**Příloha č. 5 Zadávací dokumentace**

**Zúžená technická dokumentace**

**IS KSP**

**Informačního systému pro kontrolu státní podpory ve stavebním spoření**

*(úplná Technická dokumentace tvoří pevně nesvázanou přílohu – CD, které bude poskytnuto při podpisu Smlouvy)*

|  |
| --- |
|  |
|  |

OBSAH

1 Úvod 4

1.1 Popis IS KSP 4

1.1.1 Legislativa 4

1.1.2 Základní procesy 4

1.1.3 Datová architektura 6

1.1.4 Počet uživatelů 8

2 Softwarová platforma 9

2.1 Základní softwarová platforma 9

2.2 Aplikační platforma 10

2.2.1 Java 11

2.2.2 4gl 12

2.3 Komunikační rozhraní 12

2.4 Uživatelské rozhraní systémů 12

3 Bezpečnost 13

3.1 Základní bezpečnostní principy 13

3.2 Zabezpečení databázové vrstvy 13

3.3 Zabezpečení aplikační vrstvy 14

3.4 Zabezpečení komunikačních tras pro přístup uživatelů 14

3.5 Bezpečnostní architektura systému 14

Úvod

## Popis IS KSP

### Legislativa

* *Zákon č. 96/1993 Sb., stavební spoření se státním příspěvkem a o změnách některých zákonů souvisejících s jeho zavedením, v platném znění*

Tento zákon upravuje stavební spoření se státním příspěvkem u stavebních spořitelen, činnost stavebních spořitelen a kontrolu dodržování podmínek pro poskytování státní podpory a změny některých zákonů souvisejících se zavedením penzijního připojištění.

* *Zákon č. 111/2009 Sb., o základních registrech, v platném znění*

Tento zákon

1. vymezuje obsah základních registrů, informačního systému základních registrů a informačního systému územní identifikace a stanoví práva a povinnosti, které souvisejí s jejich vytvářením, užíváním a provozem,
2. zřizuje Správu základních registrů.

* *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění*

Zákon upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států.

Zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby, pokud tento zákon nebo zvláštní zákon nestanoví jinak a na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.

* *Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), v platném znění*

Zákon upravuje evidenci obyvatel, informační systém evidence obyvatel, trvalý pobyt občanů, rodná čísla a provádění jejich změn, jejich ověřování, odstraňování zjištěných nedostatků v chybně přidělených rodných číslech. MV pro tyto účely spravuje informační systémy, kterých lze využívat jde-li o činnost ministerstev.

* *Zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, v platném znění*

Tento zákon stanoví podmínky vstupu cizince na území České republiky (dále jen "území"), jeho pobytu na něm a vycestování z území a vymezuje působnost Policie České republiky, Ministerstva vnitra (MV) a Ministerstva zahraničních věcí (MZV) v této oblasti státní správy.

Policie při výkonu státní správy podle tohoto zákona provozuje informační systémy obsahující údaje o cizincích. Údaje z informačních systémů vedených podle §158 se poskytují státním orgánům, pokud je potřebují k plnění svých úkolů.

### Základní procesy

Informace předávané stavební spořitelnou MF:

• Žádost o roční zálohu SP, zpracovává se ve třech kolech

• Informace o vracení SP

• Žádost o změnu a doplnění Údajů o účastnících

Informace předávané MF stavební spořitelnou:

• Žádost o roční zálohu SP

• Informace o vracení SP

• Žádost o změnu a doplnění Údajů o účastnících

• Přebírání údajů ze základního registru obyvatel (ROB)

• Přebírání údajů z agendového informačního systému evidence obyvatel o státních občanech České republiky (ISEO)

• Přebírání údajů z informačního systému cizinců (ISC)

• Podpora kontrolní činnosti v rámci Státního dozoru

• Podpora správního řízení o uložení opatření k nápravě zjištěných nedostatků

Umožnění aplikačního přístupu:

• Vybraným pracovníkům Exekutorské komory ČR (EK ČR)

• Vybraným pracovníkům Generálního finančního ředitelství (GFŘ)

• Vybraným pracovníkům Generálního ředitelství cel (GŘC)

• Přidělování přístupových práv do aplikací

• Výměna informací při výkonu dohledu a státního dozoru s Českou národní bankou (ČNB)

### Datová architektura

Popis datových rozhraní mezi externími systémy a IS KSP lze rozdělit na:

* rozhraní se Stavebními společnostmi
* rozhraní s Informačními systémy veřejné správy.



#### Komunikační modul pro stavební spořitelny

Zajištění výměny informací mezi KSP a informačními systémy stavebních spořitelen elektronicky dálkovým přístupem pomocí definovaného rozhraní. Komunikační modul pro stavební spořitelny zajišťuje:

* žádost o roční zálohu státní podpory
* informace o vrácení státní podpory
* žádost o změnu a doplnění údajů o účastnících
* informace o výsledku porovnání údajů o účastnících na evidenci obyvatel
* stav údajů o účastnících v IS KSP

#### Komunikační modul pro základní registry

Zajištění výměny informací mezi KSP a informačními systémy veřejné správy, které dle zákona poskytují pro výkon státní správy na úseku kontroly stavebního spoření při prověřování nároku na poskytování státního příspěvku údaje elektronicky dálkovým přístupem pomocí definovaného rozhraní. Komunikační modul pro základní registry zajišťuje:

* přebírání údajů ze základního registru obyvatel
* přebírání údajů z agendového informačního systému evidence obyvatel o státních občanech České republiky
* přebírání údajů z informačního systému cizinců
* přebírání informací z výkonu dohledu ČNB od ČNB
* předávání informací z výkonu státního dozoru Ministerstva financí do ČNB

#### Modul zpracování dat KSP

Zpracování údajů převzatých od stavebních spořitelen a doplňujících údajů z IS VS pro potřeby zpracování dle podmínek platnosti zákona. Modul zpracování dat KSP zajišťuje:

* zpracování údajů od KSP
* kontrola správnosti převzatých údajů
* aktualizace údajů z KSP
* vypočet výše státního příspěvku dle příslušných algoritmů

#### Modul analytických a prezentačních dat

Zpracování dat vytvořených v modulu zpracování dat KSP a vytvoření konsolidované datové základny pro potřeby analýzy a prezentace dat. Modul analytických a prezentačních dat zajišťuje:

* konverzi dat KSP pro potřeby analytického a prezentačního modulu
* vytvoření předefinovaných agregací a přehledů
* vytvoření dat pro předdefinované reporty

#### Prezentační modul

Prezentace výstupů ze zpracování dat koncovým uživatelům. Prezentační modul zajišťuje:

* zobrazení informací o průběhu zpracování údajů stavebních spořitelen
* zobrazení předdefinovaných výstupů uživatelům MF
* definici uživatelských výstupů
* výběr a prezentace údajů dle požadovaných kritérií
* poskytování údajů vedených v  KSP na požádání
* zobrazení vybraných výstupů externím uživatelům

#### Modul Správního řízení

Podpora správních řízení o uložení opatření k nápravě zjištěných nedostatků zahrnuje:

* zahájení správního řízení
* přerušení řízení
* zastavení řízení
* uložení předběžného opatření
* vygenerování rozhodnutí
* nabytí právní moci
* rozhodnutí v odvolání (rozkladu)
* obnovu řízení
* sledování plynutí lhůt
* sledování plnění udělených sankcí
* tvorbu přehledů o správních řízeních podle typu a subjektu

#### Modul Kontrolní činnosti

Podpora vykonávání kontrolní činnosti v rámci Státního dozoru zahrnuje:

* přípravu plánu kontrolní činnosti
* přípravu podkladů o vybraném subjektu pro jednotlivé kontroly
* evidenci údajů o kontrolách
* evidenci závěrů z kontrol
* tvorbu přehledů o kontrolní činnosti dle požadovaných kritérií

#### Monitoring aktivit

Vytváření provozních a aplikačních logů zahrnuje:

* vytváření auditních záznamů o přístupech k informacím vedených v  KSP
* vytváření auditních záznamů o přístupu k referenčním údajům ZR
* vytváření auditních záznamů o průběhu komunikací mezi KSP a externími IS
* vytváření auditních záznamů o chybových stavech aplikací
* analýzy auditních záznamů

#### Správa uživatelů

Podpora správy uživatelských účtů pro koncové uživatele KSP zahrnuje:

* zavedení uživatele
* přiřazení oprávnění
* zrušení uživatele
* změna hesla

### Počet uživatelů

IS KSP v současné době eviduje cca 6 000 uživatelů.

# Softwarová platforma

## Základní softwarová platforma

Základní softwarovou platformou je:

* OS Solaris 10 - [unixový](http://cs.wikipedia.org/wiki/UN*X) [operační systém](http://cs.wikipedia.org/wiki/Opera%C4%8Dn%C3%AD_syst%C3%A9m) firmy [Oracle](http://cs.wikipedia.org/wiki/Sun_Microsystems). Mezi nejdůležitější vlastnosti tohoto OS patři:
* Oracle Solaris Containers – virtualizace umožňující vytvořit na jedné instanci OS různá aplikační prostředí
* Oracle Solaris DTrace – sada nástrojů na sledování systému bez nutnosti upravovat aplikace
* Oracle Solaris Predictive Self Healing – OS vyhodnocuje a snaží se minimalizovat případné problémy, umožňuje automatický restart aplikace nebo služby
* Oracle Solaris Trusted Extensions – pokročilé zabezpečení dat umožňující zajistit přístup k datům dle jejich citlivosti
* Oracle Solaris ZFS – pokročilá správa souborového systému usnadňující jejich administraci
* Guaranteed Binary Compatibility – zajišťuje možnost běhu aplikací bez jejich nutné změny při změně verze OS Solaris
* Oracle Solaris Live Upgrade – mechanismus umožňující upgrade OS za běhu
* Interoperability – podporuje součinnost OS s Linux-based systémy
* Role-Based Access Control – umožňuje delegovat administrační funkce na uživatele
* Oracle Solaris Service Manager – v případě hardware nebo software chyby se pokusí zajistit pokračovaní běhu aplikace
* Oracle Solaris Fault Manager – monitoruje hardware a software chyby, provádí automatickou diagnostiku příčin.

Databáze Informix IDS 11.7 – databázový server umožňující přístup k relačním databázím. IDS podporuje alfanumerické a rozšířené typy dat:

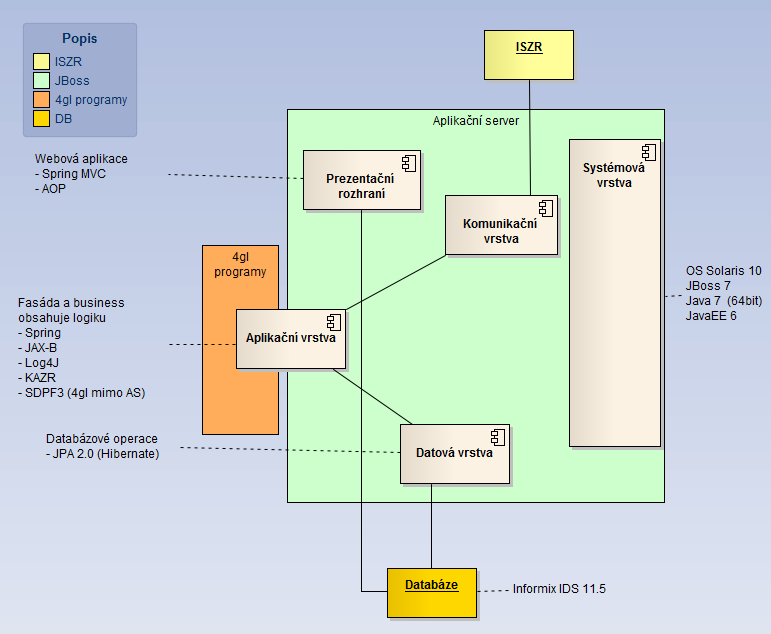
* grafické,
* multimediální,
* geografické prostorové,
* HTML,
* uživatelem definované typy.

Aplikační server JBoss 7.1.1 – aplikační server certifikovaný pro Java EE6 Full Profile podporuje následující standardy:

* EJB 3.1 Full – standard pro Enterprise Java Beany.
* CMP 2 - standard poskytující persistence manager předcházející JPA. Toto je výhodné pro aplikace využívající EJB 2.x Entity Beany.
* JAX-WS 2.2 – usnadňuje použití Web Services na EE platformě.
* JAX-RPC 1.1 – zajišťuje podporu dřívějších Java EE Web Services aplikací.
* JAX-RS 1.1 – podpora tvorby RESTful Web Services využívajících Java EE platformu.
* JavaMail 1.4 - umožňuje Java EE aplikacím pracovat s e-maily.
* JCA 1.6 - mechanismus pro komponenty třetích stran, například podporu uživatelských data sources, connection pooling a transaction management pro přístup do databáze.
* JMS 1.1 - pokročilý messaging support pro EE aplikace.
* IIOP - podpora interoperablility s dalšími aplikačními servery a non-Java CORBA klienty.
* JSR-88 – standard pro přenositelný deploy na Java EE server.

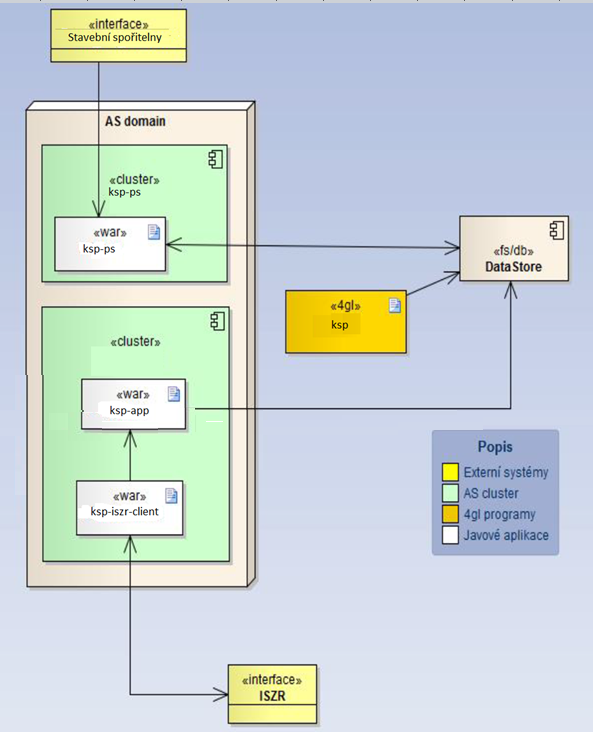
## Aplikační platforma

Z hlediska aplikace je základní softwarovou platformou Java a 4gl programy (viz Obrázek 1).



Obrázek 1 - Aplikační platforma

Rozhraním pro komunikaci Java aplikací a 4gl programů je filesystem a databáze (viz Obrázek 2).



Obrázek 2 - Rozhraní pro komunikaci Java aplikací a 4gl programů

Buildovacím frameworkem pro Java aplikace bude Maven 3.0. Aplikace jsou rozděleny do jednotlivých Maven projektů, které jsou deployvány na aplikační server.

Pro 4gl programy je využit kompilátor jazyka C.

### Java

Klientská část Java aplikace zajišťující přípravu dat (tj. zipování a podepsání certifikátem) pro přenos dat na server MF a ověření dat (tj. rozzipování a ověření certifikátu) odpovědí ze serveru MF bude využívat:

SWT – The Standart Widget Toolkit. Nástroj pro tvorbu uživatelského interface,

JavaWebStart – technologii sloužící k distribuci a následnému spuštění klientské části aplikace z webového rozhraní.

Pro práci s Java keystore lze použít například GUI aplikace Portecle (<http://portecle.sourceforge.net/>).

Serverová část je tvořena:

* webovým rozhraním (viz Uživatelské rozhraní systémů),
* modulem pro komunikaci se základními registry (viz Komunikační rozhraní).

### 4gl

Část aplikace zajišťující kontroly a samotné zpracování je tvořena množinou 4gl programů. Jde o programovací procedurální jazyk určený vytvoření programového vybavení s integrovaným modulem pro komunikaci s databází Informix

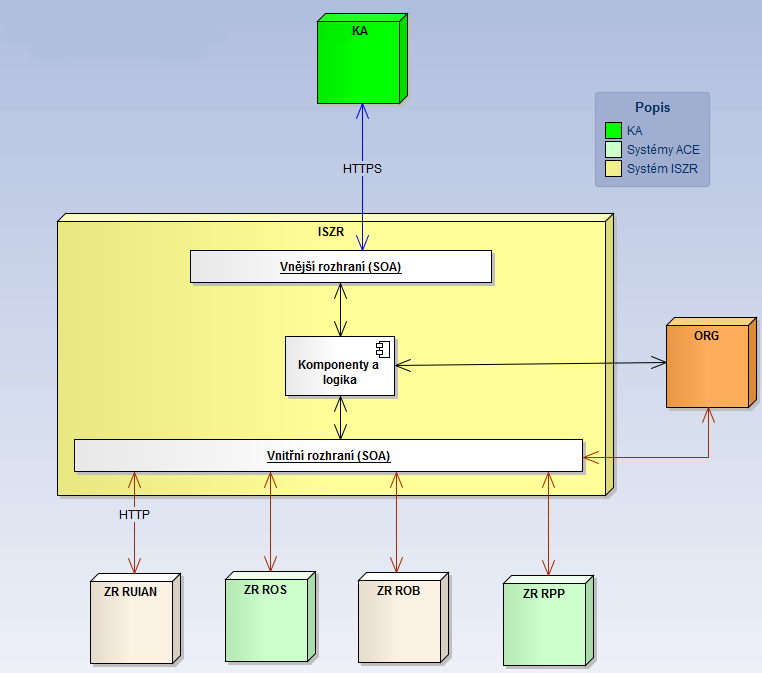
## Komunikační rozhraní

Systém obsahuje rozhraní KA pro komunikaci se základními registry (Obrázek 3). Na obrázku znázorněné zelenou barvou Toto rozhraní je realizováno pomocí Java technologií:

Spring - framework pro tvorbu Java aplikací,

Spring Integration – framework pro integraci jednotlivých Java aplikací,

Apache CXF – framework pro práci s webovými službami.



Obrázek 3 - Komunikační rozhraní

## Uživatelské rozhraní systémů

Uživatelským rozhraním pro komunikaci se stavebními spořitelnami a penzijními společnostmi bude webové rozhraní realizováno v Java frameworku.

# Bezpečnost

## Základní bezpečnostní principy

Dále uvedené bezpečnostní principy musí být informačním systémem KSP prosazeny a zajištěny napříč celým systémem a jeho jednotlivými moduly:

integrita dat

* typová kontrola,
* kontrola povinných polí,
* kontrola integrity měněné množiny dat,
* Kontrola integrity s relevantními daty v DB:
* on-line,
* dávková (kontrolní modul),
* kontrola duplicity dat;

důvěrnost informací

* důvěrnost informací (zadání, změnu i výmaz jakýchkoliv dat v systému lze spojit s konkrétním uživatelem a časem); tyto informace musí být přístupné i z uživatelského prostředí;

verifikace informací a činností

* možnost vícestupňového schválení,
* správa více verzí entity dat:
* schválených dat,
* zatím neschválených dat,
* ošetření principu integrity s ostatními relevantními daty v DB pro obě verze dat,
* možnost nastavit pro data, resp. entity dat, povinnost verifikace (schválení změny dat);

auditní stopa

* lze dohledat co, kdo, kdy prohlížel/zadával/měnil/opravoval/mazal a z jakého původního stavu informace. A lze v těchto informacích jednoduše filtrovat dle modulů, entit, uživatelů, časů, typu činnosti apod.;

ostatní

* implementace eliminující zranitelnosti systému před běžnými útoky (SQL injection, cross site scripting atd.);
* bezpečnostní řešení systému musí odpovídat zásadám standardu ISO/IEC 27001 (dříve BS 7799).

## Zabezpečení databázové vrstvy

Databázové servery budou umožňovat přístup pouze přesně vymezeným aplikacím (aplikačnímu serveru v aplikační vrstvě). Pro přístup administrátorů databází (DB) musí být definovány IP adresy jejich stanic, ze kterých bude administrace umožněna. Implementací musí být zajištěno, že jiné aplikace, než aplikace KSP, nesmí mít přímý přístup k DB.

Pro přístup k DB musí být využity schválené autentizační mechanismy. Databázový server bude fyzicky oddělen od aplikačního serveru v aplikační vrstvě a bude umístěn v samostatné zóně.

## Zabezpečení aplikační vrstvy

Při přístupu k jednotlivým službám aplikační vrstvy bude vynucena autentizace a autorizace schváleným mechanismem daného subjektu (programu nebo uživatele), který službu požaduje.

## Zabezpečení komunikačních tras pro přístup uživatelů

Při přístupu k jednotlivým službám aplikační vrstvy bude vynucena autentizace a autorizace schváleným mechanismem daného subjektu (programu nebo uživatele), který službu požaduje.

## Bezpečnostní architektura systému

Cílem bezpečnostní architektury je naplnit bezpečnostní požadavky, podpořit hierarchický model řízení bezpečnosti a dosáhnout požadované úrovně v základních pilířích, a to:

* řízení přístupu k datům,
* zajištění důvěrnosti dat,
* zajištění integrity dat,
* audit operací s daty,
* zajištění dostupnosti.