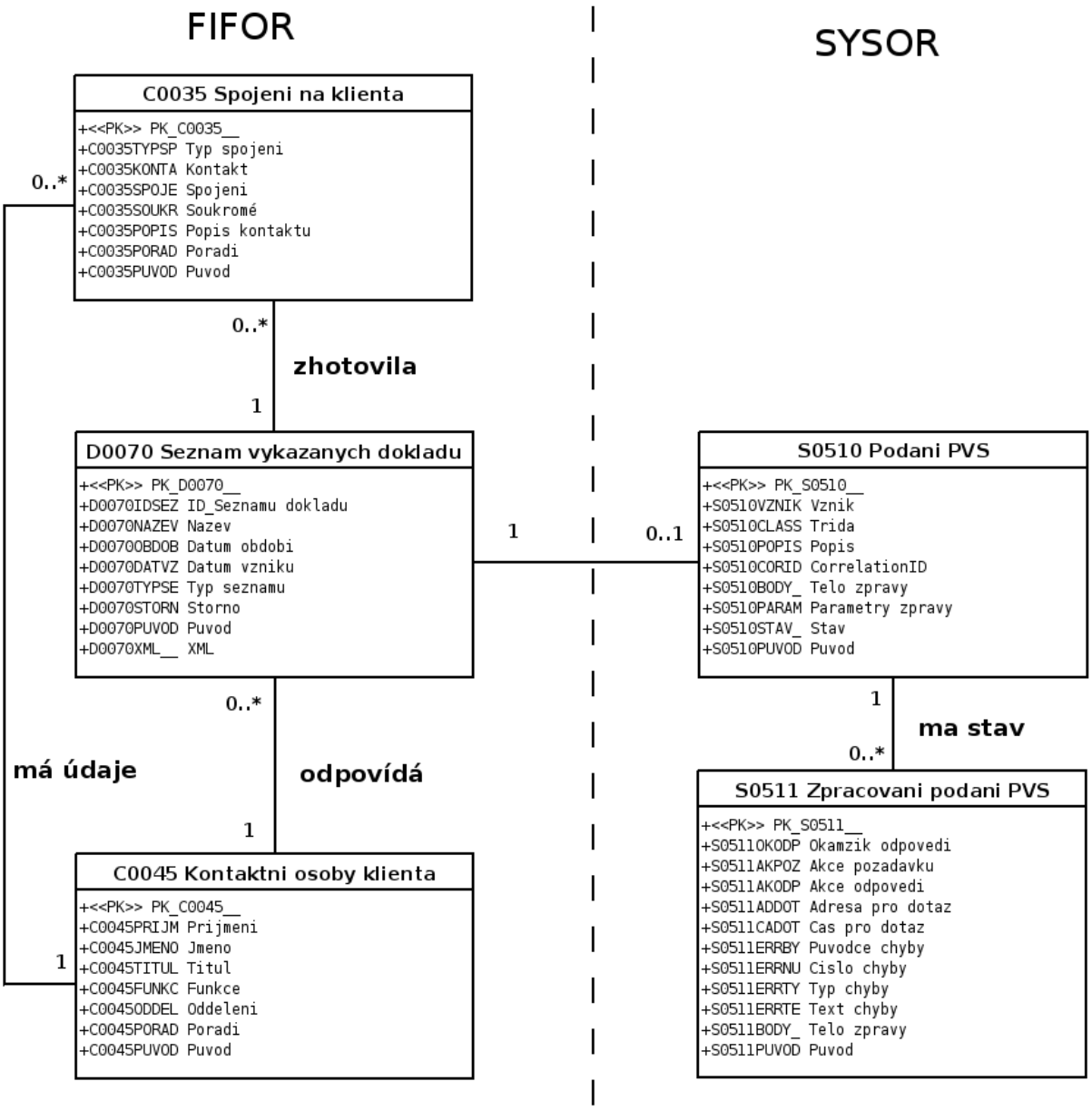
Data budou uložena v relační databázi podle níže uvedeného schématu. Data budou rozložena do 5 entit. Tabulky C0045 Kontaktní osoby klienta a C0035Spojení na klienta jsou již v systému zařazeny a ukládají se v nich pro nás potřebná data osob. Tabulky D0070 Seznam vydaných dokladů, S0510 Podání PVS a S0511 Zpracování PVS jsou určeny pro uložení dat podání, jeho průběhu a stavu. Vztahy mezi těmito entitami jsou znázorněny ER diagramem na obrázku 5.2.

5.3.1.1 D0070 Seznam vydaných dokladů

Tato entita slouží pro uložení dat vytvořených podání, určených na Českou daňovou správu, v části databáze fifor. Obsahuje základní údaje podání jako jeho ID seznamu dokladů, Název, Období, Datum vzniku a Typ seznamu, který označuje o jaký typ podání na Českou daňovou správu se jedná.

5.3.1.2 C0045 Kontaktní osoby klienta

Tato tabulka slouží pro uložení údajů osob v systému. Jsou to Příjmení, Jméno, Titul, Funkce, Oddělení a Pořadí. V našem případě jsou v ní uloženy údaje osoby, která odpovídá za zhotovené podání a údaje osoby, která podání zhotovila.



Obrázek 5.2 Rozvržení dat v databázi

5.3.1.3 C0035 Spojení na klienta

Tabulka slouží pro uložení kontaktních údajů osob v systému. Jedná se o údaje Typ spojení, Kontakt, Spojení, Popis kontaktu, Pořadí.

5.3.1.4 S0510 Podání PVS

Zde jsou zaznamenány odesílané a přijímané údaje podání. Třída udává pro jaký úřad veřejné správy je podání určeno. CorrelationID je identifikátor podání obdržený PVS. Stav udává, v které části cyklu odesílání se podání nachází. A další údaje jako Vznik, Popis, Tělo zprávy a Parametry zprávy.

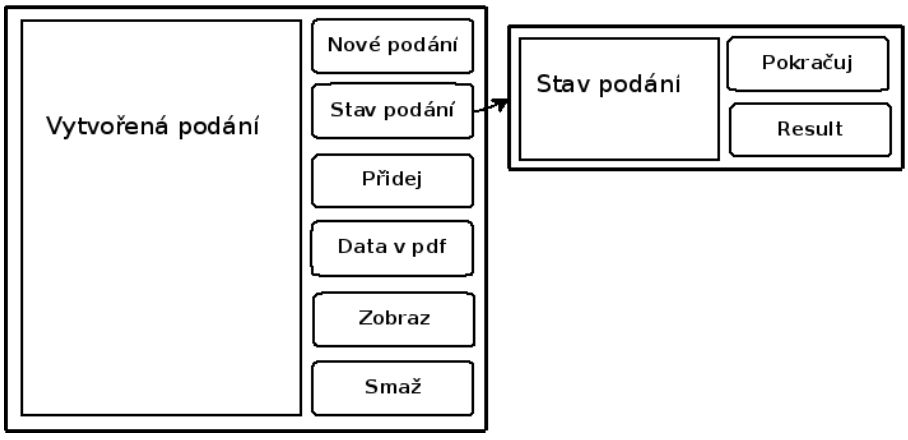
5.3.1.5 S0511 Zpracovaní podání PVS

Slouží pro zaznamenání dat odesílaných a přijímaných zpráv komunikačního cyklu. Konkrétně se jedná o Okamžik odpovědi, Akce požadavku, Akce odpovědi, Adresa pro dotaz, Čas pro dotaz, Původce chyby, Číslo chyby, Typ chyby, Text chyby, Tělo chyby, pokud nějaká nastala.

5.4 Uživatelské rozhraní

Uživatelské rozhraní je navrženo podle modelu případu užití uvedeném na obrázku 2.1 a bude rozvrženo do několika oken. Prvotní okno bude zobrazovat vytvořená podání a jejich základní data. Návrh základního rozhraní je na obrázku 5.3. V tomto okně se budou také nacházet tlačítka pro provedení akcí:

- **Přidej -** sloužící pro vytvoření nového podání na Českou daňovou správu. Po jeho stisku se otevře okno pořízení, kde se zadají a nastaví data vytvářeného podání.
- **Smaž -** vymazání označeného podání.
- **Zobraz -** zobrazí okno s daty zadanými a nastavenými při vytváření označeného podání.
- **Data v pdf -** tlačítko bude sloužit pro zpětné zobrazení dat vytvořených podání. Po jeho stisku se tyto data otevřou v příslušném formuláři formátu pdf. Pokud se bude jednat o větu podání přiznání DPH, tak v tiskopise pro papírové podání přiznání z DHP. Tyto tiskopisy však budou mít vyplněny jen ty údaje, které se odesílají elektronickou cestou na ČDS.
- **Nové podání -** tlačítkem se odešle nové ještě neodeslané podání, po jeho stisku začnou probíhat jednotlivé kroky odeslání a úkony s ním spojené (vyplnění údajů odeslání a další).
- **Stav podání** - stiskem tlačítka se zobrazí okno s údajem o stavu, v jakém se odeslané podání nachází v cyklu podání. Zde jsou další tlačítka.
  - **Pokračuj** – jeho stiskem se naváže odesílání podání v místě, kde bylo skončeno. Pokud je odeslání ukončeno toto tlačítko bude zašeděno (nefunkční).
  - **Result** – tímto tlačítkem se zobrazí okno s podrobným popisem stavu podání.



Obrázek 5.3 návrh základního rozhraní

6 Implementace

6.1 Použité vývojové prostředky

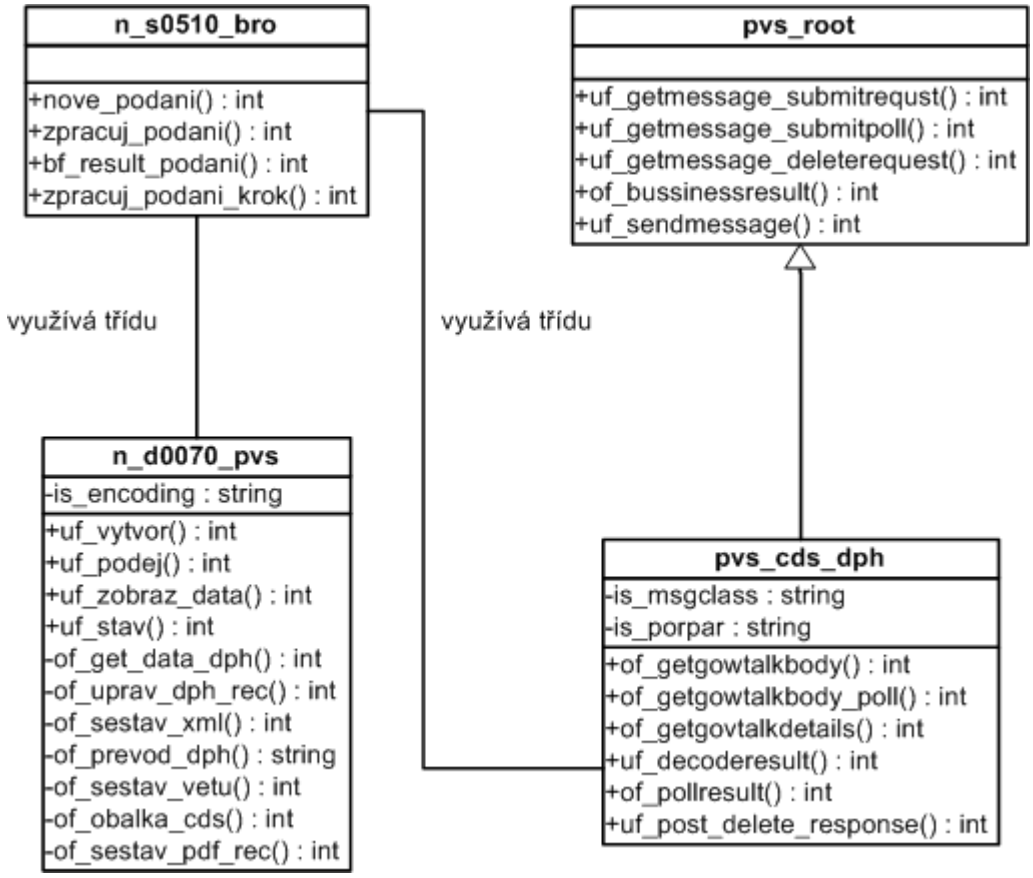
Pro implementaci jsou použity nástroje firmy Sybase. Databáze je implementována pomocí SQL Anywhere, jejíž výhodou je, že pracuje na jednom počítači, malé síti, ale i víceprocesorových serverech rozsáhlých podnikových sítí. Klienská část systému je naprogramována v prostředí PowerBuilder. Programovaní v PowerBuilderu je realizováno objektově orientovaným jazykem syntakticky podobným Basicu. Vlastní kód je zde psán nad aplikačním jádrem, které je dvojúrovňové, „malé“ a „velké ufo“. Obsahem „malého ufa“ jsou základní funkce tzv. lowlevel. Například funkce pro práci s databází, základními datovými typy a další. „Velké ufo“ předefinovává základní programové celky, z nichž se dědí okna pořízení a další často využívané programové prvky. Základní část tohoto dvojúrovňového jádra byla vyvinuta společností Unicorn, a.s. Zbývající část byla dopsána Organizační kanceláří s.r.o.

6.2 Implementace tříd

Implementace je podle návrhu rozdělena do dvou podřízených knihoven tzv. ***„bro“*** knihoven a jedné ***„aplikační“*** knihovny. První knihovna ***`bd0070`*** obsahuje metody pro práci s daty a volání potřebných mechanizmů z hlediska konkrétního úřadu, pro který je podání určeno. Druhá knihovna ***`bs0510`*** implementuje komunikaci s aplikací Elektronická podání portálu veřejné správy. Dále je zde popsána implementace šifrování a podepisování odesílaných zpráv.

6.2.1 Knihovna aplikační d1098

V této knihovně ***`d1098`*** jsou zaznamenána základní nastavení aplikace. Obsahuje hlavní aplikační okno zobrazené po spuštění aplikace. Jsou v ní definována tlačítka tohoto okna a jejich události vykonávající se po jejich stlačení.



Obrázek 6.1 Diagram tříd se zobrazením důležitých atributů a metod

6.2.2 Knihovna bs0510

V této *„bro“* knihovně je obsažena třída ***`n_s0510_bro`***, ve které jsou implementovány metody, pomocí nichž se komunikuje s aplikací Elektronická podání PVS a ukládají data do tabulek patřících do systémové části databáze ***`S0510` Podání PVS*** a ***`S0511` Zpracování podání PVS***.

Pro založení nového podání slouží metoda *„`nove_podani`“*, která vkládá nový záznam do tabulky `s0510`.

Hlavní třídy, jejich metody a atributy jsou zobrazeny na obrázku 6.1. Medota *„`zpracuj_podani`“* rozhoduje podle aktuálního stavu podání o volání metody *„`zpracuj_podani_krok`“* a do dialogového okna vypisuje informace právě provedených akcí. Metoda *„`zpracuj_podani_krok`“* obsahuje rozhodovací mechanizmus sestavování, odesílání zpráv a zpracovávání odpovědí na ně. Mechanizmus je zhotoven na základě analýzy komunikačního protokolu používaného aplikací Elektronického podání.

V tomto mechanizmu jsou volány další metody, které jsou z důvodu použitelnosti komunikační části i pro podání na jiné úřady veřejné správy obsahem jiné třídy. V tomto případě odeslání přiznání DPH na portál ČDS je to třída *„`pvs_cdsdph`“* zděděná z *„`pvs_root`“*. V *„`pvs_root`“* jsou definovány všechny externí funkce využívané komunikačním mechanizmem. Ve zděděné třídě jsou

pak upraveny pro podání na konkrétní úřad. Jsou to metody pro sestavení zpráv „*uf_getmessage_submitrequst*“, „*uf_getmessage_submitpoll*“, „*uf_getmessage_deleterequest*“. Pro získání obsahu *Body* volá „*uf_getmessage_submitrequst*“ metodu „*of_getgowtalkbody*“. Pro „*uf_getmessage_submitpoll*“ sestavuje element Body „*of_getgowtalkbody_poll*“. Metoda „*of_getgowtalkdetails*“ vyplní příslušné identifikační údaje elementu obálky *GowTalkDetails*. Metoda „*uf_decoderesult*“ získává základní údaje z odpovědí od aplikace Elektronická podání. Pokud je zjištěno doručení chybové zprávy business je volána metoda „*of_bussinessresult*“, která z ní generuje chybová hlášení. Pro dekódování zprávy se stavem podání na ČDS slouží metoda „*of_pollresult*“. Rozhodování o následujícím stavu podle stavu předchozího a nových informací získaných z příchozí zprávy má na starosti „*uf_post_delete_response*“. Odeslání sestavené zprávy je realizováno „*uf_sendmessage*“. Dále se zde nacházejí ještě další funkce pro ukládání a znovunaplnění identifikačních údajů a parametrů odeslání.

Po ukončení cyklu komunikace je pro výpis podrobného stavu podání použita metoda „*bf_result_podani*“.

Nachází se zde objekt okna „*w_s0510_stav*“, který definuje okno, ve kterém je zobrazen stav podání, jeho tlačítka a eventy vyvolávané jejich stisknutím. Konkrétně se jedná o tlačítko zobrazení podrobného stavu podání a tlačítko pro pokračování v cyklu odesílání, pokud ještě nebyl dokončen.

6.2.3 Knihovna bd0070

V této „*bro*“ knihovně je obsažena třída ***n_d0070_pvs***, která obsahuje metody pro získání dat přiznání daně z přidané hodnoty, jejich úpravu a převedení do příslušného XML tvaru určeného k odeslání na ČDS prostřednictvím PVS.

Dále je v ní obsažena třída ***n_d0070_por***, v níž je nastaveno parametrické okno sloužící pro pořízení věty podání do tabulky ***D0070 Seznam vykázaných dokladů***.

Třída ***n_d0070_pvs*** obsahuje veřejnou metodu „*uf_vytvor*“, která volá další privátní metody. Pro získání dat ze systému slouží metoda „*of_get_data_dph*“, tyto data jsou pro účel podání upravena „*of_uprav_dph_rec*“. Dále už jsou data převedena do XML tvaru definovaným Českou daňovou správou. Převod uskutečňuje metoda „*of_sestav_xml*“ využívající převodní řetězec vytvořený „*of_prevod_dph*“ a „*of_sestav_vetu*“ pro sestavení jedné věty XML.

Další veřejnou metodou je „*uf_podej*“, která získá příslušné vytvořené datové XML z databáze. Využije „*of_obalka_cds*“ pro jeho zabalení do obálky ČDS a zavolá z knihovny ***bs0510*** třídy ***n_s510_bro*** mechanizmus odeslání na PVS.

Veřejná metoda „*uf_zobraz_data*“ je volána pro zobrazení dat podání uložených v databázi ve tvaru XML. Využívá další metodu „*of_sestav_pdf_rec*“ pro převod XML dat do formátu používaného v PDF.

Zobrazení stavového okna z knihovny ***bs0510*** třídy ***n_s510_bro*** volá veřejná metoda „*uf_stav*“.

6.2.4 SQL dotazy

Při operaci s daty tabulek byly využity SQL dotazy. Jsou to dotazy pro načítání všech dat tabulek, zobrazení výběru dat osob oprávněných za odeslání přiznání DPH a zobrazení dat pro výběr osoby, která toto přiznání sestavila. Dotazy pro načítání datových vět z tabulky ***D0070*** do okna aplikace.

6.2.5 Implementace šifrovacích a podepisovacích funkcí

Implementace byla provedena do knihovny **uforoot** třídy **n_crypto**, z důvodu nefunkčnosti původních šifrovacích a podepisovacích funkcí v případě odeslání na Českou daňovou správu. Šifrovací a podepisovací třída **n_crypto** volá funkce prostřednictvím dll souboru systémové knihovny CRYPTOAPI, které provádějí samotné šifrování a podepisování dat.

6.3 Problémy při implementaci

Při implementaci jsem narazil na problém přenášení českých znaků v datové zprávě. Po jeho důkladné analýze jsem zjistil příčinu tohoto jevu. České znaky se staly nečitelnými vždy po zašifrování zprávy.

Při návrhu bylo uvažováno šifrování a podepisování odesílaných dat pomocí třídy, která je používána pro šifrování a odesílání dat na Českou správu sociálního zabezpečení. Tato třída pro šifrování používá knihovnu CAPICOM. Což je knihovna vyvinutá firmou Microsoft.

Problém nevyřešily změny šifrovacího algoritmu, ani různé formáty šifrovaných dat, z čehož vyplynulo, že je chyba zřejmě způsobena samotnou knihovnou CAPICOM. Problém byl konzultován na vývojářské diskuzi PVS https://bezpecne.dev.gov.cz/diskuze/, kde bylo zjištěno, že knihovna CAPICOM opravdu šifruje chybně. Z tohoto důvodu musely být doplněny do třídy n_crypto knihovny uforoot šifrovací a podepisovací funkce prostřednictvím základní šifrovací a podepisovací knihovny CRYPTOAPI, nad kterou je původně používaná knihovna CAPICOM napsána.

PowerBuilder však není schopen pracovat se složitějšími strukturami a ukazateli, které používají funkce z knihovny CRYPTOAPI, a proto je bylo třeba přemapovat prostřednictvím DLL souboru dll_sysutils.c jazyka C.

7 Závěr

Projekt měl za cíl vytvoření modulu pro komunikaci s portálem České daňové správy. Zadavatel kladl velký důraz na rozšiřitelnost a obecnou použitelnost komponentů modulu. Také zadal požadavek o vytvoření jednoho pilotního podání na Českou daňovou správu. Z výše popsaných důvodů bylo vybráno podání přiznání daně z přidané hodnoty.

Práce na modulu byla rozvržena do části získání a specifikace potřebných informací. V ní jsou zanalyzovány požadavky zadavatele na modul a informační systém WinFAS, pro který je určen, specifikovány využívané technologie. Dále je popsáno elektronické podání s úřady, se kterými se bude komunikace uskutečňovat, a rozbor mechanizmu komunikačního protokolu a odesílaných zpráv. Následuje část návrhu a implementace modulu. Zde je popsán cyklus podání od získání vlastních dat ze systému až po ukončení ověřování stavu odeslaného podání. Jsou zde sepsány implementační prostředky a stručný popis implementovaných knihoven, tříd a jejich metod.

V poslední části implementace byl modul úspěšně odladěn a otestován. Prostřednictvím tohoto modulu pro elektronickou komunikaci s Českou daňovou správou bylo úspěšně podáno Organizační kanceláří s.r.o. přiznání daně z přidané hodnoty. V současné době se připravuje poskytnutí tohoto elektronického podání přiznání DPH klientů používajících informační systém WinFAS.

Část modulu pro komunikaci s aplikací Elektronická podání PVS je využívána pro podání České správy sociálního zabezpečení, čímž byla ověřena obecná použitelnost modulu. Lze ho také snadno rozšířit o další podání na Českou daňovou správu. Jednalo by se pouze o doplnění části pořízení podání, kde se sestavují vlastní data. Dále je možno využít jeho komunikační část s Portálem veřejné správy pro jakékoli elektronické zasílání podporované PVS. V brzké době je plánováno využití tohoto mechanizmu pro podání na Intrastat, což je systém sběru dat pro statistiku obchodu se zbožím mezi členskými státy Evropské unie.

V dnešní době jsou moduly pro elektronická podání jednou z důležitých součástí kvalitních informačních systémů. Jejich obliba tkví v jejich jednoduchosti a rychlosti, kterou poskytují při komunikaci jak fyzických tak právnických osob s úřady České republiky.

Pro mne samotného byl tento projekt velice poučný. V praxi jsem se seznámil s mechanizmy a pravidly používanými pro elektronickou komunikaci s úřady České republiky. Zejména prostřednictvím Portálu veřejné správy. Získal jsem nové poznatky o certifikátech a oblasti, ve které se využívají. Prohloubil jsem znalosti systémových knihoven. Naučil jsem se používat šifrovací a podepisovací algoritmy a seznámil jsem se s principy, na kterých jsou založeny.

Literatura

[1] Ministerstvo financí ČR: *Česká daňová správa – elektronická podání* [online]. Poslední změna: 2008-03-15 [cit. 2008-03-20]. Dostupné na URL: <http://adisepo.mfcr.cz/adis/jepo/menu_odborne_ramce.htm?U=info>

[2] Ministerstvo vnitra: *Elektronická podání prostřednictvím PVS* [online]. ©2008 [cit. 2008-03-29]. Dostupné na URL: <http://portal.gov.cz/wps/portal/_s.155/6966/_s.155/710/place>

[3] Holaň, Jiří: *Definice obálky GovTalk v3.0* [online]. Poslední změna: 2006-09-13 [cit. 2008-03-18]. Dostupné na URL: <https://bezpecne.dev.gov.cz/diskuze/files/9/transakcni_cast_pvs/entry487.aspx>

[4] Holaň, Jiří: *Podávací a dotazovací protokol v 1.6* [online]. Poslední změna: 2005-09-02 [cit. 2008-03-18]. Dostupné na URL: <https://bezpecne.dev.gov.cz/diskuze/files/9/transakcni_cast_pvs/entry294.aspx>

[5] Hernady, Robert: *Provozní řád testovací větve transakční části PVS v 1.1* [online]. Poslední změna: 2005-09-23 [cit. 2008-03-18]. Dostupné na URL: <https://bezpecne.dev.gov.cz/diskuze/files/9/transakcni_cast_pvs/category1004.aspx>

[6] Hernady, Robert: *Dokumentace pro vývojáře pro službu daňové správy v 1.3* [online]. Poslední změna: 2005-04-11 [cit. 2008-03-20]. Dostupné na URL: <https://bezpecne.dev.gov.cz/diskuze/files/9/danova_sprava/entry283.aspx>

[7] Ministerstvo financí ČR: *Kompetence a činnosti daňové správy* [online]. ©2006 [cit. 2008-03-29]. Dokument dostupný na URL: <http://cds.mfcr.cz/cps/rde/xchg/SID-3EA9846B-22DEE6AE/cds/xsl/22.html?year=0>

[8] Matoušek, P.: *přednáška 9. Bezpečnost počítačových sítí* [online]. Poslední změna: 2007-11-20 [cit. 2008-04-10]. Dostupné na URL: <https://video1.fit.vutbr.cz/>

[9] Přibyl,T: *Svět elektronického podpisu*, PC WORLD (příloha), 8/2000 [cit. 2008-04-10]

[10] Bradley, N.: *XML kompletní průvodce.*Vydání první. Grada Publishing, Praha, 2000. s. 540. ISBN 80-7169-949-7

Seznam příloh

Příloha 1. Manuál pro odeslání DPH z WinFASu

Příloha 2. CD se zdrojovými texty, instalací informačního systému WinFAS obsahující aplikaci s modulem komunikace s ČDS

Příloha 1

Manuál pro odeslání DPH z WinFASu

Následující text popisuje odeslání daně z přidané hodnoty (DPH) přes Portál veřejné správy (PVS) České daňové správě (ČDS).

I. Podmínky pro odeslání DPH

1) Na počítači, ze kterého se bude elektronicky odesílat DPH, musí být přístup k internetu.

2) Na počítači musí být nainstalován podpisový klíč pověřeného pracovníka vydaný akreditovaným poskytovatelem certifikačních služeb (přehled udělených akreditací je k dispozici na stránkách Ministerstva vnitra).
Poznámka: klíč lze mít také vyexportovaný (zálohovaný) v souboru – doporučujeme.

3) Pracovník, který bude odesílat DPH, musí být zaregistrován na Portálu veřejné správy (PVS) ke službě ***„Daňová správa - elektronická podání“*** – tzn. má právo za organizaci odesílat DPH elektronicky. PVS mu přidělil identifikátor a heslo.

4) Ve WinFASu v aplikaci *1098 – Podání na ČDS musí být pořízená příslušná věta pro podání DPH.

II. Zjednodušený popis průběhu podání DPH na PVS (podrobně v bodě III.)

- Elektronické odeslání (podání) DPH České daňové správě (ČDS) se provádí přes Portál veřejné správy (PVS). PVS je tedy prostředník, který DPH dále předává ČDS. Podání provádí pracovník pověřený organizací k elektronickému odesílání DPH (dále uživatel).
- Uživatel ve WinFASu vybere v aplikaci *1098 – Podání ČDS DPH k odeslání. WinFAS je vloží do zprávy.
- Uživatel ve WinFASu zadá identifikátor, heslo PVS a email pro zasílání informací o zpracování podání z ČDS.
- Pokud není nainstalován důvěryhodný kořenový certifikát certifikačního úřadu ČDS, WinFAS jej nainstaluje (není myšlen podpisový klíč). Pokud již důvěryhodný kořenový certifikát ČDS je, tento bod se přeskočí.
- Dále uživatel vybere svůj podpisový klíč vydaný akreditovaným poskytovatelem certifikačních služeb, čímž zprávu s DPH podepíše.
- WinFAS zašifruje podepsané DPH a odešle pomocí internetu na PVS.
- PVS ověří, zda souhlasí identifikátor PVS a heslo PVS (zda zprávu z WinFASu posílá uživatel zaregistrovaný na PVS ke službě ***„Daňová správa - elektronická podání“***) a zda je zpráva ve

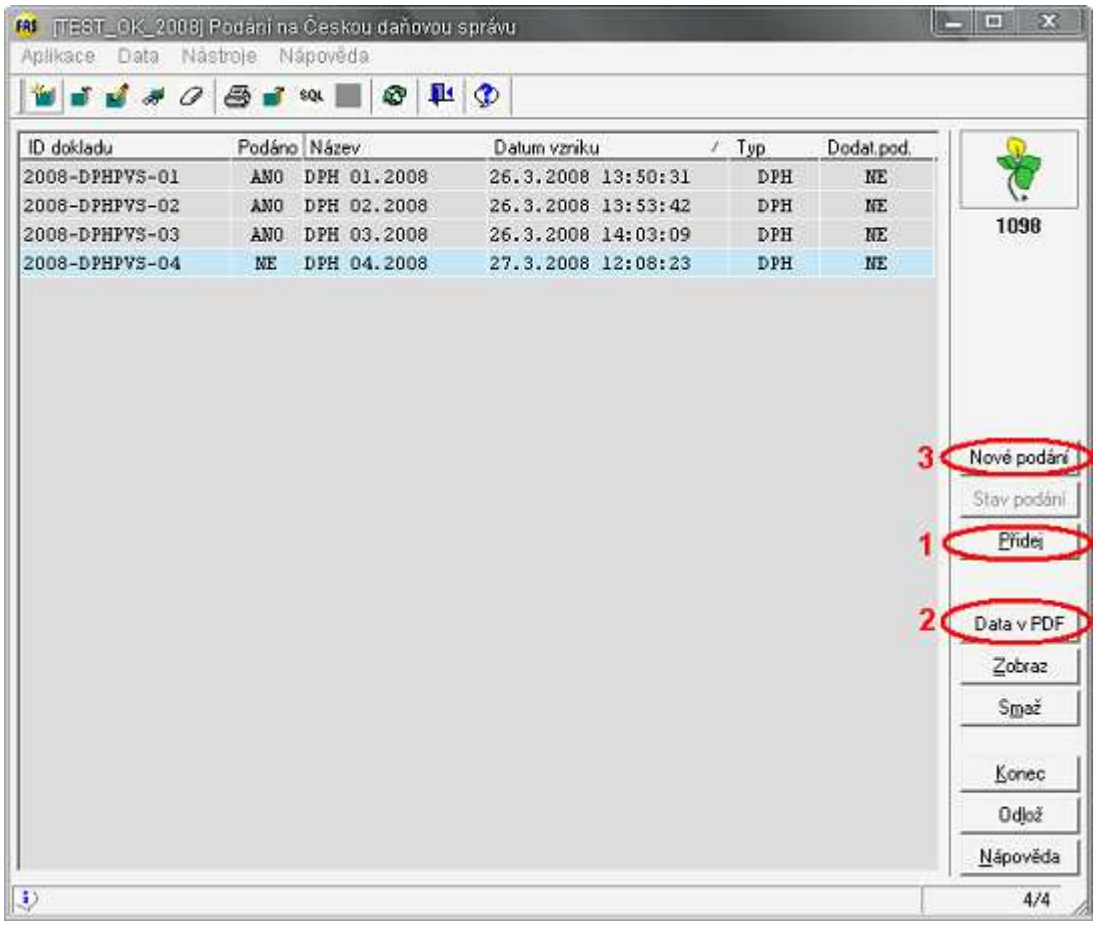
správném formátu. Poté předá DPH uvnitř zprávy na ČDS. Pokud tento krok proběhl v pořádku, dostane se podání do stavu „***zpracovává se***“.

- Další operace s daty DPH provádí ČDS. Zkontroluje elektronický podpis a správnost vyplnění DPH.
- Výsledky zpracování jsou uživateli sděleny po zaslání ***dotazu na stav,*** nebo emailem, který vyplnil ve stejném okně jako údaje pro přihlášení na PVS**.**
- Pokud byla v DPH zjištěna chyba, je třeba ve WinFASu opravit data pro výpočet DPH a znovu vytvořit a odeslat podání.

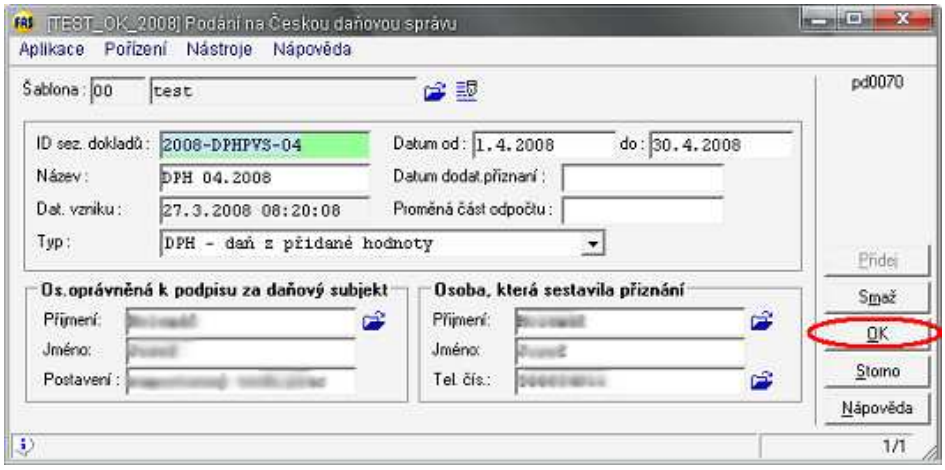
III. Podrobný popis průběhu podání DPH na PVS (zjednodušeně v bodě II.)

1) Spusťte aplikaci *1098 Podání ČDS.
Ve stromečku najděte ***Účetní knihy,*** poté DPH a v něm Podání ČDS. Nebo napište *1098 do údaje **Kód** a klepněte na tlačítko **Spusť**.

2) V aplikaci *1098 jsou zobrazeny věty podání DPH.



3) Pro vytvoření nového podání slouží tlačítko ***Přidej*** (1). Po jeho stisku se otevře okno, v kterém je třeba doplnit údaje.



4) Vyplníme údaje. Do dat je třeba zadat období. Pokud se jedná o dodatečné přiznání, vyplňuje se ***„Datum dodat. přiznání“***. V rozbalovací nabídce ***„Typ“*** vybereme DPH. Poté stisk ***OK***. Tím se vyvolá mechanizmus, který vypočítá data DPH přiznání. Jako zdrojová data jsou použita data pořízená ve WinFASu. V okně vznikla nová věta podání. Data přiznání DPH je možno zobrazit vPDF pomocí tlačítka ***Data v PDF*** (2).

5) Příslušnou větu označíme a pro odeslání použijeme tlačítko ***Nové podání*** (3).

6) V tento okamžik WinFAS založí nové podání, které se odesílá na PVS. Vybrané DPH bude označené jako „Podané PVS“ a již se nebudou nabízet k novému podání. Pokud byste kdykoli od následujícího bodu **7)** toto podání ukončili, nebo se podání nezdařilo, je možné toto podání odeslat znovu. Již se nebude odesílat přes tlačítko ***Nové podání***, ale bude se pokračovat od stavu, kde bylo podání ukončeno (viz. dále).

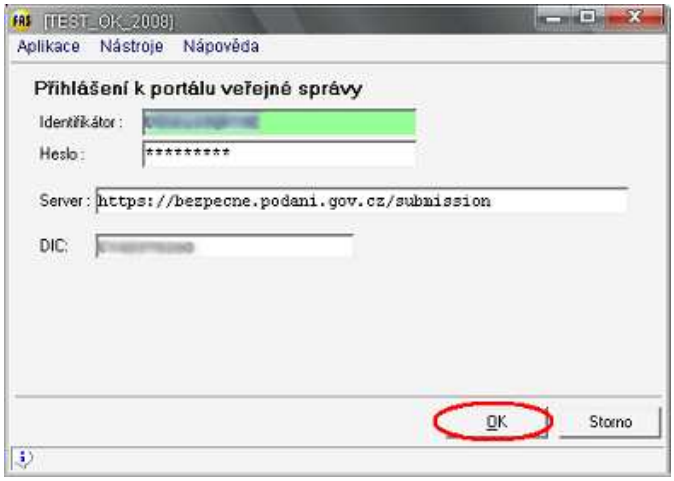
7) Následuje vyplnění okna, kde se zadávají údaje potřebné pro přihlášení k Portálu veřejné správy (PVS). Údaje identifikátor a heslo Vám byly přiděleny při registraci na PVS (viz. část I. Co musí být splněno – bod **3)**). Při zadávání hesla počítač nahrazuje znaky hvězdičkami (ochrana před zneužitím).

POZOR – rozlišují se velká a malá písmena.

Zkontrolujte adresu serveru https://bezpecne.podani.gov.cz/submission a zadejte DIC organizace včetně ***cz***.

Do kolonky ***„email:“*** zadejte emailovou adresu, na kterou chcete dostávat informační emaily o stavu podání z ČDS.

Při příštím přihlašování si WinFAS již bude tyto údaje pamatovat *(mimo hesla).*

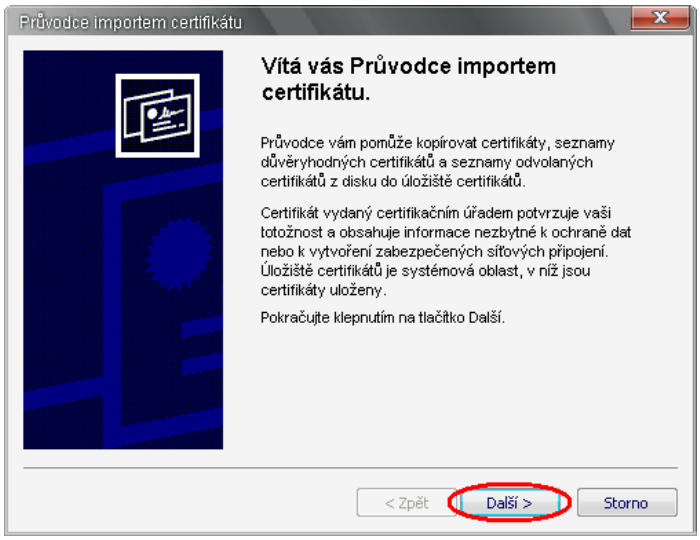


Stiskněte ***OK***.

8) Instalace důvěryhodného **kořenového** nebo **podřízeného** certifikátu certifikačního úřadu ČDS . Ve většině případů jsou již nainstalovány – potom přejděte k bodu **9)**. Pokud tento důvěryhodný **kořenový** nebo **podřízený** certifikát ČDS není nainstalován, WinFAS sám nabídne instalaci (pokud není nainstalován ani jeden z těchto certifikátu tento postup proběhne dvakrát po sobě) :

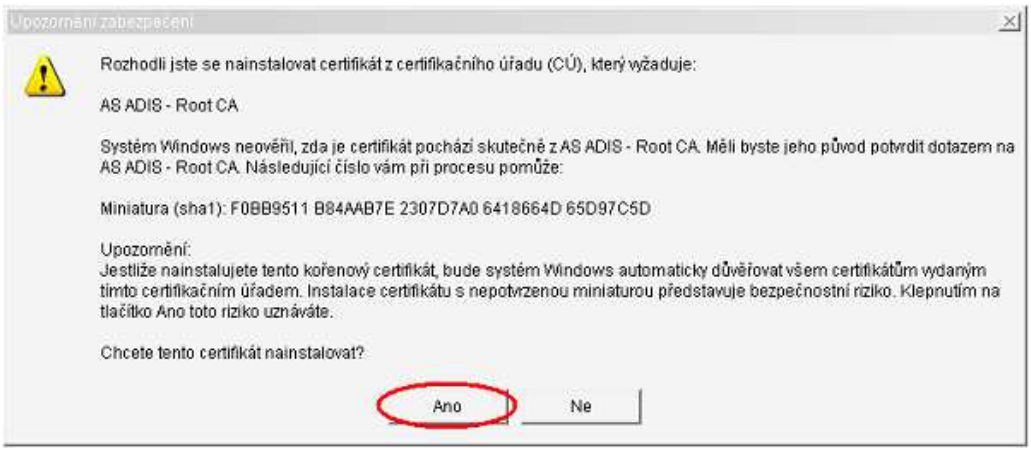
Klepněte na tlačítko ***Ano***.

Tím se otevře Průvodce importem certifikátu.

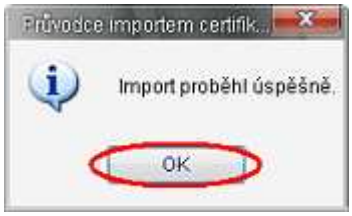


Nic nezadávejte, pouze klepejte na tlačítko ***Další*** a nakonec tlačítko ***Dokončit.***

Při instalaci kořenového certifikátu se po ukončení průvodce otevře okno „Upozornění zabezpečení“.

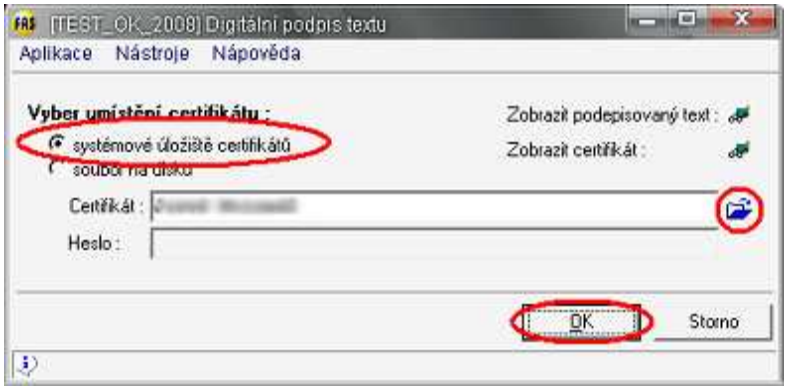


Potvrďte klepnutím na ***Ano.***



Následující okno ***Ok***.

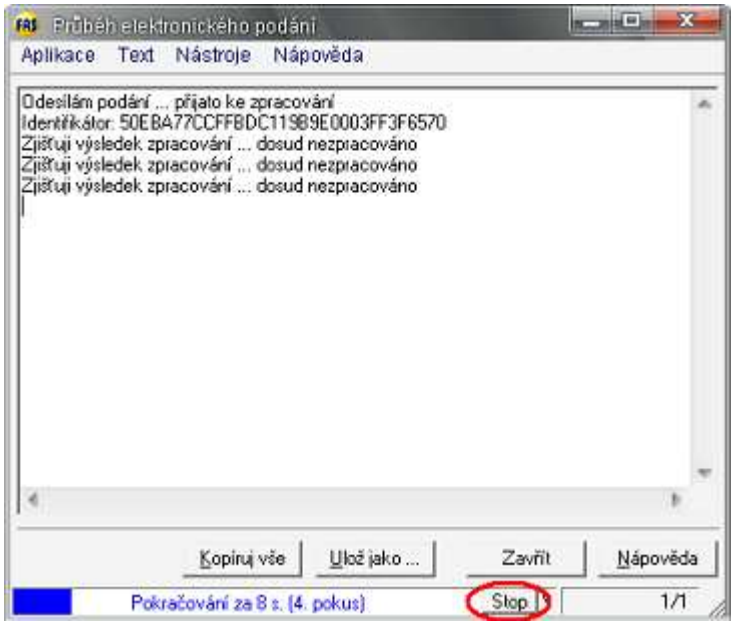
9) Digitální podpis zprávy. Vyberte systémové úložiště certifikátů. Klepnutím na modrou ikonu složky vpravo, toto úložiště otevřete a z něj vyberte certifikát (Váš podpisový klíč vydaný akreditovaným poskytovatelem certifikačních služeb).



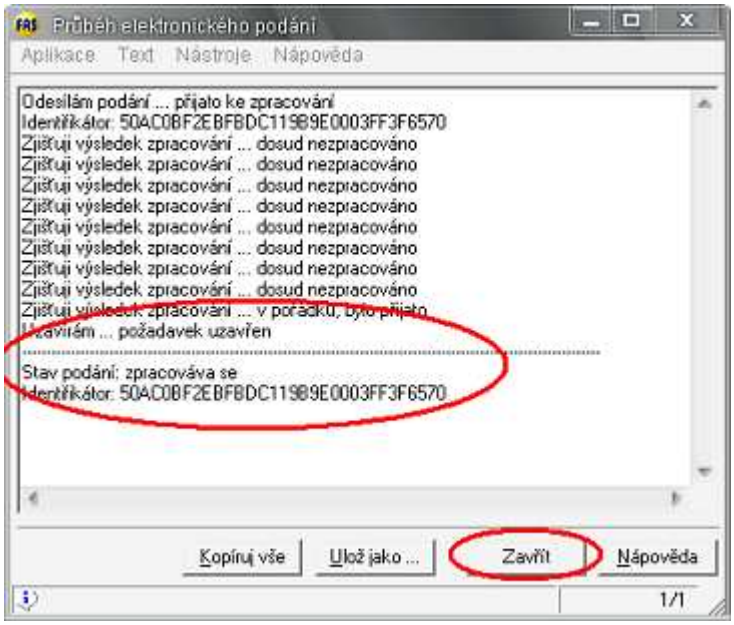
Stiskněte tlačítko ***OK***, čímž se zpráva podepíše.

10) WinFAS zprávu v podání zašifruje a odešle na Portál veřejné správy (PVS). Komunikace mezi WinFASem a PVS se zobrazuje v okně „Průběh elektronického podání“.

- PVS ověří, zda zprávu z WinFASu posílá uživatel zaregistrovaný na PVS ke službě ***„Daňová správa - elektronická podání“***.
- Pokud ano, PVS přidělí podání identifikátor a předá podepsané DPH uvnitř zprávy ČDS ke zpracování.
- Než ČDS DPH přijme ke zpracování, WinFAS se v určitých časových intervalech dotazuje PVS. V okně je zobrazen samostatným řádkem každý dotaz a jeho výsledek. Časový interval, za jak dlouho dojde k dalšímu dotazu, je zobrazován ve spodní části okna.
- WinFAS se dotazuje tak dlouho, dokud není podání Českou daňovou správou přijato (viz. dále). Za normálních okolností trvá přijetí ČDS do jedné minuty (maximálně několik minut).
- Pokud z nějakého důvodu na výsledek nemůžete déle čekat (zahlcení portálu apod.), můžete dotazování ukončit tlačítkem ***Stop*** ve spodní části okna a okno zavřít. PVS zatím stále podání vyřizuje, zastaví se pouze dotazování WinFASu. Dotazování potom můžete obnovit později, např. následující den (viz. dále).



– Konečným výsledkem dotazování je informace, že byl požadavek uzavřen. Podání je buď přijato ke zpracování (zpracovává se), nebo odmítnuto (v podání je chyba). V případě skončení chybou je vypsán její popis.



Okno zavřeme klepnutím na tlačítko ***Zavřít***.

11) Emailem přijdou zprávy o výsledku podání.

- na email zadaný při registraci na PVS:
  - PVS informuje o úspěšnosti předání DPH na ČDS.
- na email zadaný do aplikace při odesílání:
  - ČDS informuje o zpracování DPH
  - přijetí, případně popis chyb v DPH
  - ČDS informuje emailem po ukončení zpracování

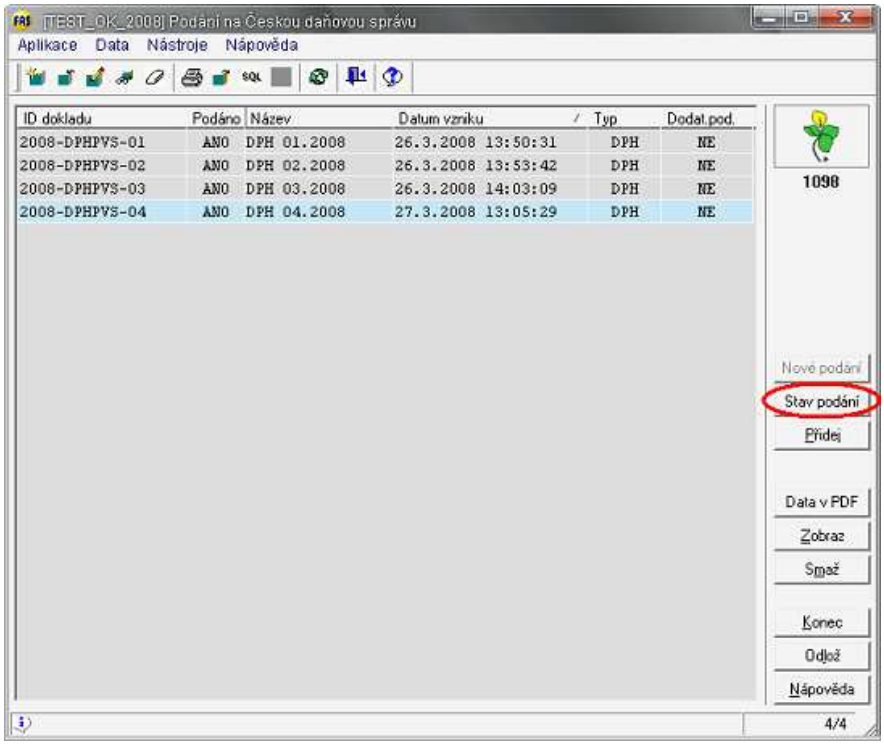
12) Pokud bylo podání zamítnuto kvůli chybnému přihlášení na PVS (chybný identifikátor PVS, chybné heslo PVS), opakujte podání se správnými přihlašovacími údaji (opakované podání viz. dále). V případě opakovaného neúspěchu kontaktujte ČDS kvůli prověření správného zaregistrování na PVS a správnosti přihlašovacích údajů. Stejně tak postupujte v případě chybného elektronického podpisu – chybný podpisový klíč ČDS.

13) Pokud bylo podání zamítnuto kvůli chybě v DPH, musíte opravit příslušná data ve WinFASu a provést celý cyklus podání znovu od začátku (od vytvoření).

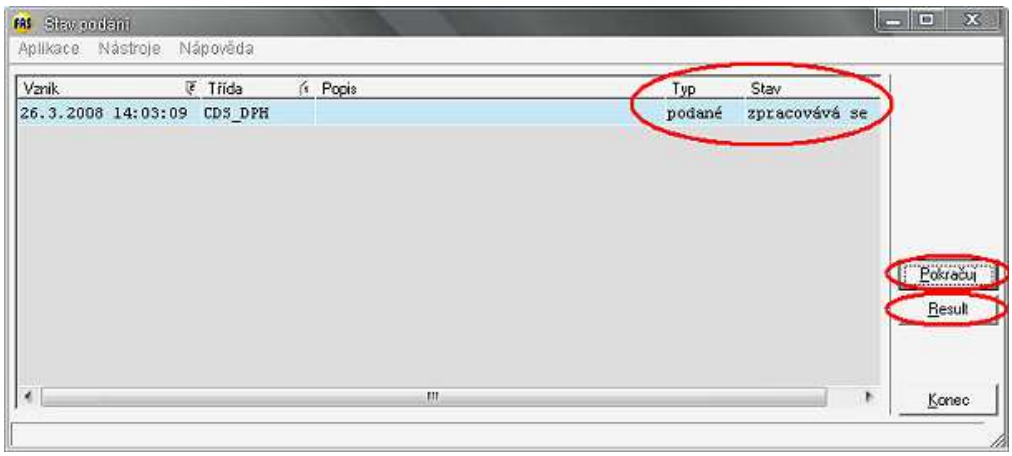
IV. Zjišťování stavu podání, opakované podání

O stavu podání na ČDS je informována osoba, která toto podání odeslala, emaily (pokud byl zadán). Pokud bylo ověřování stavu zastaveno ještě před přijmutím přiznání ČDS (uživatelem, chybou odeslání, chybným přihlášením na PVS...), je třeba obnovit zpracování a odesílání bude pokračovat, kde skončilo (viz. dále). Po úspěšném odeslání a přijetí podání ČDS je možnost kontrolovat stav podání na ČDS (viz. dále).

Zjištění stavu podání



1) Označíme příslušné podání a klepneme na tlačítko ***Stav podání*** *(tato volba je dostupná pouze u podání, která již byla odeslána na PVS).*



V tomto okně se nachází informace o stavu podání.

Sloupec Typ nabývá hodnot:

- **Podání** - následující sloupec Stav označuje v jaké fázi se nachází podání DPH
- **Podané** - následující sloupec Stav označuje v jaké fázi se nachází dotaz na stav vyřizování podání DPH na ČDS (viz. dále)

V následujícím sloupci Stav je zobrazen údaj o stavu vlastního podání DPH nebo dotazu na aktuální stav podání na ČDS a nabývá hodnot:

- **Neposlané** – podání/dotaz bylo pouze vytvořeno, ale nepředáno na PVS. Např. v případě, kdy se na PVS nepodařilo přihlásit (chybný identifikátor uživatele, chybné heslo, …).
  -> podání/dotaz bude opětovně odesláno na PVS
- **Poslané** - podání/dotaz bylo předáno na PVS a čeká na přijetí ČDS.
  -> dotazování, zda podání/dotaz bylo zpracováno
- **Zpracované** - podání/dotaz je PVS zpracováno a předáno na ČDS (buď přijala, nebo odmítla).
  -> uzavření podání/dotazu
- **Zpracovává se -** podání DPH bylo přijato ČDS, které dále přiznání DPH kontroluje a zpracovává. PVS podání vyřadil ze zpracování. Dále se pokračuje pouze odesíláním dotazů na stav podání na ČDS (není podmínkou).
  -> odeslaní dotazu
- **Uzavřené–chyba** – odeslání podání na ČDS bylo ukončeno chybou. PVS podání vyřadil ze zpracování, dále se nepokračuje. Je třeba podle chybového hlášení identifikovat příčinu chybného ukončení, odstranit ji a zaslat nové podání.
- **Uzavřené–ok** – do tohoto stavu se podání dostane pouze po odeslání dotazu na stav na ČDS (viz. dále), který vrátil dokončené zpracování. Je to konečný stav. Zpracovávání podání DPH na ČDS je dokončeno.

2) Pokud podání není přijato ČDS (neposlané, poslané, zpracované), klepněte na tlačítko ***Pokračuj***. Pokud je uzavřeno chybou, je třeba odeslat nové podání s opravenými daty. Podle stavu, ve kterém se podání nachází, bude pokračovat podle popisu v části III. Podrobný popis průběhu podání DPH na PVS viz. výše. Činnosti opakujte, dokud není podání ve stavu **Zpracovává se,** případně **Uzavřené-ok**.

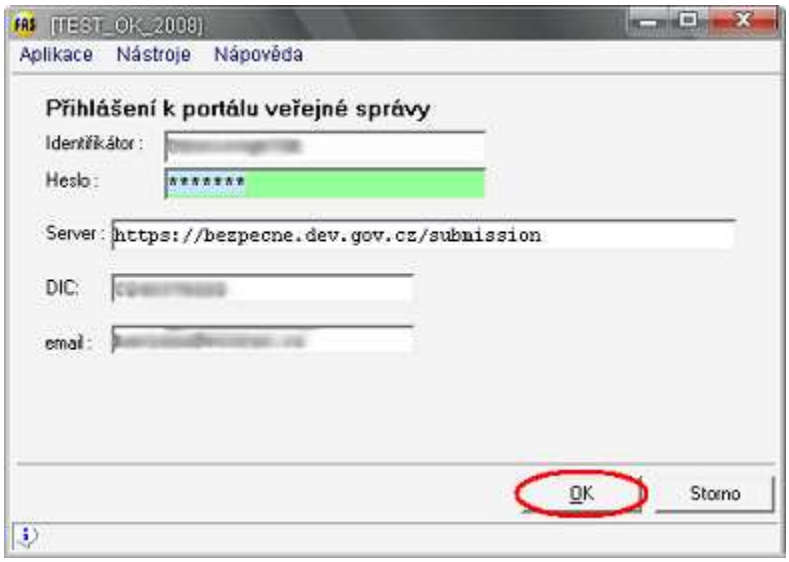
Zjišťování stavu, ve kterém je podání DPH na ČDS.

Tato část odeslání není nutná, slouží pouze pro informování o stavu podání. Tyto informace také přichází na email, který jste zadali při podání.
Pouze pokud bylo podání DPH úspěšně odesláno a přijato ke zpracování na ČDS, můžeme dále kontrolovat, v jakém stavu se nachází na ČDS. Tato zjištění stavu se provádí následovně.

1) Jako v předchozím případě označíme příslušné podání a klepneme na tlačítko ***Stav podání***.

2) V okně „***Stav podání“*** musí být zobrazeny informace **Typ - podané**, **Stav - zpracovává se**. Nyní stiskneme tlačítko ***Pokračuj***.

3) V této chvíli se již jedná o nové odeslání, které podle údajů přijatých z ČDS získaných při odeslání DPH, sestaví dotaz na stav. Tento dotaz se odesílá stejnou cestou jako vlastní podání DPH, proto je třeba opět zadat identifikační údaje pro PVS.



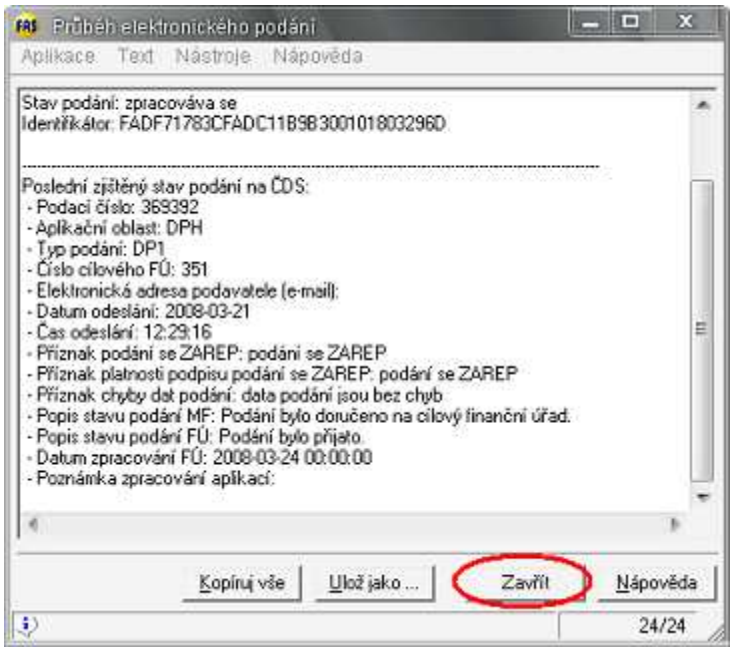
Odešleme tlačítkem ***OK***.

4) WinFAS informace v dotazu na stav zašifruje a odešle na Portál veřejné správy (PVS). Komunikace mezi WinFASem a PVS se zobrazuje v okně Průběh elektronického podání.

- PVS ověří, zda zprávu z WinFASu posílá uživatel zaregistrovaný na PVS ke službě ***Daňová správa - elektronická podání***.
- Pokud ano, PVS přidělí dotazu identifikátor a předá obsah dotazu ČDS ke zpracování.
- Než ČDS dotaz přijme ke zpracování, se WinFAS v určitých časových intervalech dotazuje PVS. V okně je zobrazen samostatným řádkem každý dotaz a jeho výsledek. Časový interval, za jak dlouho dojde k dalšímu dotazu, je zobrazován ve spodní části okna.
- WinFAS se dotazuje tak dlouho, dokud není dotaz na stav podání Českou daňovou správou přijat a vyřízen. Za normálních okolností trvá přijetí ČDS do jedné minuty (maximálně několik minut).

- Pokud z nějakého důvodu na výsledek nemůžete déle čekat (zahlcení portálu apod.), můžete dotazování ukončit tlačítkem ***Stop*** ve spodní části okna a okno zavřít. PVS zatím stále dotaz vyřizuje, zastaví se pouze dotazování WinFASu. Dotazování potom můžete obnovit později. Tlačítkem Pokračuj stejným způsobem, jak je popsáno výše v části ***Pokračování v podání v případě přerušení během odesílání.***

5) Po dokončení dotazování je jeho výsledek vypsán do okna.



Okno zavřeme klepnutím na tlačítko ***Zavřít***.

Zobrazení podrobných informací o stavu.

Informace o stavu, do kterého podání došlo, se vždy zobrazí po ukončení odeslání. Je možno zobrazit také v samostatném okně stiskem tlačítka ***Result*** v okně ***„Stav podání“*** (zobrazeno výše).