

Nabídka

VÍME JAK

Kybernetická bezpečnost pro společnost / Statutární Město Karlovy Vary

Verze 1.0

Datum vytvoření nabídky:

5. 01. 2018

Nabídka platná do:

31. 03. 2018

© 2017 AutoCont CZ a.s.

Nabídka a návrh smlouvy vytvořené společností AutoCont CZ a.s. jsou součástí know-how a obchodního tajemství společnosti AutoCont CZ a.s. a nelze je tedy bez předchozího písemného schválení společnosti AutoCont CZ a.s. dále sdělovat třetím stranám či jinak šířit. Příjemce (adresát/příjemce, jemuž je nabídka či návrh smlouvy určen) bere tuto skutečnost převzetím nabídky nebo návrhu smlouvy na vědomí a zároveň se zavazuje zabezpečit ochranu poskytnutého know-how a obchodního tajemství společnosti AutoCont CZ a.s. a zabránit jeho neoprávněnému užití jakoukoli třetí osobou. Všechny ostatní dokumenty poskytované společností AutoCont CZ a.s. (koncepty, studie, analýzy, výstupy auditů atd.) jsou chráněny jako produkt společnosti AutoCont CZ a.s. dle autorského zákona a jejich příjemce je tudíž povinen zabezpečit ochranu poskytnutého produktu společnosti AutoCont CZ a.s. a zabránit jeho neoprávněnému užití jakoukoli třetí osobou.

1 Krycí list

Krycí list nabídky veřejné zakázky „Kybernetická bezpečnost“

Zadavatel:

Název: Statutární město Karlovy Vary
Sídlo: Moskevská 21, 361 20 Karlovy Vary
IČ zadavatele: 00254657
Zastoupený: Ing. Petr Kulhánek, primátor města

Uchazeč(i):

Název: AutoCont CZ a.s.
Sídlo: Hornopolní 3322/34, 702 00 Ostarva
IČ: 47676795
DIČ: CZ47676795
Zastoupený: Ing. Zdeňkem Chobotem, ředitelem regionálního centra
Na základě: Plná moc

Kontakty v průběhu zadávacího řízení

Jméno: [redacted]
[redacted] [redacted]
[redacted] [redacted]
[redacted] [redacted]

V Karlových Varech dne 15.1.2018

[redacted]
.....
podpis

Obsah nabídky:

Dokument	Strany č:
1. Krycí list nabídky	2
2. Doklad o poskytnutí jistoty	4
3. Kopie dokladu o poskytnutí jistoty	4
4. Doklady o kvalifikaci	6
5. Čestné prohlášení o souhlasu se smluvními podmínkami	49
6. Popis nabízeného technického řešení	50
7. Údaje pro hodnocení nabídek	119
8. Kalkulace nabídkové ceny	107
Celkem stran: 148	

Rekapitulace měřitelných hodnotících kritérií:

Nabídková cena

Uvedte podle požadavků zadávací dokumentace a v následujícím členění:

<i>Nabídková cena</i>	
- bez DPH	10 972 595 Kč
- sazba DPH	21%
- výše DPH	2 304 245 Kč
- s DPH	13 276 840 Kč

Hodnotící kritérium	Hodnota	Jednotky
metodika implementace	100	body
kvalita vzdělávacích kurzů a didaktických postupů	300	body
technická úroveň nabízeného řešení	2	body

(hodnota slouží zejména pro urychlení otevírání obálek; zadavatel ji při hodnocení nabídek podrobí další kontrole)

2 Doklad o poskytnutí jistoty

Jistina 200.000 Kč – VS 47676795, byla převedena na účet zadavatele dne 10.1.2018

Zadávatel		Položka		Variabilní symbol	Císlna
Valuta	Identifikace	Císlna obrátka v oúri méné	Popis	Konstantní symbol	Specifický symbol
10.01.2018	PRÍKAZ - MULTICASH			2011327712	-818.00
10.01.2018	846299488	615.00 CZK	SATRATA MARTIN	00080	
10.01.2018	PRÍKAZ - MULTICASH			20110945	-1 503.00
10.01.2018	846299489	1 503.00 CZK	SKALA OLDŘICH	00080	
10.01.2018	PRÍKAZ - MULTICASH			2011023712	-4 475.90
10.01.2018	846299490	4 475.90 CZK	SURY KAREL	00080	
10.01.2018	PRÍKAZ - MULTICASH			2011904712	-492.00
10.01.2018	846299491	492.00 CZK	TŘEBNĚ ROMAN	00080	
10.01.2018	PRÍKAZ - MULTICASH			20110940	307.00
10.01.2018	846299492	307.00 CZK	VOJTKOVA IVANA	00080	
10.01.2018	PRÍKAZ - MULTICASH			5561574626	-289.00
10.01.2018	846299493	289.00 CZK	ACTIVE 24, S.R.O.	00080	
10.01.2018	PRÍKAZ - MULTICASH			18100187	-87 868.00
10.01.2018	846299494	87 868.00 CZK	THOMAS COOK S.R.O.	00080	
10.01.2018	PRÍKAZ - MULTICASH			8888078985	-1 089.00
10.01.2018	846299495	-1 089.00 CZK	GRANBY S.R.O.	00080	
10.01.2018	PRÍKAZ - MULTICASH			5180104818	-158.00
10.01.2018	846299496	158.00 CZK	INTERNET CZ, A.S.	00080	
10.01.2018	PRÍKAZ - MULTICASH			60762521	-486.00
10.01.2018	846299497	486.00 CZK	WED4U S.R.O.	00080	
18.01.2018	PRÍKAZ - MULTICASH			1725822457	-1 499.00
10.01.2018	846299498	1 499.00 CZK	SEND PŘEDPLATNE S.R.O.	00080	
10.01.2018	PRÍKAZ - MULTICASH			5228948487	80 000.00
10.01.2018	846299499	50 000.00 CZK	GOOGLE IRELAND, LTD.	00080	
10.01.2018	PRÍKAZ - MULTICASH			47876795	200 000.00
10.01.2018	846299500	200 000.00 CZK	STATĚKARNÍ MĚSTO KARLOVY VARY	00080	
10.01.2018	PRÍKAZ - MULTICASH			3401708880	-63 467.00
10.01.2018	846299501	63 467.00 CZK	MT LEGAL S.R.O., ADVOKÁTNÍ KANCELÁŘ	00080	

3 Identifikační údaje uchazeče

Obchodní jméno: AutoCont CZ a.s.

Právní forma: Akciová společnost

Sídlo firmy: Hornopolská 3322/34, 702 00, Ostrava

IČO: 47676795

DIČ: CZ47676795

Tel: [REDACTED]

Fax: [REDACTED]

Bankovní spojení: Česká spořitelna a.s., číslo účtu: [REDACTED]

Základní jmění: 25 000 000 Kč

Certifikace ISO: ISO 9001 – Řízení kvality
ISO 20000 – Řízení IT služeb
ISO 27001 – Řízení bezpečnosti informací
ISO 14001 – Řízení v oblasti životního prostředí

Převažující předmět činnosti:

/ komplexní dodávky výpočetních technik
/ dodávky řešení a služeb v oblasti informačních technologií

Statutární orgán představenstvo:

/ Ing. Jaroslav Bielek, předseda představenstva
/ Ing. Martin Stejskal, místopředseda představenstva
/ Ing. Vlastimil Palata, místopředseda představenstva
/ Ing. et Mgr. Ondřej Matušík, PhD., člen představenstva
/ Jindřich Zimola, člen představenstva

Kontaktní osoba pro styk se zadavatelem:

/ Jiří KLubát
/ AutoCont CZ a.s.
/ Sokolovská 996/130, 36005 Karlovy Vary
/ Tel: +42 [REDACTED]

4 Doklady o kvalifikaci

Čestné prohlášení uchazeče o kvalifikaci

Dodavatel(é):

Název: AutoCont CZ a.s.

Sídlo: Hornopolní 3322/34, 702 00 Ostrava

IČ: 47676795

I. O základní způsobilosti:

Prohlašuji tímto, že jsme způsobilý dodavatel; způsobilým není dodavatel, který

- a. byl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 ZZVZ nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží,
- b. má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
- c. má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
- d. má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- e. je v likvidaci, proti němuž bylo vydáno rozhodnutí o úpadku, vůči němuž byla nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.

Podmínku podle písm. a. splňuje

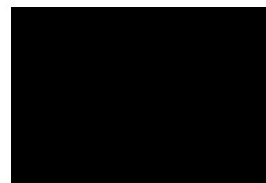
- dodavatel a zároveň každý člen statutárního orgánu;

II. O profesní způsobilosti:

Prohlašuji tímto, že jako uchazeč o veřejnou zakázku

- a. jsme zapsáni v Obchodním rejstříku;

V Karlových Varech dne 15.1.2018



.....
Ing Zdeněk Chobot
na základě plné moci

PLNÁ MOC

Zmocnitel: **AutoCont CZ a.s.**
Ostrava - Moravská Ostrava, Hornopolská 3322/34, PSČ 702 00
IČ 47676795
zapsaný do obchodního rejstříku u KS v Ostravě, oddíl B, vložka 814
jednajícím místopředsedou představenstva Ing. Martinem Stejskalem

Zmocněnec: **Zdeněk Chobot**
funkce: ředitel regionálního obchodního centra
r.č.: [REDACTED]
trvale bytem: [REDACTED]

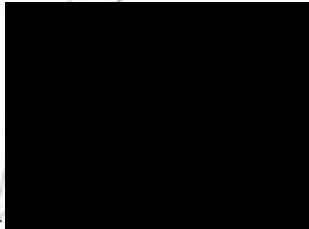
Zmocnitel uděluje tímto zmocněnci plnou moc k tomu, aby:

- 1) za zmocnitele jednal s jinými subjekty ve věcech veřejných zakázek vyhlášených podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „zákon“);
- 2) za zmocnitele podával nabídky v rámci zadávacích řízení na plnění veřejných zakázek podle zákona, podepisoval listiny související s podáváním takových nabídek včetně návrhů závazných smluv, které budou součástí takových nabídek.

Tato plná moc se uděluje na období ode dne jejího vystavení do [REDACTED]

Zmocnitel je oprávněn tuto plnou moc kdykoli písemně odvolat.

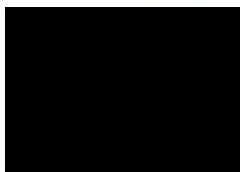
V Ostravě dne 3.1.2018



AutoCont CZ a.s.
Ing. Martin Stejskal, místopředseda představenstva

Plnou moc přijímám

V Karlových Varech dne [REDACTED]



Zdeněk Chobot
ředitel regionálního obchodního centra

Výpis ze seznamu kvalifikovaných dodavatelů

vedeného podle § 226 a násled. zákona č. 134/2016 Sb., o zadávání veřejných zakázek

Údaje o dodavateli zapsané v seznamu k 18.12.2017

1. Identifikační údaje o dodavateli**1.1. Obchodní firma/Název**

AutoCont CZ a.s.

1.2. SídloHornopolská 3322/34
70200 Ostrava - Moravská Ostrava
Česká republika**1.3. IČO**

47676795

1.4. Statutární orgán

Jméno a příjmení statutárního orgánu nebo jeho členů	Funkce ve statutárním orgánu
Ing. Jaroslav Bolek	předseda představenstva
Ing. Vlastimil Palata	místopředseda představenstva
Martin Stejskal	místopředseda představenstva
Oldřich Skála	člen představenstva
Jindřich Zimola	člen představenstva

Způsob jednání

Za společnost jedná člen představenstva samostatně.

2. Základní způsobilost, jejíž splnění dodavatel prokázal

Dodavatel prokázal Ministerstvu pro místní rozvoj, že splňuje podmínku podle:

- § 74 odst. 1 písm. a)
nebyl v zemi svého sídla v posledních 5 letech pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 zákona nebo obdobný trestný čin podle právního řádu země sídla dodavatele, k zahlazeným odsouzením se nepřihlíží, (tento požadavek splnily i všechny fyzické a právnické osoby uvedené v bodech 1.1. – 1.4. tohoto výpisu),
- § 74 odst. 1 písm. b)
nemá v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
- § 74 odst. 1 písm. c)
nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
- § 74 odst. 1 písm. d)
nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- § 74 odst. 1 písm. e)
není v likvidaci, nebylo proti němu vydáno rozhodnutí o úpadku, nebyla vůči němu nařízena nucená správa podle jiného právního předpisu nebo není v obdobné situaci podle právního řádu země sídla dodavatele.

3. Profesní způsobilost, jejíž splnění dodavatel prokázal

Dodavatel prokázal, že splňuje podmínku podle:

3.1. § 77 odst. 1 – profesní způsobilost

Výpis z obchodního rejstříku

3.2. § 77 odst. 2 písm. a) – oprávnění k podnikání

Název dokladu	Vystavil	Předmět podnikání	Obory činnosti	Datum vystavení	Datum platnosti
Výpis z živnostenského rejstříku	Magistrát města Ostravy	Činnost účetních poradců, vedení účetnictví, vedení daňové evidence		02.05.2012	
Výpis z živnostenského rejstříku	Magistrát města Ostravy	Poskytování technických služeb k ochraně majetku a osob		02.05.2012	
Výpis z živnostenského rejstříku	Magistrát města Ostravy	Viz poznámka 1 za tabulkou		02.05.2012	
Výpis z živnostenského rejstříku	Magistrát města Ostravy	Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona	Viz, poznámka 2 za tabulkou	02.05.2012	

Pozn. 1

Výroba, instalace, opravy elektrických strojů a přístrojů, elektronických a telekomunikačních zařízení

Pozn. 2

Výroba elektronických součástek, elektrických zařízení a výroba a opravy elektrických strojů, přístrojů a elektronických zařízení pracujících na malém napětí

Výroba strojů a zařízení

Zprostředkování obchodu a služeb

Velkoobchod a maloobchod

Poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a

související činnosti a webové portály

Pronájem a půjčování věcí movitých

Poradenská a konzultační činnost, zpracování odborných studií a posudků

Příprava a vypracování technických návrhů, grafické a kresličské práce

Projektování elektrických zařízení

Výzkum a vývoj v oblasti přírodních a technických věd nebo společenských věd

Testování, měření, analýzy a kontroly

Reklamní činnost, marketing, mediální zastoupení

Služby v oblasti administrativní správy a služby organizačně hospodářské povahy

Mimoškolní výchova a vzdělávání, pořádání kurzů, školení, včetně lektorské činnosti

Poskytování technických služeb


4. Datum podání žádosti o zápis do seznamu a jiné rozhodné informace

Rozhodnutí o zápisu dodavatele do seznamu nabylo právní moci dne 20.07.2005.
Poslední aktualizace zápisu v seznamu byla provedena dne 19.07.2017.

Správnost tohoto výpisu se potvrzuje
Česká republika - Ministerstvo pro místní rozvoj

Datum: 18.12.2017

Evidenční číslo: W17120000747

 Elektronicky podepsáno
dne 18.12.2017
Česká republika
Ministerstvo pro místní
rozvoj (IC: 65502221)

Veřejný rejstřík – výpisy platných

Ověřuji pod pořadovým číslem V 516/2017, že tato listina, která vznikla převedením výstupu z informačního systému veřejné správy z elektronické podoby do podoby listinné, skládající se z 3 listů, se doslovně shoduje s obsahem výstupu z informačního systému veřejné správy v elektronické podobě.

Ověřující osoba: ██████████

V Ostravě dne 18. 12. 2017

Podpis:



ROZHODNUTÍ SPOLEČNOSTI

AutoCont Holding a.s.

jako jediného akcionáře vykonávající působnost valné hromady společnosti

AutoCont CZ a.s.

AutoCont Holding a.s., společnost založená a existující podle českého práva, se sídlem Hornopolní 3322/34, Ostrava – Moravská Ostrava, PSČ 702 00, Česká republika, identifikační číslo 278 05 786, zapsaná v obchodním rejstříku vedeném Krajským soudem v Ostravě pod spisovou značkou B 3267 (dále jen "Jediný akcionář"), je jediným akcionářem společnosti **AutoCont CZ a.s.**, založené a existující podle českého práva, se sídlem Hornopolní 3322/34, Ostrava - Moravská Ostrava, PSČ 702 00, Česká republika, identifikační číslo 476 76 795, zapsané v obchodním rejstříku vedeném Krajským soudem v Ostravě pod spisovou značkou B 814 (dále jen "Společnost").

Jediný akcionář vykonávající působnost valné hromady Společnosti dle ustanovení § 12 odst. 1 zákona č. 90/2012 Sb., zákona o obchodních společnostech a družstvech (zákon o obchodních korporacích), v platném znění (dále jen "ZOK") tímto rozhoduje o tom, že:

- a) Z představenstva Společnosti se k 29. listopadu 2017 **odvolává** pan z funkce člena představenstva pan Oldřich Skála, narozený dne 24. března 1956, trvale bytem Zborovská 2080/32, Brno – Žabovřesky, PSČ 616 00, Česká republika;
- b) Pan Ondřej Matušík, dat. nar. 18. srpna 1982, trvale bytem Blatnice pod svatým Antonínkem 749, okr. Hodonín, PSČ 69671, Česká republika se ke dni 1. prosince 2017 **jmenuje** členem představenstva Společnosti.

V Praze dne 29. listopadu 2017

Za **AutoCont Holding a.s.**

Podpis:

Jméno:

Funkce:

Vlastimil Pálnita

Místopředseda představenstva

Výpis

z obchodního rejstříku, vedeného
Krajským soudem v Ostravě
oddíl B, vložka B14

Datum vzniku a zápisu:	29. dubna 1994
Spisová značka:	B 814 vedená u Krajského soudu v Ostravě
Obchodní firma:	AutoCont CZ a.s.
Sídlo:	Hornopolská 3322/34, Moravská Ostrava, 702 00 Ostrava
Identifikační číslo:	476 76 795
Právní forma:	Akciová společnost
Předmět podnikání:	Činnost účetních poradců, vedení účetnictví, vedení daňové evidence Poskytování technických služeb k ochraně majetku a osob Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona Výroba, instalace, opravy elektrických strojů a přístrojů, elektronických a telekomunikačních zařízení
Statutární orgán - představenstvo:	
předseda představenstva:	JAROSLAV BIOLEK, dat. nar. 18. června 1969 Chudčická 1310/8, Bystrc, 635 00 Brno Den vzniku funkce: 20. června 2014 Den vzniku členství: 20. června 2014
místopředseda představenstva:	VLASTIMIL PALATA, dat. nar. 11. července 1964 Vičická 699, Horní Staré Město, 541 02 Trutnov Den vzniku funkce: 20. června 2014 Den vzniku členství: 20. června 2014
místopředseda představenstva:	MARTIN STEJSKAL, dat. nar. 16. dubna 1969 Havlíčková 743, 664 01 Bilovice nad Svitavou Den vzniku funkce: 6. června 2017 Den vzniku členství: 6. června 2017
člen představenstva:	JINDŘICH ZIMOLA, dat. nar. 7. září 1979 Hlučínská 865/244b, Peřkovice, 725 29 Ostrava Den vzniku členství: 6. června 2017
člen představenstva:	ONDŘEJ MATUŠTÍK, dat. nar. 18. srpna 1982 č.p. 749, 696 71 Blatnice pod Svatým Antonínkem Den vzniku členství: 1. prosince 2017
Počet členů:	5
Způsob jednání:	Za společnost jedná člen představenstva samostatně.
Dozorčí rada:	
předseda dozorčí rady:	MARTIN GRIGAR, dat. nar. 21. května 1962 Gen. Sochora 6213/12a, Poruba, 708 00 Ostrava

	Den vzniku funkce: 1. dubna 2016 Den vzniku členství: 1. dubna 2016
člen dozorčí rady:	JAROMÍR BABINEC, dat. nar. 21. října 1969 Rytiřova 809/4, Kamýk, 143 00 Praha 4 Den vzniku členství: 20. června 2014
člen dozorčí rady:	BARBORA MÍČKOVÁ, dat. nar. 30. ledna 1963 č.p. 680, 739 45 Fryčovice Den vzniku členství: 20. června 2014
Počet členů:	3
Jediný akcionář:	AutoCont Holding a.s., IČ: 278 05 786 Hornopolsní 3322/34, Moravská Ostrava, 702 00 Ostrava
Akcie:	250 ks kmenové akcie na jméno v zaknihované podobě ve jmenovité hodnotě 100 000,- Kč
Základní kapitál:	25 000 000,- Kč Splaceno: 25 000 000,- Kč
Ostatní skutečnosti:	Obchodní korporace se podřídila zákonu jako celku postupem podle § 777 odst. 5 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech. Na základě smlouvy o prodeji části podniku ze dne 26.1.2012 uzavřené mezi společností AutoCont CZ a.s., IČ: 47676795 jako prodávající a společností Pontech s.r.o., IČ: 27977315 jako kupující byla prodána část podniku společnosti AutoCont CZ a.s. označená jako Divize SAP, která představuje samostatnou organizační složku společnosti AutoCont CZ a.s. ve smyslu ust. § 487 obchodního zákoníku, společností Pontech s.r.o. Na společnost AutoCont CZ a.s., přešla část jmění rozdělované společnosti AG COM, a.s., IČO: 47452081, se sídlem Nám. Míru 22, 503 03 Smičice, která byla uvedena v projektu rozdělení odštěpením sloučením, vyhotoveném dne 12.5.2016 a schváleném dne 20.6.2016. Na společnost AutoCont CZ a.s., jako nástupnickou společnost, přešlo v důsledku fúze sloučením jmění zanikajících společností AutoCont On Line, a.s., IČO: 26418436, se sídlem Praha - Chodov, Líbalova 2348/1, PSČ 149 00, a COMA ZÁLOHOVACÍ SYSTÉMY a.s., IČO: 60792965, se sídlem Nemocniční 987/12, Moravská Ostrava, 702 00 Ostrava.



Číslo žádosti: 244067597
Žádost doručena: 30.11.2017 09:02:00
Zpracováno: 30.11.2017 09:02:00
Počet záznamů v ČR: 0 (nula)
Počet příloh: 0 (nula)



Na žádost osoby s údaji níže uvedenými se vydává:

VÝPIS Z EVIDENCE REJSTRÍKU TRESTŮ FYZICKÝCH OSOB

Osobní údaje:

Jméno:	ONDŘEJ
Příjmení:	MATUŠTÍK
Rodné příjmení:	MATUŠTÍK
Data narození / rodné číslo:	[REDACTED]
Pohlaví:	MUZ
Místo / okres narození:	KYJOV / HODONÍN
Stát narození:	ČESKÁ REPUBLIKA
Státní občanství:	ČESKÁ REPUBLIKA

Obsah evidence Rejstříku trestů České republiky:

Nejsou žádné informace o odsouzení dotčené osoby

Konec obsahu evidence Rejstříku trestů České republiky.

Konec sestavy



Kulaté razítko a podpis

Případně nepřesné údaje mohou záležet na stavu uvedenou osobu, aby mohla být okamžitě provedeno příslušné. Tento dokument neslouží k prokazování totožnosti fyzické osoby.

Technické kvalifikace

Seznam významných dodávek a služeb:

Dodávka a implementace řešení SIEM (Security Information and Event Management) v hodnotě min. 1 milion Kč bez DPH

Objednatel	Název zakázky	Předmět plnění	doba plnění	kontakt	finanční rozsah
ČSOB Pojišťovna, a.s.	SIEM řešení	Dodávka a implementace řešení SIEM (Security Information and Event Management) na platformě IBM Security QRadar včetně servisní podpory	12/2016	[REDACTED]	více než 1 mil. Kč bez DPH
Česká republika - Úřad vlády České republiky	Nákup a implementace zařízení pro ukládání, archivování a vyhodnocování systémových událostí (logů) - SIEM a jeho podpora	Dodávka a implementace řešení SIEM (Security Information and Event Management) na platformě IBM Security QRadar včetně servisní podpory	1/2016	[REDACTED]	více než 1,5 mil. Kč bez DPH
Krajský úřad Zlínského kraje	Bezpečnostní infrastruktura a rozvoj služeb Technologického centra kraje	Dodávka a implementace řešení SIEM (Security Information and Event Management)	2/2015	[REDACTED]	více jak 1 mil. Kč bez DPH

Dodávka a implementace systému pro správu identit (IDM - Identity management) pro více než 500 spravovaných identit v hodnotě min. 800.000,- Kč bez DPH

Objednatel	Název zakázky	Předmět plnění	doba plnění	kontakt	finanční rozsah
Liberecký kraj	Řízení uživatelských přístupů ke službám TC města	Dodávka a implementace IDM systému pro více jak 500 spravovaných identit.	8/2015	Jitka Balounová [REDACTED]	více než 1 mil. Kč bez DPH
Statutární Město Brno	Řízení uživatelských přístupů ke službám TC města	Dodávka a implementace IDM systému pro více jak 500 spravovaných identit.	10/2015	Vladimír Halm, [REDACTED]	více než 4,5 mil. Kč bez DPH
Univerzita Palackého v Olomouci	Implementace Identity Management Systému/2015	Dodávka a implementace IDM systému pro více jak 500 spravovaných identit.	7/2016	[REDACTED]	více než 900tis. Kč bez DPH

Zajištění vzdělávání v oblasti ICT v rozsahu min. 300.000 Kč bez DPH

Objednatel	Název zakázky	Předmět plnění	doba plnění	kontakt	finanční rozsah
Aircraft Industries, a.s.	Podpora odborného vzdělávání ve společnosti	Vzdělávání zaměstnanců v oblasti ICT - Windows Server 2012, SQL Server 2012, SharePoint 2013, Vmware 5.5	5/2015	[REDACTED]	více jak 400 tis. Kč bez DPH
MSA, a.s.	Podpora odborného vzdělávání ve společnosti	Vzdělávání v oblasti ICT - Windows Server 2012, SharePoint 2013, Exchange Server 2013, VisualBasic .NET	9/2015	[REDACTED]	více jak 400 tis. Kč bez DPH

Provedení phishingových testů pro minimálně 50 adresátů / e-mailových schránek

Objednatel	Název zakázky	Předmět plnění	doba plnění	kontakt	finanční rozsah
Léčebné lázně Jáchymov a.s.	Poštovní a archivační systém	Součástí projektu bylo provedení phishingových testů pro 100 adresátů / e-mailových schránek	9/2017	Pavel Kvapil [redacted]	více jak 40 tis. Kč bez DPH
Nejdecká česárna vlny, a.s.	Kyberbezpečnost	Provedení phishingových testů pro 50 adresátů / e-mailových schránek včetně následného školení uživatelů	9/2017	Pavel Jirásek [redacted]	více jak 70 tis. Kč bez DPH

Realizační tým:

Jméno a příjmení	Role v projektu	Dosažené vzdělání	Zaměstnavatel	Délka odborné praxe	Certifikace
Martin Dušek	projektový manažer	vysokoškolské	AutoCont CZ a.s.	více jak 3 roky praxe v oboru informačních technologií	certifikace senior projektového manažera dle PRINCE2 na úrovni komplexního řízení projektů
Lumír Vojtěchovský	vedoucí školicího týmu	vysokoškolské	AutoCont CZ a.s.	více jak 3 roky praxe v oblasti vzdělávání	x
Luděk Mandok	specialista kybernetické bezpečnosti	středoškolské	AutoCont CZ a.s.	více jak 3 roky praxe v oblasti kontroly a řízení bezpečnosti informačních technologií	certifikace CISA v oblasti kontroly a řízení bezpečnosti informačních technologií
Jiří Svoboda	technický specialista hardware	středoškolské	AutoCont CZ a.s.	více jak 3 roky praxe v oboru serverového hardware	certifikace na implementaci a servis nabízeného serverového hardware HP Blade
Daniel Staněk	technický specialista serverové virtualizace	vysokoškolské	AutoCont CZ a.s.	více jak 5 let praxe v oblasti serverové virtualizace	certifikace pro návrh a implementaci serverové virtualizace Vmware
Leo Sedlák	technický specialista sítí	vysokoškolské	AutoCont CZ a.s.	více jak 3 roky praxe v oboru počítačových sítí	certifikace na návrh a implementaci a nabízených aktivních prvků - síťových přepínačů HP
Vladimír Kolbábek	technický specialista IDM	Vyšší odborné vzdělání	AutoCont CZ a.s.	více jak 5 let praxe v oblasti informačních technologií	x

Profesní životopis

ING., MARTIN DUŠEK
PROJEKTOVÝ VEDOUCÍ

AutoCont CZ a.s.
Adresa Hornopolní 3322/34, 702 00 Ostrava
Telefon +420 59 73 22 22
E-mail m.dusek@autocont.cz

NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ

- Období (od – do) 2002-2008
- Název a typ organizace VŠB Technická univerzita Ostrava
- Získaný titul Ing.
- Obor **Systémové inženýrství a informatika**

PROFESNÍ PRAXE

více jak 3 roky praxe v oboru informačních technologií
více jak 3 roky praxe v projektovém řízení na požadované úrovni

- Období (od – do) 2007 - doposud
- Jméno a adresa zaměstnavatele AutoCont CZ a.s. Nemocniční 12, 702 00 Ostrava
- Dosažená pozice **Projektový vedoucí**
- Hlavní pracovní náplň a odpovědnost Vedení projektů v oblastech systémové infrastruktury
Vedení týmů a řízení projektů s důrazem na náklady, kvalitu, řízení rizik, komunikaci a řízení scope a času projektů
- Období (od – do) 2006 – 2007
- Jméno a adresa zaměstnavatele Okin BPO – Ostrava, Českosobratská 3321/46, 702 00 Ostrava – Moravská Ostrava
- Dosažená pozice **Delivery Manager**
- Hlavní pracovní náplň a odpovědnost Koordinace mezinárodních projektů
Řízení projektů v rámci mezinárodních virtuálních týmů

PROJEKTY REALIZOVANÉ V AUTOCONT CZ A.S.

- Období (od – do) 3Q/2014-2Q/2015
- Název projektu **Migrace SharePoint 2010**
- Zadavatel projektu ČEZ ICT Services, a.s.
- Popis projektu Upgrade SharePoint 2010 na verzi 2013
- Role na projektu Projektový vedoucí
- kontakt Miroslav Barák, miroslav.barak@autocont.cz
- finanční rozsah projektu Více jak 2 mil. Kč bez DPH
- Období (od – do) 1Q/2014-3Q/2015
- Název projektu **DHL SharePoint 2013 Migration**
- Zadavatel projektu Microsoft s.r.o.
- Popis projektu Migrace platformy SharePoint 2007 na SharePoint 2013
- Role na projektu Projektový vedoucí
- kontakt Vlastimil Tesař, vlastimil.tesar@autocont.cz

- finanční rozsah projektu Více jak 2 mil. Kč bez DPH
- Období (od – do) 3Q/2012-3Q/2013
- Název projektu **Rozvoj eGovernmentu v Olomouckém kraji**
- Zadavatel projektu Olomoucký kraj
- Popis projektu Vybudování celků - Technologické centrum, Digitální mapa veřejné správy, Digitalizace a ukládání, Integrace vnitřního chodu úřadu, Datový sklad
- Role na projektu Projektový vedoucí
- kontakt František Jelínek, [REDACTED]
- finanční rozsah projektu Více jak 2 mil. Kč bez DPH
- Období (od – do) 2Q/2009– 3Q/2011
- Název projektu **Implementace projektů v oblastech systémové infrastruktury**
- Zadavatel projektu SYNOT Tip a.s.
- Popis projektu Implementace řešení pro zajištění vysoké dostupnosti služeb datového centra
Implementace systémové infrastruktury pro sázkový systém ČR
Implementace systémové infrastruktury pro sázkový systém SK
Implementace síťové infrastruktury pro datové centrum
Implementace technologie virtualizace diskových polí pro datové centrum
- Role na projektu Projektový vedoucí
- kontakt Michal Gajdošik [REDACTED]
- finanční rozsah projektu Více jak 2 mil. Kč bez DPH

ŠKOLENÍ A CERTIFIKACE

- Profesní školení Školení a certifikace Certificate of Completion – Cisco Sales Essentials Školení Školení a certifikace ITIL v3 foundation
Školení k certifikaci podle standardu IPMA – PM Consulting
Správa sítě MS Windows Server 2003
Školení Vedení projektových schůzek a dosahování cílů - Scott&Hagget
Školení Vyjednávání pro projektové manažery - Scott&Hagget
Školení Prezentační dovednosti - Scott&Hagget
Školení Leadership pro projektové manažery - Scott&Hagget
Školení skupinová dynamika - Interquality
Školení Přesvědčivý projev a rétorika - Scott&Hagget
Školení Řízení diskuze pro Projektové Manažery – facilitace - Scott&Hagget
Školení PRINCE2
- Certifikace Certifikace Project Management Professional (PMP)
Certifikace PRINCE2 Practitioner
Certifikace ITIL Foundation v2, v3
Cisco Sales Expert
- Členství Člen společnosti pro projektové řízení (SPŘ)
Člen Project Management Institut (PMI)

JAZYKOVÉ ZNALOSTI

MATEŘSKÝ JAZYK **Čeština**

OSTATNÍ JAZYKY

Angličtina

- Čtení VÝBRONĚ
- Psaní DOBRĚ
- Mluvený projev PLYNNĚ

Španělština

- Čtení ZÁKLADY
- Psaní ZÁKLADY
- Mluvený projev ZÁKLADY



APMG-International

THIS IS TO CERTIFY THAT

Martin Dušek

IS A

**PRINCE2[®]
Registered Practitioner**

MEETING STANDARDS to APMG/QMS/Registered Practitioner Certification as stated in the APMG Quality Management System.

DATE
01 August 2013

REGISTRATION NUMBER
P2R/NLPB190426

CERTIFICATE NUMBER
02391062-01-34CD

Alan Harpham
APMG Chairman

This certificate is valid for 5 calendar years from the Effective Date.



This certificate remains the property of The APMG Group Ltd and shall be returned immediately on request.
The APMG Group Limited, Sword House, Totteridge Road, High Wycombe, Buckinghamshire, HP11 6DG,
England
Telephone +44 (0) 1494 452 450 Fax +44 (0) 1494 459 559 www.apmg.com
Registered in England No: 2661902

This examination was based on the 2009 edition

The Swirl logo is a trade mark of The Callnet Centre
PRINCE2 is a registered trade mark of The Callnet Centre

00757421



Prohlašuji, že všechny výše uvedené informace jsou správné a úplné.

Místo: Praha

Datum: 8.1.2018



Martin Dušek

PROFESNÍ ŽIVOTOPIS – DOKLAD O ODBORNÉ KVALIFIKACI

Jméno Příjmení	LUMÍR VOJTĚCHOVSKÝ
Role	Lektor - Vedoucí školicího týmu
Zaměstnavatel	AutoCont CZ a.s.
Adresa	Hornopolská 3322/34, 702 00 Ostrava
Telefon	[REDAKCE]
E-mail	[REDAKCE]

NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ

Období (od – do)	1986 – 1991
Název a typ organizace	Vysoká škola báňská - Technická univerzita Ostrava, fakulta strojní
Úroveň v národní klasifikaci	Inženýr

CERTIFIKACE

Certifikát ECDL číslo 0303CzC000117

CELKOVÁ DÉLKA PRAXE V OBORU 23 let

PROFESNÍ PRAXE

Období (od – do)	1998 - doposud
Jméno a adresa zaměstnavatele	AutoCont CZ a.s., Hornopolská 3322/34, 702 00 Ostrava
Dosažená pozice	Ředitel školicího střediska
Hlavní pracovní náplň a odpovědnost	Řízení a rozvoj školicích středisek v ČR pro společnost AutoCont CZ a.s., vedení týmu pracovníků školicího střediska, projektové vedení klíčových projektů v oblasti vzdělávání, získávání akreditací, obchodní činnost, lektor, přednášková činnost
Období (od – do)	1994 - 1998
Jméno a adresa zaměstnavatele	AutoCont s.r.o, Nemocniční 12, 702 00 Ostrava
Dosažená pozice	Vedoucí školicího střediska
Hlavní pracovní náplň a odpovědnost	Vybudování školicího střediska pro společnost AutoCont v Ostravě, personální zajištění lektorů, obchodní činnost, organizace školicích a přidružených aktivit, lektor, přednášková činnost
Období (od – do)	1991 - 1994
Jméno a adresa zaměstnavatele	Vysoká škola báňská - Technická univerzita Ostrava, Fakulta strojní, Institut dopravy
Dosažená pozice	Odborný Asistent
Hlavní pracovní náplň a odpovědnost	Vedení cvičení v inženýrských studijních programech institutu dopravy, spolupráce na vývoji laboratoře sypkých hmot

REALIZOVANÉ PROJEKTY

- Období (od – do) Únor – Červen 2015
- Název projektu Podpora odborného vzdělávání ve společnosti
- Zadavatel projektu Aircraft Industries a.s., Kunovice
- Popis projektu Vzdělávání zaměstnanců v oblasti ICT - Windows Server 2012, SQL Server 2012, SharePoint 2013, Vmware 5.5
- Role na projektu Lektor - Vedoucí školicího týmu
- Kontakt Monika Hořáková, [REDACTED]

- Období (od – do) Duben – září 2015
- Název projektu Podpora odborného vzdělávání ve společnosti
- Zadavatel projektu MSA, a.s.
- Popis projektu Vzdělávání v oblasti ICT - Windows Server 2012, SharePoint 2013, Exchange Server 2013, VisualBasic .NET
- Role na projektu Lektor - Vedoucí školicího týmu
- Kontakt Jiří Vehovský, [REDACTED]

- Období (od – do) Červen 2016
- Název projektu Office 365 Ambassadors
- Zadavatel projektu Microsoft ČR, s.r.o.
- Popis projektu Školení ambasadů Magistrátu města Hradec Králové k produktům Microsoft Office 365 s cílem vytvoření týmů vyškolených a zkušených uživatelů, kteří pomáhají dalším uživatelům magistrátu v užívání MS Office 365.
- Role na projektu Lektor - Vedoucí školicího týmu
- Kontakt Vlastimil Tesar, [REDACTED]

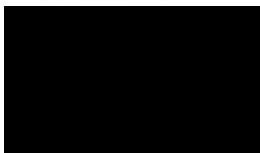
- Období (od – do) Srpen – Září 2016
- Název projektu POVEZ II
- Zadavatel projektu DIGI Czech Republic, s.r.o.
- Popis projektu Školení zaměstnanců DIGI Czech Republic, s.r.o. – Procesní řízení se zaměřením na řešení incidentů, Outlook ve firemní komunikaci a plánování a Grafické programy k tvorbě barevných manuálů
- Role na projektu Lektor - Vedoucí školicího týmu
- Kontakt Martin Gavenda, [REDACTED]

- Období (od – do) Listopad 2016 – Únor 2017
- Název projektu Školení zaměstnanců Celní správy
- Zadavatel projektu Česká republika – Generální ředitelství cel Praha
- Popis projektu Školení zaměstnanců Celní správy – Podpora a odstraňování potíží ve Windows 10
- Role na projektu Lektor - Vedoucí školicího týmu
- Kontakt Václav Dula, [REDACTED]

AUTOCONT

Prohlašuji, že všechny výše uvedené informace jsou správné a úplné.

Místo: Ostrava
Datum: 8.1.2018



PROFESNÍ ŽIVOTOPIS - DOKLAD O ODBORNÉ KVALIFIKACI

Jméno Příjmení	LUDEK MANDOK
Role	Specialista kybernetické bezpečnosti
Zaměstnavatel	AutoCont CZ a.s.
Adresa	Hornopolní 3322/34, 702 00 Ostrava
Telefon	[REDACTED]
E-mail	[REDACTED]

DÉLKA ODBORNÉ PRAXE – VÍCE JAK 3 ROKY V OBLASTI KONTROLY A ŘÍZENÍ BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ
NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ

Období (od – do)	1981-1985
Název a typ organizace	SPŠ strojní a elektrotechnická, obor měřicí a automatizační technika
Získaný titul	maturita
Úroveň vzdělání	středoškolské odborné

PROFESNÍ PRAXE

Období (od – do)	2001 - dosud
Jméno a adresa zaměstnavatele	AutoCont CZ a.s., Hornopolní 3322/34, 702 00 Ostrava
Dosažená pozice	Konzultant bezpečnosti IS
Hlavní pracovní náplň a odpovědnost	Konzultace bezpečnosti IS, návrh bezpečnostních systémů a opatření. Auditor bezpečnosti IS – zpracovávání bezpečnostních auditů, analýz rizik, bezpečnostní dokumentace, řízení bezpečnosti projektů atd.
Období (od – do)	2000 - 2001
Jméno a adresa zaměstnavatele	Norman Data Defense, ASA (Norsko)
Dosažená pozice	Specialista pre-sale
Hlavní pracovní náplň a odpovědnost	Pre-sale antivirového systému Norman Antivirus a šifrovacích systémů IronWare. Návrh bezpečnostních projektů.
Období (od – do)	1996 - 2000
Jméno a adresa zaměstnavatele	AEC, spol. s.r.o
Dosažená pozice	Specialista pre-sale a obchodník
Hlavní pracovní náplň a odpovědnost	Pre-sale a prodej antivirových systémů McAfee, F-Prot, ThunderByte a šifrovacích systémů PGP, IronWare. Návrh bezpečnostních projektů.
Období (od – do)	1994 - 1996
Jméno a adresa zaměstnavatele	SOS Trade, s.r.o
Dosažená pozice	Specialista pre-sale a obchodník
Hlavní pracovní náplň a odpovědnost	Vývoj, pre-sale a prodej antivirového systému Tři psi
Období (od – do)	1991 - 1994
Jméno a adresa zaměstnavatele	Tiskárna periodik, a.s.
Dosažená pozice	Správce počítačové sítě
Hlavní pracovní náplň a odpovědnost	Správa počítačových sítí – Apple a Novell
Období (od – do)	1985-1991
Jméno a adresa zaměstnavatele	Kancelářské stroje, k.u.ó.
Dosažená pozice	Technik výpočetních systémů
Hlavní pracovní náplň a odpovědnost	Servis počítačů SMEP SM 3-20, SM 4-20 a SM 52-11

ŠKOLENÍ A CERTIFIKACE

Období (od – do)	2009
Název	ISACA - Certified Information Systems Auditor
Získaný titul	CISA
Období (od – do)	2010
Název	ISACA - Certified in Risk and Information Systems Control
Získaný titul	CRISC
Období (od – do)	2014
Název	ISACA - Certified Information Security Manager
Získaný titul	CISM
Období (od – do)	2008 (TechU Boise, ID, USA) 2010 (TechU Boblingen, Německo)
Název	HP IPG Accredited PreSale Professional a PreSale Consultant
Získaný titul	HP IPG APP, HP IPG APC
Období (od – do)	2007
Název	ITIL – IT Service management (Foundation Certificate)
Získaný titul	ITIL v2
Období (od – do)	2010
Název	Mcafee Sales Certification
Období (od – do)	2008
Název	Proověření na úroveň D. Národní bezpečnostní úřad.
Období (od – do)	2005
Název	Symantec Security Sales Knowledge Award
Období (od – do)	2005
Název	CA Security Threat Management
Období (od – do)	2005
Název	RSA SecureWorld University

JAZYKOVÉ ZNALOSTI

MATEŘSKÝ JAZYK	čeština
OSTATNÍ JAZYKY	
	slovenština
Čtení	VÝBORNĚ
Psaní	ZÁKLADY
Mluvený projev	ZÁKLADY
	angličtina
Čtení	VÝBORNĚ
Psaní	DOBŘE
Mluvený projev	DOBŘE
	polština
Čtení	DOBŘE
Psaní	ZÁKLADY
Mluvený projev	ZÁKLADY

ŠKOLENÍ A CERTIFIKACE

Období (od – do)	2009
Název	ISACA - Certified Information Systems Auditor
Získaný titul	CISA
Období (od – do)	2010
Název	ISACA - Certified in Risk and Information Systems Control
Získaný titul	CRISC
Období (od – do)	2014
Název	ISACA - Certified Information Security Manager
Získaný titul	CISM
Období (od – do)	2008 (TechU Boise, ID, USA) 2010 (TechU Boblingen, Německo)
Název	HP IPG Accredited PreSale Professional a PreSale Consultant
Získaný titul	HP IPG APP, HP IPG APC
Období (od – do)	2007
Název	ITIL – IT Service management (Foundation Certificate)
Získaný titul	ITIL v2
Období (od – do)	2010
Název	Mcafee Sales Certification
Období (od – do)	2008
Název	Prověření na úrovni D. Národní bezpečnostní úřad.
Období (od – do)	2005
Název	Symantec Security Sales Knowledge Award
Období (od – do)	2005
Název	CA Security Threat Management
Období (od – do)	2005
Název	RSA SecureWorld University

JAZYKOVÉ ZNALOSTI

MATEŘSKÝ JAZYK	čeština
OSTATNÍ JAZYKY	slovenština
Čtení	VÝBORNĚ
Psaní	ZÁKLADY
Mluvený projev	ZÁKLADY
	angličtina
Čtení	VÝBORNĚ
Psaní	DOBŘE
Mluvený projev	DOBŘE
	polština
Čtení	DOBŘE
Psaní	ZÁKLADY
Mluvený projev	ZÁKLADY

Označení (název) zakázky	[33] Audit bezpečnosti BoomTisk
Objednatel (název, IČO a sídlo)	BOOM TISK, spol. s r.o., IČ: 61679488
Dodavatel (název, IČO a sídlo)	AutoCont CZ a.s., IČ47676795
Bližší charakteristika zakázky (dle prokázání splnění zkušeností a požadavků na danou pozici)	Zajištění provozu a bezpečnostního poradenství a auditu dle ČSN/ISO 27001, zpracování zprávy, návrh opatření.
Pozice v zakázce (popis činnosti a odpovědnosti člena týmu)	Specialista kybernetické bezpečnosti
Kontaktní osoba objednatele k příp. potvrzení reference (jméno, funkce, telefon, e-mail)	Tomáš Reiter, [REDACTED]

Označení (název) zakázky	[15] [37] Audit bezpečnosti žilinský kraj
Objednatel (název, IČO a sídlo)	VUC Žilina – žilinský krajský úřad
Dodavatel (název, IČO a sídlo)	AutoCont CZ a.s., IČ47676795
Bližší charakteristika zakázky (dle prokázání splnění zkušeností a požadavků na danou pozici)	Audit bezpečnosti, kontrola plnění požadavků MV SR, Provedení auditu, zpracování zprávy, návrh opatření
Pozice v zakázce (popis činnosti a odpovědnosti člena týmu)	Specialista kybernetické bezpečnosti
Kontaktní osoba objednatele k příp. potvrzení reference (jméno, funkce, telefon, e-mail)	Ing. Roman Kučerák, [REDACTED]

Označení (název) zakázky	[41] Technologické centrum JM kraje
Objednatel (název, IČO a sídlo)	Jihomoravský kraj, krajský úřad IČ 70888337
Dodavatel (název, IČO a sídlo)	AutoCont CZ a.s., IČ47676795
Bližší charakteristika zakázky (dle prokázání splnění zkušeností a požadavků na danou pozici)	Analýza rizik Technologického centra, zpracování bezpečnostní dokumentace – politiky, směrnice.
Pozice v zakázce (popis činnosti a odpovědnosti člena týmu)	Specialista kybernetické bezpečnosti
Kontaktní osoba objednatele k příp. potvrzení reference (jméno, funkce, telefon, e-mail)	Jan Forbelský, [REDACTED]



ISACA hereby certifies that

Mr. Ludek Mandok

has successfully met all requirements and is qualified as **Certified Information Systems Auditor**; in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

0976705

Certification Number

11 September 2009

Date of Certification

31 January 2019

Expiration Date

C. K. T. TRIAPIS

Chair, ISACA Board of Directors

MSL

Chief Executive Officer

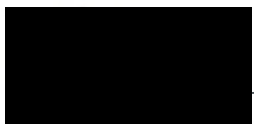
AUTOCONT



AUTOCONT

Prohlašuji, že všechny výše uvedené informace jsou správné a úplné.

Místo: Ostrava
Datum: 8.1.2018



PROFESNÍ ŽIVOTOPIS

Jméno Příjmení **JIŘÍ SVOBODA (ROZ. MRKVIČKA)**
 Pracovní pozice **Technický specialista hardware**
 Zaměstnavatel **AutoCont CZ a.s.**
 Adresa **Hornopolní 3322/3**

NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ

Období (od – do) 1997 – 2001
 Název a typ organizace SPŠ Jihlava
 Získaný titul
 Úroveň vzdělání středoškolské

PROFESNÍ PRAXE

Více jak 3 roky praxe v oboru serverového hardware
 Období (od – do) 2001 - dosud
 Jméno a adresa zaměstnavatele AutoCont CZ a.s., Hornopolní 3322/34, 702 00 Ostrava
 Dosažená pozice **Systémový specialista**
 Hlavní pracovní náplň a odpovědnost **Návrh, implementace a podpora infrastrukturních řešení serverové infrastruktury založených převážně na technologiích společností HP, IBM, Cisco, MS, VMware, Veem, Citrix**

PROJEKTY REALIZOVANÉ

V AUTOCONT CZ A.S.

Období (od – do) 2013 – 2014
 Zadavatel projektu Plzeňský kraj
 Název projektu **Implementace technologického centra Plzeňského kraje**
 Role v projektu **Technický specialista hardware**
 Popis projektu **Vybudování technologického centra kraje spolufinancovaný z projektů IOP. Předmětem bylo vybudování serverové, storage a síťové infrastruktury.**
 Kontakt Jiří Lohr,

Období (od – do) 2013 – 2014
 Zadavatel projektu Statutární město Jihlava
 Název projektu **Implementace technologického centra města Jihlava**
 Role v projektu **Technický specialista hardware**
 Popis projektu **Vybudování technologického centra spolufinancovaný z projektů IOP. Předmětem bylo vybudování serverové, storage a síťové infrastruktury.**
 Kontakt Vladimír Křivánek,

Období (od – do) 2011 – 2012
 Zadavatel projektu Kraj Vysočina
 Název projektu **Implementace technologického centra kraje Vysočina**
 Role v projektu **Technický specialista hardware**
 Popis projektu **Vybudování technologického centra kraje vysočina spolufinancovaný z projektů IOP. Předmětem bylo vybudování serverové, storage a síťové infrastruktury.**
 Kontakt Petr Pavlinec,

ŠKOLENÍ A CERTIFIKACE

Období (od – do)	2014
Název	Dell AppAssure Technical Overview, Dell Compellent Quote Center, Dell Compellent Top Gun Storage Architect Technical, Dell Blade Server Solutions – Technical, Dell PowerEdge Server Technical, Dell Technical Overview, Dell EMEA Storage Speciality Technical, Dell Storage Overview Sales, Dell PS Series Storage Array - An Introduction, Dell EqualLogic Technical, Dell PowerEdge VRTX Technical Overview
Období (od – do)	2014
Název	Veeam Sales Professional, Veeam Technical Sales Professional
Získaný titul	VSP, VTSP
Období (od – do)	2013
Název	HP Master Accred.Soulitons Expert - Storage Solutions Architect
Získaný titul	MASE SSA
Období (od – do)	2013
Název	HP Accredited Solutions Expert - Server Solutions Architect: V1, V8 HP Accredited Solutions Expert - Server Solutions Integrator: V8.1
Získaný titul	ASE SSA, SSI
Období (od – do)	2013
Název	HP Accredited Technical Professional: Rack and Tower Server Solution Integrator - V8, V8.1 Rack and Tower Server Solutions Support v8 Blade System Solutions Integrator - V8, V8.1 Server Administrator V8
Získaný titul	ATP RTS, BS, SA
Období (od – do)	2012
Název	HP Sales Certified: ExpertONE Support Services – level 1, 2
Získaný titul	SC SS
Období (od – do)	2012
Název	HP Technical Certified II: ExpertONE Enterprise Solutions
Získaný titul	TC ES
Období (od – do)	2012
Název	HP Accredited Integration Specialist: StorageWorks P4000 SAN Solutions
Získaný titul	AIS SW
Období (od – do)	2011
Název	HP Accredited System Engineer - Network Infrastructure, HP A-Series, HP Accredited Platform Specialist - Blade Servers, HP Accredited Platform Specialist – StorageWorks, HP Accredited Platform Specialist – Networking, HP Accredited Platform Specialist - ProLiant Servers
Získaný titul	ASE NI, Aseries, APS BS, APS SW, APS NET, APS PS

Období (od – do)	2010
Název	HP Accredited: - Integration Specialist - Network Infrastructure, - Integration Specialist - ProCurve Networking, - Presales Consultant - Virtualization Solutions, - Systems Engineer - ProCurve Mobility, HP Master Accredited Systems Engineer - ProCurve Mobility
Získaný titul	AIS NET, AIS PrN, APC VS, ASE PrM, MASE PrM
Období (od – do)	2006
Název	Microsoft Certified System Engineer: Windows Server 2003
Získaný titul	MCSE, MCSA
Období (od – do)	2005
Název	Microsoft Certified System Engineer: Windows Server 2000
Získaný titul	MCSE
Období (od – do)	2002
Název	Microsoft Certified Professional
Získaný titul	MCP
Období (od – do)	2007
Název	Citrix Certified Administrator for Citrix Presentation Server 4
Získaný titul	CCA
Období (od – do)	2005
Název	Citrix Certified Administrator (CCA) for MetaFrame XP Presentation Server
Získaný titul	CCA
Období (od – do)	2010
Název	McAfee System Security Technical Professional
Získaný titul	SSTP
Období (od – do)	2009
Název	IBM Service - BladeCenter servers IBM Service - Entrylevel and midrange servers (1a2 procesor) IBM Service - High performance servers (4 procesorové) IBM Service - System Storage Test IBM Service - System xServers Test
Získaný titul	S BCS, S EMS, S HPS, S-STGT, S-xST
Období (od – do)	2006
Název	IBM xServer servicing
Získaný titul	
Období (od – do)	2005
Název	IBM Tivoli Storage Management
Získaný titul	
Období (od – do)	2012
Název	VMware Certified Professional - vSphere 5
Získaný titul	VCP 5
Období (od – do)	2006 – 2010
Název	VMware Certified Professional
Získaný titul	VCP2, VCP3, VCP4
Období (od – do)	2008
Název	VMware Capacity Planner

Získaný titul	
Období (od – do)	2003-2006
Název	Cisco konfigurace firewall PIX/ASA Designing and Implementing Storage Area Networks, Cisco MDS9000 Cisco internetworking
JAZYKOVÉ ZNALOSTI	
MATEŘSKÝ JAZYK	čeština
OSTATNÍ JAZYKY	angličtina
Čtení	VÝBOENĚ
Psaní	DOBŘE
Mluvený projev	DOBŘE

HP ExpertOne



Hewlett-Packard Company hereby awards

Jiří Svoboda

the title of

**HP Accredited Technical Professional
BladeSystem Solutions Integrator V8.1**

for the successful completion of the requirements
as prescribed by HP ExpertOne.

Awarded on April 8, 2013

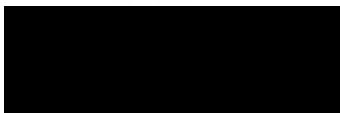
Susan Lincehill
Susan Lincehill
Vice President, HP ExpertOne

AUTOCONT

AUTOCONT

Prohlašuji, že všechny výše uvedené informace jsou správné a úplné.

Místo: Praha
Datum: 8.1.2018



Profesní životopis

DANIEL STANĚK

AutoCont CZ a.s.

Adresa Hornopolní 3322/34, 702 00 Ostrava
 Role **Technický specialista serverové virtualizace**
 Telefon [REDACTED]
 E-mail [REDACTED]

NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ

- Období (od – do) 1993-1998
- Název a typ organizace Západočeská univerzita v Plzni
 - Získaný titul Ing.
- Úroveň v národní klasifikaci Ing.

PROFESNÍ PRAXE *více jak 5 let praxe v oblasti serverové virtualizace*

- Období (od – do) 1998-2007
 - Jméno a adresa zaměstnavatele Mius a.s., U nádraží 3, Teplice 41501
 - Dosažená pozice **systemový specialista**
 - Hlavní pracovní náplň a odpovědnost síťová a serverová infrastruktura
- Období (od – do) 2007- současnost
 - Jméno a adresa zaměstnavatele AutoCont CZ a.s., Mírové náměstí 3057, Teplice 41501
 - Dosažená pozice **systemový specialista**
 - Hlavní pracovní náplň a odpovědnost síťová a serverová infrastruktura

PROJEKTY REALIZOVANÉ V AUTOCONT CZ A.S.

- Období (od – do) 2009
 - Název projektu Implementace nové infrastruktury
 - Zadavatel projektu Mehler-technologies S.p.A.
 - Role v projektu Technický specialista serverové virtualizace
 - Popis projektu Implementace nové počítačové infrastruktury v nadnárodním měřítku, virtuální infrastruktura VMWare, nadnárodní WAN, realizace VPN s partnery a dodavateli, implementace AD, Exchange, zálohování, monitoring provozu
 - Kontakt [REDACTED]
- Období (od – do) 2010
 - Název projektu Implementace nové infrastruktury
 - Zadavatel projektu Petainer Czech Holdings s.r.o.
 - Role v projektu Technický specialista serverové virtualizace

<ul style="list-style-type: none"> • Popis projektu • Kontakt 	<p>Implementace nové počítačové infrastruktury v nadnárodním měřítku, virtuální infrastruktura VMWare, nadnárodní WAN, realizace VPN - Cisco s partnery a dodavateli, implementace AD, Exchange, zálohování, monitoring provozu.</p> <p>Jindřich Kovář, [REDACTED]</p>
<ul style="list-style-type: none"> • Období (od – do) • Název projektu 	<p>2012-2013</p> <p>Technologické centrum Karlovarského kraje</p>
<ul style="list-style-type: none"> • Zadavatel projektu • Role v projektu • Popis projektu • Kontakt 	<p>Karlovarský kraj</p> <p>Technický specialista serverové virtualizace</p> <p>Implementace technologického centra na virtualizační platformě VMware</p> <p>Petr Kulda, p [REDACTED]</p>

ŠKOLENÍ A CERTIFIKACE

<ul style="list-style-type: none"> • Název • Získaný titul 	<p>VMWare Certified Professional (VCP)</p> <p>VMWare Certified Professional (VCP)</p>
<ul style="list-style-type: none"> • Název • Získaný titul 	<p>Cisco Certified Network Associate (CCNA)</p> <p>Cisco Certified Network Associate (CCNA)</p>
<ul style="list-style-type: none"> • Název • Získaný titul 	<p><i>Juniper Networks Certified Associate (JNCIA-FWV)</i></p> <p>Juniper Networks Certified Associate (JNCIA-FWV)</p>
<ul style="list-style-type: none"> • Název • Získaný titul 	<p><i>Juniper Networks Certified Associate (JNCIA-SSL)</i></p> <p>Juniper Networks Certified Associate (JNCIA-SSL)</p>
<ul style="list-style-type: none"> • Název • Získaný titul 	<p><i>Juniper Networks Certified Associate (JNCIA-JUNOS)</i></p> <p>Juniper Networks Certified Associate (JNCIA-JUNOS)</p>
<ul style="list-style-type: none"> • Název • Získaný titul 	<p><i>Juniper Networks Certified Specialist (JNCIS-SEC)</i></p> <p>Juniper Networks Certified Specialist (JNCIS-SEC)</p>
<ul style="list-style-type: none"> • Název • Získaný titul 	<p><i>Cisco Advanced Wireless Field Specialist</i></p> <p>Cisco Advanced Wireless Field Specialist</p>
<ul style="list-style-type: none"> • Název • Získaný titul 	<p><i>Aruba Certified Mobility PRO (ACMP)</i></p> <p>Aruba Certified Mobility PRO (ACMP)</p>

JAZYKOVÉ ZNALOSTI

MATEŘSKÝ JAZYK	čeština
OSTATNÍ JAZYKY	
	Angličtina
• Čtení	DOBŘE
• Psaní	DOBŘE
• Mluvený projev	DOBŘE



VMware is proud to award the title of
VMware Certified Professional

to

Daniel Stanek

in recognition of successful completion of all
certification requirements for VMware Infrastructure 3

DATE OF EXPIRY: 31st August 2017
EXAMINATION CENTER: 1920

vmware CERTIFIED PROFESSIONAL

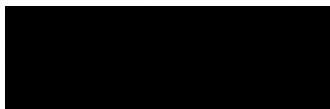
Paul M. ...
Vice President





Prohlašuji, že všechny výše uvedené informace jsou správné a úplné.

Místo: Teplice
Datum: 8.1.2018



Daniel Stanek

Profesní životopis

Jméno a příjmení:	Ing. Leo Sedlák	
Praxe	Více jak 3 roky praxe v oboru počítačových sítí	
Pozice v týmu:	Technický specialista sítí	
Zaměstnavatel:	AutoCont CZ a.s.	
Dosažené vzdělání:	1997 – 2004 Vysoké učení technické Brno, Fakulta strojní	
Profesní praxe:	<p>Období (od – do) 2010 -</p> <p>Jméno a adresa zaměstnavatele</p> <p>Dosažená pozice</p> <p>Hlavní pracovní náplň a odpovědnost</p>	<p>AutoCont CZ a.s., Hornopolní 3322/34, 702 00 Ostrava</p> <p>Certifikovaný síťový specialista – Cisco a HP</p> <p>Předprodejní podpora a konzultace návrh síťových řešení, realizace projektů, dokumentace, školení zákazníků na produktech Cisco, HP</p>
	<p>Období (od – do) 2006 - 2009</p> <p>Jméno a adresa zaměstnavatele</p> <p>Dosažená pozice</p> <p>Hlavní pracovní náplň a odpovědnost</p>	<p>AutoCont CZ a.s., Nemocniční 12, 702 00 Ostrava</p> <p>Síťový specialista</p> <p>Předprodejní podpora a konzultace, návrh síťových řešení, realizace projektů Dokumentace, školení zákazníků, síťový bezpečnostní audit, softwarový audit</p>
	<p>Období (od – do) 2001 - 2006</p> <p>Jméno a adresa zaměstnavatele</p> <p>Dosažená pozice</p> <p>Hlavní pracovní náplň a odpovědnost</p>	<p>AutoCont CZ a.s., Nemocniční 12, 702 00 Ostrava</p> <p>Servisní technik</p> <p>outsourcing koncových systémů ČTC, outsourcing koncových systémů Ahold outsourcing koncových systémů GE Money, projekt INDOŠ instalace systémů SBS Windows</p>
Referenční zakázky:	<p>Období (od – do) 2012 - dosud</p> <p>Zadavatel projektu</p> <p>Název projektu</p> <p>Role v projektu</p> <p>Popis projektu</p>	<p>Jihomoravský kraj, Žerotínovo nám. 449/3, 601 82 Brno</p> <p>Vybudování komunikační infrastruktury pro Technologické centrum kraje</p> <p>Technický specialista sítí</p> <p>Vytvoření datové a komunikační infrastruktury na produktech Cisco, HP a VMware, implementace řešení, monitoring provozu, zpracování dokumentace</p> <p>Kontakt: Jan Forbelský, [redacted]</p>

	<p>Období (od – do) 2010</p> <p>Zadavatel projektu Česká pošta s.p., Politických vězňů 909/4, 225 99 Praha 1</p> <p>Název projektu Datové centrum</p> <p>Role v projektu Technický specialista sítě</p> <p>Popis projektu Implementace komunikační infrastruktury datového centra. Řešení bylo realizováno na dodaných technologiích HP, Cisco, a dalších, zpracování dokumentace</p> <p>Kontakt: Otakar Erhart, [REDACTED]</p>
Získané certifikáty:	<p>Fortinet Certified Network Security Administrator Fortinet Certified Network Security Professional Cisco Certified Network Professional Security HP Master Accredited Systems Engineer Network Infrastructure – HP ExpertOne HP Accredited Systems Engineer Wireless Networks – HP ExpertOne</p>

HP ExpertOne



Hewlett-Packard Company hereby awards

Leo Sedlak

the title of

HP Master Accredited Systems Engineer
Network Infrastructure [2011]

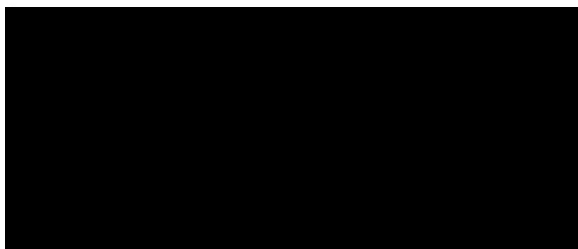
for the successful completion of the requirements
as prescribed by HP ExpertOne.

A handwritten signature in black ink that reads "Susan Lindahl".

Susan Lindahl
Vice President, HP ExpertOne

Čestně prohlašuji, že veškeré údaje uvedené v životopise jsou pravdivé.

V Praze dne 8. 1. 2018



Profesní životopis

VLADIMÍR KOLBÁBEK

Role	AutoCont CZ a.s. Technický specialista IDM
Adresa	Ostrava – Moravská Ostrava, Hornopolsní 3322/34, PSC 702 00
Telefon	+420 [redacted]
E-mail	[redacted]

NEJVYŠŠÍ DOSAŽENÉ VZDĚLÁNÍ

- | | |
|--------------------------------|--|
| • Období (od – do) | 1995 – 1998 |
| • Název a typ organizace | Vyšší odborná škola Jihlava, obor počítačové systémy |
| • Získaný titul | Diplomovaný technik |
| • Úroveň v národní klasifikaci | Vyšší odborné vzdělání |

PROFESNÍ PRAXE

- | | |
|---------------------------------------|---|
| Praxe | Více jak 5 let praxe v oblasti informačních technologií |
| • Období (od – do) | 2014 - Současnost |
| • Jméno a adresa zaměstnavatele | AutoCont CZ a.s. |
| • Dosažená pozice | Solution Architect |
| • Hlavní pracovní náplň a odpovědnost | Komunikace se zákazníkem, presales aktivity, tvorba technického designu, vývoj aplikací |
| • Období (od – do) | 2004 – 2013 |
| • Jméno a adresa zaměstnavatele | AutoCont CZ a.s. |
| • Dosažená pozice | Programátor |
| • Hlavní pracovní náplň a odpovědnost | Návrh DMS systémů, konzultace, vývoj aplikací (JAVA, .NET platforma) |
| • Období (od – do) | 2001 - 2004 |
| • Jméno a adresa zaměstnavatele | Logos spol. s r.o. |
| • Dosažená pozice | Software engineer |
| • Hlavní pracovní náplň a odpovědnost | Vývoj a návrh intranetových a internetových řešení |
| • Období (od – do) | 1999 - 2001 |
| • Jméno a adresa zaměstnavatele | STORMWARE spol. s r.o. |
| • Dosažená pozice | Programátor |
| • Hlavní pracovní náplň a odpovědnost | Vývoj ekonomického systému Pohoda |

**PROJEKTY REALIZOVANÉ
V AUTOCONT CZ A.S.**

- Období (od – do) 2014 -2015
 - Název projektu Vnitřní integrace úřadu
 - Role Technický specialista IDM
- Zadavatel projektu Krajský úřad Jihočeského kraje
 - Popis projektu Implementace Identity management systému, integrace na další systémy.
 - Kontakt František Beránek, [REDACTED]
- Období (od – do) 2013 -2015
 - Název projektu Vnitřní integrace úřadu
 - Role Technický specialista IDM
- Zadavatel projektu Krajský úřad Pardubického kraje
 - Popis projektu Implementace Identity management systému, integrace na další systémy.
 - Kontakt Martin Halámka, [REDACTED]
- Období (od – do) 2013 -2014
 - Název projektu Vnitřní integrace úřadu
 - Role Technický specialista IDM
- Zadavatel projektu Krajský úřad Jihomoravského kraje
 - Popis projektu Implementace Identity management systému, integrace na další systémy.
 - Kontakt Jan Forbelský, [REDACTED]

ŠKOLENÍ A CERTIFIKACE

- Období (od – do) 26. - 30.7.2010
 - Název školení Oracle WebLogic Server 11g Administration Essentials
 - Získaný titul -
- Období (od – do) 22. - 23.5.2012
 - Název školení Oracle WebLogic 12c Bootcamp
 - Získaný titul -
- Období (od – do) 17. - 20.6.2012
 - Název školení Oracle SOA Suite 11g Implementation Bootcamp
 - Získaný titul -
- Období (od – do) 28. - 29.8.2012
 - Název školení Oracle Service Bus
 - Získaný titul -
- Období (od – do) 12. - 15.12.2012
 - Název školení Oracle Business Process Management Suite 11g Implementation Boot Camp
 - Získaný titul -
- Období (od – do) 2012
 - Název IBM FileNet Content Manager-Administrator 4.5
IBM FileNet Content Manager-Designer 4.5
IBM FileNet Content Manager-Developer 4.5
IBM FileNet Content Manager-Technical Sales 4.5
IBM FileNet Business Process Manager-Designer 4.5

- Získaný titul IBM FileNet Business Process Manager-Developer 4.5
IBM FileNet Business Process Manager-Technical Sales 4.5
FileNet Certified Professional
- Období (od – do) 2008
 - Název FCP Business Process Manager-Administrator 4.0
FCP Business Process Manager-Developer 4.0
FCP Content Manager-Administrator 4.0
FCP Content Manager-Developer 4.0
FCP Email Manager-Administrator 4.0
FCP Email Manager-Developer 4.0
FCP Forms Manager-Administrator 4.0
FCP Forms Manager-Developer 4.0
FCP Records Manager-Developer 4.0
 - Získaný titul FileNet Certified Professional
- Období (od – do) 2003
 - Název Microsoft Certified Professional
 - Získaný titul MCP

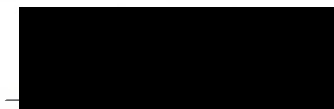
JAZYKOVÉ ZNALOSTI**MATEŘSKÝ JAZYK** Český**OSTATNÍ JAZYKY**

- Čtení Dobře
- Psaní Dobře
- Mluvený projev Základy

Prohlašuji, že všechny výše uvedené informace jsou správné a úplné.

Místo: Praha

Datum: 8.1.2018



Vladimír Kolbábek

5 Čestné prohlášení o souhlasu se smluvními podmínkami

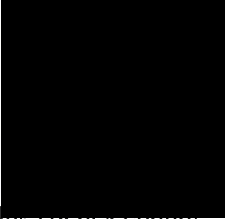
Čestné prohlášení uchazeče o smluvních podmínkách

Uchazeč(i):

Název: AutoCont CZ a.s.
Sídlo: Hornopolská 3322/34, 702 00 Ostrava
IČ: 47676795
DIČ: CZ47676795

Prohlašuji tímto, že jsme se důkladně seznámili se smluvními podmínkami, které jsou Přílohou 4 Zadávací dokumentace veřejné zakázky uvedené v záhlaví tohoto prohlášení, že s nimi souhlasíme a v případě, že budeme vybráni k plnění veřejné zakázky, podepíšeme smlouvu v souladu s těmito smluvními podmínkami

V Karlových Varech dne 15.1.2018


Ing. Zdeněk Chobot
na základě plné moci

6 Popis nabízeného technického řešení

6.1 Technické řešení

Komodita K1 - Rozšíření kapacit Technologického centra		
Část	Parametr	Popis
Virtualizační server 1 ks BL460c G10	Provedení	Blade server BL460c G10
	Procesor	2x procesor Xeon-G 6134 osmi-jádrový (dohromady 16 jader), nominální frekvence 3.2 GHz, automatické zvýšení frekvence jádra až o 0,5 GHz při nevyužití ostatních jader)
	Pevné disky	2x SSD, min. 240 GB pro hypervizor
	Řadič disků	min. RAID 0,1, zálohovaná cache pro zápis 1 GB
	Paměť	10x 32GB 2Rx4 PC4-2666V-R Smart Kit celkem 320 GB RAM, 2666 MT/s
	Rozšiřitelnost	rozšiřitelnost RAM na 700 GB bez výměny RAM modulů
	RAID	řadič RAID 0,1, 10, SAS 12 Gb, zálohovaná vyrovnávací paměť pro zápis min. 1 GB
	LAN porty	LAN 2x10Gb s podporou iSCSI a virtualizace VMware NetQueue, Microsoft VMC. Podpora partitioningu - rozdělení fyzického LAN adaptéru na více virtuálních adaptérů - 4 virtuální adaptéry na každý port
	FC porty	2x FC (fibre channel) port 16 Gb
	Vzdálená správa	Podpora vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média.
	Kompatibilita	Podpora nejrozšířenějších operačních systémů (Windows, Linux) a hypervizorů (Hyper-V, VMware)
	Kompatibilita	Plně kompatibilní se stávajícím Blade šasi HP C7000 na fyzické i elektrické úrovni
	Vysoká dostupnost	Podpora a licence pro clusterový provoz
	Management	Plná integrace s management modulem HP Blade šasi HP 7000
Záruka	Záruka 60 měsíců, oprava následující pracovní den v místě instalace – HPE Carepack	
SW licence operačních systémů Windows Server 2016 Datacenter 16 core	Operační systémy	Windows Server 2016 Datacenter 16 core - Licence 64 - bitového serverového operačního systému v aktuální verzi pro nabízený server. Licence umožňuje provoz neomezeného počtu virtuálních serverů stejné verze v prostředí stávající serverové virtualizace, dále provoz všech nabízených aplikací, management nástrojů a komponent terminálové farmy
Sítové přepínače a sondy síťových toků 4 kusy 4x JC100B HPE 5800 24G Switch 2x JC091A HPE 5800 4-port 10GbE SFP+ Module 2x JC095A HPE 5800 16-port SFP Module	Společné parametry	
	Provedení	do racku, rozměr 1RU, včetně montážního materiálu do racku
	Určení	L2, L3 switch (přepínač), spravovatelný
	Porty	4x 10 GbSFP+, 16x 1 Gb SFP, 48x 1Gb RJ-45, optické a metalické porty nesdílené
	Podavač	podpora směrování a dynamických směrovacích protokolů (min. OSPF)
	VLAN	podpora 1000 aktivních VLAN a to včetně L3 směrovaných rozhraní
	Routování	podpora tvorby virtuálních směrovacích tabulek (VRF, virtual router apod.)
	QoS	podpora QoS (8 front na port)
	Bezpečnost	podpora 802.1x
	Rozšířené funkce	podpora MPLS a VPLS, včetně routování pro napojení na MAN
	IPv6	plný dual stack IPv4 a IPv6 včetně všech služeb směrování
	Výkon	přepínání a routování 200 Gb/s a 150 Mp/s

	Sledování toků	integrovaná podpora sledování toků technologie sFlow a exportu toků protokolem Netflow nebo kompatibilním.
	Stohování	podpora rozšířeného stohování po standardizovaných 10Gb portech do minimálního počtu 8 přepínačů (technologie ekvivalentní s technologiemi VSS, IRF nebo Virtual-Chasis)
	Linková agregace	Agregace portů napříč stohem včetně kombinace 10 Gb a 1 Gb, podpora LACP
	Správa	podpora SNMP, Syslog, CLI
	Záruka	5 let včetně nároku na nové verze firmware, oprava do 2 pracovních dnů v místě instalace
	Specifické parametry	
	Porty	2 přepínače - 4x 10 Gb SFP+, 16x 1 Gb SFP, 24x 1Gb RJ-45, optické a metalické porty nesdílené
	Porty	2 přepínače - 8x 10 Gb SFP+, 24x 1Gb RJ-45, optické a metalické porty nesdílené
Kabely, optické moduly	Optické moduly	32x 1Gb SFP SM pro nabízené přepínače 8x 10 Gb SFP+ MM pro nabízené přepínače 2x 10 Gb SFP+ SM BiDi, 10 km, pro nabízené přepínače, shodné vlnové délky 2x 10 Gb SFP+ SM BiDi, 10 km, pro stávající přepínače HPE 5130 (JG934A) - kompletní vlnové délky k předchozím modulům optický konektor modulů LC záruka 36 měsíců
	Kabely	4x optický patch kabel 3m MM - LC-LC 36x optický patch kabel 3m SM - LC-SC záruka 36 měsíců
Rozšíření kapacity síťového úložiště NAS pro archivaci SIEM 12x HDD 4TB WD4002FFWX Red Pro 128MB SATAIII NAS	HDD	12x 4TB HDD SATAIII/128 MB cache. Disky jsou výrobcem určeny pro nepřetržitý provoz v NAS,
	Záruka	Záruka výrobce 5 let
Rozšíření kapacit diskových polí pro SIEM 6 ks HP HDD MDL 3TB GB / 7200 ot. min, SAS 6 Gb	HDD 3,5"	6 ks HP HDD MDL 3TB GB / 7200 ot. min, SAS 6 Gb
	Kompatibilita	Plná kompatibilita s diskovými poli HP MSA 2000G3
	Záruka	Záruka 3 roky s výměnou v místě instalace

Komodita K2 -SIEM a NBA		
Část	Parametr	Popis
SIEM &	Základní funkce	Integrovaný systém pracovních logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií
	Ovládání	Uživatelsky přívětivý přístup ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace musí probíhat z jediné řídicí konzole s jednotným GUI.

NBA AlienVault Unified Security Manager	Správa prvků	Automatické jednorázové i plánovatelné vyhledávání i ruční přidávání Prvků a detekce jejich typů a vlastností. Prvkem se rozumí hw i sw (např. OS) s IP adresou. Prvky jsou typicky zdroji dat - logů a událostí.
	Skupiny Prvků	Podpora zařazování Prvků do skupin/kategorií dle vlastností (typ, operační systém, dostupné služby, síť apod.) i metadat (umístění, hodnota apod.)
	Metadata Prvků	Možnost konfigurace metadat Prvku - min. hodnota, priorita a spolehlivost (věrohodnost) událostí
	Monitorování Prvků	Automatické monitorování stavu Prvku - dostupnost poskytované služby a základní dostupnost (odezva na ping)
	Vyhledávání Prvků	Víceparametrové vyhledávání a filtrování Prvků podle vlastností i metadat, export do souboru v běžném strojově zpracovatelném formátu (csv, xml apod.)
	Vazby	Detekce síťových prvků standardními protokoly a mapování jejich vazeb
	Detekce zranitelností	Automatická ruční i plánovaná detekce zranitelností Prvků (i nezařazených) - porovnání stavu Prvků s databází známých zranitelností průběžně aktualizovanou výrobcem
	Profily zranitelností	Vestavěné i uživatelsky definované profily detekce zranitelností – definice typů zranitelností, které mají být kontrolovány.
	Autentizace	Podpora detekce zranitelností s i bez přihlášení (autentizací) ke kontrolovanému Prvku.
	Detekce průniku	Víceúrovňová detekce průniku (intrusion detection) - na úrovni sledování síťového provozu a na úrovni Prvků.
	Instalace agentů	Podpora vzdálené instalace ID agentů (intrusion detection) min. pro operační systémy Microsoft Windows
	Detekce průniku – assety	Monitoring a analýza uživatelských aktivit, logů, integrity souborů a registrů, rootkitů či obdobného škodlivého kódu
	Detekce průniku – síť	Analýza monitorovaných síťových toků a detekce anomálií indikující možné narušení bezpečnosti politiky (NBA - Network Behavior Analysis)
	Detekce anomálií	Monitorování síťových toků technologií netflow (verze 5,9,10) či kompatibilní (ipfix, netstream) dle nabízených sond a přepínačů.
	Síťové toky hypervizor	Podpora sledování síťových toků (netflow či kompatibilní) virtuálních síťových přepínačů VMware vSphere
	Viditelnost síťových toků	Viditelnost síťového provozu - zobrazení, prohledávání, filtrování síťových toků včetně historie
	IP reputace	Integrovaná služba aktualizovaná výrobcem ohodnocující reputaci a spolehlivost veřejné IP adresy s možností změny priorit událostí, alarmů apod. Reputace založena na detekovaných (aktivitách IP adresy (spam, skenování, phishing, distribuce malware, botnet
	Protokoly	podporované protokoly min. syslog, windows events collection (pomocí agenta i bez-agentově (WMI), snmp, s/ftp, nfs, cifs, netflow
	Ukládání logů	Bezpečné ukládání logů s řízeným přístupem v nezměněné (nefiltrované) podobě (raw logy)
	Zpracování logů	Centrální zpracování logů, jejich normalizace, korelaci, grafická interpretace a archivace, včetně logů generovaných samotným řešením
	Rozšíření logů	Vytváření vlastních atributů v událostech. Automatické doplňování atributů aktuálními hodnotami z externího zdrojů. Podpora atributů v celém systému - vyhledávání, filtrace, korelace atd.
	Prohledávání logů	Pokročilé prohledávání a filtrování raw logů, podpora indexování pro zrychlení hledání
	Expirace logů	Podpora automatické rotace raw logů s nastavením doby expirace
	Zálohování logů	Podpora zálohování logů na externí síťové úložiště
	Ochrana logů	Zajištění integrity raw logů aplikací digitální podpisu. Možnost jednoduchého uživatelského ověření integrity.
	Centralizace logů	Konsolidace logů na jednom centrálním místě.
Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě	

Doplňování názvů	Automatické doplňování reverzních DNS a hostname záznamů k IP adresám.
Identifikace MAC	Automatické doplňování výrobce zařízení podle MAC adresy
Grafy událostí	Grafické znázornění událostí - četnost, typ, časová osa
Parsery	Možnost vytváření uživatelských parserů bez nutnosti externí spolupráce
Ladění parserů	On-line ladění uživatelsky vytvářených parserů v reálném čase- okamžité zobrazení rozparsovaných dat při vložení testovací zprávy/události.
Standardizace logů	Standardizace přijatých logů do jednotného formátu, parsování parametrů do předepsaných polí
Pohledy	Předpřipravené pohledy a podpora vytváření vlastních pohledů na data uživateli a jejich ukládání pro pozdější využití a zpracování dat. Včetně grafické reprezentace dat - grafy, mapy
Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových reportů. Včetně grafické reprezentace dat - grafy, mapy
Upozornění	Zasílání uživatelsky vytvořených upozornění podle uživatelsky definovaných podmínek. Možnost zahrnutí přijatých rozparsovaných dat do upozornění.
Správa uživatelů	Správa uživatelů systému musí umožnit integraci s MS Active Directory. Systém musí umožňovat i přihlašování pomocí lokálních účtů. Podpora granulárního (lokálního) nastavení uživatelských oprávnění.
Tikety	Možnost vytváření tiketů k bezpečnostním událostem s možností přiřazení řešitelů. Možnost sledování průběhu tiketů včetně historie - obsah, vykonané činnosti, eskalace. Podpora jednoduchého manuálního vytváření tiketů v průběhu vyšetřování incidentu.
Automatizace tiketů	Tickety lze vytvářet automaticky na základě vytvořené politiky k jednotlivým událostem / zranitelnostem.
Politiky	Podpora vestavěných a tvorby vlastních komplexních politik zpracování událostí. Politiky umožní spustit následující akce: odeslání emailu, vytvoření ticketu, spuštění skriptu.
Korelace	Podpora korelací událostí na základě definovaných parametru bez závislosti na typu zdroje. Vestavěné a výrobcem aktualizované korelace, podpora vytváření vlastních
Rozšířené korelace	Systém umožní tvorbu korelací nejen napříč zdroji, ale také napříč daty z interních subsystémů (detekce zranitelnosti, průniků, IP reputace). V závislosti na datech interních subsystémů je případně upravena vážnost incidentu (oproti standardní korelaci).
Upozornění	Podpora vytvářet upozornění (alertů) na základě korelovaných událostí včetně zahrnutí rozšířených korelací. Vestavěná upozornění i podpora ručního vytváření.
IT Compliance	Podpora compliance (jednání v souladu s „pravidly“) - certifikace dle obvyklých bezpečnostních standardů a norem PCI DSS, HIPAA
Auditní reporty	Vestavěné, výrobcem aktualizované šablony reportů pro podporu kontrolních a certifikačních auditů - dle standardů PCI DSS, HIPAA, NIST CSF, ISO 27001
Legislativa	Systém zajistí bezpečné, úplné a nezpochybnitelné ukládání, vyhodnocování a archivaci logů ICT prostředí zadavatele a naplnění požadavků dle zákona č. 181/2014 Sb. (ZKB) a vyhlášky č.316/2014 Sb. (VKB), o kybernetické bezpečnosti, a to v platných zněních
Provedení	Centrální část systému bude realizována jako jedna virtuální appliance
Licence	Licence pro neomezený počet sledovaných systémů (Prvků), bez licenčního omezení velikosti aktivních i archivních dat či jiných funkcionalit systému. Součástí licence bude centrální část systému a dále samostatný (sub)systém (virtuální appliance) zajišťující sběr dat a vykonávání funkcí systému (detekci Prvků, testy zranitelnosti, monitoring síťových toků, aběr logů) lokálně ve vzdálené lokalitě (U spořitelny) a předávání dat a událostí do centrální části systému).
Výkon	Trvalé zpracování AIO 1500 EPS (events per second - událostí za sekundu) - celkem z obou lokalit - Moskevská a U spořitelny
Škálovatelnost	Možnost zvýšení výkonu doplněním dalších appliance pro sběr dat a vykonávání funkcí systémů, popřípadě rozdělením systému na více serverů.
Vysoká dostupnost	Integrovaná podpora pro možnost doplnění dalšího systému (nodu) a sestavení clusteru – 2 systém, režim active/passive

	Záruka	12 měsíců včetně nároku na nové verze software a včetně aktualizací bezpečnostní a funkčních signatur (zranitelnosti, korelační pravidla, detekce průniku, detekce Prvků (typy zařízení, aplikace, operační systémy), aktualizací reportů.
--	--------	--

Komodita K3 - Správa identit		
Část	Parametr	Popis
Systém pro správu identity (Identity management - IDM)	Základní funkce	IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.
	Licence	Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databázi). Předpokládaný počet uživatelů je do 500.
AC Identita	Škálovatelnost	Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh.
	Evidence aplikací a rolí	Integrovaný registr aplikací a informačních systémů (souhrnné IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.
	Uživatelské role	Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.
	Historizace	Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku - aktuálním nebo zpětně v minulosti.
	Automatizace	Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo).
	Logování SIEM	Systém bude poskytovat auditní logy pro systém typu SIEM
	Logování systému	Systém obsahuje logování následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log)
	Správa identit	Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury.
	Systematizovaná místa	Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztahované ke konkrétnímu systemizovanému místu.
	Podpora eIDAS	Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
	Vysoká dostupnost	Systém bude možno nasadit na více serverů v režimu vysoké dostupnosti.
	Požadavky na portál - obecné	IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správě a konfiguraci Systému.
	Podpora mobilních zařízení	Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přístupováno)

Správa referenčních objektů	Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role, certifikát.
Referenční objekty	Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity
Zabezpečení referenčních objektů	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů
Rozšiřující atributy	Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.
Přehledné zobrazení	Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů (identit).
Vyhledávání - diakritika	Portál bude umožňovat vyhledávat i bez diakritiky (zadání Parizek vyhledává i Pařížek)
Správa certifikátů	Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti.
Obrázky	Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie.
Přesun identit	Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.
Kopírování rolí	Systém umožní kopírování aplikačních rolí, agendových činnostních rolí mezi jednotlivými systematizovanými místy.
Ochrana proti chybám	Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory)
Aktivní uživatelé	Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem
Slučování identit	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.
Export údajů	Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu
Filtrování	Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.
Správa oprávnění	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity)
Granularita oprávnění	Oprávnění přidělována uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identit, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět.
Oprávnění k atributům	Pro identity a referenčních objektů bude možná definovat oprávnění k jejich atributům včetně možnosti zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů.
Kontextový výběr	Na úrovni organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikačních rolí, skupiny, agendových rolí, systematizovaných míst dostupných pro identity z dané organizační jednotky.
Správa licencí	IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytváření víceúrovňových schvalovacích workflow.

Časová omezení	IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.
Vícenásobné vazby	Možnost přiřazení identit k systemizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systemizovaných místech a současně na systemizovaném místě může být evidováno více identit.
Přehled rolí	Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.
Přehled dědičnosti	IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel rolí zdědil (z organizační jednotky, systemizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegováno.
Skupiny	IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systemizovaná místa.
Zastupitelnost	IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce.
Delegování oprávnění	Možnost delegování administrátorských práv.
Správa osobních údajů	IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.
Osobní údaje	IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům.
Osobní údaje - automatizace	IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů.
Obnovení hesla	IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zaslání kódů pro reset hesla danému uživateli musí být možnou provést pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).
Žádosti	IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.
Externí subjekty	IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin.
Kontextový výběr	Samoobslužné rozhraní umožní na úrovni organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.
Individuálizace	IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně.
Workflow	Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživateli na změny v přiřazení rolí a skupin ke schválení nadřazeným - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů)

	<ul style="list-style-type: none"> - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů
Workflow - sledování	Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude ve obvyklém formátu pro zobrazení workflow aktivity diagram, BPMN nebo Archimate
Upozornění	IDM zajistí zaslání konfigurovatelných emailových upozornění pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role) problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.
Včasná upozornění	Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu je možno konfigurovat pro každý typ upozornění samostatně.
Šablony upozornění	Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám bude možné nastavovat různé příjemce pro různé části organizační struktury (odbor, oddělení). Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.
Kontext upozornění	Pro zaslání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut.
Logování	Veškeré změny vyvolané požadavky uživatele a administrátorů/správce IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.
Důvěryhodnot logování	Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových souborů jako XML, CSV z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.
Auditní report	IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, agendových rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.
Auditní report - výběr	Identit pro generování auditního reportu musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.
Report RPP	Vestavěný report pro ohlašování působnosti v Registru práv a povinností. Bude obsahovat aktuální počty úředníků na agendových rolích a možnost porovnání s počtem úředníků k vybranému, dříve vygenerovanému, reportu. Report bude exportovatelný do CSV souboru.
Reporty uživatelů	Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolmi a s aplikačními rolmi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru.
Reporty - zaslání	Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.
Reporty - historie	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.
Reporty - porovnání	Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.
Webové služby (WS)	IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.
Standardy WS	Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.

Bezpečnost WS	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.
Logování WS	Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu
Služby rozhraní WS	Rozhraní bude poskytovat minimálně následující služby: <ul style="list-style-type: none"> - Získání organizační struktury - Získání hierarchie systematizovaných míst - Získání seznamu identit - Získání nadřazené osoby pro daného zaměstnance - Získání seznamu aplikačních rolí - Získání seznamu uživatelů dané aplikace - Získání seznamu agend a agendových rolí přiřazených dané aplikaci - Zápis seznamu aplikačních rolí do IDM - Zápis certifikátů do IDM - Zápis a změna identit
Služby rozhraní WS pro ISZR	Služba pro autorizaci pro ISZR (Informační systém základních registrů) – služba ověří validnost volání služby ISZR. Služba dále ověří v IDM: <ul style="list-style-type: none"> - Zda je evidován uživatel v IDM, který je součástí požadavku na ISZR - Zda je evidována aplikace v IDM, která je součástí požadavku na ISZR - Zda má tento uživatel v IDM nastaven přístup do aplikace, která je součástí požadavku na ISZR - Zda existuje v IDM v rámci evidence organizační struktury také evidence pro dané OVM, které je uvedeno v požadavku na ISZR - Zda má aplikace, která je součástí požadavku na ISZR, v IDM povolenu agendovou činnostní rolí a agendu, které jsou rovněž uvedeny v požadavku na ISZR.
Synchronizace	Ruční i automatické spuštění synchronizací s propojenými systémy.
Synchronizace - simulace	Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.
Simulace - průběh	Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.
Synchronizace - režimy	Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): <ul style="list-style-type: none"> - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu. - Rekondilační synchronizace – synchronizace vytvoří rekondilační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému. - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.

Synchronizace - správa	Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu.
Obecné konektory	Vestavěné obecné konektory pro správu identit v napojených systémech: <ul style="list-style-type: none"> - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory - konektor pro práci s databází Microsoft SQL - konektor pro napojení na SOAP webové služby - konektor pro napojení na REST webové služby - konektor pro napojení na LDAP server s podporou LDAP v3
Aplikační konektory	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím. <ul style="list-style-type: none"> - Microsoft Active Directory - Informační systém Ginis (GORDIC spol. s r.o.) - Microsoft Exchange, včetně vytváření schránek uživatelům - elektronická spisová služba AthenA vč. modulu iUsnesení (PilsCom, s.r.o.)
Konektory pro centrální systémy - RPP	IDM bude obsahovat evidenci matice práv a rolí dle Informačního systému základních registrů (ISZR-RPP - matice RPP) s následujícími funkcemi: <ul style="list-style-type: none"> - vedoucí pracovníci mohou zadávat k jednotlivým činnostem konkrétní uživatele (systemizovaná místa) - přidělování/odebírání agend/činností zaměstnancům vedoucími zaměstnanci s vazbou na systemizovaná místa - udržování a poskytování přehledu o oznámených působnostech, jejich stavech, kontrole přeregistrace a změnách - evidence přehledu legislativy včetně vazby na jednotlivé činnosti/agendy
Napojení na centrální systémy - JIP	IDM bude obsahovat správu identit, rolí a systémů evidovaných v systému JIP (Jednotný identitní prostor) s následujícími funkcemi: <ul style="list-style-type: none"> - Obousměrná synchronizace s JIP. - Automatické pravidelné načítání aplikací a rolí z JIP do IDM. - Automatické předávání identity včetně vazby na jednotlivé aplikační a agendové činnostní role z IDM do JIP. - Možnost změny hesla uživatele v JIP prostřednictvím Portálu.
Zdrojový systém	IDM bude napojeno na personální systém FluxPaM (FLUX, spol. s r.o.). Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IDM sloužit jako zdrojové

IDM

Systém IDM, který v rámci projektů dodáváme je produkt AC Identita. AC Identita je systém společnosti AutoCont, který dlouhodobě systematicky vyvíjíme jako produkt pro řešení problematiky správy identit v rámci organizací. AC Identita splňuje veškeré požadavky ze zadávací dokumentace.

Portál IDM

Portál IDM obsahuje webové rozhraní pro administraci a rozhraní pro koncové uživatele („běžný“ uživatel, schvalovatel, atd.) řešení IDM. K webovému rozhraní je možný přístup z internetového prohlížeče protokolem HTTP a zabezpečeným protokolem HTTPS. Pro přístup jsou podporovány prohlížeče Internet Explorer, Google Chrome.

Webové rozhraní umožňuje běžnému uživateli dovolit měnit některé údaje o své identitě. Zejména musí mít běžný uživatel prostřednictvím webového rozhraní možnost si změnit heslo, které podléhá stanoveným politikám na formát hesla.

IDM Server

IDM Server obsahuje následující komponenty řešení:

Modul oprávnění

Modul oprávnění řídí jednotlivé oprávnění v systému IDM.

Pro řízení oprávnění na v systému IDM, IDM obsahuje editor rolí, který slouží jako nástroj pro individuální nastavení práv pro každou stávající i nově založenou aplikační roli aplikace IDM. Pro každou roli je možné podrobně nastavit, pro jakou sekci aplikace IDM (Číselníky, Synchronizace, Identity, apod.) rozsah oprávnění a to až do úrovně atributů a povolených aktivit (například vytváření záznamů, úprava záznamů, atd.).

Modul webových služeb

IDM poskytuje rozhraní webových služeb pro napojení dalších systémů. Základní konfigurace přístupu k webovým službám bude přístupná v portálu IDM. Webové služby komunikují SOAP protokolem.

Rozhraní poskytuje minimálně následující služby:

- Správa organizační struktury
- Správa hierarchie systematizovaných míst
- Správa identit a přidružených dat
- Získání nadřízené osoby pro daného zaměstnance
- Správa aplikační rolí
- Získání seznamu uživatelů dané aplikace
- Získání seznamu agend a agendových rolí přiřazených dané aplikaci
- Zápis seznamu aplikačních rolí do IDM
- Zápis certifikátů do IDM
- Služba pro autorizaci pro ISZR – služba ověří validnost volání služby ISZR. Služba bude ověřovat v IDM:
 - Zda je evidován uživatel v IDM, který je požadavku na ISZR
 - Zda je evidována aplikace v IDM, která je požadavku na ISZR
 - Zda má tento uživatel v IDM nastaven přístup do aplikace, která je v požadavku na ISZR
 - Zda existuje v IDM v rámci evidence organizační struktury rovněž evidence pro dané OVM, které je uvedeno v požadavku na ISZR
 - Zda má aplikace, která je v požadavku na ISZR, v IDM povolenou agendovou činnostní roli a agendu, které jsou rovněž uvedeny v požadavku na ISZR.

Modul notifikací

Modul posílání emailových notifikací obsahuje následující vlastnosti:

- Možnost notifikovat emailovou zprávou vytvoření a změny identity.
- Možnost notifikovat emailovou zprávou vytvoření a změny referenčních objektů jako systematizované místo, organizační jednotka, skupina, agenda, agendová činnostní role, aplikace, skupina aplikací, aplikační role atd.
- Mechanismus správy notifikací včetně náhledu na odeslané notifikace je přímo v portálu IDM.
- V portálu je možné v šabloně notifikace definovat příjemce, předmět a obsah dané notifikace. V rámci šablony notifikace je možné zvolit jazyk dané notifikace a podporovat tak notifikace ve více jazycích.
- U notifikací vázané k identitám je možné nastavovat pro odesílání notifikací samostatné příjemce pro různé části organizační struktury (oddělení, odbory, sekce).
- IDM obsahuje notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci je možné nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu.
- Notifikace je v IDM možné aktivovat pro jednotlivé zdrojové systémy, které v IDM změnu identity nebo referenčního objektu provedli. Jedná se například o personální systém, Portál IDM, rozhraní webových služeb atd.
- IDM obsahuje notifikační konektor, který simuluje napojení aplikace, která zatím není napojena na IDM. Pokud administrátor IDM nebo automatické pravidlo přidá, odebere identitě roli z této aplikace nebo změni identitu, pošle se emailová notifikace definovanému příjemci (administrátorovi) aplikace.

Modul reportů a logování

IDM obsahuje modul logování a reportů. Detail tohoto modulu je uveden v kapitole Návrh logování, historizace a možnosti auditu v rámci IDM dokumentu nabídky.

Modul správy identit a číselníků

IDM obsahuje modul správy identit a číselníků. Detail datového modelu těchto objektů je uveden v kapitole Návrh hrubého datového modelu dokumentu nabídky.

Modul synchronizací

IDM umožňuje spouštět synchronizaci ručně i automaticky. Synchronizace je možné spouštět i v simulačním režimu, tak aby bylo možné si ověřit stav dopadu reálného spuštění předem. Řešení umožňuje sledovat jednotlivé stavy i v průběhu synchronizace. Výstupem simulačního běhu je log, který obsahuje informace k jakým změnám a operacím by došlo v daném cílovém systému, pokud by byla synchronizace skutečně spuštěna v ostrém režimu.

Vedle ručního spuštění IDM podporuje nastavení plánovaných úloh automatické synchronizace. Pro automatické synchronizace je možné přímo v IDM nastavit datum a čas příští synchronizace, interval spuštění pravidelné synchronizace, okno odstavky synchronizace.

V průběhu synchronizace je možné si v IDM zobrazit stav synchronizace včetně procentuální indikace postupu synchronizace a také zobrazení počtu zpracovávaných změn nebo záznamů v IDM.

Veškeré záznamy o spuštěných bězích synchronizace, včetně náhledu na seznam synchronizovaných změn, je v IDM evidován v historiích synchronizací.

IDM umožňuje vedle systémové konfigurace IDM spravovat synchronizace včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavené intervalu odstavky atd.

IDM je možné konfigurovat následující nastavení pro jednotlivé synchronizované systémy:

- Konfigurace kompletní nebo změnové synchronizace
- Čas příští synchronizace
- Maximální počet změn
- Interval běhu synchronizace
- Interval odstavky běhu synchronizace
- Zapnutí emailových notifikací pro chyby při synchronizaci
- Aktivace/deaktivace synchronizace
- Organizace začleněné do synchronizace
- Nastavení spojení na dané systémy

Modul pravidel

Kromě ručního zařazení uživatele do skupiny administrátorem IDM může být uživatel při zápisu změn zařazen do skupin uplatněním pravidel pro automatické zařazení do skupin a aplikačních rolí.

Pro automatické zařazení nastaví administrátor v administrátorském rozhraní sadu pravidel, podle kterých se na základě atributů uživatele vyhodnotí sada uživatelských skupin, aplikačních rolí, do kterých má být uživatel zařazen.

Automatické zařazení uživatele do skupiny může být nastaveno podle různých atributů uživatele – např. zařazení do organizační jednotky, na pracovní místo a dalších atributů resp. kombinace atributů uživatele.

Spouštění pravidel je definováno jako synchronizovaný systém, do něhož lze nastavit interval spuštění změnové nebo kompletní synchronizace (vyhodnocení pravidel). Na základě vyhodnocení sady pravidel se uživatelé zařadí do příslušných skupin, aplikačních rolí.

Ruční zařazení do skupiny (administrátorem) má přednost před automatickým zařazením a není automatickým procesem dotčeno. Uživatelsky (administrátorem) je možné přepnout příznak automatického / ručního zařazení.

Výsledné stavy vyhodnocení pravidel:

- Beze změny
- Nové skupiny, role – uživatel se zařadí
- Chybějící skupiny, role – uživatel se vyjme. Nelze automaticky vyjmout ze skupiny nebo role, která má „automaticky = false“.

Změna zařazení do skupiny se promítne s okamžitou platností – po aplikaci pravidel.

Modul workflow

IDM obsahuje Modul workflow pro řízení životního cyklu změn identit a schvalování změn. Workflow umožňuje následující:

- vložit pro nadřízené pracovníky požadavky na změny v přiřazení rolí pro podřízené pracovníky a sledovat stav vyřizování jejich žádostí.
- schválení či zamítnutí požadavků na změny identit.
- odeslání schvalovateli upozornění ve formě emailové notifikace
- schvalovatelé si mohou zobrazit přehled úloh ke schválení
- požadavky je možné schválit či zamítnout včetně uvedení zdůvodnění.
- workflow podporuje vícekrokové schvalování
- schvalovat může jednotlivec nebo skupina schvalovatelů.
- Sledování průběhu workflow v grafickém výjádření
- Řešení zastupitelnosti a eskalace
- Možnost vložení systémových kroků

Databáze IDM

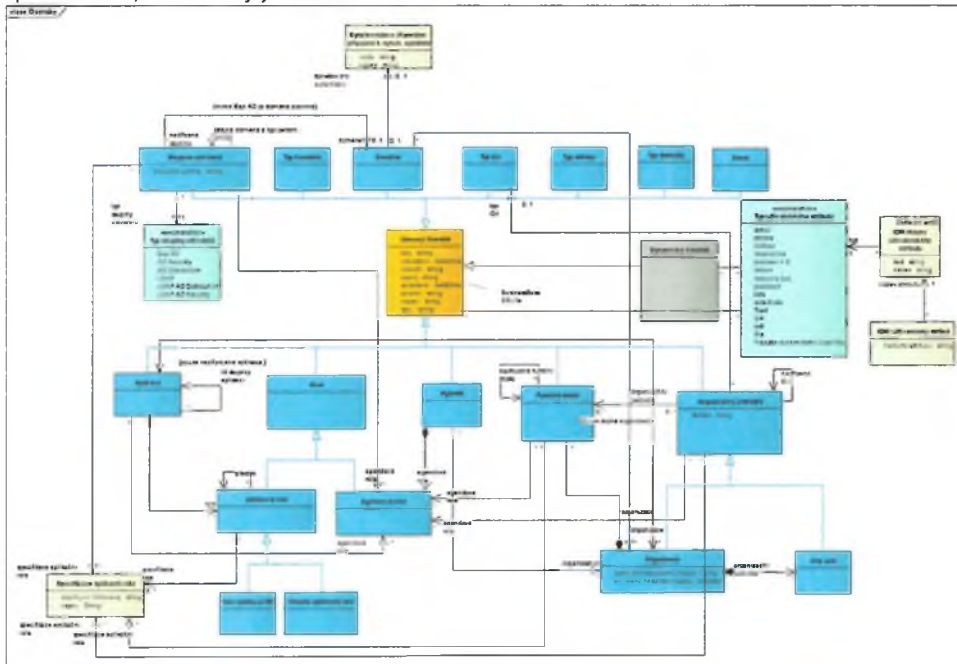
IDM udržuje identity, číselníky, skupiny identit a organizační struktury ve své vnitřní databázi. Identity ve vnitřní databázi slouží jako referenční identity pro ostatní informační systémy.

NÁVRH HRUBÉHO DATOVÉHO MODELU

V rámci doménového modelu IDM umožňuje IDM evidovat libovolný počet organizačních struktur organizačních celků, stromů organizačních struktur, struktur funkčních míst a interních i externích uživatelů. Modely jsou zpracovány ve standardu UML (Unifikovaný modelový jazyk).

Doménový model – Číselníky

Kapitola doménový model číselníků popisuje základní evidenci referenčních dat v systému IDM. Jedná se o data, která mají přímou nebo nepřímou vazbu na hlavní objekt – identita. Model číselníků zahrnuje objekty organizačních jednotek, funkčních míst, aplikací, aplikačních rolí, atd. včetně jejich vazeb.



Obrázek 1 Číselníky AC Identity

Typ OJ

Číselník typů organizačních jednotek. Zpravidla zahrnuje hodnoty:

- Odbor
- Oddělení
- Úsek, sekce
- Organizace
- Útvar

Administrátor může číselník rozšířit dle potřeby o další typy. Parametry a správa číselníku jsou konfigurovatelné přímo z grafického administračního rozhraní.

Typ adresy

Číselník typů adres. Zpravidla zahrnuje adresy: trvalá, zaměstnání, doručovací, přechodná, narození. Administrátor může číselník rozšířit dle potřeby o další typy. Parametry a správa číselníku jsou konfigurovatelné přímo z grafického administračního rozhraní.

Aplikace

SW produkt provozovaný v rámci organizace, ke kterému mají přístup vybraní uživatelé a mají přiřazené určité uživatelské role. Z pohledu IDM chápeme aplikaci jako konzumenta roli. Aplikace je v IDM slučovat konfiguračně do skupin aplikací

Uživatelé aplikace jsou zavedeni v IDM a v ideálním případě mají jednotnou autentizaci. Parametry a správa číselníku jsou konfigurovatelné přímo z grafického administračního rozhraní.

Agenda

V IDM je agendou souhrnu činností orgánů veřejné moci. Agenda je zaregistrována v základním registru práv a povinností. Tyto agendy je možné pro dané OVM načítat z registru práv a povinností.

Role

Role je abstrakce pro uživatelské a agendové role. Jednotlivé typy jsou popsány v příslušných entitách. Autorizační model IDM a model rolí je založen na RBAC (Role-Based Access Control) přístupu.

Agendová (činnostní) role

Agendové role odpovídají činnostním rolím evidovaným pro agendy registrované v základním registru RPP. Tyto agendy a role je možné pro dané OVM načítat z registru práv a povinností.

Aplikační role

Aplikační role jsou souhrnem oprávnění uživatelů v rámci určité aplikace. Jsou definovány pro jednotlivé aplikace a budou získávány prostřednictvím jednotného rozhraní z jednotlivých aplikací, nebo ručně vytvořeny v IDM. V systému IDM je údaj o roli pouze evidenční (i když jsou master), práva uživatele plynoucí z přidělených rolí spravují příslušné aplikace, pro které jsou role definovány.

Role aplikace IDM

Role aplikace IDM ovlivňují oprávnění uživatelů zaevidovaných v systému IDM ve vlastní aplikaci IDM.

Ostatní aplikační role

Role aplikací mimo IDM. Upřesňující informace může být definována libovolnou hodnotou typu string podle požadavků aplikace, která roli využívá. IDM o významu upřesňující informace nemá informaci.

Specifikace aplikační role

Každá role může mít další upřesnění - např. pro zařazení do organizační struktury.

Předpokládáme, že každá role může mít určitý typ doplňujících informací. Uživatelé se následně přiřadí role s konkrétní specifikací a to jmenovitě pro každou specifikaci.

Příklad: Role Administrátor organizace má vytvořeny specifikace pro všechny organizace v systému. Uživatelé přiřadím roli administrátora pro konkrétní organizaci.

Při přidělování specifikací aplikačních rolí je možnost nastavovat platnost od-do. Přidělování /odebíráni zajišťuje agent na straně IDM, který kontroluje datумы platností aplikačních rolí.

Země

Číselník zemí – převzato z ČSÚ. Při implementaci IDM bude číselník naplněn hodnotami staženými ze stránek ČSÚ. Tento číselník je dále spravován administrátorem číselníků IDM.

Typ dokladu

Možné typy osobních dokladů. Při implementaci je možné naplnit hodnotami, jako jsou Řidičský průkaz, Občanský průkaz, Povolení k pobytu, Cestovní pas, Pobytový štítek, Vízový štítek. Číselník může být podle potřeby rozšířen do další hodnoty administrátorem číselníků IDM.

Organizační jednotka

Organizační jednotkou (OJ) je libovolný uzel ve stromové organizační struktuře.

Počet úrovní organizační struktury není omezen. V některé úrovni stromu jsou jednotlivé organizace, které mají vlastní organizační strukturu. Vzhledem k vazbě objektů organizační jednotky na další objekty organizačních jednotek je možné v IDM vytvářet a spravovat hierarchickou strukturu a libovolný počet stromů organizačních jednotek. Struktura organizačních umožňuje evidenci jak interních organizačních struktur, tak i externích struktur a členění.

Organizace

Speciální typ organizační jednotky. Jedná se o kořenový uzel organizační struktury organizace

Jiný uzel org.struktury

Uzel organizační struktury, který není organizací.

Typ uživatelského atributu

Číselníkům i jednotlivým entitám identity (uživatelé) mohou být doplněny libovolně uživatelem definované atributy. Následující tabulka je výčtem povolených datových typů těchto atributů.

Hodnota bude uložena jako string, avšak uživatelé se bude typ jevit jako jeden z uvedených typů.

Tabulka 1 Typy atributů

Atribut	Poznámka
email «enumerace»	Pro daný atribut bude kontrola na email.

Atribut	Poznámka
Phone (telefon) «enumerace»	Pro daný atribut bude kontrola na telefonní číslo.
string (řetězec) «enumerace»	Pro daný atribut bude kontrola na řetězec - max. délka 255 znaků.
Description (popis) «enumerace»	Pro daný atribut bude kontrola na řetězec - max. délka 4000 znaků.
boolean «enumerace»	Pro daný atribut bude kontrola na Ano x Ne. Initial Value: 0;
date (datum) «enumerace»	formát dd.mm.yyyy
dateTime (datum a čas) «enumerace»	formát dd.mm.yyyy hh:mm:ss
Password (heslo) «enumerace»	Pro daný atribut bude kontrola na heslo - max. délka 255.
Login (přihlašovací jméno) «enumerace»	
int (celé číslo) «enumerace»	délka 20 - +číslice bez mezer
Float (desetinné číslo) «enumerace»	Pro daný atribut bude kontrola na typ float.
ip4 «enumerace»	Pro daný atribut bude kontrola na IP adresu nnn.nnn.nnn.nnn
ip6 «enumerace»	Pro daný atribut bude kontrola na IP adresu nnn.nnn.nnn.nnn.nnn.nnn

Dalším typem uživatelského atributu je výběr hodnoty z dynamicky definovatelného číselníku.

Typ kontaktu

Číselník kontaktních údajů. Musí být v souladu s číselníkem kontaktů v personálním systému, případně bude definováno mapování mezi jednotlivými typy kontaktů.

Doména

Atribut rozlišující příslušnost uživatelských účtů k nějaké skupině, v rámci které je možné uživatele ověřit uživatelským jménem a heslem.

Uživatel má v rámci domény jedinečné přihlašovací jméno – login. V rámci IDM může být zaregistrován pouze uživatel z domény, která je zavedena v číselníku domén IDM.

Skupina uživatelů

Skupina uživatelů seskupuje uživatele podle určitých kritérií. Zařazení uživatele do skupiny provádí zpravidla administrátor IDM, v některých případech může k zařazení do určité skupiny dojít automaticky podle definovaných parametrů (atributů). V IDM může být skupina začleněna do další skupiny. IDM umožňuje pouze však začlenit skupinu maximálně do jedné nadřazené skupiny.

Typ skupiny uživatelů

Uživatelská skupina má jeden z 6 uvedených typů:

Tabulka 2 Typy uživatelských skupin

Atribut	Poznámka
Bez AD «enumerace»	nemá odkaz v AD ani LDAP
AD Security «enumerace»	skupina vázaná se security group v AD

Atribut	Poznámka
AD Distribution «enumerace»	skupina vázaná s distribution group v AD
LDAP «enumerace»	skupina vázaná se skupinou v LDAP
LDAP + AD Security «enumerace»	skupina vázaná se skupinou v LDAP + skupina vázaná se security group v AD
LDAP + AD Distribution «enumerace»	skupina vázaná se skupinou v LDAP + skupina vázaná s distribution group v AD

Pracovní místo (také systemizované místo neboli funkční místo)

Pracovní místo je pracovní zařazení v rámci organizační struktury. Uživatel může být přiřazeno více pracovních míst. Pracovní místo je podřízeno organizaci, v rámci organizace je definován libovolný počet pracovních míst. Nemusí být definována žádná pracovní místa v organizaci (např. v příspěvkových organizacích). Pracovnímu místu mohou být přiřazeny uživatelské role z libovolných aplikací. Pracovní místo náleží do organizační jednotky (nepovinný atribut OJ). Na pracovní místo je možné je možné přiřazovat i skupiny uživatelů.

Dynamické číselníky (uživatelské číselníky)

Jedná se o číselníky, které administrátorovi slouží pro rozšíření předdefinovaných číselníků.

Atributy dynamických číselníků jsou:

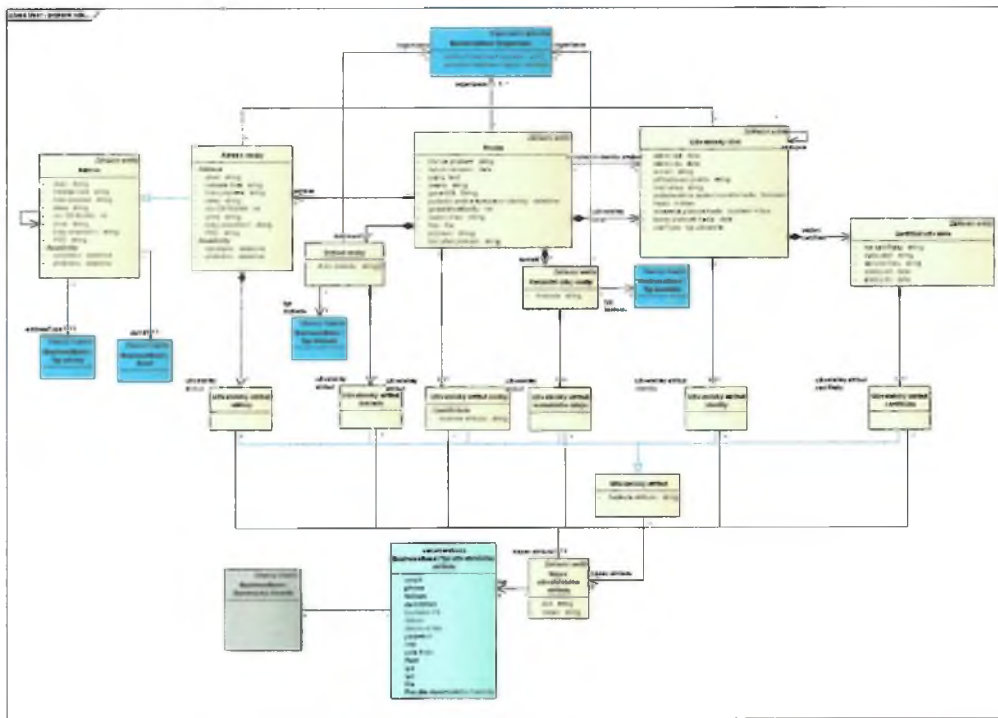
- Kód
- Název
- Popis

Doménový model - Uživatel (identita)

Doménový model identit obsahuje definici identit a údaje spojené s evidencí identit – uživatelů.

Identita je definována jako relace objektu osoby a jejich účtů včetně dalších vazebních objektů uvedených na datových modelech identit níže. Identita je v IDM svázána k jednotlivým fyzickým osobám (popř. aplikacím v případě technických/aplikačních účtů) s vazbami. Identita s vazbou na fyzickou osobu (popř. aplikacím v případě technických/aplikačních účtů) je evidována v systému IDM pouze jednou s jednoznačným identifikátorem generUID, osobní číslo případně jiným.

Datové modely identit:



Obrázek 2 identita – popisné údaje

Uživatelský účet

Synchronizovaný uživatel, uživatelský účet.

Jde o dílčí identitu s ohledem na práci v integrovaných informačních systémech.

Uživatel - osoba, která je oprávněna přihlásit se do sítě a provádět úkony, ke kterým ji opravňují přiřazené uživatelské role. Jednoznačným identifikátorem uživatele v rámci domény je doména a uživatelské jméno – login.

Údaje uživatele mohou být editovány ve všech stavech životního cyklu administrátorem případně změnou ve zdrojovém systému.

Uživatel je zařazen do kmenové organizační jednotky v rámci organizace.

Uživatel může mít přiřazeno primární pracovní místo, případně další pracovní místa definovaná v rámci jeho organizace.

Uživatel může být zařazen do libovolných uživatelských skupin.

Uživateli mohou být přiřazeny aplikační a činnostní role a to buď přímo, nebo prostřednictvím organizační jednotky, pracovního místa, uživatelské skupiny.

IDM umožňuje u vazby aplikační rolí na uživatele definovat datumy platnosti: aktivní od, aktivní do. K vazbě uživatele na roli je dále možné dodefinovat další požadované atributy. Pokud období uplyne nebo ještě nenastalo, není přiřazení uplatněno.

Vazby uživatelského účtu:

Jedná se o vazby na následující objekty:

Specifikace aplikační role – identita může několik specifikací aplikační role/rolí.

IDM umožňuje u vazby aplikační rolí na uživatele definovat datumy platnosti: aktivní od, aktivní do. K vazbě uživatele na roli je dále možné dodefinovat další požadované atributy. Pokud období uplyne nebo ještě nenastalo, není přiřazení uplatněno.

Agendová role – identita může mít vazbu na několik agentových rolí

Skupina – identita může mít vazbu na několik skupin

Doména – identita může mít vazbu pouze na jednu doménu

Organizace – identita může mít vazbu na několik organizací

Organizační jednotka – identita může mít vazbu na několik organizačních jednotek

IDM umožňuje u vazby organizační jednotky na uživatele definovat datumy platnosti: aktivní od, aktivní do. Pokud období uplyne nebo ještě nenastalo, není přiřazení uplatněno.

Funkční místo – identita může mít vazbu na několik funkčních míst

Dynamický číselník – identita může mít skrze uživatelské atributy vazbu na několik dynamických číselníků

Detail k vázaným objektům je u uveden v kapitole 6.1.2.1 Doménový model – Číselníky dokumentu nabídky.

Typ uživatelského účtu

Uživatelský účet má jeden ze 4 možných typů:

- Účet v AD (LDAP)
- E-mailová schránka v MS Exchange
- Kontakt v MS Exchange
- Interní účet

Certifikát uživatele

Uživatel může mít evidován v IDM libovolný počet certifikátů. Administrátor může k záznamu libovolného uživatele evidovat certifikát.

V metadatach se eviduje sériové číslo certifikátu, platnost a stav (platný, neplatný), certifikační autorita, typ certifikátu.

Typ uživatelského atributu

Číselníkům i jednotlivým entitám identity (uživatele) mohou být doplněny libovolné uživatelem definované atributy. Následující tabulka je výčtem povolených datových typů těchto atributů.

Hodnota bude uložena jako string, avšak uživateli se bude typ jevit jako jeden z uvedených typů.

Tabulka 3 Typy atributů

Atribut	Poznámka
email «enumerace»	Pro daný atribut bude kontrola na email.
Phone (telefon) «enumerace»	Pro daný atribut bude kontrola na telefonní číslo.
string (řetězec) «enumerace»	Pro daný atribut bude kontrola na řetězec - max. délka 255 znaků.
Description (popis) «enumerace»	Pro daný atribut bude kontrola na řetězec - max. délka 4000 znaků.

Atribut	Poznámka
boolean «enumerace»	Pro daný atribut bude kontrola na Ano x Ne. Initial Value: 0;
date (datum) «enumerace»	formát dd.mm.yyyy
dateTime (datum a čas) «enumerace»	formát dd.mm.yyyy hh:mm:ss
Password (heslo) «enumerace»	Pro daný atribut bude kontrola na heslo - max. délka 255.
Login (přihlašovací jméno) «enumerace»	
int (celé číslo) «enumerace»	délka 20 - +-číslíce bez mezer
Float (desetinné číslo) «enumerace»	Pro daný atribut bude kontrola na typ float.
ip4 «enumerace»	Pro daný atribut bude kontrola na IP adresu nnn.nnn.nnn.nnn
ip6 «enumerace»	Pro daný atribut bude kontrola na IP adresu nnn.nnn.nnn.nnn.nnn.nnn

Dalším typem uživatelského atributu je výběr hodnoty z dynamicky definovatelného číselníku.

NÁVRH LOGOVÁNÍ, HISTORIZACE A MOŽNOSTÍ AUDITU V RÁMCI IDM

Kapitola popisuje logování dat a událostí v IDM včetně podrobnosti úrovně logování. V IDM je dále možné nastavit mechanismus, pravidla a interval pro archivaci nebo promazávání logů. Rozsah a nastavení konkrétních pravidel logování, uchovávání dat, historizace, analýz a reportů bude podrobně specifikováno v průběhu analytických prací v návrhové fázi projektu implementace IDM.

Systém zapisuje sledované události IDM do příslušných logů.

Jednotlivé typy logů dále zahrnují detailní informace závislé na typu logu.

Při činnosti systému vznikají následující typy logů:

- ✓ **Aplikační log** – zaznamenává události systému. Tento typ logu je umístěn na file systému IDM serveru a zahrnuje následující části:
 - Log aplikačního serveru,
 - Logy aplikace IDM, IDM používá pro zápis Log4j komponentu.
- ✓ **Auditní log** – zaznamenává změnu entit evidovaných v systému IDM včetně hodnot před a po změně. Jde o auditovatelnou historii, která je přístupná z uživatelského rozhraní IDM. Logovány jsou změny entit objektů identit, číselníků, ale i změny konfigurace nastavení a správy systému. Záznam historie obsahuje seznam všech provedených změn dané entity (tj. všech změnových požadavků). Příklad historie entity uživatele:

Záznamů na stránce: 10 Stránka: 1 (Zobrazeno 1 - 9 z 9)			
Vytvořil	Popis	Datum zpracování Od Do	Stav
Poskočil Jiří	Přidělení specifikace aplikační role u	26.06.2014 13:23:49	Úspěšná akce
Poskočil Jiří	Přidělení specifikace aplikační role u	26.06.2014 13:23:49	Úspěšná akce
Poskočil Jiří	Změna uživatelského atributu [Osol	26.06.2014 13:23:49	Úspěšná akce
Poskočil Jiří	Změna uživatelského atributu [Uvol	26.06.2014 13:23:49	Úspěšná akce
Poskočil Jiří	Změna uživatelského atributu [Veře	26.06.2014 13:23:49	Úspěšná akce
Poskočil Jiří	Zavedení nového uživatele	26.06.2014 13:22:34	Úspěšná akce

Obrázek 4 Příklad historie entity uživatele

Základními informacemi v historii jsou, kdo změnu vytvořil, popis změny, datum vytvoření změny a úspěšnost operace. Pro každý záznam v historii si lze zobrazit detail. V detailu jsou podrobně zachyceny provedené změny jednotlivých atributů. Příklad detailu záznamu historie:

Měněný atribut	Nová hodnota	Původní hodnota	Priorita změny
Typ uživatelského účtu	Interní účet		1
Stav	Aktivní		1
Organizační jednotka	Externí organizace		1
Organizace	Externí organizace		1
Doména	Externí		1
Uživatelský účet	absolon		1
Aktivní od	26.06.2014 00:00:00		1
Neomezená platnost hesla	Ne		1
Nové heslo	Ano		1

Obrázek 5 Příklad detailu záznamu historie

Synchronizační log – zaznamenává průběh synchronizací IDM s dalšími systémy.

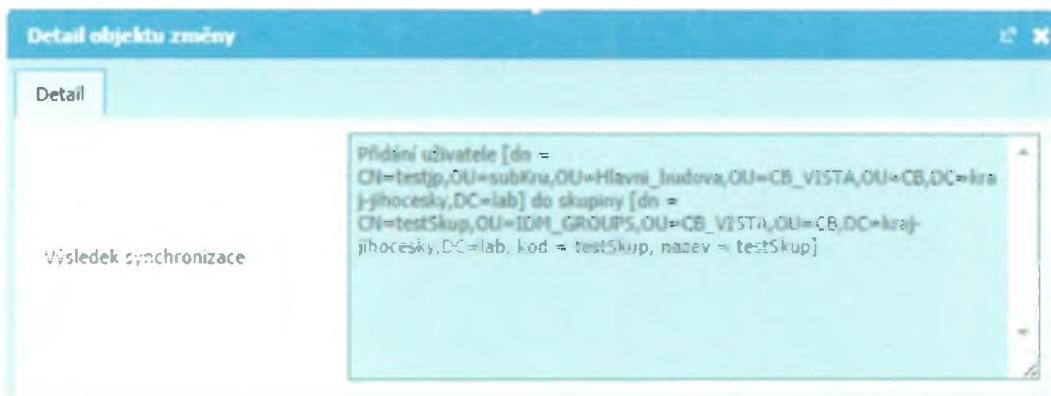
Jde o historii změn provedených některým ze synchronizovaných systémů, která je přístupná z uživatelského rozhraní IDM. Záložka Historie synchronizací se nachází v detailu každé entity (tj. v detailu uživatelských účtů, číselníků, synchronizovaných systémů atd.), která je zpracovávána prostřednictvím synchronizace. Obsahuje seznam všech provedených synchronizací dané entity ze zdrojových a do cílových synchronizovaných systémů. Příklad historie synchronizovaného záznamu:

Typ změny	Popis události	Stav propsání	Jméno systému	Typ synchronizace	Čas události
	Synchronizace identity	Úspěšně	ESB Identity úřad	Kompletní	10.07.2014 14:23:40
	Synchronizace identity	Úspěšně	ESB Identity úřad	Kompletní	09.07.2014 20:49:30
	Synchronizace identity	Úspěšně	ESB Identity úřad	Změnová	03.07.2014 10:19:31
Odebrání uživatele ze :		Úspěšně	Pravidla interní PK	Změnová	02.07.2014 15:52:11
Odebrání uživatele ze :		Úspěšně	Pravidla interní PK	Změnová	02.07.2014 15:52:11
	Aktualizace účtu	Úspěšně	Active Directory	Změnová	02.07.2014 15:49:27
	Editace uživatelského	Úspěšně	GINIS interní PK	Změnová	27.06.2014 15:02:07
	Editace uživatele	Úspěšně	GINIS interní PK	Změnová	27.06.2014 15:02:04
	Synchronizace identity	Úspěšně	ESB Identity úřad	Změnová	27.06.2014 13:53:35
	Přidání uživatele do sk.	Úspěšně	Active Directory	Kompletní	26.06.2014 16:49:26

Obrázek 6 Příklad historie synchronizovaného záznamu

Základními informacemi v historii synchronizací záznamu jsou typ změny, popis události, stav propsání, jméno synchronizovaného systému, typ synchronizace a datum a čas synchronizace.

Pro každý záznam v seznamu změn si lze zobrazit detail s popsávanými změnami.



Obrázek 7 Příklad historie synchronizovaného záznamu - Detail

Záznamy z historie synchronizací lze souhrnně zobrazit i pro synchronizovaný systém a zvolený běh synchronizace. Obsahuje seznam všech provedených synchronizací daného synchronizovaného systému.

ID synch. cy	Typ	Uživatelský t	Jméno	Příjmení	Typ spuštěn	Počet chyb	Počet všech	Začátek	Konec
461	Změnová	poskocil	Jiří	Poskočil	Ruční	0	1	16.07.2014	16.07.2014
459	Změnová	poskocil	Jiří	Poskočil	Ruční	0	5	16.07.2014	16.07.2014
456	Změnová	poskocil	Jiří	Poskočil	Ruční	0	1	15.07.2014	15.07.2014
454	Změnová	poskocil	Jiří	Poskočil	Ruční	0	2	15.07.2014	15.07.2014
440	Změnová	poskocil	Jiří	Poskočil	Ruční	0	3	10.07.2014	10.07.2014
435	Změnová	rezler	David	Rezler	Ruční	0	123	09.07.2014	09.07.2014
423	Změnová	poskocil	Jiří	Poskočil	Ruční	0	2	07.07.2014	07.07.2014
420	Změnová	poskocil	Jiří	Poskočil	Ruční	0	2	07.07.2014	07.07.2014
416	Změnová	poskocil	Jiří	Poskočil	Ruční	0	2	07.07.2014	07.07.2014
413	Změnová	poskocil	Jiří	Poskočil	Ruční	0	5	07.07.2014	07.07.2014

Obrázek 8 Seznam provedených synchronizací

Základními informacemi v historii synchronizací jsou typ synchronizace, kdo synchronizaci spustil (uživatelské jméno, jméno, příjmení), typ spuštění, počet chybně zpracovaných záznamů v rámci dané synchronizace, počet všech synchronizovaných záznamů a datum a čas synchronizace.

Pro každý záznam v historii synchronizací si lze zobrazit seznam všech změn zahrnutých do vybrané synchronizace.

Seznam změn provedených synchronizací

Záznamů na stránce 10 Stránka 1 (Zobrazeno 1 - 5 z 5)

Typ změny	Popis události	Stav popsání Vše	Objekt	Typ objektu	Čas události Od Do
	Vytvoření uživatele	Úspěšně	kedro	Uživatelský účet	16.07.2014 08:19:27
	Aktualizace hesla uživatele	Úspěšně	kedro	Uživatelský účet	16.07.2014 08:19:27
	Aktualizace účtu	Úspěšně	kedro	Uživatelský účet	16.07.2014 08:19:27
	Přidání uživatele do skupiny	Úspěšně	kedro	Uživatelský účet	16.07.2014 08:19:28
	Aktualizace uživatele	Úspěšně	balek	Uživatelský účet	16.07.2014 08:19:29

Záznamů na stránce 10 Stránka 1 (Zobrazeno 1 - 5 z 5)

Zavřít

Obrázek 9 Seznam všech změn zahrnutých do synchronizace

Pro každý záznam v seznamu změn provedených synchronizací si lze zobrazit detail s popsáními změnami.

Detail objektu změny

Detail Seznam změnových požadavků

Výsledek synchronizace

Synchronizace identity [bicik], Iniciační vektor zprávy
[UsVvzmQ5o4f+qMI6IEDgKw==]

Zavřít

Obrázek 10 Detail objektu změny

Z historie synchronizací je také možno zobrazit související změnové požadavky včetně detailu požadavku.

/ **Error log** – zaznamenává chyby v průběhu práce systému.

Chybové zprávy a případný detail chyby bývá zaznamenán do aplikačních logů, případně do logu synchronizace (viz předchozí typy logů).

/ **Notifikační log** – zaznamenává odeslané notifikace.

V uživatelském rozhraní IDM lze pro každou z notifikačních šablon zobrazit seznam vygenerovaných notifikací. Notifikace jsou sloučeny do tzv. notifikačních balíčků.

Identifikátor	E-mail	Předmět	Stav	Čas odeslání
146	administrator@pk-test.cz	Vytvoření identity	Odeslaný	15.07.2014 16:55:00
141	administrator@pk-test.cz	Vytvoření identity	Odeslaný	08.07.2014 10:25:00
137	administrator@pk-test.cz	Vytvoření identity	Odeslaný	07.07.2014 17:00:00
132	administrator@pk-test.cz	Vytvoření identity	Odeslaný	07.07.2014 16:10:00
130	administrator@pk-test.cz	Vytvoření identity	Odeslaný	07.07.2014 15:35:00
127	administrator@pk-test.cz	Vytvoření identity	Odeslaný	04.07.2014 12:45:00
123	administrator@pk-test.cz	Vytvoření identity	Odeslaný	04.07.2014 11:30:00
122	administrator@pk-test.cz	Vytvoření identity	Odeslaný	04.07.2014 11:05:00
121	administrator@pk-test.cz	Vytvoření identity	Odeslaný	04.07.2014 10:40:00
117	administrator@pk-test.cz	Vytvoření identity	Odeslaný	03.07.2014 11:25:00

Obrázek 11 Seznam vygenerovaných notifikací

Atribut Stav udává, v jaké fázi zpracování je daný notifikační balíček. Balíček ve stavu „Čekající“ je balíček vygenerovaný, ale dosud nezpracovaný emailovým agentem, tzn. jednotlivé notifikace z daného balíčku dosud nebyly odeslány. Balíček ve stavu „Odeslaný“ obsahuje notifikace již odeslané příslušným adresátům. Balíček ve stavu „Chybový“ je vygenerovaný, nepodařilo se jej však odeslat (např. z důvodu nedostupnosti SMTP serveru). Balíček v chybě je možné znovu odeslat přes UI IDM.

Další informace ohledně činnosti notifikačního agenta lze nalézt v aplikačním logu (viz. předchozí popisované typy logů).

/ **Administrační log** – zaznamenává události související s administrací a konfigurací systému.

Jde o aplikační historii přístupnou přes uživatelské rozhraní IDM. Do této historie se zapisují změny v konfiguraci IDM, konfiguraci konektorů jednotlivých synchronizovaných systémů, změny na synchronizovaných systémech apod. Způsob logování je podobný auditnímu logu (viz. předchozí popisované typy logů).

/ **Simulační log** – zaznamenává události související se simulací běhu synchronizace

V portálu IDM je možné spouštět simulační běh synchronizace pro daný systém. Výstupem simulačního běhu je log soubor, který je ke stažení přímo z portálu IDM a obsahuje informace k jakým změnám a operacím by došlo v daném cílovém systému, pokud by byla synchronizace skutečně spuštěna v ostrém režimu.

```

15 13:15:52 Spuštění kontrolního modu
15 13:15:52 Synchronizace spuštěna. Typ synchronizace [COMPLETE]. Nastaven prázdný modul
15 13:15:54 Přesun uživatele [login: irena.adamka, původní DN: CN=Irena Adamka,OU=Interní,OU=Uzivatele,DC=muck,DC=local, nové DN: CN=irena.adamka,OU=Interní,OU=Uzivatele,DC=muck,DC=local]
15 13:15:54 Simulace. Aktualizace uživatele [login: irena.adamka]. [initials: null -> IA]
15 13:15:54 Simulace. Aktualizace uživatele [login: irena.adamka]: [accountExpires: null -> 0]
15 13:15:54 Přesun uživatele [login: frantisek.testovac, původní DN: CN=frantisek.testovac,OU=Interní,OU=Uzivatele,DC=muck,DC=local, nové DN: CN=frantisek.testovac,OU=Interní,OU=Uz
15 13:15:54 Simulace. Aktualizace uživatele [login: frantisek.testovac]. [initials: null -> FT]
15 13:15:54 Simulace. Aktualizace uživatele [login: frantisek.testovac]: [accountExpires: null -> 1309417560000000], [userAccountControl: 512 -> 514]
15 13:15:56 Synchronizace ukončena pro [AD_INT]. Typ synchronizace [COMPLETE].
15 13:16:56 Ukončení kontrolního modu

```

Obrázek 12 - ukázka simulačního logu

Uživatel v roli administrátora IDM a administrátora organizace může zadat parametry a vygenerovat report.

V IDM jsou dostupné následující reporty:

- Report uživatele z auditních logů

Umožňuje zobrazit uživateli s přidělenou aplikační rolí Administrátor IDM nebo Administrátor organizace či organizační jednotky stav uživatelského účtu (uživatelských účtů) k vybranému datu. Report je možné sestavit jak pro vybraného uživatele, tak také pro vybranou množinu uživatelů, vybranou organizační jednotku či doménu. Dalším parametrem reportu je datum (aktuální nebo z minulosti), pro které má být report vygenerován. Reporty se generují na pozadí,

výstupem reportu je XML. Vygenerovaný report zůstává v IDM a je možné zobrazit/stáhnout i později. Příklad vygenerovaného reportu:

```
<exHistoryResponse>
  <reportDate>2015-08-05T11:09:00.045+02:00</reportDate>
  <toDate>2015-08-05T00:00:00+02:00</toDate>
  <identities>
    <record>
      <idUser>21</idUser>
      <userAccount>
        <activeFrom>2015-07-21T00:00:00+02:00</activeFrom>
        <login>tomas</login>
        <status>ACTIVE</status>
        <userType>1</userType>
        <basicOrgUnitCode>DOHODY</basicOrgUnitCode>
        <basicOrgUnitName>DOHODY</basicOrgUnitName>
        <userAgendRoles/>
        <userApplicationRoles>
          <record>
            <applicationCode>IDM</applicationCode>
            <roleCode>IDMUsr</roleCode>
            <roleSpecification>Bez specifikace</roleSpecification>
            <roleSpecificationName>Bez specifikace</roleSpecificationName>
            <applicationName>Identity Management</applicationName>
            <roleName>Uživatel IDM</roleName>
          </record>
          <record>
            <applicationCode>ANT</applicationCode>
            <roleCode>AntiRole</roleCode>
            <roleSpecification>Bez specifikace</roleSpecification>
            <roleSpecificationName>Bez specifikace</roleSpecificationName>
            <applicationName>Antispam</applicationName>
            <roleName>Antispam </roleName>
          </record>
        </userApplicationRoles>
        <userGroups>
          <record>
            <code>a2</code>
            <groupType>NO_AD</groupType>
            <groupName>a2</groupName>
          </record>
        </userGroups>
        <userOrgUnits/>
        <userWorkingPositions>
          <record>
            <code>AntiSpam</code>
            <name>Antispam místo</name>
          </record>
        </userWorkingPositions>
        <userAttributes>
          <attribute>
            <name>Osoba krizového řízení</name>
            <value>>false</value>
            <code>OSOBA_KRIZOVEHO_RIZENI</code>
          </attribute>
        </userAttributes>
      </userAccount>
    </person>
    <firstName>Franta</firstName>
    <surname>Tomáš</surname>
    <personalId/>
    <personAddresses/>
    <personContacts/>
    <personDocuments/>
    <userAttributes>
      <attribute>
        <name>Pohlaví</name>
        <value>muž</value>
        <code>GENDER</code>
      </attribute>
    </userAttributes>
  </identities>
</exHistoryResponse>
```

```

<attribute>
  <name>Povolit sdílení kontaktních údajů</name>
  <value>>false</value>
  <code>CONTACT_PUBLISHING</code>
</attribute>
</userAttributes>
</person>
</record>
</identities>
</exHistoryResponse>

```

- Delepace.

Report obsahuje uživatele, kteří mají zděděné nějaké aplikační role od jiných uživatelů. Výstupem reportu je CSV soubor. Vygenerovaný report zůstává v IDM a je možné zobrazit/stáhnout i později. Příklad vygenerovaného reportu:

Tabulka 4 Report delepace

Uživatel- ský účet	Organi- zace	Doména	Aplikace	Aplikační role	Specifikace	Delegováno	Aktivní od	Aktivní do	Stav
novak [Jan No- vák]	X	IDM [IDM]	Identity Ma- nagement [IDM]	Administrátor organizace [OrgAdmin]	Gymnázium [9909]	pony [Petr Pony]	1.7. 2015		Aktivní
novakj [Jana No- váková]	X	IDM [IDM]	Antispam [ANT]	Antispam [AntiRole]	Bez specifi- kace [Bez specifikace]	pony [Petr Pony]	1.7. 2015	8.7. 2015	Neaktivní

Komodita K4 - Školení kybernetické bezpečnosti		
Část	Parametr	Popis
Obsah školení	Legislativní rá- mec	Zákon č. 181/2014 Sb., a informační bezpečnost v organizaci
	GDPR	Základní seznámení s nařízením GDPR (General Data Protection Regulation) - Obecným nařízením o ochraně osobních údajů- viz např. https://www.uoou.cz/gdpr-a-ro-leuouu/d-23082
	Škodlivý soft- ware	projevy, druhy, obrana, preventivní chování, praktická ukázka provádění kontroly anti- virovým programem
	Elektronická ko- munikace s úřady	datová schránka — co to je, k čemu slouží, zřízení a práce s datovou schránkou, elek- tronický podpis — co to je, jak s ním pracovat, jeho výhody a nevýhody
	Data vs. infor- mace	kategorizace (osobních) dat, zásady a povinnosti zpracování z pohledu zaměstnava- tele a zaměstnance, šifrování, praktická ukázka šifrování dat
	Ochrana dat	zálohování, archivace a mazání dat, praktická ukázka zálohování dat
	Přístup k síti	PIN / heslo a jeho uložení, správné heslo, zásada prázdného stolu
	Web	Používání webu, HTTPS, chatování, Skype, Facebook, výhody a rizika sociálních sítí, praktické ukázky
	Elektronická identita	ztráta identity se mě (ne)týká?
	Mobilita	Používání mobilních zařízení, používání veřejných sítí a WIFI
	Mailování bez- pečně	co e-mailem nikdy neposílat, spamy, phishing, hoax, bezpečné přihlášení/odhlášení, zálohování e-mailů, phishing
	Kyberšikana	co to je, jaké jsou její formy a jaká preventivní opatření
Incidenty	bezpečnostní incidenty a události, hlášení v organizaci,	

	Závěr	obecný bezpečnostní test
--	-------	--------------------------

Hodnocené parametry	
Parametr	Popis
Snížení nároků na správu systému	
1	System pro správu identit komodity K3 bude využívat pro ukládání dat databázový server MS SQL
Uživatelské přívětivost a snížení nároků na správu	
2	Kompletní uživatelské prostředí i prostředí pro běžnou správu a konfiguraci systému pro správu identit komodity K3 bude v českém jazyce

6.2 Obecné požadavky

- (1) Uchazeč v rámci zakázky navrhne:
 - (a) způsob rozšíření kapacit TC ORP a LAN pro implementaci a spolehlivý provoz nabízených komodit,
 - (b) způsob sběru logů systémů úřadu, jejich vyhodnocování a detekci bezpečnostních událostí,
 - (c) způsob automatizace správy identit a uživatelských účtů včetně způsobu napojení na SIEM,
 - (d) obsah uživatelských školení pro zvýšení povědomí uživatelů o kybernetických hrozbách a způsobech předcházení bezpečnostním událostem a incidentům,
- (2) Veškerá dokumentace vytvořená v rámci veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, PDF) používaných zadavatelem na datovém nosiči a 1x v papírové formě. Papírová forma bude logicky a věcně strukturovaná, bude připravena pro použití (např. provozní dokumentace ve formě vhodné pro použití administrátory v serverovně). Struktura i forma dokumentace bude před předáním předána ke kontrole a výslovně schválena zadavatelem.

6.3 Specifické požadavky K1 – Rozšíření kapacit Technologického centra ORP

- (1) Cílem rozšíření kapacit TC ORP je doplnění stávajících technologií tak, aby zajistily dostatek výpočetních zdrojů a diskových úložných kapacit pro dlouhodobě spolehlivý provoz nabízených komodit.
- (2) Součástí rozšíření kapacit diskových polí bude i provedení odpovídajících změn konfigurace navázaných systémů – diskové a serverové virtualizace.
- (3) Bude provedena modernizace síťové vrstvy „core“ LAN. Modernizací bude navýšena kapacita páteřních tras na 10 Gb a doplněna možnost exportu síťových toků pro SIEM.
- (4) Pro začlenění serveru budou využity stávající licence VMware vSphere a Veeam Backup & recovery.
- (5) Implementace předmětu plnění negativně neovlivní dostupnost ani neomezí funkčnost aplikací uživatelů. Součástí návrhu a realizace bude vhodný scénář postupu implementačních prací zpracovaný v Provděcí dokumentaci

6.4 Specifické požadavky K2 – SIEM a NBA

- (1) Implementací systému SIEM (Security Information and Event Management) dojde k zastřešení infrastrukturních, informačních a bezpečnostních systémů úřadu a získání přehledu o jejich provozu.
- (2) Informace o provozu a potenciálních zranitelnostech informačních systémů umožní zavádění preventivních opatření a předcházení případným bezpečnostním incidentům.
- (3) Zavedením systému úřad také získá schopnost detekce bezpečnostních incidentů a informace pro jejich rychlejší a efektivnější řešení.

- (4) Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly“) organizace.
- (5) Systém umožní provádění tzv. NBA (Network Behavioral Analysis), tj. automatického trvalého monitorování síťového provozu, stavu a činností sledovaných zařízení s cílem detekce (potenciálně) nebezpečného provozu, stavu či chování.
- (6) Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu.
- (7) Implementace systému bude provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

6.5 Specifické požadavky K3 – Správa identit

- (1) Cílem je zavedení správy interních a externích elektronických identit a souvisejících uživatelských účtů a oprávnění v aplikacích a automatizace řízení jejich životního cyklu.
- (2) Automatizace zajistí kontrolu nad tokem a využitím informací zpracovávaných v informačních systémech s cílem zamezit jejich neoprávněnému použití či zcizení.
- (3) Součástí systému pro správu identit bude detailní logování prováděných změn pro možnost zjištění uživatelských oprávnění v libovolném času v minulosti (od nasazení systému).
- (4) Systém pro správu identit bude čerpat data o uživateli (identitách) z personálního systému FLUX-PAM.
- (5) Systém pro správu identit bude integrován s klíčovými systémy MMKV a v těchto systémech bude spravovat uživatelské účty, jejich oprávnění a další parametry vázané na uživatele či jejich skupiny - zakládání e-mailových schránek.
- (6) Součástí dodávky bude i zajištění potřebné funkcionality včetně případné licence na straně integrovaných systémů.
- (7) Automatizací správy identit dojde k odstranění nebo alespoň významnému omezení rutinních činností správců systémů spojených se správou identit a dále ke zrychlení reakcí na změny v organizaci (např. změny oprávnění v systémech při změně pozice zaměstnance), snížení chybovosti způsobené ručním zadáváním údajů do systémů a/nebo nedodržením procesů (včasným nenahlášením odchodu zaměstnance všem správcům systémů nedojde včas nebo vůbec ke zrušení přístupových účtů zaměstnance) a získání okamžitého detailního přehledu o stavu identit a jejich oprávnění v systémech MMKV.
- (8) Implementace systému bude provedena v souladu s § 19 Nástroj pro řízení přístupových oprávnění Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

6.6 Specifické požadavky K4 – Školení kybernetické bezpečnosti

- (1) Náplní komodity je proškolení zaměstnanců MMKV a příspěvkových organizací (celkem cca. 600 zaměstnanců) na problematiku kybernetické bezpečnosti. Seznam příspěvkových organizací je k dispozici na <https://mmkv.cz/cs/prispevkove-organizace>.
- (2) Před zahájením školení proběhne test phishingu (podvodné a nebezpečné jednání, typicky škodlivý odkaz nebo příloha v emailu), na školení bude provedeno seznámení s výsledky a vysvětlení, jak se bránit phishingu, po cca 5-6 měsících bude provedeno opakované provedení obsahově odlišného testu a jeho vyhodnocení.
- (3) Kurz bude koncipovaný jako kombinace e-learningového vzdělávacího programu (webináře) a prezenčních workshopů.
- (4) Před zahájením školení bude obsah kurzu upraven dle specifické bezpečnostní politiky MMKV a bude nastaveno prostředí webináře.
- (5) Uchazeč zajistí provedení 10 prezenčních workshopů, každý bude v délce minimálně 4 výukových hodin, realizace bude po skupinách 60 osob. Každý účastník tak absolvuje e-learning v rozsahu minimálně 2 výukových hodin a dále prezenční workshop v rozsahu minimálně 4 výukových hodin, účastník tedy absolvuje celkem alespoň 6 výukových hodin. Workshopy budou probíhat v sídle zadavatele nebo jiných vhodných prostorách určených zadavatelem v lokalitě Karlovy Vary.

(6) Zadavatel si vyhrazuje možnost po dohodě s dodavatelem přizpůsobit skupiny účastníci se vzdělávání, tj. počet i složení účastníků, stanovit termíny jednotlivých aktivit.

(7) E-learningový webinář, jehož obsahem budou prezentované informace a bude zakončen povinným obecným bezpečnostním testem v rozsahu 20 otázek s možností volby mezi připravenými odpověďmi, bude dostupný na internetu po dobu minimálně 3 měsíců od prvního workshopu (očekává se průběžné skládání testů skupinami zaměstnanců, kteří budou absolvovat konkrétní běh školení). Každý zaměstnanec absolvuje školení formou webináře včetně závěrečného testu. Po 5-6 měsících budou muset zaměstnanci provést opakovaný test a případně pro připomenutí zopakovat webinář (bude přístupný po dobu 3 měsíců od opakovaného testu). Předpokládá se, že každý účastník bude absolvovat e-learningový webinář samostatně.

(8) Součástí plnění bude poskytnutí studijních materiálů pro prezenční workshopy. Obsah studijního materiálu bude odpovídat rozsahu vzdělávaného tématu. Studijní materiály budou obsahovat mimo jiné kontakt na odborné realizátory (lektory) vzdělávání tak, aby je v případě potřeby mohli účastníci kontaktovat i po skončení kurzu. Studijní materiály budou poskytnuty všem účastníkům vzdělávací aktivity v elektronické podobě. Současně budou studijní materiály poskytnuty v listinné podobě účastníkům, a to přímo na daném workshopu.

(9) Pro každý workshop (každé prezenční školení) zpracuje poskytovatel prezenční listinu, která bude vlastnoručně podepsána účastníky kurzu a lektorem/lektory. Všichni účastníci po absolvování vzdělávacího programu obdrží osvědčení o účasti. Poskytovatel zajistí rovněž fotodokumentaci aktivity, která bude prokazatelně evidovat, že aktivita proběhla — budou zaznamenáni lektori, účastníci workshopu, aktivity. Prezenční listiny z proběhlých aktivit budou zahrnovat: datum realizace aktivity, jméno a příjmení osob účastníků kurzů, název aktivity, místo poskytování aktivity a podpis účastníků a lektora/ů.

Součástí plnění je provedení evaluace - získání zpětné vazby ze strany účastníků školení, kteří se zúčastní se vzdělávacích aktivit. Průběh evaluace bude probíhat dle uvážení uchazeče, a to formou dotazníku ihned po ukončení dílčí části. Výstupy budou zadavateli dodány v elektronické podobě ve formátu MS Word/Excel nejpozději do 20 dnů od ukončení každé dílčí části.

Specifikace školení a metodika vzdělávání je uvedena v příloze č. 2 nabídky