SMLOUVA O NAVRŽENÍ, ZHOTOVENÍ A IMPLEMENTACI POČÍTAČOVÉHO PROGRAMU, POSKYTNUTÍ LICENCE, A POSKYTOVÁNÍ SERVISNÍCH SLUŽEB

Číslo smlouvy Zadavatele: 47481/2018-SŽDC-GŘ-O8

Číslo smlouvy Dodavatele: _____

(dále jen „**Smlouva**“)
uzavřená podle ustanovení § 1746 odst. 2, § 2358 a násl. a § 2586 a násl. Občanského zákoníku níže uvedeného dne, měsíce a roku mezi těmito Stranami:

Zadavatel: **Správa železniční dopravní cesty, státní organizace**
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl A, vložka 48384,
se sídlem: Praha 1 - Nové Město, Dlážděná 1003/7, PSČ 110 00, Česká republika,
IČO: 709 94 234, DIČ: CZ70994234,
bankovní spojení: xxxxxxxxxxxxxxxxxxxxxx

číslo účtu: xxxxxxxxxxxxx
zastoupená **Tomášem Drmolou, MBA**, náměstkem GŘ pro správu majetku
(dále jen „**Zadavatel**“)

a

Dodavatel: **ČD - Informační Systémy, a.s.**
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl B, vložka 17064,
se sídlem: Pernerova 2819/2a, Žižkov, 130 00 Praha 3,
IČO: 248 29 871, DIČ: CZ24829871,
bankovní spojení: Komerční banka, a.s.,
číslo účtu: 43-7795830287/0100
zastoupená **Ing. Tomášem Vackem,** členem představenstva **a**
Ing. Miloslavem Kopeckým, předsedou představenstva
(dále jen „**Dodavatel**“)

(Zadavatel a Dodavatel dále společně uváděni jako „**Strany**“ a každý z nich jednotlivě jako „**Strana**“).

PREAMBULE

Vzhledem k tomu, že

(A) Zadavatel zahájil oslovením dodavatelů prostřednictvím elektronického nástroje E-ZAK dne 17. 08. 2018 zadávací řízení k podlimitní sektorové veřejné zakázce v souvislosti s výkonem relevantní činnosti dle §151 odst. 1 zákona a v souladu s § 158 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, s názvem: *„Správa identit – Identity Management"* číslo 41225/2018-SŽDC-GŘ-O8 (dále jen „Veřejná zakázka"), jejíž předmět je uveden v čl. 2. Výzvy k podání nabídky na předmětnou veřejnou zakázku. Nabídka Dodavatele byla Zadavatelem vybrána jako ekonomicky nejvýhodnější;

(B) Zadavatel má zájem na Implementaci jednoho stabilního a unifikovaného podnikového Počítačového programu (jak je tento pojem definován níže) tak, aby Počítačový program mimo jiné umožnil správu a řízení identit, které přistupují k jakýmkoliv prostředkům SŽDC a splnění požadavků zákona č. 181/2014 Sb. o kybernetické bezpečnosti, který definuje požadavky na provozovatele nebo správce kritické informační infrastruktury nebo významného informačního systému dle zákona 432/2010 Sb. Implementací Idm jsou především řešeny § 19 Nástroj pro řízení přístupových oprávnění a § 11 Řízení přístupu a bezpečné chování uživatelů Vyhlášky č. 316/2014 Sb.;

(C) Zadavatel požaduje, aby Počítačový program byl otevřený stávajícím i budoucím dodavatelům technologií aplikací či služeb, jakož i umožnil Zadavateli vývoj, rozvoj a inovaci Počítačového programu;

(D) Dodavatel má zájem Počítačový program pro Zadavatele navrhnout, zhotovit a implementovat způsobem a za podmínek podle této Smlouvy, jejích příloh a Projektové dokumentace.

dohodly se Strany takto:

Článek 1.
Definice

1.1. Pro účely této Smlouvy

a) „**Akceptační protokol**" má význam uvedený v **odstavci 7.1.** této Smlouvy;

b) „**Autorský zákon**" znamená zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů;

c) „**Celková cena**" má význam uvedený v **odstavci 10.1.** této Smlouvy;

d) „**Časový harmonogram**" má význam uvedený v **3.1.** této Smlouvy;

e) „**Další plnění**" má význam uvedený v **odstavci 17.7.** této Smlouvy;

f) „**Dílo**" má význam uvedený v **odstavci 2.1.** této Smlouvy;

g) „**Důvěrné informace**“ mají význam uvedený v **odstavci 13.1.** této Smlouvy;

h) „**Implementace**“ znamená vytvoření jednoho Počítačového programu a jeho instalaci, konfiguraci, přizpůsobení díla dle požadavků SŽDC, otestování, odladění a zprovoznění na infrastruktuře Zadavatele v souladu s touto Smlouvou, jejími přílohami a Projektovou dokumentací. Pro vyloučení pochybností Strany výslovně sjednávají, že Implementace je součástí Díla;

i) „**Insolvenční zákon**“ znamená *zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon)*, ve znění pozdějších předpisů;

j) „**Licence**“ má význam uvedený v **odstavci 9.1.** této Smlouvy;

k) „**Nabídka**“ znamená nabídku Dodavatele podanou Dodavatelem do zadávacího řízení k Veřejné zakázce, včetně protokolů z jednání o nabídce;

l) „**Občanský zákoník**“ znamená *zákon č. 89/2012 Sb., občanský zákoník*, ve znění pozdějších předpisů;

m) „**Počítačový program**“ má význam uvedený v **odstavci 2.1.1.** této Smlouvy;

n) „**Projektová dokumentace**“ má význam uvedený v **odstavci 5.1.** této Smlouvy;

o) „**Projektová schůzka**“ má význam uvedený v **odstavci 4.14.** této Smlouvy;

p) „**Projektové orgány**“ mají význam uvedený v **odstavci 4.1.** této Smlouvy

q) „**Projektoví manažeři**“ mají význam uvedený v **odstavci 4.12.** této Smlouvy;

r) „**Projektový tým**“ má význam uvedený v **článku 4.** této Smlouvy;

s) „**Předávací protokol**“ má význam uvedený v **odstavci 8.1.** této Smlouvy;

t) „**Řídící výbor**“ má význam uvedený v **článku 4.** této Smlouvy;

u) „**Poddodavatel**“ má význam uvedený v **odstavci 14.1.** této Smlouvy;

v) „**Širší projektový tým**“ má význam uvedený v **článku 4.** této Smlouvy;

w) „**Veřejná zakázka**“ má význam uvedený v **bodě (A)** preambule této Smlouvy;

x) „**Zákon o DPH**“ znamená *zákon č. 235/2004 Sb., o dani z přidané hodnoty*, ve znění pozdějších předpisů;

y) „**Zákon o ochraně osobních údajů**“ znamená *zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů*, ve znění pozdějších předpisů;

z) „**Zákon o zadávání veřejných zakázek**“ znamená *zákon č. 134/2016 Sb., o zadávání veřejných zakázek*, ve znění pozdějších předpisů;

aa) „**Záruční doba**“ má význam uvedený v **odstavci 12.1.** této Smlouvy.

Článek 2.
Předmět Smlouvy

2.1. Předmětem této Smlouvy je závazek Dodavatele provést pro Zadavatele na svůj náklad, nebezpečí, s nejvyšší odbornou péčí a v nejvyšší možné jakosti dílo s nehmotným výsledkem, které spočívá v:

2.1.1. softwarovém zpracování a zajištění informačního systému identity managementu, coby jednoho programu na řízení a správu identit;

2.1.2. přizpůsobení díla dle požadavků zadavatele s ohledem na zavedené principy a postupy ve společnosti. Zadavatel klade vysoký důraz na přizpůsobení díla dle již zavedených principů a postupů ve společnosti, protože s ohledem na velikost společnosti a velký počet aktiv není možné tyto principy a postupy zásadně měnit. Jedná se především o principy a postupy, které společnost využívá ke správě životního cyklu identit;

2.1.3. zpracování základních business rolí, vycházejících z již existujících poloautomatických procesů ve společnosti zavedených, s návazností na připojované systémy;

2.1.4. připojení dvou vybraných aktiv společnosti, resp. koncových systémů a zpracování automatických procesů, které skrze business role řídí autorizaci v koncových systémech;

2.1.5. připojení zdrojových systému personálních dat;

2.1.6. zpracování všech požadavků dle kapitoly 6 (Rozsah dodávky) přílohy č. 1 této Smlouvy „Technická specifikace“.

2.2. Dodavatel se dále zavazuje poskytnout Zadavateli v souladu s Občanským zákoníkem a Autorským zákonem Licenci v rozsahu a za podmínek sjednaných Stranami v **článku 9** této Smlouvy.

2.3. Předmětem této Smlouvy je dále povinnost Dodavatele poskytovat Zadavateli Služby podle této Smlouvy, jejích příloh a Projektové dokumentace.

2.4. Dodavatel tímto prohlašuje, že se s předmětem a obsahem této Smlouvy před jejím uzavřením dostatečně a náležitě seznámil, že plnění závazků Dodavatele z této Smlouvy není plněním nemožným ve smyslu ustanovení § 580 odst. 2 Občanského zákoníku, a dále že Dílo může být řádně provedeno způsobem a ve lhůtách uvedených v této Smlouvě, jejích přílohách a Projektové dokumentaci.

2.5. Dodavatel se zavazuje provést Dílo a poskytovat Služby podle této Smlouvy v souladu s platnými právními předpisy.

2.6. Zadavatel se zavazuje zaplatit Dodavateli za plnění uvedená v tomto **článku 2** této Smlouvy úplatu ve výši a za podmínek sjednaných v **článku 11** této Smlouvy.

Článek 3.
Termín a místo plnění Díla

3.1. Dodavatel se zavazuje provést Dílo řádně a v souladu s časovým harmonogramem, který Dodavatel předloží na prvním řídícím výboru ke schválení, a to nejpozději 12 kalendářních měsíců od účinnosti této Smlouvy.

3.2. Dodavatel je povinen navrhnout a zhotovovat Dílo na svých hardwarových prostředcích a ve svém softwarovém a technickém prostředí. Na hardwarových prostředcích a v softwarovém a technickém prostředí Zadavatele je Dodavatel oprávněn Dílo nasadit a uvést do provozu a provádět jeho Implementaci s využitím dálkového přístupu, jakož i osobně na místě u Zadavatele, k čemuž Zadavatel poskytne na základě žádosti Dodavatele nezbytně nutnou součinnost.

3.3. Dodavatel je povinen zhotovovat Dílo dle níže uvedených základních projektových etap:

- Projektová etapa č. I obsahuje:

  a) Analýza potřeb Zadavatele a implementace Identity managementu v prostředí SŽDC.

  b) Analýza principů a postupů, které společnost využívá ke správě životního cyklu identit a návrh budoucího řešení.

  c) Vypracování detailního postupu jednotlivých projektových etap

  d) Vypracování detailního časového harmonogramu celého projektu, s vyznačenými milníky akceptace jednotlivých etap.

- Projektová etapa č. II obsahuje:

  a) Analýza přizpůsobení díla dle požadavků SŽDC s ohledem na zavedené principy a postupy ve společnosti.

  b) Analýza a zpracování základních business rolí, vycházejících z již existujících poloautomatických procesů ve společnosti zavedených, s návazností na připojované systémy.

  c) Analýza a zpracování business rolí pro připojované systémy v projektové etapě č. IV.

- Projektová etapa č. III obsahuje:

a) Softwarové zpracování a zajištění informačního systému identity managementu na řízení a správu identit, dle vypracovaných analýz v projektových etapách I. a II.

b) Připojení na zdroje personálních dat.

c) Přizpůsobení díla dle požadavků SŽDC s ohledem na zavedené principy a postupy ve společnosti.

d) Implementace business rolí, vycházejících z projektové etapy II. písmena b) a c).

- Projektová etapa č. IV obsahuje:

e) Připojení 2 vybraných aktiv společnosti, resp. koncových systémů a zpracování automatických procesů, které skrze business role řídí autorizaci v koncových systémech.

f) Testování informačního systému identity managementu.

g) Testovací provoz systému identity managementu s napojením na koncové systémy.

h) Nasazení do ostrého provozu.

i) Předání a akceptace díla dle **článků 2.1.1. – 2.1.6.**

Článek 4.
Organizace a kontrola provádění Díla

4.1. Provádění Díla organizuje a kontroluje zejména řídící výbor (dále jen „**Řídící výbor**"), projektový tým (dále jen „**Projektový tým**") a širší projektový tým (dále jen „**Širší projektový tým**") (dále společně jen „**Projektové orgány**").

4.2. O závěrech jednání Projektových orgánů se sepisuje zápis, který předkládá Zadavateli ke schválení Dodavatel. Zápis bude vyhotoven ve dvou (2) stejnopisech.

4.3. Ustanovením předchozího odstavce není dotčeno právo Zadavatele kontrolovat provádění Díla nezávisle na Projektových orgánech.

Řídící výbor

4.4. Řídící výbor je nejvyšším Projektovým orgánem.

4.5. Do působnosti Řídícího výboru náleží:

a) řešení strategických a koncepčních záležitostí při provádění Díla;

b) řešení sporných a nejasných záležitostí při provádění Díla, nedojde-li k jejich řešení na úrovni Projektového týmu;

c) řešení záležitostí, které není oprávněn řešit Projektový tým;

d) dohled nad plněním Časového harmonogramu;

e) identifikace víceprací a vyhodnocení jejich potřebnosti; a

f) součinnost při akceptaci jednotlivých Projektových etap, Modulů a při předání Díla,

jakož i další jednání a činnosti svěřené Řídícímu výboru v této Smlouvě, jejích přílohách anebo Projektové dokumentaci.

4.6. Řídící výbor je tvořen stejným počtem zástupců Zadavatele a Dodavatele. Každá ze Stran může jakéhokoli svého zástupce v Řídícím výboru nahradit jinou osobou, o čemž

je povinna neprodleně informovat druhou Stranu. Zadavatel je oprávněn odmítnout změnu ve složení Řídícího výboru provedenou Dodavatelem.

4.7. Schůzi Řídícího výboru svolává a organizuje Dodavatel. Schůzi Řídícího výboru může svolat také Zadavatel. Záležitosti ve své působnosti řeší Řídící výbor prostou většinou hlasů všech svých členů, přičemž v případě rovnosti hlasů má rozhodující slovo pro závěry Řídícího výboru Zadavatel.

4.8. Schůze Řídícího výboru se vedle členů Řídícího výboru účastní i Projektoví manažeři.

Projektový tým

4.9. Projektový tým je výkonným Projektovým orgánem. Projektovému týmu náleží organizace a průběžná kontrola provádění Díla, není-li konkrétní jednání v působnosti jiného Projektového orgánu či přímo některé ze Stran.

4.10. Projektový tým je odpovědný Řídícímu výboru.

4.11. Projektový tým připravuje a dodává Řídícímu výboru potřebné podklady a informace pro výkon působnosti Řídícího výboru a poskytuje Řídícímu výboru vysvětlení, zprávy a veškerou asistenci týkající se Díla a jeho zhotovování a Implementace, a to ve formě požadované Řídícím výborem.

4.12. Projektový tým se skládá z projektových manažerů Zadavatele a Dodavatele (dále společně jen „**Projektoví manažeři**“). Jména a kontaktní údaje jednotlivých Projektových manažerů, postup při svolání Projektové schůzky a další podrobnosti ohledně činnosti Projektového týmu budou uvedeny v Projektové dokumentaci.

4.13. Každá ze Stran může jakéhokoli svého Projektového manažera odvolat a nahradit jej jinou osobou. O tom je tato Strana povinna neprodleně informovat druhou Stranu.

4.14. Dodavatel se zavazuje zajišťovat a organizovat pravidelné schůzky Projektového týmu za účelem kontroly provádění Díla (dále jen „**Projektová schůzka**“).

4.15. Projektová schůzka se koná zpravidla jednou (1) za čtrnáct (14) kalendářních dnů. Za svolání Projektové schůzky je odpovědný Dodavatel, zejména je povinen včas vyzvat Projektové manažery k účasti na Projektové schůzce a sdělit jim datum a čas jejího konání. Projektovou schůzku může svolat také Zadavatel.

4.16. Místem konání Projektové schůzky je sídlo Zadavatele, nedohodnou-li se Strany jinak.

Širší projektový tým

4.17. Širší projektový tým je výkonným Projektovým orgánem podřízeným Projektovému týmu. Úkoly, personální obsazení a bližší podrobnosti činnosti Širšího projektového týmu budou stanoveny Projektovou dokumentací.

4.18. Širší projektový tým je odpovědný Projektovému týmu.

4.19. Širší projektový tým dále dodává Projektovému týmu potřebné podklady, na vyžádání odpovídá Projektovému týmu na jeho dotazy a poskytuje Projektovému týmu vysvětlení, zprávy a veškerou asistenci týkající se Díla a jeho zhotovování a Implementace, a to ve formě požadované Projektovým týmem.

Článek 5.
Projektová dokumentace

5.1. Účelem Projektové dokumentace je podrobněji upravit práva a povinnosti Stran ze závazkového vztahu založeného touto Smlouvou týkající se provedení Díla a poskytování Služeb, jež se budou odvíjet od Dodavatelem navrženého technického řešení Počítačového programu, a nebylo tedy možné je v podrobnostech vymezit předem. Projektová dokumentace musí být v souladu s touto Smlouvou a jejími přílohami. Tato Smlouva má přednost před Projektovou dokumentací.

5.2. Dodavatel se zavazuje zhotovit Projektovou dokumentaci i její návrh tak, aby jejím obsahem byl úplný a podrobný popis alespoň následujících klíčových oblastí zhotovování a Implementace Počítačového programu a poskytování Služeb podle této Smlouvy:

a) manažerské shrnutí obsahující alespoň cíle Díla, rozsah zpracovávaných dat Díla, fáze a Časový harmonogram zhotovování a Implementace Díla a organizační zajištění Díla;

b) projektový záměr Díla obsahující alespoň popis výchozí situace, cíle Díla, zdůvodnění Díla, rozsah Díla a jeho interakce s ostatními projekty a systémy Zadavatele;

c) seznam a podrobný popis jednotlivých Projektových etap zhotovování a Implementace Díla;

d) Časový harmonogram s doplněním lhůt pro dokončení Projektových etap č. I. až IV. v souladu s Nabídkou, nedohodnou-li se Strany při přípravě Projektové dokumentace na jiných délkách těchto lhůt;

e) podrobný popis zamýšlených výstupů Díla včetně podrobného popisu zejména:

i. jednorázových výstupů v průběhu zhotovování a Implementace Díla,
ii. trvalých výstupů v průběhu zhotovování a Implementace Díla, a
iii. výstupů z každé Projektové etapy;

f) podrobný popis akceptace každé Projektové etapy včetně jejího podrobného popisu, zejména:

i. pravidel akceptace,
ii. akceptační procedury, a
iii. vad a nedodělků, které nebrání řádnému užívání Díla;

g) podrobný popis organizace zhotovování a Implementace Díla včetně podrobného popisu zejména:

i. Řídícího výboru,
ii. Projektového týmu, a
iii. Širšího projektového týmu;

h) podrobný popis požadavků na součinnost Stran a jejich komunikaci při zhotovování a Implementaci Díla, včetně způsobu vedení komunikace;

i) podrobný popis řízení rizik a problémů a řízení změn Díla včetně podrobného popisu zejména těchto částí:

i. identifikace rizik
ii. řešení problémů,
iii. proces řízení rizik a problémů,
iv. eskalační procedury, a
v. řízení změn;

j) podrobný popis dalších podmínek a způsobu poskytování Služeb Dodavatelem Zadavateli, a

k) ujednání mezi Zadavatelem a Dodavatelem o úrovni služeb technické podpory a servisu Počítačového programu, jehož obsahem bude zejména:

i. kategorizace vad,
ii. stanovení lhůt k odstranění vad a následků pro Dodavatele v případě nedodržení těchto lhůt, a
iii. stanovení dob, v rámci kterých bude Dodavatel oprávněn dočasně pozastavit funkce Počítačového programu za účelem jeho údržby, jakož i následků pro Dodavatele v případě překročení těchto dob,

a dalších oblastí, jejichž zařazení do Projektové dokumentace stanovuje tato Smlouva nebo které vyplynou z jednání Stran, Řídícího výboru, Projektového týmu nebo jejichž zařazení do Projektové dokumentace bude Zadavatel požadovat.

5.3. Projektovou dokumentaci je Dodavatel povinen zhotovovat v úzké součinnosti se Zadavatelem a s Projektovým týmem a průběžně ji s nimi konzultovat tak, aby Projektová dokumentace v nejvyšší možné míře odpovídala potřebám Zadavatele, a zapracovávat za tímto účelem připomínky a návrhy Zadavatele.

5.4. Zadavatel může návrh Projektové dokumentace odsouhlasit nebo jej vrátit Dodavateli k dopracování anebo sám určit obsah Projektové dokumentace, za předpokladu, že bude v souladu s touto Smlouvou a jejími přílohami. Pokud bude Zadavatel vracet návrh Projektové dokumentace k dopracování, učiní tak vždy do pěti (5) pracovních dnů ode dne, kdy obdržel předmětný návrh Projektové dokumentace.

5.5. Projektová dokumentace je pro Strany závazná ode dne jejího podpisu oběma Stranami, a v případě jejího určení Zadavatelem ode dne jejího podpisu Zadavatelem.

5.6. Finální znění Projektové dokumentace se podepisuje ve dvou (2) vyhotoveních, z nichž jedno (1) obdrží Dodavatel a jedno (1) Zadavatel.

Článek 6.
Změny Projektové dokumentace

6.1. Kterákoliv Strana je oprávněna před předáním a převzetím Díla navrhnout změnu Projektové dokumentace. Návrh musí být písemný. Součástí návrhu na změnu Projektové dokumentace musí být popis navrhované změny, a v případě návrhu podaného Dodavatelem i odůvodnění navrhované změny.

6.2. Změna Projektové dokumentace nabývá účinnosti písemným odsouhlasením návrhu změny Projektové dokumentace oběma Stranami.

Článek 7.
Akceptace Projektových etap a Modulů

7.1. O ukončení a akceptaci každé z Projektových etap č. I. až IV. této Smlouvy vyhotoví Strany písemný protokol (dále jen „**Akceptační protokol**“). Za účelem ukončení a akceptace Projektové etapy nebo Modulu je Dodavatel povinen svolat schůzi Řídícího výboru.

7.2. Bude-li Projektová etapa nebo Modul vykazovat jakékoliv vady či nedodělky, uvede Zadavatel tyto vady a nedodělky, popř. včetně lhůty k jejich odstranění, do zápisu ze schůze Řídícího výboru. Zadavatel není povinen ukončit a akceptovat příslušnou Projektovou etapu na základě Akceptačního protokolu dříve, než budou odstraněny všechny vady a nedodělky.

7.3. Po odstranění vad a nedodělků uvedených v zápisu ze schůze Řídícího výboru svolá Dodavatel další schůzi Řídícího výboru za účelem ukončení a akceptace předmětné Projektové etapy nebo Modulu.

7.4. Dodavatel průběžně a v dostatečném předstihu před uplynutím termínu pro ukončení každé Projektové etapy informuje Zadavatele o postupu při zhotovování každé Projektové etapy a o předpokládaném průběhu jejího ukončování a akceptace.

7.5. Dodavatel seznámí Zadavatele s výstupem a/nebo výsledky z každé Projektové etapy a Modulu v dostatečném předstihu před uplynutím termínu pro ukončení každé Projektové etapy, a v případě Modulu před Dodavatelem plánovaným datem pro jeho ukončení, a to tak, aby Zadavatel mohl takový výstup a/nebo výsledky posoudit a sdělit k nim připomínky.

Článek 8.
Předání a převzetí Díla

8.1. K převzetí Díla Zadavatelem dojde podpisem písemného předávacího protokolu (dále jen „**Předávací protokol**“) Zadavatelem za podmínky, že

a) došlo k ukončení a akceptaci Projektové etapy č. IV. na základě Akceptačního protokolu, a

b) Dílo nevykazuje vady a nedodělky bránící řádnému užívání Díla.

Dílo je ve smyslu ustanovení § 2604 Občanského zákoníku provedeno, bylo-li předáno a dokončeno bez vad a nedodělků.

8.2. Za účelem převzetí Díla je Dodavatel povinen svolat schůzi Řídícího výboru. Místem převzetí Díla je sídlo Zadavatele.

8.3. Bude-li Dílo vykazovat vady či nedodělky bránící řádnému užívání Díla, k předání a převzetí Díla nedojde. Po odstranění vad a nedodělků bránících řádnému užívání Díla svolá Dodavatel další schůzi Řídícího výboru za účelem předání a převzetí Díla. Strany vyhotoví nový Předávací protokol.

8.4. Bude-li Dílo vykazovat vady či nedodělky nebránící řádnému užívání Díla, nebrání tyto vady či nedodělky předání a převzetí Díla. Zadavatel tyto vady a nedodělky uvede do Předávacího protokolu, popř. včetně lhůty k jejich odstranění. O odstranění vad a nedodělků nebránících řádnému užívání Díla vyhotoví Strany písemný dodatek k Předávacímu protokolu.

8.5. Dodavatel je před podpisem Předávacího protokolu povinen předat Zadavateli

(i.) aktuální elektronické verze zdrojových kódů Počítačového programu včetně dokumentace

(ii.) aktuální elektronické verze zdrojových kódů softwaru, který se stal součástí Počítačového programu včetně dokumentace, a

(iii.) veškeré přípravné koncepční materiály, uživatelské příručky a další relevantní dokumenty, jakož i veškeré podklady a informace potřebné k výkonu Licence,

o čemž Strany sepíší samostatný předávací protokol.

8.6. Dnem převzetí Díla přechází na Zadavatele vlastnické právo k Dílu včetně všech jeho součástí, jakož i k veškerým věcem, na kterých bylo Dílo Zadavateli předáno.

Článek 9.
Licence

9.1. Dodavatel v souladu s Autorským zákonem na základě této Smlouvy poskytuje Zadavateli veškerá svá oprávnění k výkonu práv duševního vlastnictví:

(i.) k Počítačovému programu jako autorskému dílu dle ustanovení § 2 Autorského zákona, a to nezávisle na tom, zda jej vytvořil sám či s využitím Poddodavatele;

(ii.) k Projektové dokumentaci, zdrojovým kódům včetně dokumentace a přípravným koncepčním materiálům, které vytvořil při zhotovování Díla sám Dodavatel nebo jeho Poddodavatel, zejména, nikoliv však výlučně, k programovým analýzám a obdobným materiálům, a

(iii.) k veškerým dalším autorským dílům, která Dodavatel vytvořil či vytvoří sám nebo prostřednictvím svého Poddodavatele při vývoji, inovaci či jiné změně Díla,

(dále jen „**Licence**“).

9.2. Dodavatel tímto poskytuje Zadavateli nevýhradní Licenci ve smyslu §2361 Občanského zákoníku, přičemž vše, co bude vyvíjeno nad rámec standartního vybavení informačního systému pro Zadavatele, bude výhradní licencí. Zadavatel požaduje licenci v:

(i.) v prostorově a množstevně neomezeném rozsahu, obsahující:

- neomezené počty instancí produktu
- neomezené počty uživatelů
- neomezené počty koncových systémů
- neomezené počty konektorů
- neomezené počty procesorových jader, velikost paměti a jiných hardwarových, softwarových či aplikačních parametrů

(ii.) jako neodvolatelnou, trvalou a bez povinnosti Zadavatele ji užít.

9.3. Dodavatel na základě této Smlouvy poskytuje Zadavateli k autorskému dílu, na které se vztahuje Licence podle této Smlouvy, veškerá majetková užívací práva ve smyslu ustanovení § 12 odst. 4 Autorského zákona. Zadavatel je oprávněn užít autorské dílo, na které se vztahuje Licence podle této Smlouvy, i jinými způsoby než způsoby dle předchozí věty.

9.4. Dodavatel poskytuje Zadavateli Licenci podle této Smlouvy jako úplatnou. Strany se výslovně dohodly, že odměna za poskytnutí Licence podle této Smlouvy Dodavatelem Zadavateli je obsažena v Ceně za Dílo a tvoří **dvacet procent (20 %) z Ceny za Dílo**. Dodavateli nevzniká právo na jakékoliv jiné plnění v souvislosti s poskytnutím Licence podle této Smlouvy.

9.5. Dodavatel tímto závazně prohlašuje, že je podle právních předpisů oprávněn poskytnout Zadavateli Licenci v rozsahu a za podmínek stanovených v této Smlouvě, tedy zejména, že v souladu s Autorským zákonem a Občanským zákoníkem získal souhlasy dotčených osob nebo zaměstnanců Dodavatele k poskytnutí Licence v rozsahu a za podmínek dle této Smlouvy ani není na základě příslušných licenčních ujednání se svými Poddodavateli nebo jinými osobami omezen v poskytnutí Licence v rozsahu a za podmínek sjednaných v této Smlouvě. Ukáže-li se prohlášení Dodavatele podle

tohoto **odstavce 9.7** Smlouvy jako nepravdivé, zavazuje se Dodavatel zahájit bez zbytečného odkladu nezbytné právní kroky a postupy k tomu, aby Licence byla poskytnuta v rozsahu a za podmínek sjednaných Stranami v této Smlouvě.

9.6. Zadavatel je oprávněn libovolně měnit, upravovat či jinak zasahovat do zdrojového kódu Počítačového programu, který Dodavatel předal Zadavateli dle této Smlouvy. Dodavatel se zavazuje, že toto z tohoto jednání neplynou pro Zadavatele žádné další povinnosti.

9.7. Pokud dojde v důsledku činnosti, ke které je povinen Dodavatel, ke změně, úpravě či jinému zásahu do zdrojového kódu Počítačového programu nebo do zdrojového kódu softwaru, který se stal součástí Počítačového programu, způsobujícího jeho změnu, zavazuje se tímto Dodavatel předat Zadavateli v sídle Zadavatele na datovém nosiči aktuální verzi takového zdrojového kódu Počítačového programu nebo softwaru, který je jeho součástí, a to nejpozději do sedmi (7) pracovních dnů ode dne, kdy došlo k předmětné změně, úpravě či jinému zásahu do zdrojového kódu Počítačového programu nebo takového softwaru.

9.8. Dodavatel není oprávněn tuto Smlouvu co do poskytnutí Licence Zadavateli vypovědět ani od ní odstoupit.

Článek 10.
Cena a platební podmínky

10.1. Zadavatel se zavazuje zaplatit Dodavateli za plnění Dodavatele podle **článku 2** této Smlouvy způsobem a za podmínek uvedených v této Smlouvě cenu v celkové výši **2.896.000,- Kč** (slovy: dva miliony osm set devadesát šest tisíc korun českých) **bez DPH** (dále jen „Celková cena“). Celková cena je nejvyšší možná a nepřekročitelná a zahrnuje veškeré náklady Dodavatele nutné k řádnému splnění předmětu této Smlouvy, včetně nákladů spočívajících zejména v licenčních, správních či jiných poplatcích nebo odměnách třetím osobám.

10.2. Cena za Dílo je splatná po podpisu Akceptačního protokolu ohledně **Projektové etapy č. IV.** Zadavatelem;

Podmínkou splatnosti Ceny za Dílo je, že Dodavatel vystaví fakturu, jež bude daňovým dokladem a jejíž přílohou bude:

- Akceptační protokol podepsaný Zadavatelem,
- Předávací protokol podepsaný Zadavatelem, ve kterém nebudou uvedeny žádné vady a nedodělky, nebo
- Předávací protokol podepsaný Zadavatelem s uvedenými vadami či nedodělky nebránícími řádnému užívání Díla a zároveň písemný dodatek k Předávacímu protokolu ve smyslu **odstavce 8.4** této Smlouvy podepsaný Zadavatelem, z něhož bude vyplývat, že všechny tyto vady a nedodělky byly odstraněny,

a tuto fakturu i s takovou přílohou doručí Zadavateli. Faktury jsou splatné ve lhůtě uvedené v **odstavci 10.3** této Smlouvy.

10.3. Zadavatel je povinen uhradit Dodavateli řádně vystavenou fakturu nejpozději do třiceti (30) dnů ode dne doručení předmětné faktury Zadavateli.

10.4. Faktura musí obsahovat též

1) číslo této Smlouvy,

2) název projektu podle této Smlouvy, tj. „*Správa identit – Identity Management*“,

3) identifikaci její přílohy uvedené v **odstavci 10.2** této Smlouvy,

a dále veškeré náležitosti daňového dokladu uvedené v ustanoveních § 29 a § 29a Zákona o DPH a informace uvedené v ustanovení § 435 odst. 1 Občanského zákoníku.

10.5. Pokud faktura nebude obsahovat náležitosti nebo přílohy podle této Smlouvy nebo náležitosti uvedené ve faktuře či jejích přílohách budou nesprávné, nepřesné či neúplné, je Zadavatel oprávněn takovou fakturu vrátit Dodavateli k opravě či doplnění. Odesláním takové faktury Dodavateli zaniká povinnost Zadavatele fakturu uhradit, a to s účinky od počátku. Dodavatel je povinen Zadavatelem vrácenou fakturu opravit či doplnit tak, aby splňovala požadavky sjednané v této Smlouvě, a takto opravenou či doplněnou fakturu odeslat zpět Zadavateli. Dnem doručení řádně opravené či doplněné faktury splňující požadavky sjednané v této Smlouvě Zadavateli počíná běžet nová lhůta její splatnosti v délce uvedené v **odstavci 10.3** této Smlouvy.

10.6. Veškeré úhrady faktur a jiné platby peněžitých částek podle této Smlouvy budou probíhat v korunách českých. Dodavatel je oprávněn přičíst k částce fakturované Zadavateli na základě této Smlouvy daň z přidané hodnoty (DPH) ve výši podle právních předpisů platných a účinných ke dni uskutečnění zdanitelného plnění.

Článek 11.
Smluvní pokuty

11.1. Dodavatel se zavazuje zaplatit Zadavateli smluvní pokutu ve výši **0,05 % z Ceny za Dílo** za každý i započatý den prodlení Dodavatele s dokončením Díla nejpozději do dvaceti čtyř (24) měsíců ode dne uzavření této Smlouvy.

11.2. Dodavatel se zavazuje zaplatit Zadavateli smluvní pokutu ve výši **0,025 % z Ceny za Dílo** za každý i započatý den prodlení Dodavatele s ukončením kterékoli z Projektových etap č. 1, 2, 3, 4 v termínech podle Časového harmonogramu, a to vždy **počínaje třicátým (30.) dnem** trvání takového prodlení.

11.3. Uvede-li Zadavatel do Předávacího protokolu vady či nedodělky nebránící řádnému užívání Díla a Dodavatel je neodstraní ve lhůtě uvedené v Předávacím protokolu, a v případě neuvedení takové lhůty do třiceti (30) dnů ode dne vyhotovení Předávacího protokolu, zavazuje se Dodavatel zaplatit Zadavateli za každý i započatý den trvání

prodlení s odstraněním předmětných vad či nedodělků smluvní pokutu ve výši **0,025 % z Ceny za Dílo**.

11.4. Dodavatel se zavazuje zaplatit Zadavateli smluvní pokutu ve výši **10 % z Ceny za Dílo** za jakékoliv porušení pravdivosti prohlášení Dodavatele uvedeného v **odstavci 9.1** této Smlouvy, a dále smluvní pokutu ve výši **400 000,- Kč (slovy: čtyři sta tisíc korun českých)** za každý i započatý měsíc trvání nepravdivosti prohlášení Dodavatele uvedeného v **odstavci 9.1** této Smlouvy, a to počínaje třicátým (30.) dnem trvání takové nepravdivosti prohlášení Dodavatele.

11.5. Dodavatel se zavazuje zaplatit Zadavateli smluvní pokutu ve výši **5 % z Ceny za Dílo** za jakékoliv porušení povinnosti Dodavatele předat Zadavateli aktuální elektronické verze zdrojových kódů uvedené v **odstavci 8.5 bodě (i.) nebo (ii.)** této Smlouvy nebo v **odstavci 9.9** této Smlouvy, a dále smluvní pokutu ve výši **200 000,- Kč (slovy: dvě stě tisíc korun českých)** za každý i započatý měsíc trvání porušení jakékoliv povinnosti Dodavatele uvedené v tomto **odstavci 11.5** této Smlouvy, a to počínaje patnáctým (15.) dnem trvání takového porušení povinnosti Dodavatele.

11.6. Dodavatel se zavazuje zaplatit Zadavateli smluvní pokutu ve výši **1 000 000,- Kč (slovy: jeden milion korun českých)** za každé jednotlivé porušení povinnosti Dodavatele zachovávat mlčenlivost o Důvěrných informacích a uchovávat Důvěrné informace v tajnosti podle **článku 13** této Smlouvy.

11.7. Dodavatel se zavazuje zaplatit Zadavateli smluvní pokutu ve výši **1 000 000,- Kč (slovy: jeden milion korun českých)**, použije-li jako poddodavatele jinou osobu než Poddodavatele ve smyslu **odstavce 14.1** této Smlouvy nebo bez předchozího písemného souhlasu změní Poddodavatele, a to za každou takovou osobu.

11.8. Dodavatel se zavazuje zaplatit Zadavateli smluvní pokutu ve výši **1 000 000,- Kč (slovy: jeden milion korun českých)** za porušení povinnosti Dodavatele ve smyslu **odstavce 16.7** této Smlouvy udržovat po celou dobu poskytování plnění podle této Smlouvy a po celou dobu trvání Záruční doby v platnosti pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě, a dále, počínaje třicátým (30.) dnem trvání porušení takové povinnosti Dodavatele, smluvní pokutu ve výši **300 000,- Kč (slovy: tři sta tisíc korun českých)** za každý i započatý kalendářní měsíc trvání předmětného porušení.

11.9. Strany se dohodly, že celková výše smluvních pokut zaplacených Dodavatelem podle této Smlouvy nepřekročí částku rovnající se Celkové ceně podle **odstavce 10.1** této Smlouvy.

11.10. Dodavatel je povinen zaplatit Zadavateli smluvní pokutu podle **odstavců 11.6 až 11.9** této Smlouvy i tehdy, došlo-li k ukončení této Smlouvy co do poskytování Služeb a Dodavatel neodstraní včas vadu, na kterou se vztahuje záruka dle **odstavce 12.1** této Smlouvy.

11.11. Ujednáním ani zaplacením jakékoli smluvní pokuty podle tohoto **článku 11** není dotčeno právo Zadavatele na náhradu škody a nemajetkové újmy v plné výši vedle smluvní pokuty.

Článek 12.
Záruka za jakost

12.1. Dodavatel tímto ve smyslu ustanovení § 2619 Občanského zákoníku zaručuje, že Dílo si po dobu dvou (2) let ode dne převzetí Díla Zadavatelem (dále jen „**Záruční doba**“) zachová veškeré technické podmínky, specifikace, funkcionalitu, vlastnosti a parametry uvedené v této Smlouvě, jejích přílohách a Projektové dokumentaci.

12.2. Dodavatel je povinen odstranit vadu, na kterou se vztahuje záruka podle **odstavce 12.1** této Smlouvy, v reakční době podle důležitosti příslušného servisního požadavku Zadavatele, a to bez ohledu na to, zda došlo k ukončení této Smlouvy co do poskytování Služeb.

12.3. Záruční doba se prodlužuje o dobu, po kterou mělo Dílo vadu bránící jeho řádnému užívání Zadavatelem.

12.4. Dodavatel se zavazuje uhradit Zhotoviteli náklady, které Zadavatel účelně vynaložil při uplatnění práva z vady, a jakoukoliv újmu, která Zadavateli vznikla v důsledku vady.

Článek 13.
Důvěrné informace

13.1. Dodavatel se zavazuje zachovávat mlčenlivost o všech informacích a skutečnostech, které mu Zadavatel v ústní, elektronické, písemné nebo jakékoliv jiné podobě zpřístupnil při jednání o obsahu této Smlouvy či po jejím uzavření a týkají se zejména dodavatelů, poddodavatelů, zákazníků anebo obchodních či finančních plánů, strategií, návrhů, příležitostí, záměrů anebo koncepcí Zadavatele, a dále skutečnosti a informace, které přímo či nepřímo souvisejí s plněním této Smlouvy, obsahem této Smlouvy anebo Zadavatelem, nebo které jsou takového charakteru, že by jejich zveřejnění mohlo Zadavateli způsobit škodu či újmu, či jsou jako důvěrné Zadavatelem označeny, anebo které ve smyslu ustanovení § 504 Občanského zákoníku tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení (dále jen „**Důvěrné informace**“). Dodavatel je povinen uchovávat Důvěrné informace v tajnosti.

13.2. Dodavatel se zavazuje provést veškerá možná technická, organizační a jiná potřebná opatření k tomu, aby vyloučil anebo v co nejvyšší míře zamezil úniku Důvěrných

informací či získání Důvěrných informací třetí osobou. Dodavatel se zavazuje nezpřístupnit Důvěrné informace v jakékoliv formě třetí osobě.

13.3. K porušení povinnosti zachovávat mlčenlivost o Důvěrných informacích a uchovávat je v tajnosti podle této Smlouvy však nedojde v případě, že

a) poskytnutí Důvěrné informace je Dodavateli uloženo na základě zákona, přímo použitelného předpisu Evropské unie či vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament České republiky souhlas a jíž je Česká republika vázána; nebo

b) k poskytnutí konkrétní Důvěrné informace získal Dodavatel předchozí písemný souhlas Zadavatele; nebo

c) Důvěrná informace je Dodavatelem poskytnuta osobě, která má zákonem uloženou povinnost mlčenlivosti; nebo

d) Důvěrná informace se stane veřejně přístupnou jinak než porušením povinnosti Dodavatele zachovávat mlčenlivost o takové Důvěrné informaci nebo ji uchovávat v tajnosti podle této Smlouvy.

Pokud Dodavatel v souvislosti s plněním této Smlouvy získá informace či údaje, které budou osobními údaji ve smyslu Zákona o ochraně osobních údajů, je povinen přijmout taková technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu neoprávněných osob k těmto osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

13.4. Uveřejnění smlouvy v registru smluv:

- Smluvní strany berou na vědomí, že tato smlouva podléhá uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „ZRS"), a současně souhlasí se zveřejněním údajů o identifikaci smluvních stran, předmětu smlouvy, jeho ceně či hodnotě a datu uzavření této smlouvy.
- Zaslání smlouvy správci registru smluv k uveřejnění v registru smluv zajišťuje obvykle SŽDC. Nebude-li tato smlouva zaslána k uveřejnění a/nebo uveřejněna prostřednictvím registru smluv, není žádná ze smluvních stran oprávněna požadovat po druhé smluvní straně náhradu škody ani jiné újmy, která by jí v této souvislosti vznikla nebo vzniknout mohla.

13.5. Obchodní tajemství a neuveřejňované informace:

- Smluvní strany výslovně prohlašují, že údaje a další skutečnosti uvedené v této smlouvě, vyjma částí označených ve smyslu následujícího odstavce této smlouvy, nepovažují za obchodní tajemství ve smyslu ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „obchodní tajemství"), a že se nejedná ani o informace, které nemohou být v registru smluv uveřejněny na základě ust. § 3 odst. 1 ZRS.

– Jestliže smluvní strana označí za své obchodní tajemství část obsahu smlouvy, která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, nese tato smluvní strana odpovědnost, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, která ze stran smlouvu v registru smluv uveřejnila. S částmi smlouvy, které druhá smluvní strana neoznačí za své obchodní tajemství před uzavřením této smlouvy, nebude SŽDC jako s obchodním tajemstvím nakládat a ani odpovídat za případnou škodu či jinou újmu takovým postupem vzniklou. Označením obchodního tajemství ve smyslu předchozí věty se rozumí doručení písemného oznámení druhé smluvní strany SŽDC obsahujícího přesnou identifikaci dotčených částí smlouvy včetně odůvodnění, proč jsou za obchodní tajemství považovány.

Článek 14.
Poddodavatelé

14.1. Dodavatel je oprávněn splnit část plnění podle této Smlouvy prostřednictvím třetí osoby pouze v případě, že poddodavatelem je osoba uvedená v Nabídce nebo osoba, s níž Zadavatel vyslovil předchozí písemný souhlas (dále jen „**Poddodavatel**“). Dodavatel je oprávněn změnit Poddodavatele pouze s předchozím písemným souhlasem Zadavatele.

14.2. Plní-li Dodavatel část plnění podle této Smlouvy prostřednictvím Poddodavatele, odpovídá tak, jako by plnil sám.

14.3. Poskytne-li Dodavatel Důvěrné informace svému Poddodavateli, neporuší tím svoji povinnost zachovávat mlčenlivost o Důvěrných informacích a zachovávat je v tajnosti dle **článku 13** této Smlouvy. Dodavatel je však povinen zajistit, aby Poddodavatel byl vůči Dodavateli smluvně zavázán k ochraně Důvěrných informací alespoň v rozsahu podle **článku 13** této Smlouvy. Dodavatel je vůči Zadavateli odpovědný za to, že Poddodavatel zajistí ochranu Důvěrných informací alespoň v rozsahu podle **článku 13** této Smlouvy. Vyzrazení Důvěrných informací Poddodavatelem či jejich únik od něj se pro účely této Smlouvy považují za vyzrazení Důvěrných informací Dodavatelem.

Článek 15.
Odstoupení od Smlouvy

15.1. Zadavatel je oprávněn odstoupit od této Smlouvy, pokud Dodavatel poruší tuto Smlouvu podstatným způsobem ve smyslu ustanovení § 2002 Občanského zákoníku. Dodavatel poruší tuto Smlouvu podstatným způsobem zejména tehdy, pokud

a) Dodavatel poruší svoji povinnost ukončit jakoukoli Projektovou etapu podle Časového harmonogramu, a nesplní ji ani v dodatečné lhůtě třiceti (30) dnů od výzvy Zadavatele k nápravě;

b) Dílo bude vykazovat vady či nedodělky nebránící řádnému užívání Díla a tyto vady a nedodělky nebudou odstraněny ani ve lhůtě uvedené v Předávacím

protokolu, a v případě neuvedené takové lhůty do třiceti (30) dnů od vyhotovení předmětného Předávacího protokolu;

c) Dodavatel poruší svoji povinnost

(i.) předat Zadavateli aktuální elektronické verze zdrojových kódů uvedené v **odstavci 8.5 bodě (i.) nebo (ii.)** této Smlouvy nebo v **odstavci 9.7** této Smlouvy, nebo

(ii.) i přes poskytnutí dodatečné lhůty předat Zadavateli veškeré přípravné koncepční materiály, uživatelské příručky a další relevantní dokumenty, jakož i veškeré podklady a informace potřebné k výkonu Licence;

d) prohlášení učiněné Dodavatelem podle **odstavce 9.7** této Smlouvy se ukáže nepravdivým a Dodavatel jej neučiní pravdivým ani do čtyřiceti pěti (45) dnů poté, co byl Zadavatelem vyzván k nápravě, nebo

e) Dodavatel poruší svoji povinnost podle **odstavce 17.6** této Smlouvy udržovat po celou dobu poskytování plnění podle této Smlouvy a po celou dobu trvání Záruční doby v platnosti pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě, a porušení předmětné povinnosti trvá více než třicet (30) dnů ode dne, kdy byl Zadavatelem vyzván k nápravě.

15.2. Aniž by tím bylo dotčeno právo Zadavatele odstoupit od této Smlouvy podle jejího **odstavce 15.1**, je kterákoliv Strana oprávněna odstoupit od této Smlouvy pouze tehdy, pokud

a) druhá Strana na sebe jako dlužník podá insolvenční návrh ve smyslu ustanovení § 97 a násl. Insolvenčního zákona;

b) příslušný insolvenční soud pravomocně rozhodne ve smyslu ustanovení § 136 a násl. Insolvenčního zákona o tom, že druhá Strana je v úpadku nebo že jí úpadek hrozí;

c) příslušný správce daně rozhodne ve smyslu ustanovení § 106a Zákona o DPH o tom, že druhá Strana je nespolehlivým plátcem; nebo

d) povinná Strana této Smlouvy je v prodlení s plněním svého peněžitého závazku o více než devadesát (90) kalendářních dnů, a tento svůj závazek nesplní ani v dodatečně lhůtě poskytnuté jí v písemné výzvě oprávněnou Stranou. Délka dodatečné lhůty nesmí být kratší než třicet (30) kalendářních dnů.

15.3. Strany se tímto dohodly a výslovně souhlasí s tím, že Dílo má pro Zadavatele ve smyslu ustanovení § 2004 odst. 2 věta druhá Občanského zákoníku význam pouze jako celek. Pokud kterákoliv Strana odstoupí od této Smlouvy přede dnem předání a převzetí Díla, zruší se tím tato Smlouva jako celek s účinky od počátku. V takovém případě jsou Strany povinny vrátit si navzájem plnění přijatá na základě této Smlouvy, a to nejpozději do třiceti (30) kalendářních dnů ode dne zrušení této Smlouvy na základě odstoupení. Dodavatel není oprávněn započíst si peněžitou hodnotu toho plnění, které

mu v důsledku odstoupení od Smlouvy nelze vrátit, oproti plnění, které je povinen vrátit Zadavateli.

15.4. Odstoupení od Smlouvy se nedotýká práva Stran na zaplacení smluvní pokuty, úroků z prodlení, práva Stran na náhradu škody vzniklé z porušení smluvní povinnosti, ani ujednání, která mají vzhledem ke své povaze zavazovat Strany i po odstoupení od Smlouvy.

Článek 16.
Kontaktní osoby a kontaktní údaje Stran

16.1. Pokud není v této Smlouvě, jejích přílohách nebo Projektové dokumentaci stanoveno jinak a nevyžaduje-li tato Smlouva či zákon písemnou formu právního jednání, jsou Strany povinny v souvislosti s plněním Smlouvy komunikovat výhradně prostřednictvím následujících kontaktních osob a adres:

a) Kontaktní osoby Dodavatele:

Jméno a příjmení: xxxxxxxxxxxxx
Telefonní číslo: xxxxxxxxxxxxx
Emailová adresa: xxxxxxxxxxxxx

b) Kontaktní osoby Zadavatele:

Jméno a příjmení: xxxxxxxxxxxxx

Telefonní číslo: xxxxxxxxxxxxx
Emailová adresa: xxxxxxxxxxxxx

16.2. Vyžaduje-li tato Smlouva či zákon písemnou formu právního jednání, jsou Strany povinny si veškeré písemnosti zasílat doporučenou poštou, osobním předáním či emailovou zprávou se zaručeným elektronickým podpisem na následující kontaktní adresy:

a) Kontaktní adresa Dodavatele:

Název: xxxxxxxxxxxxx
Adresa: Sokolovská 131/86, 186 00 Praha 8
K rukám: xxxxxxxxxxxxx
Emailová adresa: xxxxxxxxxxxxx

b) Kontaktní adresa Zadavatele:

Název: **Správa železniční dopravní cesty, státní organizace**

Adresa: Dlážděná 1003/7, 110 00 Praha 1 - Nové Město,
K rukám: xxxxxxxxxxxxx
Emailová adresa: xxxxxxxxxxxxx

16.3. Dokud Strana neoznámí písemně druhé Straně změnu výše uvedené kontaktní osoby nebo adresy, je druhá Strana oprávněna komunikovat výhradně prostřednictvím dosavadních kontaktních osob a adres či na adresu uvedenou v záhlaví této Smlouvy či

v obchodním rejstříku. Změna kontaktních osob a adres není dle dohody Stran považována za změnu Smlouvy.

16.4. Splnila-li odesílající strana požadavky stanovené v tomto **článku 16** této Smlouvy, je zásilka obsahující písemnost považována za doručenou i odmítnutím jejího převzetí ze strany adresáta, marným uplynutím lhůty pro její uložení na poště či jejím vrácením jako nedoručitelné.

Článek 17.
Povinnosti Dodavatele a součinnost Stran

17.1. Dodavatel prohlašuje, že mu jsou známy všechny požadavky Zadavatele týkající se technických podmínek, specifikace, funkcionality, vlastností a parametrů Díla uvedených v **příloze č. 1** této Smlouvy, a že ke dni podpisu této Smlouvy převzal od Zadavatele veškerou dokumentaci a získal veškeré informace potřebné pro navržení, zhotovení a Implementaci Díla.

17.2. Dodavatel je povinen chránit oprávněné zájmy Zadavatele a postupovat v souladu s jeho pokyny a vnitřními předpisy, pokud s nimi byl seznámen.

17.3. Dodavatel je povinen udržovat v platnosti veškerá osvědčení a certifikáty stanovené pro jeho kvalifikaci v Zadávací dokumentaci a udržovat v pravdivosti veškerá prohlášení učiněná v souvislosti s Veřejnou zakázkou nebo touto Smlouvou.

17.4. Dodavatel je povinen navrhnout, zhotovit a Implementovat Dílo výhradně samostatně. Zadavatel poskytne Dodavateli na základě jeho písemné žádosti pouze nezbytně nutnou součinnost pro plnění povinností Dodavatele. V případě pochybností se má za to, že součinnost není nezbytně nutná. Dodavatel je při plnění této Smlouvy povinen provádět veškeré činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz Zadavatele ani jeho pracovišť.

17.5. Dodavatel je povinen na žádost Zadavatele poskytnout nevyšší možnou součinnost každé třetí osobě, která bude pro Zadavatele zhotovovat, implementovat, servisovat a/nebo udržovat v provozu software, který bude propojen a/nebo bude jakkoliv spolupracovat s Počítačovým programem.

17.6. Dodavatel je při plnění této Smlouvy povinen předložit Zadavateli zprávu o stavu plnění této Smlouvy nebo informaci o jakékoliv skutečnosti související s touto Smlouvou, a to kdykoliv k žádosti Zadavatele a v jím stanovené lhůtě.

17.7. Dodavatel je povinen udržovat po celou dobu poskytování plnění podle této Smlouvy a po celou dobu trvání Záruční doby v platnosti pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě, přičemž třetí osobou se po účely tohoto ustanovení rozumí i Zadavatel, a limit pojistného plnění (za jednu pojistnou událost) vyplývající z příslušné pojistné smlouvy nesmí být nižší než **3 000 000,- Kč (slovy: dvacet milionů korun českých)**. Doklad prokazující toto pojištění tvoří **přílohu č. 2** této Smlouvy.

17.8. Zadavatel je za podmínek stanovených Zákonem o veřejných zakázkách oprávněn vyžádat si písemně u Dodavatele poskytnutí dalších plnění souvisejících s předmětem této Smlouvy (dále jen „**Další plnění**“). Dodavatel je povinen nejpozději do dvaceti (20) kalendářních dnů ode dne, kdy obdržel žádost Zadavatele o Další plnění, vyhotovit písemný návrh podmínek poskytování Dalšího plnění včetně navržení technického řešení a rozsahu poskytnutí takového plnění, jeho časového harmonogramu, ceny a podmínek její úhrady, a v případě zájmu Zadavatele uzavřít se Zadavatelem za navržených podmínek smlouvu o poskytnutí takového Dalšího plnění.

Článek 18.

Závěrečná ustanovení

18.1. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Stranami a účinnosti nabývá nejdříve dnem jejího uveřejnění v Registru smluv.

18.2. Tato Smlouva může být měněna pouze písemně formou vzestupně číslovaných dodatků.

18.3. Dodavatel není oprávněn bez předchozího písemného souhlasu Zadavatele postoupit žádnou pohledávku podle této Smlouvy ani tuto Smlouvu třetí osobě.

18.4. Dodavatel není oprávněn bez předchozího písemného souhlasu Zadavatele započítat žádnou svoji pohledávku vůči pohledávce Zadavatele za Dodavatelem.

18.5. Strany se dohodly, že ustanovení § 1764 věta druhá, § 1765 a § 1766 Občanského zákoníku se na smluvní vztah založený touto Smlouvou nepoužijí.

18.6. V případě, že se kterékoli ustanovení této Smlouvy ukáže neplatným, neúčinným či nevymahatelným, zavazují se Strany bez zbytečného odkladu nahradit takové neplatné, neúčinné či nevymahatelné ustanovení ustanovením novým, které bude platné, účinné a vymahatelné a zachová v nejvyšší možné míře účel původního ustanovení.

18.7. Tato Smlouva se řídí českým právem, zejména Občanským zákoníkem. Strany tímto vylučují aplikaci obecně zachovávaných obchodní zvyklostí a zvyklostí zachovávaných v příslušných odvětvích na tuto Smlouvu.

18.8. Strany se dohodly, že veškeré spory z této Smlouvy budou řešeny před věcně a místně příslušným soudem dle sídla Zadavatele.

18.9. Jednacím jazykem mezi Zadavatelem a Dodavatelem bude pro veškerá plnění vyplývající z této Smlouvy výhradně čeština, a to včetně veškeré dokumentace vztahující se k předmětu této Smlouvy.

18.10. Tato Smlouva je sepsána ve čtyřech (4) vyhotoveních, z nichž každá Strana obdrží po dvou (2) vyhotoveních.

18.11. Nedílnou součást této Smlouvy tvoří její

příloha č. 1 - Detailní technická specifikace

příloha č. 2 – Doklad o pojištění dle čl. 17.7. této Smlouvy

příloha č. 3 – Seznam poddodavatelů

Strany tímto prohlašují, že si text této Smlouvy přečetly, že jejímu obsahu plně rozumí, a že tato Smlouva nebyla uzavřena za nápadně nevýhodných podmínek, pod tlakem či v tísni, na důkaz čeho umísťují oprávnění zástupci Stran níže své podpisy.

Za Zadavatele:

V Praze, dne 1. 10. 2018

Správa železniční dopravní cesty, státní organizace
Jméno: **Tomáš Drmola, MBA**
Funkce: náměstek GŘ pro správu majetku

Za Dodavatele:

V Praze, dne 15. 10. 2018

ČD – Informační Systémy, a.s.

Jméno: **Ing. Tomáš Vacek**
Funkce: člen představenstva

Jméno: **Ing. Miloslav Kopecký**
Funkce: člen představenstva

Tato smlouva byla uveřejněna prostřednictvím registru smluv dne .....

IDM

Identity management

Technická specifikace

1 Obsah

Tato technická specifikace v bodech 2 - 5 popisuje požadavky, které jsou kladeny na informační systém identity managementu, které musí obecně splňovat, byť nejsou součástí dodávky uvedené v bodě 6 a nebudou implementovány v rámci této veřejné zakázky.

2 Obecná specifikace

2.1 Obecný popis přínosů po zavedení IdM:

- Nepopíratelná odpovědnost - jednoznačná identifikace uživatele oproti identitě.
- Správa přístupů a oprávnění do všech prostředků v SŽDC (IS, aplikace, systémy atd.).
- Správa identit a uživatelů přistupujících k systémům a prostředkům SŽDC.
- Správa přidělování oprávnění uživatelům.
- Evidence všech rolí oprávnění (aplikačních rolí) všech systémů a aplikací a identit, jejich uživatelů včetně přidělených oprávnění.
- Omezení vlivu lidského faktoru a automatizace procesů spojených s nástupy, změnami pozic a výstupy zaměstnanců a externích pracovníků.
- Zavedení schvalovacích procesů do řízení života identit, přidělování oprávnění i samotného zavádění do koncových systémů.
- Naplnění podmínky zákona o kybernetické bezpečnosti.
- Centralizace správy uživatelů napříč IT systémy.
- Úspora práce administrátorů zvýšením automatizace.
- Reporting aktuálního stavu uživatelských účtů a zpětný audit.
- Časově omezené přidělování přístupů a ukončování uživatelů.
- Zavedení business rolí ve vazbě na procesní analýzu.
- Omezení chyb na vstupu informací o uživatelích.
- Eliminace manuálních zásahů a eliminace chyb obsluhy.
- Recertifikace existujících oprávnění uživatelů.
- Automatizované řízení přidělování oprávnění od schválení až po zavedení do koncového systému.
- Logování a monitorování veškerých změn oprávnění, včetně exportu logů mimo dosah administrátorů IdM.

2.2 Zkratky a pojmy

SŽDC	Správa železniční dopravní cesty, státní organizace
IdM	Identity Management
MS AD, AD	Adresářová služba Microsoft Active Directory
PPV	Pracovněprávní vztah
SoD	Segregation of Duties, kontrola konfliktních oprávnění
KS	Koncový systém
WS	Webová služba
Konektor	Komponenta umožňující připojení koncových systémů, nebo autoritativních zdrojů dat.
Autoritativní zdroje dat	Aplikace, které evidují všechny pracovníky a jejich PPV, organizační strukturu atd.
Liferay	Portálové řešení napříč organizací SŽDC
Exchange	Emailové řešení v SŽDC
Certifikace, Recertifikace, někdy také Atestace	Smyslem certifikace je v pravidelných intervalech ověřovat, zda uživatel má přiděleny stále ta oprávnění, která má mít vzhledem ke své pozici, projektu či procesu, který vykonává. Nadbytečná oprávnění jsou po ukončení certifikace odebrána. Proces certifikace je možné chápat jako dodatečnou kontrolu automatických rutin pomocí lidského faktoru, kterým je například nadřízený uživatele nebo auditor.
Koncový systém, koncová aplikace	Aplikace napojená (přímo nebo nepřímo pomocí notifikací) na IdM.
Rekonciliace	Při rekonciliaci se prochází všechny uživatelské účty na koncovém systému a na základě definovaných akcí se aktualizují identity uživatelů v Identity Manageru. Jde o uvedení účtů do souladu s IdM. Tedy účtům v koncových systémech se přidělují vlastníci (identity IdM) na základě logických podmínek např. korelace uživatelského jména, emailu apod. Účty bez vlastníka jsou reportovány, nebo rovnou mazány z koncového systému (podle nastavení IdM). Procesem rekonciliace je vynucen soulad a řád v koncových systémech.
Entitlement	Schopnost nebo nárok přistupovat ke službě či zdroji. Příklad: nový zaměstnanec má nárok (entitlement) na přístup k firemnímu emailu. Ten je mu však přidělen až poté, co je založen v informačních systémech (proběhne provisioning) a jsou mu nastavena patřičná oprávnění.
Business Role	Samostatná entita, která v sobě nese aplikační role do koncových systémů nebo jiné business role.
Aplikační Role	Samostatná entita, která odpovídá objektu v koncovém systému (např. Skupině v Active Directory, Skupině oprávnění v koncové aplikaci).
RBAC, Role-Based Access Control	Model, ve kterém jsou uživateli přiřazeny role, které mu dávají určitý stupeň přístupu ke zdroji. Přiřazení role garantuje uživateli definovanou sadu entitlementů (nároků na oprávnění), které jsou přiřazeny buď automaticky, nebo po splnění určité podmínky, nebo na základě schválení odpovědnými osobami. Výhodou modelu RBAC je opětovná použitelnost přidělených rolí a možnost definování atributů role – např. popis.
Delegace	Je to možnost delegovat vybraný požadavek ke schválení (nebo vybranou skupinu požadavků) na jiného zvoleného schvalovatele.
Zastupování	Je to možnost nastavit zástupce pro všechny požadavky, které budou na určenou dobu směrované na jiného schvalovatele.
Autentizace	Autentizace znamená potvrzení, že uživatel požadující služby je platným uživatelem poskytovaných síťových služeb. Autentizace je dosažena pomocí představení identity a jistého pověření nebo tajemství. Mezi různé typy tajemství patří například hesla, pověření na jedno použití, digitální certifikáty nebo

	telefonní čísla (ať už volající nebo volaná).
Autorizace	Autorizace znamená udělení specifického typu služby (včetně „žádné služby“) uživateli, na základě jeho autentizace, služeb, které požaduje a aktuálního stavu systému. Autorizace může být založena na omezeních, například omezení na určité hodiny v rámci dne, nebo omezení na fyzickou polohu, nebo omezení vícenásobného přihlášení jednoho uživatele. Autorizace určuje povahu služby, která je poskytnuta uživateli. Typy služeb jsou například: filtrování IP adres, přidělení adresy, přidělení cesty, QoS, řízení šířky pásma/řízení toku, tunelování do konkrétního koncového bodu, nebo šifrování.
Eskalace	Eskalace definuje pravidla, která se mají uplatnit tehdy, pokud v určeném časovém období nedojde k rozhodnutí žádosti, nebo dojde k bezpečnostnímu incidentu. Možnosti jsou například: připomenutí emailem, postoupení na nadřízeného pracovníka, či automatické schválení/zamítnutí žádosti.
SSO	Single Sign On

2.3 Systémové požadavky

- Podpora operačního systému Windows nebo Unix.
- Jediné úložiště dat (repository), a to relační databázi Oracle 12c R1.
- Řešení, které podporuje skriptovací jazyk.
- Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC.
- Řešení podporuje kódování UTF-8 i UTF-16.
- Řešení podporuje Single sign on s možností konfigurace využívaného protokolu. Toto řešení podporuje všechny standardní protokoly, jež jsou definovány v rámci konfigurace systému.

2.4 Licence a další požadavky

- Zadavatel požaduje, aby počet licencí byl bez omezení ve všech těchto aspektech:
  1. Neomezené počty instancí produktu
  2. Neomezené počty uživatelů
  3. Neomezené počty koncových systémů
  4. Neomezené počty konektorů,
  5. Neomezené počty procesorových jader, velikost paměti a jiných hardwarových, softwarových či aplikačních parametrů.
- Součástí dodávky je i předání kompletních zdrojových kódů.

- Zadavatel požaduje možnost připojení budoucích nových koncových systémů a vložení jejich přístupových rolí a logiky do systému IdM bez dodatečných licenčních nákladů.
- Dodavatel se zaručuje, že v dodávce jsou zahrnuty licence třetích stran a používání díla jako celku nevyžaduje žádné další dodatečné náklady.
- Dodavatel se zaručuje, že při uplatnění práv třetí osobou na autorská práva nese následky případných sporů dodavatel.

- Licence opravňuje objednatele k tomu, aby:
  1. Bez omezení využíval dílo v rámci své podnikatelské činnosti
  2. Pořídil si neomezený počet kopií díla pro vlastní potřebu
  3. Sám nebo prostřednictvím třetích osob měnil, rozšiřoval a jinak upravoval dílo v souladu se svými potřebami.

3 Technické požadavky

3.1 Obecné požadavky na uživatelské rozhraní v IdM

Nabízené řešení musí splňovat následující požadavky:

- Kompletní lokalizace do českého jazyka v uživatelské úrovni, administrační prostředí je povoleno i v jazyce anglickém;
- Webové rozhraní pro administrátory i pro koncové uživatele;
- Vyhledávání libovolného obsahu v agendách podle libovolného atributu;
- Možnost grafického přizpůsobení korporátní identitě (rozhraní je možné upravovat dle potřeb zadavatele).

3.2 Autoritativní zdroje dat

Nabízené řešení musí být schopno se napojit na autoritativní zdroje dat, které mohou obsahovat:

- Zdroj pro komunity: interní a externí uživatelé, zákazníci apod.
- Možnosti napojení: CSV import, LDIF import, přímý přístup do DB, preferovány jsou webové služby

3.3 Active Directory

Nabízené řešení musí být schopno spolupracovat s Active Directory. Mezi základní parametry AD patří:

- Multidoménová a multiforestová struktura
- Možnosti napojení: LDAPS, PowerShell, ADSI, .NET, vše v zabezpečených variantách.

3.4 Autorizační model v IdM

- Autorizační model musí být založen na RBAC (Role-Based Access Control) a musí umožňovat nastavit, k jaké části uživatelského rozhraní IdM a k jakým objektům v IdM mají uživatelé přístup až do úrovně atributů.
- Autorizace v IdM se neliší od ostatních KS. Oprávnění k jednotlivým objektům a částem v IdM budou definovány v aplikačních/business rolích.
- Autorizační model v IdM musí být nastaven tak, aby IdM bylo schopno pracovat samo se sebou jako s dalším KS a zároveň vůči IdM jako KS vystupovat.

3.5 Autentizace v IdM

- Je požadováno, aby autentizace do IdM byla prováděna proti AD pomocí SSO. Základem je podpora multiforestového, resp. multidoménového modelu.

3.6 Certifikace oprávnění

Nabízené řešení musí podporovat certifikace a u nich umožnit:

- plánované (automaticky spouštěné) certifikace a certifikace na vyžádání.

- schvalování/zamítnutí přístupů jednotlivě.
- automatické akce při zamítnutí přístupu (např. zamčení účtu v aplikaci).
- definovat rozsah recertifikací (u koho, na jakých rolích, na jaké org. str.).
- logovat a reportovat stav o krocích a o výsledku recertifikace.

3.7 Delegace a zastupování

Nabízené řešení musí podporovat delegace a zastupování:

- Na definovanou dobu (od-do) nastavit zástupce pro všechny požadavky, které budou v době od-do směrované na schvalovatele; zastupování musí být aditivní – původní schvalovatel musí být stále schopen požadavek schválit stejně, jako kdyby zástup nebyl nastaven.
- Po definovanou dobu nastavit plnou zastupitelnost na zvoleného uživatele.
- Možnost nastavení delegace i na již rozpracované požadavky.

3.8 Firemní pravidla

Nabízené řešení musí mít vestavěnou možnost zavádění, vynucování a kontroly firemních pravidel a politik.

3.8.1 Politiky hesla

Nabízené řešení musí umožnit konfiguraci politiky hesel tak, aby byla v souladu s politikou hesel na SŽDC. Nastavení politiky hesel musí být plně konfigurovatelné. Politika hesel nebude automaticky načítána z AD do IdM.

Aktuální politika hesel je:

- Heslo má minimální délku dvanáct znaků.
- Password Complexity ve Windows 2012 R2/2016, popř. vyšší:
    - Heslo obsahuje alespoň tři z následujících čtyř požadavků:
        - nejméně jedno velké písmeno (A – Z),
        - nejméně jedno malé písmeno (a – z),
        - nejméně jednu číslici (0 – 9) nebo
        - nejméně jeden nealfanumerický znak (t.j. ~!@ #$%^&*_-+=`|\(){}[]:;"'<>,.?/).
    - Heslo nesmí obsahovat řetězec vlastního samAccountName (účtu), je-li jeho délka 3 a více znaků, bez ohledu na velká či malá písmena.
    - Heslo nesmí obsahovat název účtu (displayName, fullName), a to bez ohledu na velká či malá písmena. Všechny části názvu účtu oddělené mezerou nebo oddělovacími znaménky a delší než dva znaky se posuzují zvlášť.

3.8.2 Pravidla tvorby názvu účtu

Nabízené řešení musí umožnit univerzální konfigurovatelné nastavení pravidel pro název účtu - minimální a maximální délka, povolené znaky, zakázaná slova v názvu (například *admin*, *info*), kontrola na platný formát emailové adresy. Nastavení pravidel tvorby účtu musí být plně konfigurovatelné.

Aktuální pravidla pro tvorbu jména účtu v AD jsou:

- Účet (samAccountName) v Active Directory a poště je u jmenných účtů uživatelů vytvářen z příjmení bez diakritiky.
- Pokud v daném systému (doméně AD, poště) již takový účet existuje, doplní se za příjmení další rozlišovací znak, případně znaky z křestního jména, bez diakritiky.
- Po vyčerpání možností se řetězec doplní zprava nejnižší možnou číslicí od 2 výše tak, aby bylo dosaženo v daném systému jedinečnosti.
- Vyplňuje se plynule bez mezer nebo jiných oddělovacích znamének. Příjmení i jméno použité v aliasu začíná vždy velkým písmenem, např.: Novotny, NovotnyJ, NovotnyJa, NovotnyJan, NovotnyJan2, atd.

Aktuální pravidla pro tvorbu emailové adresy jsou:

- Všichni uživatelé v rámci SŽDC mají primární emailovou adresu obecně tvořenou jako <Prijmeni>@szdc.cz, kde před zavináčem vystupuje řetězec popsaný v tvorbě účtu (viz výše) ve jmenném prostoru @szdc.cz, např.: Novotny@szdc.cz, NovotnyJan2@szdc.cz.
- Speciální jednotka TÚDC má výše uvedené adresy nastaveny jako sekundární; primární adresa je obecně tvořena jako <Jmeno>.<Prijmeni>@tudc.cz, kde <Jmeno> je první křestní jméno bez diakritiky, <Prijmeni> je v případě potřeby doplněno zprava nejnižší možnou číslicí od 2 výše tak, aby bylo dosaženo v daném systému jedinečnosti, např.: Marie.Novotna@tudc.cz, Marie.Novotna2@tudc.cz atd.
- V případě, že uživatel oficiálně uvádí dvě příjmení, použijí se v emailové adrese obě, bez mezery, bez pomlčky, např.: Marie.NovotnaAbelova@tudc.cz
- V případě, že org. celek používá standard emailových adres, který zahrnuje křestní jméno, a uživatel má více křestních jmen, použije se v emailové adrese pouze první z nich, např.: Novotná Marie Anna: Marie.Novotna@szdc.cz

3.9 Rozhraní pro integraci

Nabízené řešení musí poskytovat rozhraní pro integraci a splňovat následující požadavky:

- Za pomoci Web service API (SOAP/WSDL) nebo REST API číst, nebo zapisovat všechna data a volat operace nad objekty v IdM.
- Volat ekvivalent jakékoli funkcionality, která je dosažitelná z webového rozhraní (možnost volání jen některých funkcí jádra IdM je pro tyto potřeby nedostatečná).

Rozhraní musí splňovat následující parametry:

- Umožňovat bezpečný přenos dat mezi IdM a rozhraním koncového systému (např. SSL/TLS, pro AD Kerberos nebo NTLM2).
- IdM se k rozhraní autentizuje dedikovaným technickým uživatelem.
- Aplikační rozhraní (WS SOAP, REST, Java API, Powershell apod.) nebo rozhraní datového úložiště (LDAP, DB procedury, DB tabulka).
- Návratové kódy při zpracování operace.

3.10 Požadavky na integraci

Všechny konektory musí podporovat NTLM2 nebo Kerberos.

3.10.1 Defaultní konektory

Součástí nabízeného IdM systému musí být připojení minimálně k následujícím typům aplikací pomocí konfigurace:

- Active Directory (ADSI, .NET)
- Podpora Powershell
- LDAP
- Databáze

Připojení k těmto typům systémů musí být konfigurovatelné, nesmí se jednat o vývoj nebo využití komponenty třetí strany.

3.10.2 Podpora konektorů do koncových systémů

Nabízené řešení musí podporovat vytváření a vývoj vlastních konektorů.

Jedná se minimálně o:

- Připojení k různorodým webovým službám a využití jejich metod
- Připojení k různým typům a strukturám databází a čtení a zápis dat
- Připojení pomocí LDAP

Cílem zadavatele je vytvořit na straně koncových systémů sadu standardizovaných webových služeb tak, aby různorodost konektorů do těchto koncových systémů byla co nejmenší. Připojování nových koncových systémů tak bude dosaženo pomocí již typově existujících konektorů a jejich využití.

3.11 Synchronizace a rekonciliace

Nabízené řešení musí podporovat:

- Synchronizace změn v reálném čase s odolností proti výpadkům informačních systémů - vestavěná podpora opakování propagace změn v případě neúspěchu.
- Obousměrná synchronizace dat jak z IdM do koncového systému (např. uživatele a jejich atributy), tak z koncového systému do IdM (např. role v konkrétním koncovém systému).
- Mapování atributů mezi koncovými systémy na základě pravidel/vzorců.
- Práce s komplexními (tabulky) či binárními atributy uživatele - certifikáty, fotografie, autentizační tokeny
- Rekonciliace účtů - pravidelná automatická kontrola stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu.
- Rekonciliace účtů - zaznamenání stavu účtu vzhledem k ne/existenci vlastníka v IdM.
- Rekonciliace oprávnění - pravidelná automatická kontrola stavu oprávnění na koncových systémech oproti stavu chtěnému a náprava (notifikace, zápis do logů, výmaz nadbytečných oprávnění apod.).
- Nastavení pravidel pro párování mezi identitou a účtem (například email identity na login účtu) skrze všechny koncové systémy.

3.12 Emailové notifikace

Nabízené řešení musí podporovat:

- Možnost definice šablon emailů s podporou vícejazyčnosti a HTML
- Podpora skriptovacího jazyka s možností čerpání dat z databáze
- Možnost konfigurace parametrů odesílání zpráv (SMTP server apod.)
- Odesílání pomocí SMS gateway zadavatele
- Vkládání hypertextových odkazů na konkrétní odkazované záznamy

3.12.1 Notifikované akce

Nabízené řešení musí minimálně podporovat notifikaci následujících akcí:

- vytvoření, změna, smazání identity,
- přiřazení a odebrání role,
- výzva k akci,
- zakázání a povolení uživatele,
- přejmenování uživatele,
- požadavek na schválení role a na atestaci,
- libovolné akce ve workflow.

3.13 Delegování správy

- Nabízené řešení musí podporovat delegovanou správu.
- Delegovaní správci musí mít administrátorská práva nad zvolenými komunitami, nad skupinami uživatelů nebo obecně nad definovanými objekty IdM - účelem je umožnit lokálnímu administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty).

3.14 Workflow

Nabízené řešení musí podporovat tvorbu workflow a u nich umožnit:

- Administrátor IdM musí vytvářet nové definice workflow a modifikovat stávající, pro které se používají nejčastěji základní typy procesů:
    - Procesy monitorování – systém zjišťuje stavy záznamů, atributů a při splnění podmínky nastartuje proces s upozorněním emailem.
    - Řízení toku záznamů (např.: schvalovací workflow pro business role, kde business roli reprezentuje záznam v systému) – systém automaticky přiděluje úkoly zodpovědným lidem, jak je postupně záznam zpracováván.
    - Spouštění workflow uživatelem.
- Všechny workflow mohou spouštět aplikační funkce systému nad zpracovávanými záznamy.
- Workflow dále umožňuje:
    - neomezený počet schvalovacích kroků,
    - neomezený počet schvalovatelů,
    - schválení typu „jeden z X“ a typu „všichni musí schválit“,
    - paralelní schvalování a step-by-step schvalování,
    - definici schvalovatelů na základě jejich členství v roli, funkci nebo v organizační struktuře,

    - automatické schválení na základě hodnoty atributů,
    - automatické schválení na základě pracovního místa, funkce nebo zařazení v organizaci.

- Notifikovat schvalovatele minimálně emailem.
- Zobrazit schvalovatelům přehled svých úloh.
- Úlohu schválit či zamítnout včetně uvedení zdůvodnění.
- Administrátor IdM musí být schopen pracovat se všemi úlohami (pro řešení nestandardních situací).
- Administrátor IdM musí být schopen dynamicky nastavovat workflow (pomocí GUI nebo formou skriptů) bez součinnosti dodavatele.
- Možnost definovat podmíněné kroky (například přiřadit všechny aplikační role až po změně úvodního hesla).

3.15 Rekonciliace

Nabízené řešení musí podporovat rekonciliace a u nich umožnit definovat pro každý připojený systém zvlášť:

- plánované (automaticky spouštěné) rekonciliace a rekonciliace na vyžádání,
- nastavit plán rekonciliací,
- definovat seznam rekonciliovaných objektů,
- definovat typ rekonciliovaných objektů,
- nastavit korelační pravidla,
- podporovat rekonciliaci všech typů objektů (uživatele, role, org. strukturu),
- logovat a reportovat stav výsledku rekonciliace,
- nastavit spuštění akce na základě výsledku rekonciliace (např. spuštění workflow).

3.15.1 Online a offline rekonciliace

Nabízené řešení musí kromě online řízení oprávnění a identit do připojených aplikací podporovat i tzv. offline řízení oprávnění a identit na základě manuálního potvrzení akce odpovědnou osobou nebo na základě informací získaných z exportu aplikace.

3.15.2 Hromadné akce

Nabízené řešení musí nabízet spouštění hromadných akcí, např. hromadné přiřazení rolí uživatelům, kteří vyhovují podmínkám, hromadné schvalování přidělených úkolů atp. Každá změna hromadné akce musí být auditovaná.

3.16 Reporting

Nabízené řešení musí nabízet možnost exportovat minimálně do všech následujících formátů: PDF, CSV, HTML, XML a do formátu kompatibilního s MS Word a MS Excel.

3.16.1 Audit report

Nabízené řešení musí podporovat generování auditního reportu o všech aktivitách v IdM:

- Kompletní přehled změn provedených nad identitou – například synchronizace atributů, přidělení role včetně časového omezení, změn atd.
- Kompletní přehled změn provedených nad libovolnými entitami - role, organizace, definice politik a konfigurací.
- Záznam o přihlášení (úspěšném i neúspěšném) uživatele do webového rozhraní IdM.

3.16.2 Uživatelské reporty

Nabízené řešení musí podporovat generování reportů o stavu objektů v IdM:

- Minimálně informace o tom, jaké mají identity přiřazené role a účty v koncových systémech.
- Možnost nastavit filtr pro výběr identit (např. identity patřící do zvolené organizace).

3.16.3 Report o rekonciliacích

Nabízené řešení musí podporovat generování reportů o rekonciliacích:

- Přehled účtů v koncových systémech, které jsou známy IdM.
- Možnost identifikace účtů, ke kterým nebyl v IdM nalezen vlastník.

3.16.4 Další doporučené reporty

- Seznam uživatelů IdM
- Seznam rolí přidělených identitám v IdM
- Seznam přidělených KS
- Přehled statusů identit v IdM
- Historie změn nad identitou v IdM
- Historie změn nad identitami směrem do vybraného KS
- Historie změn nad rolemi v IdM
- Historie změn nad org. strukturou v IdM
- Přehled úloh v IdM a jejich status
- Přehled spuštěných workflow v IdM
- Přehled zprocesovaných workflow v IdM
- Přehled přihlášení identit do GUI
- Přehled stavů a výsledků rekonciliací

3.17 Agendy a správa objektů

3.17.1 Uživatelé

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu uživatelů bez nutnosti instalovat dodatečný SW.
- Správu skrze integrační vrstvu, tzn. přebírání identit z autoritativních zdrojů.
- Evidence atributů identity.
- Zajištění unikátní identity.
- Zplatnění/zneplatnění identity k určitému datu.
- Přiřazení koncových systémů, rolí či organizace k identitě.
- U koncových systémů evidence uživatelských jmen ve vazbě na identitu (heslo pouze při vytvoření nového účtu).
- Vyhledávání a filtrování podle libovolného (i uživatelsky definovaného) atributu.

- Při vytvoření nového uživatelského účtu bude z bezpečnostních důvodů tento účet bez přiřazení rolí do doby změny úvodního hesla v AD (IdM nepřiřadí aplikační role dřív, než si uživatel změní úvodní heslo).

3.17.1.1 Oddělení komunit

Nabízené řešení musí podporovat oddělené komunity uživatelů. Řešení musí nabízet možnost nastavit tato omezení:

- Konfigurovat přístupová práva určená pro jednu komunitu tak, že nelze přiřadit identitám v jiné komunitě koncové systémy komunity původní;
- Do organizační struktury určené jedné komunitě nelze přiřadit identity z jiné komunity;
- Delegovat správu konkrétní komunity jinému administrátorovi;
- Delegovat správu konkrétní organizační struktury jinému administrátorovi.

3.17.1.2 Koncoví uživatelé

Nabízené řešení musí podporovat minimálně:

- Přehled přiřazených koncových systémů;
- Přehled přiřazených oprávnění (aplikačních rolí) na koncových systémech (pokud je nakonfigurováno);
- Přehled přiřazení do org. struktury;
- Schvalování či zamítnutí vznesených požadavků;
- Spouštění reportů.

3.17.1.3 Definice rolí v IdM

Níže je uveden minimální seznam rolí, které musí být podporovány v rámci IdM nástroje.

- **Administrátor IdM** - Zasahuje do poloautomatických procesů, řeší výjimečné stavy, kontroluje reporting a flow identit, plně správuje IdM. Může delegovat svá oprávnění a přidělovat oprávnění s granularitou až na jednotlivé funkce a objekty.
- **Delegovaný administrátor, Delegovaný správce** - Má administrátorská práva nad zvolenými komunitami, organizační strukturou, koncovými systémy, nad skupinami uživatelů nebo obecně nad definovanými objekty IdM. Účelem je umožnit delegovanému administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty).
- **Tvůrce business rolí -** Má všechna nezbytná práva pro tvorbu a úpravu business rolí v IdM. Může do nich zařazovat jiné business role, aplikační role a/nebo koncové systémy.
- **Přidělovatel rolí -** Má všechna nezbytná práva pro přidělování business rolí a aplikačních rolí v IdM. Může identitám v IdM přidělovat business role, aplikační role a/nebo koncové systémy.
- **Správce koncového systému** - Má všechna nezbytná práva pro úpravu definic KS v IdM a jejich aplikačních rolí.
- **Běžný uživatel** - Běžný uživatel, který má práva prohlížet informace o své identitě a přidělených prostředcích v IdM.

3.17.2 Organizační struktura

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu stromové struktury;
- Správu skrze integrační vrstvu;
- Možnost vytváření libovolného počtu stromů organizačních struktur;
- Možnost vytváření nezávislých entit (pracovní pozice, funkční místa) ve stromě;

- Možnost definovat atributy entit ve stromě;
- Možnost přiřazovat entitám ve stromě jiné objekty, minimálně uživatele, role, organizace z jiných stromů, účty v koncových systémech;
- Možnost vizualizace entit pomocí stromové struktury;
- Entity ve stromě přiřazovat k libovolnému objektu, minimálně k roli a k identitě;
- Identita nebo role může být přiřazena ve více entitách stromu zároveň;
- Identita nebo role může být přiřazena ve více stromech zároveň;
- Identita může mít různé role v různých strukturách (nadřízený v jedné organizační struktuře může být v jiné struktuře podřízený apod.);
- Možnost nastavit časové období od-do pro přiřazení identity do stromové struktury; pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení identity do stromu uplatnit.

3.17.3 Business role

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu business rolí.
- Správu skrze integrační vrstvu
- Evidenci business rolí, včetně popisných atributů.
- Business role musí být možné hierarchicky skládat
- Vazbu business rolí na uživatele obsaženého v jakékoliv komunitě či organizační struktuře, označující garanta business role. Tato vazba může být v kardinalitě 1:N ve smyslu hlavní garant, zástupce apod. Tato vazba je rozhodující ve workflow při přiřazování přístupů apod.
- Vazbu na koncové systémy přiřazené do business role v kardinalitě 1:N.
- Vazbu na konkrétní identitu (uživatele) v kardinalitě 1:N a možnost nastavení platnosti přiřazení od-do.
- Možnost nastavení platnosti business role od-do, pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení business role uplatnit.
- Při vytváření nových business rolí upozornit na duplicitní definice rolí s jejich výčtem.
- Do business rolí přiřazovat jiné business role, aplikační role, resp. koncové systémy
- Podporovat definici pravidel business rolí včetně možnosti použít regulární výrazy.
- Správu effective rights v rámci tvorby nových business rolí.
- Možnost širšího managementu business rolí.
- Při tvorbě nových business rolí je vyžadována podpora schvalovacích procesů obsahující všechny garanty jednotlivých koncových systémů.
- Delegování správy business rolí.
- Podporu pro vyhledávání duplicitních business rolí ve smyslu duplicity v přiřazení oprávnění do koncových systémů a aplikačních rolí.

3.17.4 Koncové systémy

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu koncových systému.
- Správu přes integrační vrstvu.
- Evidenci koncových systémů, včetně popisných atributů jejich funkce, umístění apod.
- Vazbu koncových systémů na uživatele obsaženého v jakékoliv komunitě, či organizační struktuře, označující garanta koncového systému. Tato vazba může být v kardinalitě 1:N ve smyslu hlavní garant, zástupce apod. Tato vazba je rozhodující ve workflow při vytváření business rolí, přiřazování přístupů apod.
- Vazbu na aplikační role přiřazené ke koncovému systému v kardinalitě 1:N.
- Vazbu na administrátora koncového systému, kterého může představovat uživatel obsažený v jakékoliv komunitě, či organizační struktuře. Tato vazba může být v kardinalitě 1:N ve smyslu hlavní administrátor, zástupce apod.

- Možnost nastavení stavu správy koncového systému na povoleno, či blokováno. Toto nastavení má přímý dopad na řízení přístupů ke koncovému systému.
- Delegování správy koncových systémů

3.17.5 Aplikační role

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu rolí (soubor oprávnění).
- Správu skrze integrační vrstvu.
- Roli je možné přiřazovat koncovým systémům.
- Možnost nastavení platnosti aplikační role s dopadem na řízení přístupů ke koncovému systému.
- Možnost nastavit další atributy přiřazení (např. dle lokality identity).
- Možnost dynamického výpočtu u schvalovací role.
- Role musí být možné hierarchicky skládat.
- Možnost systému nastavit pravidla pro vzájemně se vylučující role (tzv. SoD), musí umět reportovat a notifikovat konfliktní práva.
- Ochranu systému v případě pokusu o přiřazení konfliktní role - pokud dojde k pokusu o přiřazení role identitě, která již má jinou konfliktní roli, musí systém konflikt oznámit a vlastní přiřazení neprovede.
- Možnost recertifikace rolí - opakované spouštění schvalování.

4 Připojení koncových systémů a propagace unikátní identity

Zadavatel v rámci implementace požaduje připojení koncových systémů a propagaci unikátní identity. Připojení koncových systémů a řízení identit lze rozdělit do několika následujících bodů:

4.1 Plně automatické připojení

Plně automatické připojení ke koncovému systému splňuje tyto požadavky:

- IdM přebírá informace o identitách z autoritativního zdroje a vytváří uživatele v IdM. Na základě rozlišovacích atributů uživatele slučuje do jedné unikátní identity, kterou nadále takto propaguje.
- Na základě rozlišovacích atributů ji přiřazuje do komunit, organizačních struktur.
- Na základě rozlišovacích atributů ji přiřazuje do business rolí. Business role lze přiřazovat i ručně administrátorem, který má potřebná oprávnění.
- Na základě business rolí jsou unikátní identitě přiřazeny koncové systémy a aplikační role v koncových systémech.
- IdM automaticky skrze konektory provádí akce spojené se správou autorizace v koncových systémech.
- IdM automaticky skrze konektory provádí pravidelnou kontrolu stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu a eskalací bezpečnostního incidentu skrze workflow a notifikace.

4.2 Read-only připojení

Read-only připojení ke koncovému systému splňuje tyto požadavky:

- IdM přebírá informace o identitách z autoritativního zdroje a vytváří uživatele v IdM. Na základě rozlišovacích atributů uživatele slučuje do jedné unikátní identity, kterou nadále takto propaguje.
- Na základě rozlišovacích atributů ji přiřazuje do komunit, organizačních struktur.
- Na základě rozlišovacích atributů ji přiřazuje do business rolí. Business role lze přiřazovat i ručně administrátorem, který má potřebná oprávnění.
- Na základě business rolí jsou unikátní identitě přiřazeny koncové systémy a aplikační role v koncových systémech.
- IdM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IdM automaticky skrze konektory provádí pravidelnou kontrola stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu a eskalací bezpečnostního incidentu skrze workflow.

4.3 Offline připojení

Offline připojení ke koncovému systému splňuje tyto požadavky:

- IdM přebírá informace o identitách z autoritativního zdroje a vytváří uživatele v IdM. Na základě rozlišovacích atributů uživatele slučuje do jedné unikátní identity, kterou nadále takto propaguje.
- Na základě rozlišovacích atributů ji přiřazuje do komunit, organizačních struktur.
- Na základě rozlišovacích atributů ji přiřazuje do business rolí. Business role lze přiřazovat i ručně administrátorem, který má potřebná oprávnění.
- Na základě business rolí jsou unikátní identitě přiřazeny koncové systémy a aplikační role v koncových systémech.
- IdM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IdM neprovádí automaticky kontrolu stavu účtů na koncových systémech, ale pomocí webového rozhraní a v rámci workflow procesu umožňuje administrátorovi potvrzení splnění přiděleného úkolu.

4.4 Ruční řízení a připojení

Ruční řízení a připojení ke koncovému systému splňuje tyto požadavky:

- Administrátor s patřičným oprávněním vytváří uživatele v IdM. Na základě rozlišovacích atributů uživatele IdM kontroluje, zda nedochází k duplicitním záznamům a vytváří unikátní identitu, kterou nadále takto propaguje.
- Administrátor s patřičným oprávněním přiřazuje identitu do komunit, organizačních struktur a IdM kontroluje, zda nedochází k porušování pravidel spojených s komunitami a organizačními strukturami.
- Administrátor s patřičným oprávněním přiřazuje identitu do business rolí a IdM provádí kontrolu, zda nedochází ke konfliktním přiřazením oprávnění.
- Administrátor nemůže přiřadit identitě přímo koncový systém a aplikační roli.
- Ke správě autorizace v koncových systémech je možno využít všechny výše popsané metody správy, jedná se tedy o:
    - Plně automatickou správu
    - Read-only správu
    - Offline správu

4.5 Eskalace chyb a neplnění úkolů při správě autorizace v koncových systémech

Zadavatel požaduje konfigurovatelnou správu a eskalaci chyb při správě autorizace v koncových systémech. IdM tak musí umožňovat nastavit tyto parametry:

- Pro plně automatické připojení
  - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na administrátora IdM
  - Počet opakování pokusů spojení s koncovým systémem skrze konektory v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na garanta koncového systému a administrátora IdM.
  - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení a identifikaci akce, při které došlo k chybě.
- Pro Read-only připojení
  - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na administrátora IdM
  - Počet opakování pokusů spojení s koncovým systémem skrze konektory v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na garanta koncového systému a administrátora IdM.
  - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení a identifikaci akce, při které došlo k chybě.
- Pro Offline připojení
  - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání workflow s notifikací na administrátora IdM
  - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení a identifikace akce, při které došlo k chybě.
  - Časový interval pro splnění úkolu, notifikovaného administrátorovi.
  - Počty a intervaly pro upozornění administrátorovi o nesplnění přiděleného úkolu, před vypršením termínu splnění úkolu.
  - Při nepotvrzení splnění úkolu a vypršení termínu splnění úkolu vyvolání workflow s notifikací na garanta koncového systému a administrátora IdM.
- Pro Ruční řízení a připojení dle typu:
  - Plně automatickou správu viz výše.
  - Read-only správu viz výše.
  - Offline správu viz výše.

4.6 Operace spojené s připojením do koncových systémů

Níže je uveden rozsah operací, které musí podporovat IdM ve vztahu k rozhraní koncového systému (KS) tak, aby mohly být řízeny uživatelské účty uložené v tomto koncovém systému. Je uveden maximální rozsah operací, které ale rozhraní koncového systému nemusí podporovat. Jedná se například o zplatnění/zneplatnění účtu, změna hesla apod. Konkrétní implementaci operací rozhraní

koncového systému a jejich význam pro data určuje vlastník koncového systému. Jakékoliv operace nesmí být IdM vyžadovány ke své funkčnosti, jedná se o volitelnou možnost. U každého koncového systému bude v rámci analýzy rozhodnuto, zda a v jakém rozsahu budou operace s rolemi mezi IdM a koncovým systémem využity.

4.6.1 Vytvoření účtu

Systém IdM skrze konektor vytváří v koncovém systému nového uživatele a propaguje jeho unikátnost pomocí jedinečného identifikátoru. Dle typu uživatele a přiřazených business rolí vytváří konkrétní přístupy. Vytvoření nového uživatele v koncovém systému tak může být například metodou „Create_user“, která musí splňovat tyto podmínky:

- IdM přenáší do koncového systému unikátní identifikátor.
- IdM vytváří dle firemních pravidel a politik nové heslo, které pokud je to vyžadováno, přenáší do koncového systému.
- IdM vytváří dle firemních pravidel a politik nové uživatelské jméno, které přenáší do koncového systému.
- IdM přenáší do koncového systému všechny požadované atributy, jako jsou například: jméno, příjmení, uživatelské jméno apod.
- IdM vytváří dle firemních pravidel a politik novou emailovou adresu, kterou přenáší do koncového systému.
- IdM notifikuje uživatele o vytvoření uživatelského jména a hesla a tyto informace mu zasílá na email, nebo pomocí sms brány na mobilní telefon. V případě, že uživatel nemá ani email, ani telefon, nebo v jiném vhodném případě tyto informace zasílá přímému nadřízenému, který je identifikován skrze organizační strukturu.
- V případě, že se jedná o uživatele, který má mít účet v AD, IdM nepřiřazuje jakékoliv další business role a tím pádem přístupy do dalších koncových systémů, dokud si uživatel nezmění přidělené heslo. IdM tak kontroluje, zda bylo prvotní heslo změněno, a pokud ano, pokračuje v dalším zpracování business rolí.
- Po přiřazení všech business rolí resp. přístupů do koncových systémů, provádí IdM okamžitou kontrolu přiřazených oprávnění a v případě nesouladu provádí notifikace na administrátora IdM a garanta koncového systému, u kterého došlo k nesouladu.

4.6.2 Aktivace a deaktivace účtu

Systém IdM skrze konektor a pokud to koncový systém umožňuje, provádí aktivaci a deaktivaci konkrétního uživatele. K identifikaci používá přidělený unikátní identifikátor. Jedná se tak například o metody enable_user a disable_user, kde základní parametry jsou:

- Enable_user (unikátní identita, status)
- Disable_user (unikátní identita, status)

Výsledná podoba tak například může být:
- Enable_user (0000-00000000-000000000000000000000000000000001, -1)
- Disable_user (0000-00000000-000000000000000000000000000000001, 0)

4.6.3 Čtení informací o účtu

Systém IdM skrze konektor a pokud to koncový systém umožňuje, čte informace o zavedeném uživateli. Jedná se tak především o atributy, jako jsou například:
- Jméno
- Příjmení
- Uživatelské jméno

- Jiné atributy informačního charakteru, které se u jednotlivých koncových systémů mohou různit.

V žádném případě nelze touto metodou přenášet heslo uložené v koncovém systému, pokud koncový systém heslo ukládá.
Pro identifikaci účtu se výhradně používá jeho unikátní identifikátor.

4.6.4 Update informací účtu

Systém IdM skrze konektor umožňuje aktualizovat zadané informace v koncových systémech. Jedná se o shodné atributy, které jsou přenášeny v rámci metody vytváření účtu, a tato metoda může obsahovat i změnu hesla.
Pro identifikaci účtu se výhradně používá jeho unikátní identifikátor.

4.6.5 Přiřazení aplikačních rolí

Systém IdM skrze konektor umožňuje přiřazení aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity a unikátní ID aplikační role. Na základě volání této metody koncový systém přiřazuje aplikační roli unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.6.6 Odebrání aplikačních rolí

Systém IdM skrze konektor umožňuje odebrání aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity a unikátní ID aplikační role. Na základě volání této metody koncový systém odebírá aplikační roli unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.6.7 Odebrání všech aplikačních rolí

Systém IdM skrze konektor umožňuje odebrání všech aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity. Na základě volání této metody koncový systém odebírá všechny aplikační role unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.6.8 Seznam přiřazených aplikačních rolí

Systém IdM skrze konektor umožňuje čtení informací o všech přiřazených aplikačních rolích unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity. Na základě volání této metody koncový systém vrací seznam všech přiřazených aplikačních rolích unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.6.9 Seznam aplikačních rolí

Systém IdM skrze konektor umožňuje čtení informací o aplikačních rolích v koncovém systému. Na základě volání této metody koncový systém vrací seznam aplikačních rolí v koncovém systému.

4.6.10 Seznam uživatelů v koncovém systému

Systém IdM skrze konektor umožňuje čtení informací o všech uživatelích (unikátních identitách), které jsou v koncovém systému zavedeny. Na základě volání této metody koncový systém vrací

seznam všech unikátních identit, které jsou v systému zavedeny, spolu se všemi dostupnými atributy. Seznam těchto atributů se může lišit v závislosti na konkrétním koncovém systému.

4.7 Požadavky na dokumentaci

Všechna dokumentace musí být verzována, opatřena seznamem autorů, přehledem změn jednotlivých verzí a musí být obsahově úplná pro tu část systému, kterou popisuje. Dokumentace musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem. Požadujeme jako součást dodávky následující dokumentaci:

4.7.1 Dokumentace jádra systému

Dokumentace jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace bude obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

4.7.2 Dokumentace pro vývoj nových konektorů

Dokumentace pro vývoj nových konektorů bude obsahovat kompletní popis tvorby nových konektorů, včetně vazeb na systém IdM tak, aby nově vzniklý konektor bylo možné zapojit do všech již existujících procesů v IdM.

4.7.3 Příručka administrátora IdM

Příručka bude distribuována úzké skupině uživatelů, správců systému. Musí obsahovat kompletní popis všech funkcí pro práci s administrací IdM. Příručka bude využívána jako materiál pro školení nových administrátorů. Příručka musí obsahovat solidně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek.

4.7.4 Uživatelská příručka

Příručka bude distribuována uživatelům. Musí obsahovat kompletní popis všech uživatelských funkcí pro práci s IdM. Příručka bude využívána jako základní materiál pro školení nových uživatelů. Příručka musí obsahovat solidně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek.

5 Další požadavky

5.1 GDPR

Výsledné dílo musí splňovat požadavky na GDPR, obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation), novou legislativu EU, která výrazně zvyšuje ochranu osobních dat.

6 Rozsah dodávky

Zadavatel požaduje dodat dílo v tomto rozsahu:

6.1 Instalace

Instalace IdM do tří nezávislých prostředí Zadavatele (Development, Test, Production). Jeden node (ne cluster) - s možností rozšíření do budoucna. Hardwarové požadavky budou upřesněny v rámci analýzy.

6.2 Napojení na autoritativní zdroj dat

Zadavatel požaduje jednosměrné napojení (čtení) na data HR SAP co by autoritativního zdroje personálních dat. Data budou zadavatelem exportována do DB tabulek ve formátu (1x pro identity, 1x pro organizace). Konsolidace dat, resp. konsolidace identit bude upřesněna v rámci před implementační analýzy a je požadována v rámci této dodávky.

6.3 Koncové systémy

Zadavatel požaduje připojení dvou koncových systémů:

- Active directory a to pomocí LDAPS, PowerShell, nebo ADSI. Možnosti napojení budou specifikovány v rámci před implementační analýzy.
- 1 kritická aplikace Zadavatele a její napojení skrze webovou službu. Přesná specifikace aplikace bude součástí před implementační analýzy.

Zadavatel požaduje plně automatické napojení, přičemž v rámci implementace bude testováno i napojení read-only a offline.

V souvislosti s koncovými systémy Zadavatel požaduje:
- Načítání uživatelů z koncových systémů.
- Načítání aplikačních rolí z koncových systémů.
- Eskalaci zjištěných nesouladů mezi koncovým systémem a IdM a to formou emailové notifikace určeným osobám. (Administrátor, Správce koncového systému, další množina uživatelů) a formou reportu.

6.4 Životní cyklus identit a další požadavky

Zadavatel požaduje implementace následujícího životního cyklu:

- Načítání personálních informací o identitách z autoritativního zdroje SAP HR v definovaných periodách, jejich konsolidaci a vytvoření unikátní identity. V případě více záznamů v SAP HR z důvodu více pracovních úvazku uživatele, vytvoří IdM z těchto záznamů unikátní identitu, kterou bude následně propagovat do koncových systémů. Konsolidace uživatelů bude prováděna dle metodiky, kterou Zadavatel předloží Dodavateli v rámci před implementační analýzy.
- Dynamické vytváření objektů organizační struktury v IdM dle organizační struktury v SAP HR.

- Dynamické vytváření uživatelů v IdM, atributy uživatele evidované IdM provázané se SAP HR, procesy (založení, aktualizace, aktivace/deaktivace identity, přejmenování, změna organizační struktury, operace s aplikačními rolemi apod.) a mechanismus generování centrálního username, password a emailové adresy. E-mailová notifikace. Doručení iniciálního hesla vedoucímu nového uživatele emailem.
- Vytvoření max. 10 Business rolí.
- Automatizace přiřazení do Business rolí na základě informací ze SAP HR. Implementace podmínky: (jestliže atribut uživatele=hodnota) tak přiřaď Business roli. Migrace max. 10 podmínek, ostatní případné podmínky budou imnplementovány ze strany Zadavatele.
- Generování unikátního ID (neměnné číslo) pro každou identitu.
- Vytváření IdM procesů v návaznosti na informace ze SAP HR a do koncových systémů (založení, aktualizace, aktivace/deaktivace identity, přejmenování, změna organizační struktury, operace s aplikačními rolemi apod.) v těchto variantách:
- První založení uživatele v koncových systémech:
    - Založení uživatele v Active Directory, nastavení atributů a přiřazení do skupin, dle Business role IdM.
    - Pozastavení procesu propagace identity do doby, než si uživatel poprvé změní heslo v Active Directory.
    - Propagace do dalších koncových systémů, založení uživatele, nastavení atributů a přiřazení do aplikačních rolí dle Business role IdM.
    - Rekonciliace.
- Aktualizace uživatele v koncových systémech:
    - Aktualizace všech atributů identity, které jsou vzájemně evidovány v IdM a koncových systémech na základě informací ze SAP HR.
- Aktivace a deaktivace v koncových systémech:
    - Pokud to koncový systém dovoluje, aktivování nebo deaktivování uživatele v koncovém systému na základě informací ze SAP HR a atributů platnost od a do.
- Přiřazení a odebrání aplikačních rolí
    - Přiřazování a odebírání aplikačních rolí v koncových systémech na základě Business rolí, nebo ručním zásahu administrátora.
- Načítání aplikační rolí z koncových systémů a eskalaci zjištěných nesouladů mezi koncovým systémem a IdM.
- Načítání uživatelů v koncových systémech a eskalaci zjištěných nesouladů mezi koncovým systémem a IdM.
- Dvou-krokové workflow pro přidání/odebrání rolí uživateli včetně schvalování.
- Rozhraní pro uživatele, ve kterém si budou moci žádat o přidělení nových aplikačních rolí.
- Vytvoření max. 5 rolí, které zajišťují autorizaci uživatele pro práci v IdM (např. administrátor, správce rolí, koncový uživatel apod., dle bodu 3.17.1.3)
- Přihlášení do IdM pomocí SSO.
- Emailovou notifikaci s ohledem na operace s uživateli, rolemi a eskalaci zjištěných nesouladů mezi koncovým systémem a IdM.
- Dodávku následujících reportů:
    - Report oprávnění, která jsou u uživatele přiřazena v koncovém systému, ale nejsou přiřazena jako role v IdM.
    - Report účtů, ke kterým existuje v IdM vlastník, ale které vznikly mimo vědomí IdM.
    - Uživatelský report, auditní report (změny provedené přes IdM), rekonciliační report.
- Školení:
    - Školení administrátora v rozsahu 1 MD a max. pěti uživatelů.
    - Školení uživatelů v rozsahu 2 MD a max. 20 uživatelů.
    - Školení vývoje nových konektorů v rozsahu 1 MD a max. 3 uživatelů.

Allianz pojišťovna, a.s.

13/SD1/015/15

Allianz

Dodatek č. 5 k pojistné smlouvě č. 400 030 963 / 01

Pojistitel: **Allianz pojišťovna, a. s.**
Ke Štvanici 656/3, 186 00 Praha 8
Česká republika
IČ: 471 15 971
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 1815

DĚKUJEME ZA ZASLÁNÍ PODEPSANÉHO DOKUMENTU ZPĚT

a

Pojistník: **ČD - Informační Systémy, a. s.**
Praha 3 - Žižkov, Pernerova 2819/2a, PSČ 130 00,
IČ: 248 29 871
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 17064

uzavírají následující dodatek k pojistné smlouvě o pojištění odpovědnosti (provozní činnost, výrobek) - Oddíl 1 a pojištění profesní odpovědnosti IT společností - Oddíl 2. Pojistná smlouva č. 400 030 963 ve znění dodatku č. 5 ze dne 11.12.2017 je úplným zněním s účinností od 01.01.2018.

Všeobecné pojistné podmínky: Pojištění se řídí zákonem č. 89/2012 Sb., občanský zákoník a Všeobecnými pojistnými podmínkami pro pojištění odpovědnosti (provozní činnost, výrobek) OSPP-03 vydanými s platností od 1. ledna 2014 (dále jen všeobecné pojistné podmínky), které jsou nedílnou součástí této pojistné smlouvy.
Pojištění se řídí zákonem č. 89/2012 Sb., občanský zákoník, Všeobecnými pojistnými podmínkami pro pojištění profesní odpovědnosti VPP-PO 1/15 vydanými s platností od 1. září 2015 (dále jen VPP) a Zvláštními pojistnými podmínkami pro pojištění profesní odpovědnosti IT společností ZPP PO IT 02/15, vydanými s platností od 01. prosince 2015 (dále jen ZPP), které jsou nedílnou součástí této pojistné smlouvy.

Pojištěný: **ČD - Informační Systémy, a. s.**
Praha 3 - Žižkov, Pernerova 2819/2a, PSČ 130 00,
IČ: 248 29 871
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 17064

Oddíl 1: Pojištění odpovědnosti (provozní činnost, výrobek)

Rozšiřující smluvní ujednání:
- pro časovou působnost pojištění
- zachraňovací náklady
- pro pojištění odpovědnosti za škodu způsobenou na užívaných nemovitostech a budovách č. 41-05
- pro pojištění vzájemných nároků
- pro pojištění odpovědnosti za škodu způsobenou na převzatých a užívaných věcech
- pro pojištění odpovědnosti za jiné majetkové škody

Pojištěná provozní činnost: dle výpisu z obchodního rejstříku vedeného Městským soudem v Praze, oddíl B, vložka 17064, platného ke dni 31. 12. 2012.
V rámci předmětu podnikání „Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona" jsou pojištěny pouze obory činností uvedené ve výpisu ze živnostenského rejstříku, platného ke dni 31. 12. 2012.

Pojištění se vztahuje též na jiné pojištěným oprávněně vykonávané činnosti, které povinnosti zápisu do obchodního rejstříku nepodléhají (včetně odpovědnosti za škodu způsobenou při pořádání odborných kurzů, školení a jiných vzdělávacích akcí včetně rekvalifikačních kurzů).

Pojištění se vztahuje též na odpovědnost pojištěného za škody nebo jiné újmy vyplývající z vlastnictví, držby, správy nebo provozu nemovitostí.

Územní platnost: Česká republika

Rozsah pojištění: Odpovědnost za škodu nebo jinou újmu z provozní činnosti uvedené v pojistné smlouvě dle čl. 2 výše uvedených všeobecných pojistných podmínek.
Odpovědnost za škodu nebo jinou újmu způsobenou vadou výrobku dle čl. 4 výše uvedených všeobecných pojistných podmínek. Toto pojištění se vztahuje pouze na výrobky pojištěného dodávané pojištěným na trh v rámci výše uvedené pojištěné provozní činnosti.

Sjednaný limit plnění:

50.000.000,- Kč	**celkový limit plnění pro odpovědnost za škodu nebo jinou újmu způsobenou provozní činnost a vadou výrobku, max. 50.000.000,- Kč pro všechny pojistné události za jedno pojistné období**
50.000.000,- Kč	pro škody na užívaných nemovitostech a budovách č. 41-05 (v rámci celkového limitu plnění), maximálně 50.000.000,- Kč pro všechny pojistné události za jedno pojistné období
50.000.000,- Kč	pro vzájemné nároky (v rámci celkového limitu plnění), maximálně 50.000.000,- Kč pro všechny pojistné události za jedno pojistné období
2.000.000,- Kč	pro škody způsobené vadou výrobku a vadou vykonané práce po jejím předání (v rámci celkového limitu plnění), maximálně 2.000.000,- Kč pro všechny pojistné události za jedno pojistné období
10.000.000,- Kč	pro škody na věcech převzatých (v rámci celkového limitu plnění), maximálně 10.000.000,- Kč pro všechny pojistné události za jedno pojistné období
2.000.000,- Kč	pro škody na věcech užívaných (v rámci celkového limitu plnění), maximálně 2.000.000,- Kč pro všechny pojistné události za jedno pojistné období
2.000.000,- Kč	pro jiné majetkové škody (újmy na jmění) (v rámci celkového limitu plnění), maximálně 2.000.000,- Kč pro všechny pojistné události za jedno pojistné období

Spoluúčast:

1.000,- Kč	pro každou pojistnou událost v případě regresů zdravotních pojišťoven, náhrad dávek nemocenského pojištění, škod na věcech převzatých a užívaných a jiných majetkových škod
20.000,- Kč	pro každou pojistnou událost v případě jiných majetkových škod
5.000,- Kč	pro každou pojistnou událost v případě ostatních škod nebo jiných újem do výše 50.000,- Kč
10%, min. 20.000,- Kč	pro každou pojistnou událost v případě ostatních škod nebo jiných újem od výše 50.001,- Kč do výše 5.000.000,- Kč
1.000.000,- Kč	pro každou pojistnou událost v případě ostatních škod nebo jiných újem od výše 5.000.001,- Kč

Oddíl 2: Pojištění odpovědnosti za škodu způsobenou profesní odpovědností IT společností

Pojištěná provozní činnost: Poskytování IT služeb v oblasti drážní dopravy a logistiky
(Pozn. pojištěná činnost může být upřesněna dle vyplněného dotazníku a požadavků klienta)

Územní platnost: Česká republika

Retroaktivní datum: 01.01.2017

Allianz pojišťovna, a.s.

Závěrečné prohlášení: Pojistník podpisem potvrzuje, že si je vědom specifického způsobu sjednání pojištění prostřednictvím na pojistiteli nezávislého poradce (pojišťovací makléř), a prohlašuje, že mu byl obsah pojištění makléřem vysvětlen, popřípadě že ho makléř upozornil na odchylky nabízeného pojištění a jeho požadavků. Podpisem smlouvy pojistník stvrzuje, že sjednané pojištění odpovídá jeho potřebám a požadavkům, případně že s tímto pojištěním na základě doporučení pojišťovacího makléře souhlasí, ač byl upozorněn na odchylky oproti svým požadavkům.

Poznámka: Tato smlouva nabývá účinnosti zveřejněním v registru smluv podle zákona č. 340/2015 Sb. Pojistník se zavazuje, že zajistí takové zveřejnění bez zbytečného odkladu po uzavření této smlouvy, nejpozději však do 20 dní od jejího uzavření a toto zveřejnění prokáže pojistiteli bez zbytečného odkladu zasláním potvrzení vydaného správcem registru smluv podle uvedeného zákona do datové schránky ID: vfcqvw.

Přílohy:
Všeobecné pojistné podmínky
Všeobecné pojistné podmínky pro pojištění profesní odpovědnosti VPP-PO 1/15
Zvláštní pojistné podmínky pro pojištění profesní odpovědnosti IT společností ZPP PO IT 02/15
Rozpis pojistného

Podpis a razítko pojistitele: Allianz pojišťovna, a.s.

V Praze dne **11.12.2017**

Podpis:

Allianz pojišťovna, a. s.
generální ředitelství
Bezpečnostní spolehlivost pojištění
[redacted]

Jméno: [redacted]

Razítko:

Podpis a razítko pojistníka: ČD - Informační Systémy, a.s.

V Praze dne

Podpis:

Jméno:

Razítko:

[redacted]

[redacted]

[redacted]

Příloha č. 3 Smlouvy – Seznam poddodavatelů

IDENTIFIKACE PODDODAVATELE (obchodní firma, IČO a sídlo)	ROZSAH PODDODÁVKY
Obchodní firma: AMI Praha a.s. **IČO:** 257 15 909 **Sídlo**: Hanusova 826/29, Michle, 140 00 Praha 4	- Návrh, dodání a nasazení Identity Managementu, coby samostatného programu