Kraj V
KRAJ
Odbor
Žižkova

KUJIP01BV4JI

Kraj Vysočina

2695/19

SMLOUVA O DÍLO

uzavřená podle § 2586 a násl. zákona 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník")

mezi

I. Smluvní strany

Kraj Vysočina
se sídlem Žižkova 57, 587 33 Jihlava
zastoupený: MUDr. Jiřím Běhounkem, hejtmanem kraje
IČO: 70890749
bankovní spojení: Sberbank CZ, a.s. Jihlava
číslo účtu: 4050005000/6800
dále jen "Objednatel"

a

VISITECH a.s.
se sídlem: Košinova 655/59
zastoupení: Pavlem Kocourem, předsedou představenstva
IČO: 25543415
DIČ: CZ25543415
bankovní spojení: Raiffeisenbank a.s. účet č.: 1017756001/5500

dále jen " Dodavatel "

II. Účel Smlouvy

Účelem této smlouvy je analýza a nasazení systému pro řízení privilegovaných a systémových účtů v prostředí Krajského úřadu Kraje Vysočina (dále jen „kraje") (dále jen „dílo").

III. Předmět Smlouvy

Předmět této smlouvy je vymezen v příloze č. 1 a 2 této smlouvy.
Součástí předmětu díla je instalace, kompletní oživení systému a základní zaškolení obsluhy pro práci s dodávkou.

IV. Čas, místo a způsob plnění

1) Smluvní strany se dohodly, že dílo bude zahájeno po nabytí účinnosti této smlouvy a bude dokončeno takto:
   Fáze 1 – max. 3 měsíce od nabytí účinnosti této smlouvy.
   Fáze 2 – max. 3 měsíce od úspěšné akceptace fáze 1.
   Fáze 3 – max. 3 měsíce od pokynu Objednatele, nejpozději 24 měsíců od podpisu smlouvy; přičemž pokud Objednatel nevydá pokyn k zahájení fáze 3 do 24 měsíců od podpisu smlouvy, fáze 3 nebude realizována.

2) Místem plnění této Smlouvy (provedení a předání díla) jsou prostory Objednatele, pokud není dohodnuto jinak.

V. Cena za dílo

1) Celková cena, kterou se Objednatel zavazuje zaplatit za řádné splnění předmětu této

Smlouvy, činí 3 579 416,- Kč (slovy: tři milióny pět set sedmdesát devět tisíc čtyři sta šestnáct korun českých) bez DPH.

2) Cena za jednotlivé fáze je stanovena takto:
   Cena za fázi 1 činí 340 000,- Kč (slovy: tři sta čtyřicet tisíc korun českých) bez DPH
   Cena za fázi 2 činí 3 226 348,- Kč (slovy: tři milióny dvě sta dvacet šest tisíc tři sta čtyřicet osm korun českých) bez DPH
   Cena za fázi 3 činí 13 068,- Kč (slovy: třináct tisíc šedesát osm korun českých) bez DPH
3) K celkové ceně bude připočteno DPH v zákonné výši.

VI. Platební podmínky

1) Cena za dílo bude uhrazena po řádném předání a převzetí jednotlivých částí díla Objednatelem, a to na základě faktury vystavené Dodavatelem. Minimální lhůta splatnosti faktury je 30 dnů ode dne jejího doručení Objednateli.
2) Cena je stanovena jako nejvýše přípustná a jsou v ní zahrnuty veškeré náklady Dodavatele spojené s plněním povinností vyplývajících z této Smlouvy.
3) Účastníci sjednávají, že cena bude navýšena, a to v případě zvýšení zákonné sazby DPH v době od uzavření smlouvy do protokolárního předání příslušné části díla. Navýšení sjednané ceny musí odpovídat zvýšení hodnoty DPH v závislosti na zvýšení zákonné sazby DPH. Účastníci sjednávají, že cena díla bude snížena, a to v případě snížení zákonné sazby DPH v době od uzavření smlouvy do protokolárního předání příslušné části díla. Snížení sjednané ceny musí odpovídat snížení hodnoty DPH v závislosti na snížení zákonné sazby DPH. Smluvní strany se dohodly, že v případě zákonné změny sazby DPH nebudou uzavírat dodatek k této smlouvě, ale bude fakturovaná cena včetně zákonné sazby DPH.
4) Dodavatel na sebe převzal v souladu s ustanovením § 1765 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**") nebezpečí změny okolností, přičemž před uzavřením Smlouvy plně zvážil hospodářskou, ekonomickou i faktickou situaci a je si plně vědom okolností Smlouvy, jakož i okolností, které mohou po uzavření Smlouvy nastat. Tuto Smlouvu nelze měnit rozhodnutím soudu v jakékoliv její části.
5) Bankovní účet uvedený Dodavatelem na jím vystaveném daňovém dokladu za účelem úhrady kupní ceny musí odpovídat bankovnímu účtu zveřejněnému dle ustanovení § 98 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**zákon o DPH**") příslušným správcem daně způsobem umožňujícím dálkový přístup. V opačném případě je Zadavatel Dodavatelem vystavený daňový doklad Dodavateli vrátit.
6) Pokud se po dobu účinnosti této smlouvy Dodavatel stane nespolehlivým plátcem ve smyslu ustanovení § 106a zákona o DPH, smluvní strany se dohodly, že Zadavatel uhradí DPH za zdanitelné plnění přímo příslušnému správci daně. Zadavatelem takto provedená úhrada je považována za uhrazení příslušné části smluvní ceny rovnající se výši DPH fakturované Dodavatelem.
7) Daňový doklad Dodavatele musí být vystaven v souladu s požadavky právních předpisů na daňové doklady. Daňový doklad platí jako došlý v den, kdy byl v originále s přílohami prokazatelně doručen Zadavateli. Zadavatel je oprávněn vrátit daňový doklad do 14 kalendářních dnů od doručení s písemným odůvodněním, neodpovídá-li Smlouvě či obecně platným právním předpisům, nebo není-li možné jej zkontrolovat. Byl-li daňový doklad takto vrácen, není Zadavatel v prodlení s placením ceny. Lhůta splatnosti se počítá ode dne doručení opraveného daňového dokladu Zadavateli. Není-li daňový doklad ve lhůtě 14 kalendářních dnů vrácen, platí, že s ním Zadavatel souhlasí.

VII. Požadavky na součinnost

1) Dodavatel se zavazuje provést proces implementace řešení tak, aby nedošlo k ohrožení ani omezení provozu .....
2) Dodavatel se zavazuje provést proces implementace tak, aby nedošlo k ohrožení ani omezení provozu zdrojových aplikací a databází.
3) Dodavatel se zavazuje provést proces implementace v souladu s provozním řádem

Technologického centra kraje.

4) Dodavatel je povinen plnit Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kraje Vysočina uvedené v příloze č. 3 této smlouvy.
5) Objednatel se zavazuje poskytnout Dodavateli nezbytnou součinnost spočívající v:
    a. Přístupu do lokalit potřebných pro implementaci a realizaci požadavků objednatele.
    b. Poskytnutí veškerých informací potřebných pro implementaci a následné řešení požadavků objednatele.
    c. Vyplnění use-casu hesel a jejich správy
    d. Zajištění integrace a neodkladné spolupráce třetích stran nezbytných pro realizaci implementace a splnění požadavků objednatele na funkčnost systému.

VIII. Ochrana nehmotných statků, důvěrnost a ochrana informací

1) Tento článek smlouvy se uplatní tehdy, jestliže součástí díla bude nehmotný statek, jenž je předmětem úpravy zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Dodavatel touto smlouvou poskytuje objednateli právo na jakékoliv v současnosti známé využití, zejména další zpracování a úpravu díla, jakož i nehmotných statků, které jsou v tomto díle zpracovány, včetně práva objednatele udělit dalším osobám podlicenci k využití díla včetně nehmotných statků v tomto dokumentu zpracovaných.
2) Dodavatel udílí objednateli nevýhradní licenci k užití díla.
3) Objednatel je oprávněn dílo užít všemi způsoby. Za tímto účelem je objednatel oprávněn dílo dále zpracovávat a upravovat.
4) Objednatel je oprávněn udělit podlicenci k užití díla. Objednatel je oprávněn zejména udělit bezúplatnou podlicenci k užití díla V případě, že o udělení podlicence bude požádáno v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, bude podlicence poskytnuta za jednorázovou úplatu ve výši 10 000 000 Kč.
5) Odměna za užití nehmotného statku je již zahrnuta do ceny za dílo.
6) Licence je poskytnuta na dobu trvání majetkových práv k dílu.
7) Objednatel není povinen licenci využít.
8) Vzhledem k veřejnoprávnímu charakteru Objednatele Dodavatel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zák. č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Smluvní strany se zavazují, že obchodní a technické informace, které jim byly svěřeny druhou stranou, nezpřístupní třetím osobám bez písemného souhlasu druhé strany a nepoužijí tyto informace k jiným účelům, než je k plnění podmínek této smlouvy.

IX. Bezpečnost informací

1) Dodavatel je povinen dodržovat platnou legislativu ČR i EU, která se týká bezpečnosti informací.
2) Dodavatel se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kraje Vysočina uvedené v příloze č. 2 této smlouvy.
3) Dodavatel je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto smlouvou ve stejné míře u všech případných subdodavatelů či jiných osob, které mají přístup k informačním aktivům Kraje Vysočina prostřednictvím dodavatele.
4) Dodavatel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které mu byly v souvislosti s touto smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi zhotovitel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění zhotovitele veřejně přístupnými stanou (dále jen „důvěrné informace"). Zhotovitel nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo

třetích osob a nesmí je použít ani v neprospěch objednatele. Povinnosti dle tohoto odstavce je zhotovitel povinen zachovávat i po zániku této smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění zhotovitele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je zhotovitel povinen zveřejnit důvěrnou informaci na základě povinnosti uložené zhotoviteli právním předpisem nebo rozhodnutím orgánu veřejné moci.

5) Za nesplnění kterékoliv povinnosti obsažené v tomto článku, je objednatel oprávněn účtovat zhotoviteli smluvní pokutu ve výši 100 000 Kč, a to za každé jednotlivé porušení povinností obsažených v tomto článku.

X. Předání a akceptace

1) Předání a akceptace plnění proběhne podpisem příslušného předávacího nebo akceptačního protokolu vedoucími projektu Objednatele a Dodavatele. Podrobný popis akceptace je uveden v příloze č. 1 této smlouvy.
2) V případě, že plnění popř. část plnění vykazuje drobné vady, které nebrání užití této části plnění, je toto plnění převzato s výhradou a součástí akceptačního protokolu je i termín odstranění těchto vad.
3) Jestliže předané plnění popř. části plnění vykazují větší množství vad je akceptační řízení ukončeno s neúspěšným výsledkem a plnění/části plnění je vráceno Dodavateli k dopracování. Dodavatel je v prodlení do odstranění těchto vad nebo jejich snížení pod hranici většího množství vad, kdy je plnění akceptováno nebo akceptováno s výhradou dle odst. 3) tohoto článku Smlouvy.
4) Za větší množství vad (podstatné porušení smlouvy) je považováno – jedna (1) nebo více Vad kategorie A, nebo tři (3) nebo více Vad kategorie B, nebo dvacet (20) nebo více Vad kategorie C.
5) Vada kategorie A je vada znemožňující užívání klíčové části díla, bez možnosti náhradního postupu, tj. způsobují "zamrznutí", "zhroucení" celého systému nebo způsobuje nenávratnou ztrátu nebo porušení dat během běžného užívání a zároveň neexistuje postup pro náhradní řešení problému, přičemž vadu není možné odstranit užitím běžných postupů v kompetenci správce systému.
6) Vada kategorie B je vada způsobující provozní problémy omezující užívání plnění/části plnění; tj. způsobuje významné problémy při používání, a není překonatelná dočasným náhradním postupem.
7) Vada kategorie C je překonatelná dočasným náhradním postupem, nebo dočasným nevyužíváním příslušné funkcionality, bez toho, aby byly ohroženy procesy klíčové pro činnost Objednatele.

XI. Záruka za vady

1) Dodavatel se zavazuje, že předmět plnění bude odpovídat specifikaci uvedené v technické dokumentaci a dalších relevantních dokumentech vzniklých v rámci plnění dle této Smlouvy.
2) Dodavatel poskytuje na funkčnost a kvalitu dodaného díla záruku v trvání 60ti měsíců ode dne převzetí díla Objednatelem.

XII. Smluvní pokuty a sankce

1) Dodavatel je povinen uhradit smluvní pokutu ve výši 0,5 % z celkové ceny díla za každý započatý den prodlení s plněním stanovených termínů pro realizaci kterékoliv části díla. Zaplacením smluvní pokuty není dotčen nárok na náhradu škody.
2) V případě neodstranitelných vad vzniklých v průběhu plnění předmětu této Smlouvy, které brání řádnému užívání díla, je Dodavatel povinen uhradit smluvní pokutu ve výši 5% Kč

z celkové ceny díla. Zaplacením smluvní pokuty není dotčen nárok na náhradu škody, ani nárok na odstoupení od Smlouvy ze strany Objednatele.

3) V případě prodlení Objednatele se zaplacením faktury vystavené Dodavatelem je prodávající oprávněn účtovat kupujícímu úrok z prodlení ve výši 0,05% z nezaplacené částky, a to za každý i započatý den.

XIII. Platnost a trvání Smlouvy

1) V případě závažného porušení povinností Dodavatelem může Objednatel odstoupit od Smlouvy okamžitě. Závažným porušením Smlouvy se považuje neplnění termínu předání a nesplnění požadovaných vlastností hotového díla nebo jeho částí.
2) Obě smluvní strany jsou oprávněny odstoupit od Smlouvy v případě podstatného porušení Smlouvy druhou smluvní stranou. Podmínky odstoupení od Smlouvy se řídí ustanoveními občanského zákoníku. O záměru odstoupit od Smlouvy z důvodu podstatného porušení Smlouvy druhou smluvní stranou je ta smluvní strana, která chce odstoupit od Smlouvy povinna písemně upozornit druhou smluvní stranu 15 kalendářních dní předem a vyzvat jí k nápravě zjištěného porušení Smlouvy, s poskytnutím přiměřené lhůty. V případě, že druhá smluvní strana řádně napraví zjištěné porušení Smlouvy v poskytnutém termínu, pomíjí důvod pro odstoupení od Smlouvy dle čl. XII odst. 3 této Smlouvy.
3) Objednatel má právo vypovědět tuto smlouvu v případě, že v souvislosti s plněním účelu této smlouvy dojde ke spáchání trestného činu. Výpovědní doba činí 3 dny a začíná běžet dnem následujícím po dni, kdy bylo písemné vyhotovení výpovědi doručeno dodavateli.

XIV. Závěrečná ustanovení

1) Veškeré právní vztahy založené, resp. vyplývající z této Smlouvy, které zde nejsou výslovně upravené, včetně eventuálních řešení vzájemných sporů, se řídí ustanoveními příslušných právních předpisů České republiky.
2) Vzhledem k veřejnoprávnímu charakteru Objednatele Dodavatel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním této smlouvy v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Dodavatel prohlašuje, že výslovně souhlasí se zveřejněním celého textu smlouvy včetně podpisů v informačním systému veřejné správy - Registru smluv. Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 zákona o registru smluv splní Objednatel. Současně bere Dodavatel na vědomí, že v případě nesplnění zákonné povinnosti je smlouva do tří měsíců od jejího podpisu bez dalšího zrušena od samého počátku.
3) Tato Smlouva může být měněna pouze formou písemných očíslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran (tj. pouze statutárními zástupci podle jejich oprávnění vyplývajícího z obchodního rejstříku nebo osobami, které jsou uvedeny v záhlaví Smlouvy). Smluvní strany výslovně sjednávají, že e-mail nebo jiná obdobná forma elektronické komunikace se nepovažují za písemný dodatek k této Smlouvě dle tohoto ustanovení.
4) Situace neupravené touto Smlouvou se řídí občanským zákoníkem, a dalšími obecně závaznými právními předpisy České republiky.
5) Vůle smluvních stran je vyjádřena též v dále uvedených dokumentech a podkladech, které tvoří nedílnou součást této Smlouvy: Příloha č. 1 – Specifikace předmětu plnění, příloha č. 2 Oblasti provozní dokumentace a Příloha č. 3 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kraje Vysočina.

V Jihlavě dne 4.5.2019

Objednatel

.....

MUDr. Jiří Běhounek
hejtman kraje

V Brně dne 18.4.2019

Dodavatel

VISITECH a.s.
Košinova 59, 612 00 Brno
DIČ: CZ25543415

.....

Pavel Kocour
Předseda představenstva

Kraj Vysočina
Žižkova 57, 587 33 Jihlava

Příloha č. 1
Technická specifikace

Předmětem veřejné zakázky je analýza a nasazení systému pro řízení privilegovaných a systémových účtů v prostředí Krajského úřadu Kraje Vysočina (dále jen kraje). Systém bude sloužit k řízení, správě, monitoringu a zabezpečení privilegovaných a systémových účtů na platformách MS Windows a FreeBSD/Linux v níže uvedených verzích:

- Windows
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - MS SQL Server 2008 R2
  - MS SQL Server 2014
  - MS SQL Server 2016
- FreeBSD/Linux (vždy v aktuálních stabilních verzích popř. LTS)
  - GNU/Linux v různých distribucích (Debian, CentOS, RedHat, Ubuntu, apod.)
  - FreeBSD

Dílo bude realizováno v těchto fázích:

- Fáze 1. – Předimplementační analýza, PoC
- Fáze 2. – Implentace a dodávka licencí pro interní uživatele
- Fáze 3. – Implentace a dodávka licencí pro externí uživatele

Implementace systému a postup realizace veřejné zakázky musí být naplněn následujícím způsobem:

- **Fáze 1.**
  - Provedení před-implementační analýzy - analýza stávajícího prostředí kraje, detailní návrh postupu – harmonogram, požadavky na součinnost na straně kraje, návrh architektury řešení
  - implementace systému v režimu tzv. proof-of-concept, což znamená instalace a konfigurace všech potřebných komponent do stavu, ve kterém bude možné provést základní PoC akceptační testy. Všechny komponenty musí být instalovány do virtuálního prostředí na platformě VMware.
  - Zadavatel si vyhrazuje právo odstoupit od realizace zakázky v případě, že v první fázi implementace systému nebudou naplněny základní PoC akceptační testy. Zadavatel se v tomto případě zavazuje uhradit dodavateli náklady na realizaci implementace systému v režimu proof-of-concept, přičemž výše těchto nákladů musí být v rámci nabídky vyčíslena odděleně od celkové částky za realizaci zakázky.
- **Fáze 2.**
  - K této fázi může dojít až po úspěšném splnění všech základních PoC akceptačních testů a potvrzení zadavatele v pokračování implementace sytému.
  - Dokončení implementace systému v plném režimu, což znamená instalace a konfigurace všech potřebných komponent do stavu, ve kterém bude možné provést doplňující akceptační testy. Všechny komponenty musí být instalovány do virtuálního prostředí na platformě VMware a v režimu vysoké dostupnosti.
  - K této fázi implementace se váže dodávka první sady licencí, jak je uvedeno v požadavcích na licencování systému.
  - Školení uživatelů systému
  - Školení administrátorů systému
  - Zpracování dokumentace finálního vyhotovení, která musí minimálně obsahovat oblasti uvedené v příloze č. 2 smlouvy
- **Fáze 3.**
  - Dodávka a implementace druhé sady licencí, jak je uvedeno v požadavcích na licencování systému.

Požadavky na systém:

- Licencování systému:
  - Dodávka licencí systému bude probíhat ve dvou krocích – kroky dodávka licencí odpovídají 2. a 3. fázi implementace systému:
    - Ve fázi 2. se zadavatel zavazuje odebrat první sadu licencí systému, které pokrývají rozsah 20 interních uživatelů (administrátorů ICT) a 400 koncových systémů (serverů či jiných podporovaných zařízení).

        - Ve fázi 3. si zadavatel vyhrazuje právo odebrat (i neodebrat) licence pro dalších 60 externích uživatelů (administrátorů ICT ze stran dodavatelů koncových systémů) a to nejpozději do dvou let od podpisu smlouvy.
    - Licence nesmí omezovat počet řízených účtů na straně serverů či počet naplánovaných úloh/jobů/skripů/služeb apod.
    - V rámci veřejné zakázky je však soutěžena celková cena systému, která pokrývá oba kroky licencování, tedy takový rozsah, aby byl systém použitelný pro 20 interních uživatelů (administrátorů ICT), 60 externích uživatelů (administrátorů ICT ze stran dodavatelů koncových systémů) a 400 koncových systémů (serverů či jiných podporovaných zařízení).
- Systém musí umožnit ukládání a přenos autentizačních prostředků (hesel, klíčů) ve vlastní bezpečné komponentě (tzv. trezor hesel). Bezpečnost komponenty musí být založeny na vícefázové autentizaci a na silných kryptografických protokolech, algoritmech a klíčích:
    - Symetrická šifra AES s délkou klíče minimálně 256 bitů
    - Asymetrická šifra RSA s délkou klíče alespoň 2048 bitů nebo šifrování nad eliptickými křivkami s délkou klíče minimálně 256 bitů
    - HTTPS protokol pro publikování webového klienta
    - Pokud budou použity hash funkce, tak musí splňovat tyto parametry:
        - Pro ukládání hesel musí být použity tzv. pomalé hashovací funkce (bcrypt, Argon2, scrypt nebo PBKDF2)
        - Pro ostatní použití (např. kontrolní součty) musí být použity hashe z rodiny SHA-2.
    - Bezpečnost systému musí být v souladu se standardem FIPS 140-2 alespoň v úrovni jedna.
- Systém musí umožnit pracovat administrátorům ICT pod jednou identitou a té na základě definovaných politik zpřístupňovat koncové systémy (Windows a FreeBSD/Linux servery) pod definovanými lokálními nebo doménovými privilegovanými účty a tím pádem zabránit administrátorům ICT přímému přístupu k autentizačním prostředkům účtů na koncových systémech.
- Systém musí umožnit připojení k cílovým systémům prostřednictvím minimálně těchto protokolů a způsobů: RDP, SSH, HTTPS, připojení přes terminálový server s restrikcí pouze na vybranou klientskou aplikaci (např. terminálové spuštění aplikace Microsoft SQL Server Management Studio)
- Systém musí poskytovat jednoduché uživatelské rozhraní pro snadný přístup administrátora ICT k cílovým systémům. Vedle webové konzole musí systém nabízet tyto možnosti:
    - vygenerovat RDP soubor s předkonfigurovaným connection stringem na cílový systém
    - integrace na běžně dostupné RDP session manažery (minimálně Remote Desktop Connection Manager)
    - integrace na běžně dostupné SSH session manažery/klienty (minimálně PuTTY)
- Systém musí umožnit silné ověření ICT administrátora pomocí vícefázové autentizace nejen ke koncovému systému, ale i k systému samotnému (PAM) - tedy jména a hesla ve spojení s druhou metodou ověření, která je založená na vlastnictví klíče na čipové kartě či tokenu nebo mobilní telefonu (nikoliv však telefonního čísla, ideálně mobilní aplikace). Druhá metoda ověření musí být volitelná v závislosti na typu administrátora ICT (interní zaměstnanec vs. dodavatel) a systém musí umožnit kombinaci těchto druhých metod.
- Autentizace pomocí jména a hesla musí být systémem provedena vůči Active Directory.
- Systém musí umožnit nahrávání činností ICT administrátorů v závislosti na použitém protokolu připojení k cílovému systému – např. při použití RDP bude zaznamenávat komprimovaná videa či obrázky dané relace, při použití SSH protokolu bude zaznamenávat příkazy odeslané přes příkazovou řádku. Způsob zaznamenávání musí umožnit:
    - indexaci záznamů
    - fulltextové vyhledávání v záznamech (např. vyhledání použitého příkazu).
    - nastavení retenčních pravidel pro uchování a archivaci záznamů
- Systém musí umožnit automatizovanou správu privilegovaných účtů na koncových systémech (serverech) jak lokálních (Windows i FreeBSD/Linux), tak doménových (Active Directory).
- Definování politik
    - Systém musí umožnit granulární definování politik minimálně tímto způsobem:
        - Politiky přístupů ke koncovým systémům
            - Pravidla definující matici cílových systémů, cílových uživatelů a přístupových metod pro konkrétní uživatele či skupiny uživatelů systému
            - Pravidla pro zaznamenání činností uživatelů či skupin uživatelů
        - Politiky správy hesel a jiných autentizačních prostředků

                - Pravidla pro tvorbu a kvalitu (komplexitu) hesel či kryptografických klíčů
                - Pravidla pro jejich rotaci - v naplánovaných intervalech, na základě události (např. přihlášení uživatele ke koncovému systému nebo zobrazení hesla z trezoru)
            - Politiky zobrazování hesel a jiných autentizačních prostředků
                - Pravidla určovaná na základě uživatele, skupin uživatelů, času, koncového systému
                - Pravidla vynucení akce před zobrazení hesla, např. opětovná autentizace uživatele, a po zobrazení hesla poslání e-mailové notifikace, zaznamenání zobrazení hesla, změna hesla, apod.
        - Politiky musí umožňovat definování pravidel jak na uživatele, tak na skupinu uživatelů
- Systém musí umožnit automatizovanou správu systémových účtů, které slouží pro běh naplánovaných úloh, jobů, skriptů, služeb, apod. Automatizovanou správou těchto účtů se mimo jiné rozumí i automatická rotace hesel dle definovaných pravidel a politik na straně kraje včetně automatického zajištění spuštění služby s novým/aktuálně platným heslem.
- Systém musí umožňovat definovat různá přístupová oprávnění k samotnému systému na základě minimálně těchto rolí, které bude možné kombinovat:
    - Správce systému – správa systému
    - Správce politik – definice a editace politik
    - Auditor – R/O přístup k definovaným politikám a logům o činnosti systému a uživatelů
    - Uživatel – přístup k heslům a koncovým systémům dle definovaných politik
- Logování
    - Systém musí umožnit logování činností minimálně v tomto rozsahu:
        - Přihlášení a odhlášení všech uživatelů včetně neúspěšných pokusů – jak do systému pro správu přístupů, tak do koncových systémů
        - Činnosti provedené administrátory systému
            - přidělení/odebrání/reset oprávnění
            - založení/smazání/ uživatele či přidělení/odebrání role
            - vytvoření/změna/smazání politiky
            - změna způsobu logování
            - neprovedení operací v důsledku nedostatečných oprávnění
            - změna hesel
        - Činnosti provedené uživateli systému
            - Zobrazení hesel
            - Nahrávání činností ICT administrátorů (uživatelů systému) na koncových zařízeních – požadavky zmíněny výše v této dokumentaci.
    - zaznamenané události musí obsahovat minimálně tyto informace:
        - přesný datum a čas vzniku události (zdrojem je systém)
        - název aplikace/modulu, kterého se událost týká
        - typ události
        - původce události (uživatel + IP adresa)
        - úspěch/neúspěch události
    - Systém musí umožnit zasílat logy do monitorovacího nástroje SIEM (protokolem syslog, syslog over TLS případně jiným standardním způsobem)
    - Systém musí umožnit synchronizaci systémového času s NTP objednatelem definovaným NTP serverem

Základní PoC akceptační testy první fáze:

- Pokud je v akceptačních testech zmíněna dvoufázová autentizace, přičemž v druhé fázi autentizace musí být použit klíč uložený na čipové kartě, musí být pro akceptační test použit stávající autentizační prostředek administrátora ICT zadavatele, tedy stávající klíč vydaný certifikační autoritou I.CA na stávajících kartách (Starcos 3.5, certifikáty TWINS).
- Úspěšné automatické založení jednoho uživatele systému (administrátora ICT) Úspěšné přihlášení vybraného interního administrátora ICT k jednomu Windows serveru pomocí protokolu RDP včetně dvoufázového ověření prostřednictvím jména a hesla vůči Active Directory (1. fáze autentizace) a klíče uloženého na čipové kartě (2. fáze autentizace). RDP spojení musí být v tomto případě navázáno z prostředí RDP session managera, který je nainstalován na pracovní stanici.
- Úspěšné přihlášení jednoho vybraného interního administrátora ICT k jednomu FreeBSD/Linux serveru pomocí protokolu SSH včetně dvoufázového ověření prostřednictvím jména a hesla vůči Active Directory (1. fáze autentizace) a klíče uloženého na čipové kartě (2. fáze autentizace). SSH spojení musí být v tomto případě navázáno z prostředí SSH session managera, který je nainstalován na pracovní stanici.

- Úspěšné přihlášení jednoho vybraného interního administrátora ICT k jednomu FreeBSD/Linux serveru pomocí protokolu SSH včetně dvoufázového ověření prostřednictvím jména a hesla vůči Active Directory (1. fáze autentizace) a klíče uloženého na čipové kartě (2. fáze autentizace). Autentizace mezi systémem a serverem musí proběhnout pomocí SSH klíčů (např. RSA).
- Úspěšné přihlášení jednoho vybraného externího administrátora ICT k vybranému Windows serveru a FreeBSD/Linux serveru pomocí odpovídajících protokolů (RDP a SSH) včetně dvoufázového ověření prostřednictvím jména a hesla vůči Active Directory jako 1. fáze autentizace (vůči jiné doméně než v předchozích případech) a mobilní aplikace jako 2. fáze autentizace.
- Úspěšné zaznamenání/nahrání činností čtyř administrátorů připojených k Windows serveru a FreeBSD/Linux serveru prostřednictvím RDP, SSH, terminálového připojení a webové konzole.
- Úspěšné zaindexování záznamů a vyhledání vybraných činností administrátorů v záznamu činností dle následujících scénářů:
  - Vyhledání všech činností (celého záznamu) podle jména administrátora
  - Vyhledání všech činností podle jména administrátora a definovaného rozmezí času
  - Vyhledání všech činností všech administrátorů dle zadaného příkazu na koncovém serveru
- Úspěšné připojení jednoho vybraného uživatele k MS SQL Serveru prostřednictvím terminálového připojení a aplikace MS SQL Server Management Studio včetně dvoufázového ověření prostřednictvím jména a hesla vůči Active Directory (1. fáze autentizace) a klíče uloženého na čipové kartě (2. fáze autentizace). Součástí tohoto testu musí být i úspěšná demonstrace zavedené restrikce na spuštění pouze MS SQL Server Management Studio aplikace na terminálovém serveru (tzn., že takto přihlášený uživatel nesmí být schopen na terminálovém serveru spustit jinou než povolenou aplikaci).
- Změna hesla jednoho lokálního administrátora, který bude definován na vybraném Windows serveru prostřednictvím systému pro řízení privilegovaných účtů.
- Změna hesla jednoho lokálního uživatele, který bude definován na vybraném FreeBSD/Linux serveru prostřednictvím systému pro řízení privilegovaných účtů.
- Změna hesla jednoho vybraného účtu určeného pro administraci serveru, který bude definován v Active Directory, po přihlášení interního administrátora ICT ke koncovému systému prostřednictvím systému pro řízení privilegovaných účtů.
- Změna hesla jednoho vybraného doménového systémového účtu sloužícího pro běh naplánované úlohy Windows prostřednictvím systému pro řízení účtů v PAM. Změna hesla nesmí mít vliv na běh naplánované úlohy Windows, která je na daném systémovém účtu závislá, automaticky musí dojít k předání hesla dané úloze, aby byl zajištěn její chod.
- Úspěšné předvedení tzv. „life session", tedy on-line sledování všech činností přihlášeného administrátora.
- Úspěšné předvedení funkcionality zadání důvodu přístupu k serveru u 1 interního a 1 externího administrátora ICT.

Doplňující akceptační testy (pro druhou fázi implementace):

- Pokud je v akceptačních testech zmíněna dvoufázová autentizace, přičemž v druhé fázi autentizace musí být použit klíč uložený na čipové kartě, musí být pro akceptační test použit stávající autentizační prostředek administrátora ICT zadavatele, tedy stávající klíč vydaný certifikační autoritou I.CA na stávajících kartách.
- Úspěšné založení zbývajících devatenácti uživatelů systému (administrátorů ICT)
- Test vysoké dostupnosti – provedení odstávky a update/upgrade jedné instance systému bez odstávky řešení jako celku.
- Úspěšné přihlášení všech interních uživatelů systému (administrátorů ICT) do systému prostřednictvím dvoufázového ověření – 1. fáze jméno a heslo ověřené vůči AD, 2. fáze přes privátní klíč uložený na čipové kartě (PKI).
- Úspěšné přihlášení vybraného interního administrátora ICT k pěti Windows serverům prostřednictvím třech různých účtů a pomocí protokolu RDP včetně dvoufázového ověření prostřednictvím jména a hesla vůči Active Directory (1. fáze autentizace) a klíče uloženého na čipové kartě (2. fáze autentizace). RDP session musí být otevřena jak kliknutím ve webovém rozhraní systému, tak pomocí session/connection managera či prostřednictvím uloženého RDP souboru.
- Úspěšné přihlášení jednoho vybraného interního administrátora ICT k pěti FreeBSD/Linux serverům pomocí protokolu SSH včetně dvoufázového ověření prostřednictvím jména a hesla vůči Active Directory (1. fáze autentizace) a klíče uloženého na čipové kartě (2. fáze autentizace). SSH session musí být otevřena jak kliknutím ve webovém rozhraní systému tak pomocí aplikace PuTTY z prostředí MS Windows.

- Úspěšné zaznamenání/nahrání činností čtyř administrátorů připojených k Windows serveru a FreeBSD/Linux serveru prostřednictvím RDP, SSH, terminálového připojení a webové konzole.
- Úspěšné zaindexování záznamů a vyhledání vybraných činností administrátorů v záznamu činností dle následujících scénářů:
    - Vyhledání všech činností (celého záznamu) podle jména administrátora
    - Vyhledání všech činností podle jména administrátora a definovaného rozmezí času
    - Vyhledání všech činností všech administrátorů dle zadaného příkazu na koncovém serveru bez ohledu na platformu (Windows nebo FreeBSD/Linux)
- Úspěšné připojení jednoho vybraného uživatele k MS SQL Serveru prostřednictvím terminálového připojení a aplikace MS SQL Server Management Studio včetně dvoufázového ověření prostřednictvím jména a hesla vůči Active Directory (1. fáze autentizace) a klíče uloženého na čipové kartě (2. fáze autentizace). Součástí tohoto testu musí být i úspěšná demonstrace zavedené restrikce na spuštění pouze MS SQL Server Management Studio aplikace na terminálovém serveru (tzn., že takto přihlášený uživatel nesmí být schopen na terminálovém serveru spustit jinou než povolenou aplikaci).
- Změna hesla jednoho lokálního administrátora, který bude definován na pěti vybraných Windows serverech prostřednictvím systému pro řízení privilegovaných účtů na základě:
    - Časových kritérií – v daný čas a periodicky každých X hodin
    - Akce provedené uživatelem – vyzvednutí hesla v trezoru a přihlášení na koncový systém pod definovaným uživatelem
- Změna hesla jednoho lokálního uživatele, který bude definován na pěti vybraných FreeBSD/Linux serverech prostřednictvím systému pro řízení privilegovaných účtů na základě:
    - Časových kritérií – v daný čas a periodicky každých X hodin
    - Akce provedené uživatelem – vyzvednutí hesla v trezoru a přihlášení na koncový systém pod definovaným uživatelem
- Změna hesla jednoho vybraného doménového systémového účtu sloužícího pro běh naplánované úlohy Windows prostřednictvím systému pro řízení privilegovaných účtů. Změna hesla nesmí mít vliv na běh naplánované úlohy Windows, která je na daném systémovém účtu závislá, automaticky musí dojít k předání hesla dané úloze, aby byl zajištěn její chod.

Příloha č. 2 - Oblasti provozní dokumentace

Cílem zpracování této dokumentace je popsat a zdokumentovat provozní postupy pro zajištění správného, bezchybného a bezpečného provozování vybavení pro zpracování informací.
Oblasti:

Instalace systému

Cíl dokumentu: popsat a zdokumentovat postupy, kroky a činnosti vedoucí k instalaci informačního systému/aktiva.

- Forma dokumentu: textová, může být doplněno o návodné obrázky.
- Systémové požadavky (architektura procesoru, verze operačního systému, minimální požadavky na výkon HW, apod.)
- Instalační média (CD, síť, soubor, ...) a cesta k nim
- Konkrétní kroky vedoucí k instalaci systému, způsob instalace serverové části, způsob instalace klientské části, apod.

Konfigurace systému

Cíl dokumentu: popsat a zdokumentovat podrobnou konfiguraci (jak proces, tak stav) systému.

- Forma dokumentu: textový popis (může být i např. formou okomentovaného config souboru)
- konfigurace sítě (nastavení IPv4, IPv6), konfigurace FW pravidel, apod.
- Nastavení připojení/komunikace na další systémy (např. DB, web server, AD,...), nastavení portů na kterých služba naslouchá, kam data odesílá, ...
- Spuštění potřebných modulů, registrování knihoven, úprava registrů OS Windows, ...
- Nastavení automatických úloh, nastavení systémových účtů, ...

Způsob zpracování informací

Cíl dokumentu: popsat, jakým způsobem jsou zpracovávány informace v rámci informačního systému + případně v rámci ostatních systémů, na které je daný IS navázán.

- Forma dokumentu: textový popisu nebo i schéma
- Vytváření dat (datové vstupy)
  - manuálně|strojově|automaticky|uživatelsky
  - kdy jsou data vytvářena? (např. nějaká událost, naplánovaná událost, apod.)
  - ...
- Přenosy dat
  - Odkud kam (např. agent>master, do jiných systémů, mezi moduly, apod.)?
  - Jakým protokolem?
- Uložení dat
  - Databáze (typ?)
  - File (typ?)
  - ...
- Výstupy systému (dat)
  - User Interface (webový formulář, GUI aplikace, konzole, ...)
  - E-mail|sms|voice call
  - Soubor (formáty)?
  - Tisk
  - Datová pumpa
  - Do jiných systémů

Způsob zálohování a četnost

Cíl dokumentu: popsat a zdokumentovat, jakým způsobem, kdy, kam a jak často jsou zálohována data v rámci daného informačního systému.

- Forma: může být i formou zálohovacího plánu (backup schedule), textový popis
- Způsob zálohování – plná, přírůstková, rozdílová záloha
- Kdy a jak často je záloha prováděna
- Jak dlouhou dobu jsou zálohy uloženy a kde
- Jak často se provádí testování záloh

Postupy řešení problémů

Cíl dokumentu: popsat, jakým způsobem se řeší případ nějakého problému, typicky nefunkčnost systému.

- Základ dokumentace: kontakty (e-mailové adresy, telefonní čísla, url helpdesku)
- V jakém případě, koho a prostřednictvím čeho (e-mailu, helpdesku, sms, telefonu) kontaktovat

Vazby na jiné systémy

Cíl dokumentu: popsat, jakým způsobem je daný systém navázán na jaké systémy.

- Forma: nejlépe schéma s popisem, může být ale i textový popis
- Výčet (stálých) systémů, na jaké je daný systém navázán (DB, aplikační servery, fileservery, UI, pracovní stanice, zdroje informací /vstupy/, výstupy, datové pumpy, jiné IS, apod.)
- Protokoly (příp. rozhraní) připojení na jiné systémy
- Porty, ip adresy

Postupy pro restart a obnovu

Cíl dokumentu: popsat a zdokumentovat postupy a konkrétní kroky, které povedou k bezpečnému restartu systému či obnově systému po jeho selhání nebo obnově.

- Forma dokumentu: textový popis (může být doplněn o obrázkové návody)
- Posloupnost kroků (co a jak udělat), které je třeba provést pro bezpečné restartování systému
  - Např. informování uživatelů, ověření odhlášení všech uživatelů, provedení zálohy systému, restart systému, základní kontrola funkčnosti, informování uživatelů
- Posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému po jeho selhání do jeho plně funkčního stavu
  - Typicky obnova ze zálohy
  - Disaster Recovery, havarijní plán obnovy systému

Monitoring

Cíl dokumentu: popsat a zdokumentovat jaké události jsou monitorovány.

- Výčet událostí, které jsou logovány (př. přihlášení/odhlášení uživatele, provozní/chybové stavy, přidělení/odebrání oprávnění, ...)
- Uložení zalogovaných událostí
  - Kde – soubor, databáze, vzdálený server
  - Jak dlouho
- Protokol logování (např. syslog, snmp, prtg, ...)

Základní uživatelská příručka

Cíl dokumentu: vytvořit základní návod pro ovládání uživatelského rozhraní systému pro běžného uživatele. Zjednodušit běžnému uživateli základní orientaci v uživatelském rozhraní systému.

- Forma dokumentu: textový popis, textový popis doplněný o obrázky
- Popis provedení základních/běžných/rutinních funkcí, kroků a postupů, které uživatel může provádět

Základní administrátorská příručka

Cíl dokumentu: vytvořit základní návod pro ovládání administračního rozhraní systému pro administrátora. Zjednodušit privilegovanému uživateli základní orientaci v administračním rozhraní systému.

- Forma dokumentu: textový popis, textový popis doplněný o obrázky
- Popis provedení standardních (základních/běžných/rutinních) operací, které vedou k běžné administraci systému
- Popis provedení nestandardních (málo běžných) operací, pokud je třeba

Popis klíčových komponent

Cíl dokumentu: popsat a zdokumentovat účel, význam, úlohu a způsob použití klíčových komponent systému

- Forma dokumentu: textový popis (může být doplněno i o schéma)
- Základní fungování, účel, úloha jednotlivých klíčových komponent + jakou platformou (softwarem) jsou jednotlivé komponenty zajištěny
  - Např. master(server), agent(klient), různé typy použitých serverů, moduly, zdroje informací, příjemci informací (systémy), apod.

Popis vzájemných datových vztahů

Cíl dokumentu: popsat a zdokumentovat datové vztahy mezi daným IS a jinými systémy, případně v rámci „modulární" architektury daného IS.

- Forma dokumentu: textový popis nebo schéma s popisem
- Forma a struktura dat, obecný popis dat
- způsob přenášení dat (použité protokoly), toky dat z a do kterých systémů
- naplánované úlohy přenosu dat (např. datové pumpy), apod.

Back-out plán

Cíl dokumentu: popsat a zdokumentovat posloupnost základních kroků, které vedou k obnově systému do posledního funkčního stavu.

- Forma dokumentu: textový popis, může být součástí dokumentace **Postupy pro restart a obnovu**
- Typicky postup obnovení systému a dat ze zálohy

Technický popis funkcionality

Cíl dokumentu: v případě, že je systém velmi složitý nebo jeho fungování není obecně známé (např. proprietární sw), by měl dokument popsat a zdokumentovat technickou funkcionalitu daného systému. Dokument bude obsahovat spíše specifika, která nebudou obsažena ve výše uvedených dokumentech.

- Forma: textový popis nebo schéma s popisem
- Popis základní architektury systému, popis komponent, použité komunikační protokoly, apod.

Příloha č. 3
Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kraje Vysočina

- Bezpečnost přístupových oprávnění
  - Poskytovatel je povinen chránit veškeré přístupové údaje k informačním aktivům Kraje Vysočina včetně přístupů k informačním aktivům Poskytovatele, které umožňují přístup k informačním aktivům Kraje Vysočina či umožnují jejich správu.
  - Poskytovatel je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
    - min. délka hesla 10 znaků
    - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
      - malá písmena
      - velká písmena
      - číslice
      - speciální znaky
    - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě (dle bodu kryptografie)
    - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
    - platnost hesla musí být maximálně 1 rok.
  - Poskytovatel je povinen používat personifikované účty, které jsou nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
  - Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
  - Pokud by Poskytovatel zřizoval přístupová oprávnění třetí straně, je Poskytovatel povinen o této skutečnosti informovat Kraj Vysočina. Kraj Vysočina má v tomto případě právo zřízení přístupu zamítnout.
- Řízení kybernetických bezpečnostních incidentů:
  - Poskytovatel je povinen na KrÚ hlásit veškeré kybernetické bezpečnostní incidenty, které se týkají informačních aktiv Kraje Vysočina nebo informačních aktiv Poskytovatele, pokud se kybernetický bezpečnostní incident týká informací či informačních aktiv Kraje Vysočina.
  - Poskytovatel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Kraje Vysočina.