



SMLOUVA O DÍLO

121/OV2/NK/2013

I. SMLUVNÍ STRANY:

OBJEDNATEL:

se sídlem:
rektor:
osoba oprávněná jednat
ve věcech technických:

IČ:

DIČ:

bankovní spojení:

č.ú.:

(dále jen „objednatel“) na straně jedné

UNIVERZITA PALACKÉHO V OLOMOUCI

Křížkovského 8, 771 47 Olomouc
prof. RNDr. Miroslav Mašláň, CSc.

RNDr. Hana Matochová, vedoucí oddělení vývoje aplikací
Centra výpočetní techniky, tel. 585631821, e-mail:
hana.matochova@upol.cz

61989592

CZ61989592

Komerční banka, a.s., pobočka Olomouc

19-1096330227/0100

a

ZHOTOVITEL:

se sídlem:
zápis v obchodním rejstříku:
statutární orgán:
osoba oprávněná jednat
ve věcech smluvních:
osoba oprávněná jednat
ve věcech technických:

IČ:

DIČ:

bankovní spojení:

č.ú.:

(dále jen „zhotovitel“) na straně druhé

BCV solutions s. r. o.

7. května 1168/79, Praha 4 – Chodov, 149 00
v Praze oddíl C vložka 136075.
jednatel

Ing. Lukáš Církva

Zdeněk Burda

28360851

CZ28360851

2800049696/2010

Objednatel se zhotovitelem uzavírají tuto smlouvu o dílo v důsledku skutečnosti, že nabídka zhotovitele na dodávku předmětu plnění dle této smlouvy byla objednatelem vybrána ve výběrovém řízení jako nabídka nejvhodnější.

II. Předmět plnění

1. Zhotovitel se touto smlouvou zavazuje provést na své náklady a nebezpečí pro objednatele dílo - systém pro správu identity osob – identity management (dále jen „IDM“) včetně případných modulů, konektorů a klientů, dále zahrnující v písemné formě detailní analýzu a návrh řešení architektury a procesů IDM včetně vazeb na vybrané moduly informačního systému Univerzity Palackého v Olomouci, vytvoření prováděcího projektu systému, návrh harmonogramu nasazení systému s návrhem pilotního provozu, provedení instalace systému a jeho kompletní implementace, dodání příslušné dokumentace, školení obsluhy systému a školení programátorů zaměřené na možnosti rozvoje systému vlastními silami včetně dodávky potřebných licencí a zdrojů, to vše v souladu s technickými specifikacemi uvedenými v nabídce zhotovitele ze dne **02. 05. 2013**, podané zhotovitelem v rámci poptávkového řízení, které předchází podpisu této smlouvy. Zhotovitel se dále zavazuje poskytovat záruční servis díla za podmínek stanovených dále touto smlouvou.

2. Provedení díla bude v souladu s přílohou č. 1 této smlouvy rozčleněno do 2 fází. V první fázi zhotovitel provede a dodá objednateli v písemné formě detailní analýzu a návrh řešení architektury a procesů IDM včetně vazeb na vybrané moduly informačního systému Univerzity Palackého v Olomouci a návrh harmonogramu nasazení systému s návrhem pilotního provozu. V druhé fázi uchazeč dodá prováděcí projekt systému, provede instalaci systému a jeho kompletní implementaci, dodá příslušnou dokumentaci a provede školení obsluhy systému a školení programátorů zaměřené na možnosti rozvoje systému vlastními silami, a to včetně dodávky potřebných licencí a zdrojů.

3. Zhotovitel je povinen na základě požadavků zadavatele písemný výstup 1. fáze provedení díla před jeho předáním podrobit připomínkovému řízení ze strany objednatele, připomínky vzešlé z tohoto řízení do výstupu zpracovat a zohlednit v rámci druhé fáze provádění díla.

4. Druhá fáze provádění díla, zejména instalace a implementace systému IDM bude prováděna v termínu plnění dle čl. III. této smlouvy průběžně, a to formou dálkového přístupu. K datovanému protokolárnímu předání a převzetí této fáze díla dojde po jeho úplné instalaci a implementaci. Objednatel je povinen zhotoviteli umožnit během realizace díla dálkový přístup ke stávajícímu univerzitnímu informačnímu systému.

5. Objednatel se zavazuje převzít dílo, resp. jeho jednotlivé fáze za podmínek dále stanovených touto smlouvou a zaplatit za něj cenu dle čl. IV. této smlouvy.

6. O předání a převzetí jednotlivých fází díla jsou smluvní strany povinny sepsat předávací protokol, v němž bude uvedeno datum předání díla. Objednatel v protokolu uvede, zda bylo dílo předáno řádně a včas, popř. zda uplatňuje u zhotovitele vady díla. Tento předávací protokol je za objednatele oprávněna podepsat RNDr. Hana Matochová nebo jí pověřená osoba.

5. Po předání a převzetí 2. fáze díla objednatel dílo obstarává sám prostřednictvím svého předem proškolených zaměstnanců, čímž zaručuje, že dílo nebude znehodnoceno neodbornými zásahy.

7. Vlastnické právo ke zhotovovanému dílu přechází v plném rozsahu na objednatele okamžikem předání a převzetí 2. fáze díla. Zhotovitel bere na vědomí, že dílo vytvořené podle této smlouvy je dílem vytvořeným na objednávku ve smyslu § 61 autorského zákona a objednatel je oprávněn užít dílo k účelu vyplývajícímu z této smlouvy, tj. zejména ze specifikace obsažené ve smlouvě o dílo. Zhotovitel bere na vědomí, že nebude v podmínkách pro provozování díla uplatňovat žádné dodatečné licenční podmínky, a to ani SW produktů třetích stran.

8. Zhotovitel je povinen na základě požadavků objednatele výstup 1. fáze provedení díla před jeho předáním podrobit připomínkovému řízení ze strany objednatele a připomínky vzešlé z tohoto řízení do výstupu zpracovat.

9. Dílo musí být plně funkční, bez dalších dodatečných nákladů ze strany kupujícího.

III. Termín a místo dodání

1. Výstup 1. fáze díla (tj. písemně zpracovaná detailní analýza a návrh řešení architektury a procesů IDM včetně vazeb na vybrané moduly informačního systému Univerzity Palackého v Olomouci a návrh harmonogramu nasazení systému s návrhem pilotního provozu) je uchazeč povinen zadavateli dodat nejpozději do 2 měsíců od podpisu smlouvy. Druhá fáze díla (tj. dodávka prováděcího projektu systému, provedení instalace systému a jeho kompletní implementace, dodávka příslušné dokumentace a provedení školení obsluhy systému a školení programátorů zaměřené na možnosti rozvoje systému vlastními silami, a to včetně dodávky potřebných licencí a zdrojů) bude zahájena nejdříve po předání a převzetí písemného výstupu první fáze a jeho odsouhlasení zadavatelem, a provedena nejpozději do 4 měsíců od jejího zahájení.

2. Místo plnění: Centrum výpočetní techniky UP, Biskupské nám. 1, 771 11 Olomouc. Pověřená osoba pro převzetí díla na základě datovaného protokolu o předání: RNDr. Hana Matochová, nebo jí pověřená osoba.

IV. Cena za dílo

1. Objednatel se zavazuje zaplatit zhotoviteli za konečné dílo dle této smlouvy cenu ve výši **732000 Kč** (slovy: sedm set třicet dva tisíc korun českých) bez DPH, DPH 21 % činí 153720 Kč. Celková cena za dílo včetně DPH činí 885720 Kč.

2. Celková cena za kompletní dílo je stanovena jako cena pevná, nejvýše přípustná a maximální, zahrnuje veškeré náklady zhotovitele spojené s provedením a dodáním díla (zejména doprava na místo plnění, clo, pojištění atd.), a s poskytováním záručního servisu objednateli. Změna ceny za dílo je možná pouze a jen za předpokladu, že dojde po uzavření této smlouvy ke změnám sazeb daně z přidané hodnoty.

3. Zhotovitel odpovídá za to, že sazba daně z přidané hodnoty v okamžiku fakturace je stanovena v souladu s platnými a účinnými právními předpisy.

V. Platební podmínky

1. Sjednaná cena díla je splatná na základě řádně vystaveného daňového dokladu (dále jen „faktury“) řádně vystavené zhotovitelem, ve lhůtě splatnosti 30 dnů. Právo na zaplacení ceny vzniká řádným splněním závazku, způsobem a v místě plnění v souladu s touto smlouvou. Fakturace proběhne po předání a převzetí obou fází díla. Dokladem o řádném splnění závazků uvedených v předchozí větě prodávajícím jsou datované předávací protokoly opatřené podpisy oprávněných osob obou smluvních stran.

2. Zhotovitelem vystavená faktura musí obsahovat všechny náležitosti daňového dokladu v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a náležitosti obchodní listiny podle § 13a obchodního zákoníku a současně identifikaci smlouvy, na jejímž základě bylo plněno. Fakturu prodávající opatří razítkem a podpisem osoby oprávněné je vystavit.

3. Nebude-li faktura vystavená zhotovitelem obsahovat některou povinnou náležitost nebo zhotovitel chybně vyúčtuje cenu nebo DPH, je objednatel oprávněn před uplynutím lhůty splatnosti vrátit fakturu zhotoviteli k provedení opravy s vyznačením důvodu vrácení. Zhotovitel provede opravu vystavením nové faktury. Dnem odeslání vadné faktury zhotoviteli přestává běžet původní lhůta splatnosti a nová lhůta splatnosti běží znovu ode dne doručení nové faktury objednateli.

4. Smluvní strany se dohodly na tom, že závazek zaplatit cenu za danou fázi díla je splněn dnem odepsání příslušné částky z účtu objednatele ve prospěch účtu zhotovitele uvedeného v záhlaví této smlouvy.

VI. Odpovědnost prodávajícího za vady

1. Zhotovitel poskytuje objednateli na dílo záruku za jakost ve smyslu § 429 a násl. obchodního zákoníku v délce trvání **1 měsíce** ode dne protokolárního předání a převzetí druhé fáze díla. Zárukou se rozumí zajištění technické kompatibility a funkčnosti v rozsahu odpovídajícím stavu v den protokolárního předání a převzetí druhé fáze díla.

VII. Smluvní pokuty

1. Zhotovitel se zaváže uhradit objednateli smluvní pokutu ve výši 1.000,- Kč za každý započatý den prodlení se smluvně stanovenými termíny předání jednotlivých fází díla.

2. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně v plné výši vedle smluvní pokuty.

3. Splatnost vyúčtovaných smluvních pokut a úroků z prodlení je 30 dnů od data doručení písemného vyúčtování příslušné smluvní straně a za den zaplacení bude považován den odepsání částky smluvní pokuty z účtu příslušné smluvní strany ve prospěch účtu, který bude uveden ve vyúčtování smluvní pokuty.

4. Smluvní pokuty je objednatel oprávněn započíst proti pohledávce zhotovitele na úhradu ceny za dílo.

VIII. Závěrečná ujednání

1. Objednatel si vyhrazuje právo zveřejnit obsah uzavřené smlouvy o dílo.

2. Smluvní strany se v souladu s ust. § 262 odst. 1 zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů (dále jen obchodní zákoník), výslovně dohodly, že veškerá práva a povinnosti stanovená touto smlouvou, jakož i práva a povinnosti z této smlouvy vyplývající se řídí obchodním zákoníkem.

3. Ujednání této smlouvy jsou vzájemně oddělitelná. Pokud jakákoli část závazku podle této smlouvy je nebo se stane neplatnou či nevymahatelnou, nebude to mít vliv na platnost a vymahatelnost ostatních závazků podle této smlouvy a smluvní strany se zavazují nahradit takovouto neplatnou nebo nevymahatelnou část závazku novou, platnou a vymahatelnou částí závazku, jejíž předmět bude nejlépe odpovídat předmětu původního závazku. Pokud by smlouva neobsahovala nějaké ujednání, jehož stanovení by bylo jinak pro vymezení práv a povinností odůvodněné, smluvní strany učiní vše pro to, aby takové ujednání bylo do smlouvy doplněno.

4. Změnit nebo doplnit tuto smlouvu mohou smluvní strany pouze formou písemných dodatků, které budou vzestupně číslovány, výslovně prohlášeny za dodatek této smlouvy a podepsány oprávněnými zástupci smluvních stran.

5. Objednatel je oprávněn odstoupit od této smlouvy pro její podstatné porušení zhotovitelem, přičemž podstatným porušením smlouvy se rozumí:

prodlení zhotovitele s dodáním jednotlivých fází díla delším než 20 dní,

nedodržení technické specifikace díla uvedené v nabídce zhotovitele.

Odstoupení od smlouvy musí být učiněno písemně a nabývá účinnosti dnem doručení písemného oznámení druhé smluvní straně. V případě odstoupení od této smlouvy objednatelem z důvodu výše uvedených podstatných porušení smlouvy zhotovitelem, nemá zhotovitel nárok na náhradu jakýchkoliv do té doby vzniklých nákladů.

6. Zhotovitel není oprávněn bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí z této smlouvy třetí osobě.

7. Tato smlouva o dílo nabývá účinnosti dnem jejího podpisu oběma smluvními stranami.

8. Tato smlouva o dílo je vyhotovena v pěti vyhotoveních s povahou originálu podepsaných oprávněnými zástupci smluvních stran, přičemž objednatel obdrží tři a zhotovitel dvě vyhotovení.

9. Zhotovitel se zavazuje v souladu s § 147a odst. 4 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, že objednateli předloží seznam subdodavatelů podílejících se na plnění předmětu této smlouvy, ve kterém uvede subdodavatele, jímž za plnění subdodávky uhradil více než 10 % z celkové kupní ceny, a to nejpozději do 60 dnů od splnění této smlouvy. Současně platí, že má-li subdodavatel zhotovitele formu akciové společnosti, je přílohou seznamu i seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10 % základního kapitálu, vyhotovený ve lhůtě 90 dnů před dnem předložení seznamu subdodavatelů.

10. Nedílnou součástí této smlouvy o dílo tvoří přílohy:

Příloha č. 1 – Nabídka zhotovitele ze dne 02. 05. 2013.

V Olomouci, dne 29. 05. 2013

UNIVERZITA PALACKÉHO V OLOMOUCI
rektorát
Křížkovského 8, 771 47, Olomouc

prof. RNDr. Miroslav Mašláň, CSc.
rektor

V Praze, dne 29. 05. 2013

ECV solutions s.r.o.

7. května 1168/70
149 00 Praha 4 - Chodov
IČ: 293 60 851

Ing. Lukáš Cirkva
jednatel

Příloha č. 1 – Nabídka zhotovitele ze dne 02. 05. 2013.

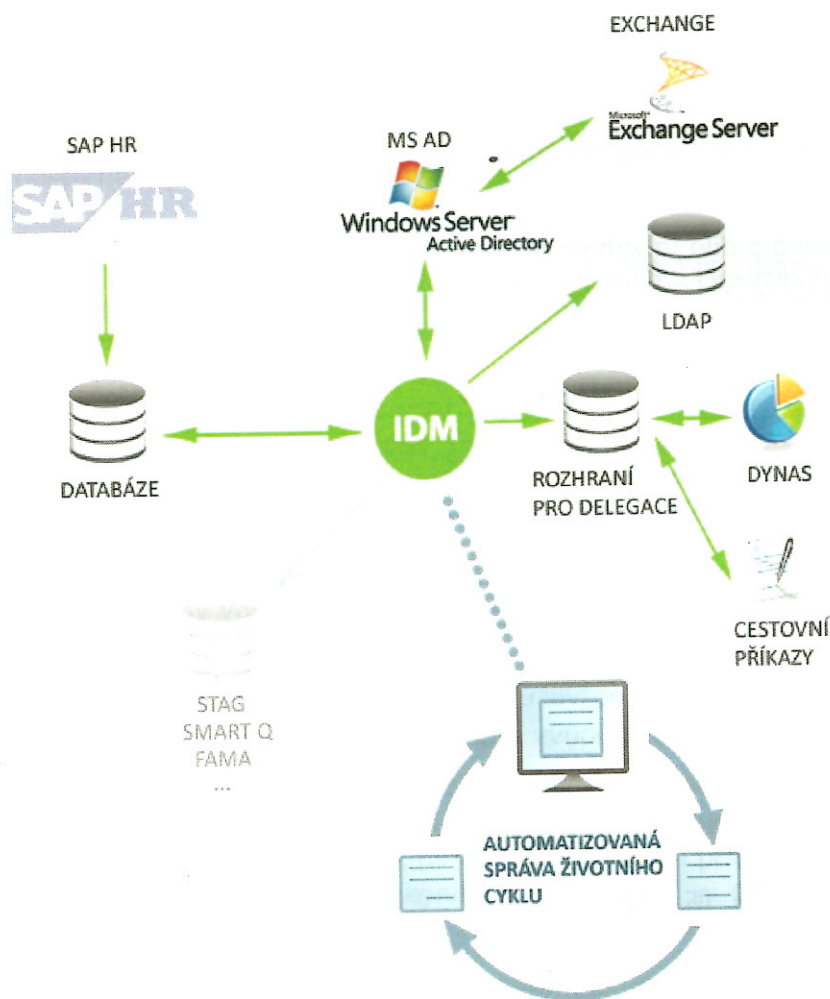
Technická specifikace a podrobná cenová kalkulace

V této kapitole Vám představíme řešení správy uživatelských účtů prostřednictvím nástroje **CzechIdM**.

Popis a schéma architektury řešení

Správa identit vyžaduje instalaci jeho základní komponenty Identity Manageru. Pro správu identit bude využito produktu CzechIdM (dále jen IdM nebo Identity Manager). Identity Manager bude centrálně řídit životní cyklus zaměstnanců univerzity, do budoucna se předpokládá správa identit studentů nebo externích pracovníků

Informace o identitách interních uživatelů budou přebírány prostřednictvím databáze z personalistiky do IdM a po zpracování budou, dle definovaných pravidel a procesů propagovány do spravovaných aplikací.



Tok dat při správě identit interních uživatelů

Automatizované procesy správy identit umožňují kompletní řízení životního cyklu identity a zabraňují chybám při správě identit vlivem lidského faktoru. IdM se tak stává autoritativním zdrojem všech dat o uživatelích prostředí.

Uživatelé budou mít do Identity Manageru přístup přes webové rozhraní. Uživatelské rozhraní zajišťuje samoobsluhu, kde si uživatelé mohou zkontrolovat správnost údajů o nich v Identity Manageru vedených, existenci uživatelských účtů a oprávnění v koncových aplikacích a

v přístupu k datům. Samoobslužné rozhraní také umožňuje uživateli z jednoho místa provést změnu hesla, případně požádat o přístup do nové aplikace nebo o změnu oprávnění ke stávajícímu účtu a v tomto případě i zadat delegaci pro příslušný koncový systém. Identity Manager obsahuje webové uživatelské rozhraní jako standardní součást. Funkčnost rozhraní může být přenesena do portálu ve formě portletu, který bude komunikovat s Identity Managerem přes webové služby.

Administrátorské rozhraní je také dostupné přes web, přístup do něj budou mít pouze oprávnění administrátoři, kteří zajišťují správu uživatelů. Administrátorské rozhraní umožňuje správu uživatelských účtů, rolí, reportů, procesů a mnoho dalších funkcí. Operace s uživateli, které bude Identity Manager provádět automaticky, může správce s potřebným oprávněním v IdM také provést ručně přes webové administrátorské rozhraní.

Identity Manager bude pracovat s více druhy uživatelských účtů. Minimální dělení bude na zaměstnance a studenty. Popis správy jednotlivých typů účtů uživatelů bude součástí analýzy řešení.

Identity Manager provádí správu uživatelských účtů standardní cestou přes tzv. konektory, kterými se připojuje ke spravovaným systémům. Dále umožňuje zpracovávat automatizované procesy a zpřístupnit data o uživateli přes webové služby.

Procesy správy identit

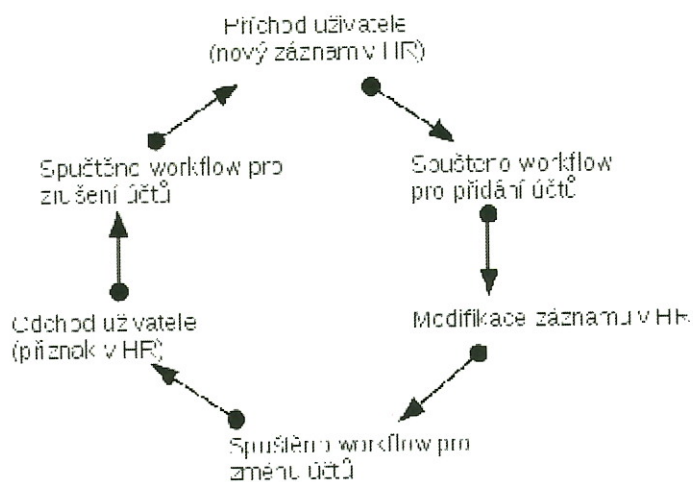
CzechIdM řídí správu identit skrz parametrizovatelné a dle potřeby upravitelné procesy. Tyto procesy zajišťují kompletní správu životního cyklu identity. Bude se jednat minimálně o tyto procesy:

- Příchod nového zaměstnance
- Odchod zaměstnance
- Změna uživatele
- Změna organizačního zařazení
- Karanténa

Definice konkrétních procesů a jejich vazeb bude definována v rámci analýzy řešení.

Uvedené procesy budou při implementaci upraveny na míru prostředí a dle požadavků zadavatele.

Všechny procesy lze spouštět automaticky na základě přijaté události od autoritativního systému, automaticky dle naplánované úlohy nebo manuálně pokud k tomu má uživatel oprávnění. Vybrané procesy jako je žádost o přidělení role nebo účtu v aplikaci lze zpřístupnit uživatelům v uživatelském rozhraní a tím zajistit možnost jejich samoobsluhy.



ukázka procesu v rámci životního cyklu identit

Role management

Správa rolí je součástí správy identit. Role přidělují uživateli různá oprávnění do koncových aplikací nebo do Identity Manageru. Přiřazením role definované podle funkčního místa dostane uživatel okamžitě všechna oprávnění do aplikací potřebná pro svou práci.

CzechIdM obsahuje mechanismy pro role, které umožní efektivní fungování procesů správy identit. Definice rolí je prováděna administrátorem přes webové rozhraní. Přiřazování rolí uživatelům může být realizováno ručně přes webové rozhraní, automaticky v procesu správy identit nebo automaticky na základě organizační struktury – funkčního místa uživatele.

Mechanismu rolí v kombinaci s organizační strukturou umožňuje delegovat různá oprávnění v Identity Manageru na jednotlivé uživatele. Lze například delegovat správu uživatelů (zamykání účtů, kontrola stavu, reset hesla) pro konkrétní pobočku organizace na místního správce. Uživatelé se potom mohou s běžnými úkony obracet na svého lokálního správce.

Zabezpečení dat

CzechIdM bude s uživateli a administrátory komunikovat pouze skrz zabezpečené webové rozhraní – http protokolem. Komunikace se spravovanými aplikacemi bude v závislosti na jejich konfiguraci využívat obvyklý způsob zabezpečení pro danou aplikaci.

Všechny procesy (workflow) IdM budou auditovány, viz kapitola Reporty a Logy.

Data aplikací včetně jejich logů budou na samostatném serveru, na kterém nepoběží žádné další aplikace třetích stran a ke kterému budou mít přístup pouze oprávněné osoby.

Naplnění požadavků zadavatele

Požadavek	Splňuje	Poznámka
IDM musí pracovat s minimálně 5000 identitami zaměstnanců a minimálně 30 000 identitami studentů. Součástí nabídkové ceny je licence pro tento počet identit.	ANO	Ano viz licenční podmínky, licence neomezuje počet uživatelů.
IDM musí připojit libovolné množství spravovaných systémů. Licence musí umožňovat připojení nového systémů zadavatele bez licenčních nákladů.	ANO	Ano viz licenční podmínky, licence neomezuje počet spravovaných systémů.
IDM musí pracovat s více samostatnými instancemi. Licence musí umožňovat spuštění další instance bez licenčních nákladů zadavatele.	ANO	Ano viz licenční podmínky, licence neomezuje počet instancí.
IDM musí udržovat a spravovat kompletní životní cyklus identity uživatele.	ANO	Standardní vlastnost CzechIdM
IDM musí umožnit práci s více stromovými strukturami (např. zaměstnanci, studenti, externisté).	ANO	Standardní vlastnost CzechIdM
IDM musí umožnit obousměrnou synchronizaci dat tedy jak z IDM do spravovaného systému (např. uživatele a jejich atributy), tak ze spravovaného systému do IDM (např. role v konkrétním systému, využitelné pro další účely).	ANO	Standardní vlastnost CzechIdM
IDM musí mít rozhraní pro správu hesel a musí umožnit zaměstnancům samostatnou změnu hesla.	ANO	Standardní vlastnost CzechIdM
IDM musí mít centrální rozhraní pro samostatnou delegaci uživatelských oprávnění zaměstnanců. IDM bude řídit delegace ve spravovaných systémech, kontrolovat jejich platnost a tyto informace zaznamenávat. Součástí řešení nejsou úpravy ve spravovaných systémech zadavatele, řešící vnitřní logiku těchto delegací.	ANO	Standardní vlastnost CzechIdM
IDM disponuje jednoduchou správou rolí: • Vytvoření nové role • Změna oprávnění pro roli • Smazání role	ANO	Standardní vlastnost CzechIdM. Součástí implementace, ale není Role management.

IDM musí umožňovat synchronizaci identit v spravovaném systému (vstupně/výstupní operace) prostřednictvím těchto rozhraní: • databázová tabulka, view • webová služba SOAP • CSV textový soubor • XML struktura (soubor) • LDAP (Tivoli a AD)	ANO	Standardní vlastnost CzechIdM
Systém musí umožnit v rámci toků dat jejich automatickou modifikaci.	ANO	Standardní vlastnost CzechIdM
Systém musí umožnit realizaci konektorů pomocí volání externích programů s parametry.	ANO	Standardní vlastnost CzechIdM
Systém musí být provozovatelný minimálně na Linuxové platformě.	ANO	Prostředí je multiplatformní
Interní konektory musí umožňovat realizaci proprietárních protokolů na bázi TCP/IP.	ANO	Standardní vlastnost CzechIdM
Konektory musí realizovat: • založení účtů se všemi náležitostmi v systémech Netware, Aix, Linux, AD, LDAP, Exchange, FreeRadius • smazání účtů se všemi náležitostmi (včetně uživatelských adresářů a dat) v systémech Netware, Aix, Linux, AD, LDAP, Exchange, FreeRadius • úpravu oprávnění v IDP Shibboleth pro jednotlivé účty či skupiny • úpravu poštovních aliasů v systému řízení směrování el. pošty (SendMail) a hromadných poštovních klubů.	ANO	CzechIdM disponuje všemi těmito konektory a množstvím dalších.
Synchronizace identit probíhá v reálném čase; tj. změna údajů v jednom systému se okamžitě projeví i v ostatních propojených systémech.	ANO	Standardní vlastnost CzechIdM
IDM musí mít kompletní podporu českého jazyka i z hlediska dat, se kterými pracuje IDM včetně možnosti případného ořezání diakritiky	ANO	Standardní vlastnost CzechIdM
V rámci implementace musí být zajištěno školení administrátorů prostředí (pro max.	ANO	Viz kapitola školení

12 osob)		
IDM musí udržovat heslo uživatelů v nerozšifrovatelné podobě	ANO	Standardní vlastnost CzechIdM
Vybrané operace nad identitami jsou zaznamenány v auditním logu.	ANO	Standardní vlastnost CzechIdM

Požadavek	Splňuje	Poznámka
Návrh architektury IDM a vazeb na vybrané informační systémy (topologie, technické požadavky, rozhraní, protokoly, grafické schéma celého řešení). Vybrané informační systémy jsou specifikovány níže.	ANO	Bude realizováno v rámci řešení.
Návrh a harmonogram nasazení IDM.	ANO	Bude realizováno v rámci řešení.
Návrh metodiky pro správu identit.	ANO	Bude realizováno v rámci řešení.
Návrh doporučení a metodiky pro správu identit, práv a popis rozhraní v nově nasazovaných informačních systémech.	ANO	Bude realizováno v rámci řešení.
Návrh procesů správy životního cyklu uživatelů a způsob integrace IDM. Minimálně budou zpracovány tyto procesy: • Příchod uživatele • Odchod uživatele • Změna uživatele • Žádost o přidělení role • Změna organizačního zařazení • Karanténa • Delegace oprávnění uživatelů ve spravovaných aplikacích	ANO	Bude realizováno v rámci řešení.

Návrh mechanismu rolí pro přístup do jednotlivých IS a specifikace jejich oprávnění.	ANO	Bude realizováno v rámci řešení. V rámci řešení nebude řešen Role Management v rámci organizace.
Specifikaci vývojového, testovacího a produkčního prostředí IDM.	ANO	Bude realizováno v rámci řešení.
Návrhu pilotního provozu a akceptačních kritérií.	ANO	Bude realizováno v rámci řešení.
Návrh postupu přechodu do produkce.	ANO	Bude realizováno v rámci řešení.
Definici bezpečnostních zásad a pravidel pro práci s IDM.	ANO	Bude realizováno v rámci řešení.
To vše v písemně zpracované podobě.	ANO	Bude realizováno v rámci řešení.

Požadavek	Splňuje	Poznámka
Zadavatel si vyhrazuje možnost změny zapojených systémů na základě písemných výsledků analýzy.	ANO	
Zdroj identit pro IDM Personální systém v SAP. Na základě informací ze zdroje identit, IDM realizuje následující procesy životního cyklu: • Příchod uživatele • Odchod uživatele • Změna uživatele • Změna organizačního zařazení • Karanténa	ANO	Uvedené procesy budou implementovány jako standardní procesy CzechIdM. Napojení SAP bude realizováno prostřednictvím poskytnutého databázového rozhraní.
Systémy spravované IDM		
MS Active Directory IDM musí minimálně zajišťovat: • založení uživatele • změnu atributů u uživatele • zrušení uživatele	ANO	Standardní funkčnost napojení CzechIdM na MS Active Directory.

MS Exchange Server IDM musí spolupracovat (bude upřesněno po analýze)	ANO	CzechIdM bude spravovat MS Exchange Server prostřednictvím napojení MS Active Directory.
LDAP IDM musí minimálně zajišťovat: • založení uživatele • změnu atributů u uživatele • zrušení uživatele Obecné vlastnosti obou LDAPů: • změna zařazení ve skupinách • správa skupin • schvalovací workflow pro zařazení do skupin	ANO	Standardní funkčnost napojení CzechIdM na LDAP. Schvalovací workflow pro zařazení do skupin bude implementováno pomocí standardních prostředků CzechIdM.
Dynamický nákupní systém DYNAS (portálová aplikace) IDM musí minimálně zajišťovat: • Rozhraní pro delegaci uživatelských oprávnění	ANO	Řešení bude poskytovat požadované rozhraní společně pro všechny aplikace, ve kterých má smysl delegaci uvažovat. Konkrétní akce v koncovém systému bude v režii napojeného systému.
Aplikace Cestovní Příkazy (portálová aplikace) IDM musí minimálně zajišťovat: • Rozhraní pro delegaci uživatelských oprávnění	ANO	Řešení bude poskytovat požadované rozhraní společně pro všechny aplikace, ve kterých má smysl delegaci uvažovat. Konkrétní akce v koncovém systému bude v režii napojeného systému.
V analýze a v přípravných krocích musí být zahrnuto budoucí připojení minimálně těchto systémů: Stag (studijní agenda), Identifikační karty včetně navazujících systémů (SmartQ a vstupní systémy Cevis, ubytovací systém ISKAM, stravovací systém KREDIT), Courseware, FaMa, Smlouvy, Elektronická spisová služba Magion, INIS.	ANO	Požadované body budou v analýze zahrnuty.

Požadavek webové rozhraní IdM bude:	Splňuje	Poznámka
Poskytovat uživatelské rozhraní pro manuální uživatelskou editaci vybraných informací z uživatelského profilu, včetně fotografie a editace bezpečnostních prvků, jako je uživatelské heslo a informace uživatele o nepřítomnosti na pracovišti.	ANO	CzechIdM umožňuje spolu s identitou spravovat libovolná data pomocí takzvaných extended atributů.
Zajistit správu identit uživatelů a jejich případnou úpravu, jako je založení, změna či smazání.	ANO	Standardní vlastnost CzechIdM. Správa identit je možná ručním zásahem v administrátorském rozhraní, hromadnou programovatelnou akcí nebo automaticky na základě stavu zdrojového systému.
Umožnit delegace uživatelských oprávnění ve spravovaných aplikacích.	ANO	Řešení poskytuje uživatelské rozhraní pro delegaci uživatelských oprávnění ve spravovaných aplikacích.
Mít k dispozici odlišné prostředí pro uživatele a administrátory a v nich dále definovat jednotlivé úrovně oprávnění k identitám a stromové struktuře.	ANO	Standardní vlastnost CzechIdM. Úrovně oprávnění mohou být definovány na základě stromové organizační struktury.
Logovat veškeré požadavky, které provedou uživatelé v rozhraní IDM tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM identitách a organizační struktuře.	ANO	Standardní vlastnost CzechIdM.
Nastavení schvalovacího workflow (při přidělení práva, role atd.), včetně emailových notifikací a potvrzování.	ANO	Standardní vlastnost CzechIdM. Administrátor CzechIdM může definovat schvalovací workflow z webového rozhraní.
Být plně lokalizováno do českého jazyka i anglického jazyka a to včetně nápovědy.	ANO	Standardní vlastnost CzechIdM.
Musí být na základě výsledků analýzy začleněno do portálu.	ANO	Portál bude obohacen o přímý odkaz do webového rozhraní CzechIdM
Musí být připravena možnost tisku identifikačních karet.	ANO	CzechIdM může být použito k odesílání dat a příkazů do systému pro tisk identifikačních karet.

czechidm

Přihlášený uživatel: **ldmuser**
[Nápověda](#) | [Odhlásit](#)

BCV solutions

Osobní údaje

Úkoly

Změna mého hesla

Nastavení

Změna hesla

Nastavit heslo

Obnovit data

Zavřít

Nastavte nové heslo

Heslo*

Heslo (kontrola)*

Vyberte systémy, ve kterých bude změněno heslo

Název

ldm:☐

Roundcube database (JDBC connector): Default☐

Nastavit heslo

Obnovit data

Zavřít



Přihlášený uživatel: **admin**
[Napověda](#) | [Odhlásit](#)



[Uživatelé](#)
[Úkoly](#)
[Role](#)
[Systémy](#)
[Naplanované úlohy](#)
[Workflow](#)
[Reporty](#)
[Politiky](#)
[Konfigurace](#)

[Uživatelé](#)
[Vyhledávání uživatelů](#)
[Organizace](#)

Editace uživatele: idmuser

[Uložit](#)
[Obnovit data](#)
[Zavřít](#)

Osobní údaje
Změna hesla
Uživatelské role a kontrolované organizace
Uživatelské účty
Uživatelské atributy

Uživatelské jméno*

Jméno

Příjmení

E-mail

Vedoucí

Domovská organizace*

Zablokovaný účet

idmuser

Vybrat
Odebrat

Vybrat

[Uložit](#)
[Obnovit data](#)
[Zavřít](#)

Požadavek	Splňuje	Poznámka
Auditní reporty – přehled uživatelů a jejich rolí v systémech spravovaných IDM, včetně historie delegování práv.	ANO	Standardní vlastnost CzechIdM pro všechny systémy, kde je správa interních systémových rolí součástí napojení.
Rozdílové reporty – atributové rozdíly mezi identitami uloženými v IDM a jednotlivých spravovaných systémech.	ANO	Standardní vlastnost CzechIdM.
Možnost vytváření reportů z šablon nebo vlastních reportů.	ANO	Standardní vlastnost CzechIdM. Reporty jsou vytvářeny dynamicky na míru požadavkům administrátora.

Definice rizik navrhovaného řešení

Identity Manager se po nasazení do sítě stává centrálním místem, odkud jsou spravovány uživatelské identity a jejich oprávnění ve všech systémech na který je napojen. Identity Manager přistupuje ke spravovaným systémům s poměrně vysokým oprávněním umožňujícím správu uživatelů. V případě chybného nastavení oprávnění pro administrátory IdM mohou administrátoři znepřístupnit velmi snadno všechny spravované systémy. Z toho důvodu je nutné považovat IdM za kritický systém z bezpečnostního hlediska. Všechny operace prováděné IdM jsou auditovány a pro kritické operace bude zaveden „limit“ vyžadující další potvrzení.

Zavedením automatizace některých procesů správy uživatelů je kladen důraz na správnost dat v autoritativních systémech, jako je personalistika. Případná chybně zadaná data mohou způsobit v závislosti na aplikaci automatických pravidel a procesů různé nežádoucí stavy. Těmto situacím předcházíme důkladnou analýzou a vhodným návrhem automatických procesů.

Důležitou součástí správy uživatelských identit je i správa rolí. Role definují oprávnění uživatelů ve spravovaných systémech. Některé role dostávají uživatelé automaticky podle zařazení v organizační struktuře, jiné role jsou uživatelům přiřazeny na základě ruční žádosti. Je proto důležité definovat správně životní cyklus rolí a zajistit jejich správnou definici.

Hlavní oblasti, ve kterých bude nutné v průběhu analýzy a návrhu definovat rizika a jejich ošetření jsou:

- Přístupová oprávnění IdM ke spravovaným systémům
- Oprávnění administrátorů a uživatelů v systému IdM
- Správnost definice procesů správy životního cyklu identity a rolí
- Správnost definice obsahu rolí
- Bezpečnost záloh systému IdM

Dokumentace

Dokumentace řešení bude vytvářena v českém jazyce a bude zahrnovat následující dokumenty:

- „Analýza a Návrh řešení“ bude na základě analýzy popisovat aktuální stav a navrhovaný stav. Tento dokument bude sloužit jako výchozí pro realizaci celého řešení.
- „Dokumentace skutečného řešení“ bude obsahovat všechny změny platné pro prostředí zadavatele proti standardní konfiguraci jednotlivých komponent případně změny provedené proti návrhu řešení.
- Dokumenty „Administrátorská dokumentace“ a „Uživatelská dokumentace“ budou popisovat základní pracovní postupy.

Dokument **analýza a návrh řešení** obvykle obsahuje následující body:

- Úvod
- Účel a cíle dokumentu
- Zadání a hranice řešení
- Stávající stav správy identity u Zákazníka
- Funkční specifikace řešení
 - Komponenty systému
 - Organizační struktura
 - Kategorie uživatelských účtů
 - Politiky pro generování řetězců
 - Role
 - Notifikace
 - Eskalace
 - Delegace schvalování
 - Hardware
- Připojované aplikace k CzechIdM
- Název aplikace x
 - Napojení systému k CzechIdM
 - Synchronizace dat s CzechIdM
 - Rekonciliace a prvotní naplnění
 - Analytický model systému
 - Identifikátor účtu systému
 - Mapování atributů mezi IdM a systémem
 - Procesy inicializované ze systému
- Procesní analýza životního cyklu identit
 - Závislosti mezi procesy
 - Proces 1
 - Souhrn
 - Popis procesu 1
 - Diagram procesu
- Zabezpečení aplikací
 - Zabezpečení komunikace
 - Zabezpečení přístupu k aplikaci
 - Fyzické zabezpečení
 - Zabezpečení IdM při zálohování
- Obnova dat Identity Manageru
 - Způsob obnovy dat
 - Předpoklady pro obnovu dat
 - Vzorové scénáře obnovy Identity Manageru po výpadku
 - Výpadek aplikačního serveru IdM
 - Možné příčiny výpadku
 - Doba výpadku
 - Obnova

- Vysoká dostupnost Identity Manageru
- Metriky úspěšnosti projektu - akceptační testy

Dokumentace skutečného provedení obvykle obsahuje obvykle tyto kapitoly (v závislosti na dokumentu analýza a návrh) :

- Připojené systémy
- Napojení na personální systém
 - Data ze systému
 - Export změn ze systému
 - Import změn do systému
- Napojení na systém x
 - Atributy účtu a identifikátor účtu
 - Komunikace mezi konektorem a koncovým systémem
 - Způsob provádění operací
- atd.

Administrátorská dokumentace obvykle obsahuje tyto kapitoly:

- Úvod
- Tipy na obsah dokumentace
- Struktura systému
- Třívrstvá architektura Moduly a jejich topologie
- Webové rozhraní
- Aplikační vrstva
 - Úvod
 - Přihlašování
- Workflow, pravidla a e-mailové šablony
 - Bussiness konstanty
 - Pravidlo getExtendedAttributesNames
 - Modul Utils
 - Datová vrstva
 - Entity
 - Obecné třídy uchovávající data
 - View handlers
 - Získání pohledu na existující entitu - metoda Data.checkoutView
 - Získání ořezaného pohledu na existující entitu - metoda
 - Specifika metody Data.checkinView pro parametr typu UserView
 - Další užitečné metody na třídě Data
 - Kritéria
- Prezentační vrstva
 - Použité technologie
 - Členění uživatelského rozhraní
 - Třída GenericManagedBean
 - JSF šablony
 - Psaní formulářů pomocí JSF a workflow
- Workflow
 - Jak vytvořit workflow
 - Notifikace pomocí e-mailu
 - Workflow engine
- Pravidla
 - Pravidla
 - Ukázkové pravidlo
 - Rule engine.
 - Transformační pravidla
 - Pravidla pro výpočet nové hodnoty atributu
 - Korelační pravidla
 - Pravidla pro blokování účtů

- Pravidla before provisioning a after provisioning.
- Logování
 - Co všechno je logováno?
 - Auditní informace
 - Uživatelské požadavky
 - Jak logovat z kódu
- Schvalování
 - Schvalovací proces
 - Plánování úloh
 - Scheduler a task executer
- Koncové systémy
 - Definice koncového systému
 - Přilinkování uživatelského účtu
 - Vypnutí reálných modifikací systému
 - Aktualizace hodnot atributů účtů na koncových systémech
- Identity Connectors
 - Definice konektoru
 - Funcionalita konektorů
- Typické procesy správy životního cyklu identit
 - Závislosti mezi procesy
- Konfigurace
 - Přehled konfiguračních parametrů
- Testování
 - Testování kódu
 - Jak napsat jednoduchý test
 - Práce s výjimkami
 - Když záleží na pořadí
 - Psaní testů EJB session bean
 - Psaní testů Seam bean
 - Jak testovat workflow
 - Pokrytí testy

Dokument uživatelská dokumentace obsahuje obvykle tyto body:

- CzechIdM
- Systém CzechIdM
 - Přihlášení uživatele do systému
 - Odhlášení uživatele ze systému
 - Zapomenuté heslo
- Uživatelské prostředí
 - Osobní údaje
 - Přidělené role
 - Úkoly
 - Změna hesla
 - Nastavení

Školení

Součástí projektu je i níže uvedená školení pro administrátory a pověřené uživatele identity manageru. Školení bude probíhat v sídle zadavatele na testovacím prostředí IdM

Popis školení:

Délka školení	0,5 dne
Účastníci	Pověření uživatelé (pro max. 12 uživatelů)
Obsah školení	seznámení s implementovanými procesy správy životního cyklu identity a jejich dopady, schvalovací proces

Seznam použitého SW

Název SW	Výrobce	Licence	www	Počet uživatelů	Počet Instancí	Počet spravovaných systémů
CzechIdM	BCV solutions	CzechIdM BCV licence*	www.czechidm.cz/	není omezen	není omezen	není omezen

* Dílo vytvořené Dodavatelem dle předmětu Smlouvy je považováno za dílo v souladu se zákonem č. 121/2000 Sb., autorský zákon v platném znění. Obě strany se dohodly, že spolu s řádným předáním Díla dle této Smlouvy uděluje Dodavatel Zadavateli trvalé a s výhradou v této Smlouvě uvedené dále nepřevoditelné výhradní právo ke všem způsobům užití Díla, případně těch jeho částí, které naplňují definici Díla dle autorského zákona. Územní rozsah poskytnutých práv není jakkoli omezen (dále jen „Licence“).

2. K přenechání Licence jiným osobám se vyžaduje předchozí písemný souhlas Dodavatele. Žádost o sublicenci musí obsahovat určení oprávněné osoby, její detailní specifikaci a návrh smlouvy o sublicenci. Žádost musí dále uvádět vztah mezi Objednatelem a oprávněnou osobou za sublicence, projekt, na který se bude sublicence vztahovat. Žádost o sublicenci jiným než Dceřiným společnostem nebude bezdůvodně odmítnuta.

3. Zadavatel není oprávněn jednotlivá nebo všechna oprávnění uvedená shora poskytnout Dceřiným společnostem (jak je tento pojem definován dále) bez předchozího souhlasu Poskytovatele. Dceřinými společnostmi Zadavateli rozumí jakékoli obchodní společnosti, včetně družstev nebo jiných obdobných společností či státních organizací, s nimiž Zadavatel tvoří concern nebo je přímo či nepřímo ovládá.

4. Licence se uděluje na dobu neurčitou, a to ode dne účinnosti Licence. Poskytnutí Licence je účinné dnem řádného předání a převzetí Díla dle této Smlouvy a příslušného Dodatku.

5. Dodavatel za tímto účelem při předání případného Díla vzešlého z plnění poskytnutého dle této Smlouvy prohlašuje, že do doby předání Díla neposkytl jakékoli třetí osobě k Dílu výhradní či nevýhradní licenci, a že si není vědom jakýchkoli práv třetích osob k Dílu, vyjma takových práv, se kterými bude Zadavatel seznámen a s nimiž bude současně souhlasit.

- Zadavatel jako nabyvatel Licence oznámí Dodavateli, a to bez zbytečného odkladu po jejich zjištění, následující skutečnosti:
- užívání jakékoli jiné licence či systému, o kterém se dozví, jež porušuje nebo je způsobilé porušit práva Objednatele z této Smlouvy nebo způsobit Zadavateli škodu či újmu;

- jakékoli podezření, že provozování Díla nebo užívání Licencí je považováno třetí stranou za nekalosoutěžní jednání, způsobené přivodit této třetí osobě újmu nebo pokud porušuje práva třetí osoby z uzavřené smlouvy; a
- třetí osoba uplatnila proti Zadavateli práva z titulu nekalosoutěžního jednání nebo porušení právních předpisů v důsledku provozování Díla nebo užívání Licencí.

Technologické zázemí

Jedná se o navržené parametry prostředí identity managementu, přesná konfigurace HW bude upřesněna v analýze řešení.

CzechIDM

Účel serverů	Doporučená konfigurace HW	Počet serverů
Testovací prostředí pro identity management		
Identity Manager, Databáze pro IdM	2 jádra CPU, 8GiB RAM	1
Produkční prostředí pro identity management		
Identity Manager	4 jádra CPU, 8GiB RAM	1
Databáze pro IdM	2 jádra CPU, 4GiB RAM, 10k RPM HDD	1

Součinnost zadavatele

Zákazník se zavazuje uchazeči poskytovat veškeré informace a prostředky níže popsané nejpozději do pěti (5) pracovních dnů od výzvy uchazeče.

Konkrétně se jedná o tyto požadavky související s projektem:

- Zajistit veškerou dokumentaci dotčených informačních systémů vzhledem ke správě identit.
- Zpřístupnit vzdálené připojení – VPN do vývojového/testovacího prostředí.
- Poskytnout vývojové a testovací prostředí připojovaných systémů včetně reprezentativního vzorku dat.
- Vytvořit organizační, časové a materiální podmínky pro zaměstnance do projektu začleněných, včetně nastavení potřebných kompetencí. Zejména se jedná o nekuřácký pracovní prostor, připojení k internetu, dostupnost zodpovědných osob na straně Zadavatele atd.
- Zajistit pověřené zodpovědné pracovníky na straně Zadavatele – zejména projektového manažera odpovědného za akceptaci plnění a správce systémů.
- Zajistit spolupráci třetích stran, nebude-li možné toto zajistit pracovníky Zadavatele. Lze i formou pověření, tak aby měl Uchazeč pravomoc s třetí stranou jednat.
- Bude využívána pouze nutná součinnost pro zajištění optimálního výsledku nasazení identity managementu. Pracovníci zadavatele nebudou využíváni k zajištění projektového vedení, zápisy ze schůzek, domlouvání organizačních věcí a schůzek, zjišťování informací od třetích stran
- Zajistit HW pro běh IdM.

Harmonogram realizace

Mílníky a jejich části	Termín dokončení ve dnech
Podpis smlouvy	T0
Fáze 1 – dle smlouvy Definice rizik, eskalací, metrik projektu Definice projektového a řídicího výboru Komunikační matice Kick-off týmu - formální i neformální Sběr požadavků od zástupců zákazníka Tvorba katalogu požadavků Analýza současného stavu a požadavků zákazníka Návrh řešení Tvorba dokumentu "Analýza a návrh"	T1=T0+60
Fáze 2 – dle smlouvy Vytvoření vývojového prostředí Psaní workflow, pravidel, formulářů,... Připojování systémů Finální testování Vytvoření produkčního prostředí Instalace, konfigurace a zprovoznění IdM Dokumentace skutečné realizace Školení obsluhy a administrátorů	T2=T1 + 120
Pilotní provoz (zvýšený dohled nad již běžícím IdM) Pravidelná kontrola logů Oprava drobných chyb	T3=T2 + 15

Cenová Kalkulace

Milníky projektu	Cena bez DPH	DPH	Cena celkem s DPH
Fáze 1 – dle smlouvy Definice, Analýza a návrh řešení • SAP • AD • LDAP • Dynas a Cestovní příkazy • Procesy	360000	75600	435600
Fáze 2 – dle smlouvy Implementace řešení • Instalace – zprovoznění prostředí • SAP • AD • LDAP • Dynas a Cestovní příkazy • Automatizované procesy • Převedení do produkčního prostředí • Testování • Dokumentace • Školení	372000	78120	450120
Uživatelská identita student (počet studentů není rozhodující, licence umožňuje využít pro libovolné množství uživatelů, bez ohledu na jejich typ)	0	0	0
Celkem	732000	153720	885720