Smlouva
o dodávce automatické správy hesel privilegovaných účtů

uzavřená podle § 269 odst.2 zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů a zákona č.120/2001 Sb. autorský zákon, ve znění pozdějších předpisů

Smluvní strany

Česká národní banka
Na Příkopě 28, 115 03 Praha 1
zastoupení: Ing. Vladimír Mojžíšek, ředitel sekce informatiky
a
Ing. Zdeněk Virius, ředitel sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel" nebo také „ČNB")

a

Risk Analysis Consultants, s. r.o.
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze
oddíl C, vložka 36666
jednající: Ing. Michal Žipaj, MBA, jednatel
Konviktská 24, 110 00 Praha 1, Česká republika
IČ: 63672774
DIČ: CZ63672774

(dále jen „poskytovatel")

Článek I
Předmět smlouvy a místo plnění

1. Poskytovatel se zavazuje dodat, nainstalovat a implementovat produkt, kterým je softwarové řešení pro zajištění automatické správy hesel privilegovaných účtů v prostředí ČNB, včetně centrální správy, jehož bližší specifikace je uvedena v příloze č. 1 (dále jen" SW řešení" nebo "SW"). SW řešení a příslušné aktualizace musí splňovat veškeré požadavky objednatele uvedené v příloze č. 2 této smlouvy.
2. Součástí plnění je dále zaškolení zaměstnanců objednatele, poskytnutí spolupůčasti poskytovatele při akceptačních testech a dodání dokumentace podle čl. II odst. 1 písm. b).
3. Poskytovatel se zavazuje v rámci plnění podle této smlouvy nainstalovat nejnovější verzi programových prostředků, která bude výrobcem v době plnění uvedena na trh.
4. Předmětem této smlouvy je dále závazek poskytovatele poskytovat objednateli po dobu účinnosti této smlouvy provozní podporu spočívající v odstraňování vad.
5. Dále se poskytovatel zavazuje poskytovat po dobu účinnosti této smlouvy podporu licencí spočívající v poskytování aktualizací SW.

6. Místem plnění budou prostory výpočetního střediska v objektu objednatele na adrese: Na Příkopě 28, 115 03 Praha 1.
7. Objednatel se zavazuje za poskytnutá plnění hradit ceny dle čl. V.

Článek II
Průběh plnění

1. Plnění podle čl. I odst. 1 a 2 bude realizováno v etapách takto:

   a) První etapa – **ANALÝZA a vypracování implementačního postupu:**

   - poskytovatel se zavazuje na základě analýzy systémového prostředí ČNB vypracovat implementační postup.
   - **implementační postup** bude obsahovat:
     - Popis nasazení SW do prostředí objednatele včetně konfigurace
     - Harmonogram implementace SW
     - Nároky na součinnost objednatele

   b) Druhá etapa – **IMPLEMENTACE**:

   tato fáze zahrnuje především:

   - kompletní dodávku, instalaci a nastavení SW řešení v systémovém prostředí ČNB;
   - provedení funkčních testů SW řešení v prostředí ČNB
   - vypracování a předání dokumentace SW řešení v českém nebo anglickém jazyce:
     - Uživatelská dokumentace
     - Administrátorská dokumentace
     - Instalační dokumentace (podrobný instalační postup)
   - zajištění školení v rozsahu minimálně 2 pracovních dnů (1 den = 8 pracovních hodin), spočívajícího zejména v
     - používání a konfigurování řídící komponenty,
     - ovládání a nastavování vlastního produktu.
   - předání médií (CD, DVD, disk), na kterých je uložena instalace SW řešení a veškerá dokumentace v jednom z formátů MS Office 2003, PDF.

   c) Třetí etapa – **AKCEPTAČNÍ TESTY**:

   - Objednatel provede akceptační testy SW řešení jako celku ve lhůtě do tří pracovních dnů od převzetí druhé etapy. Poskytovatel souhlasí s tím, že akceptační testování bude provádět objednatel.
   - Objednavatel rovněž ověří zda dodané SW řešení splňuje požadavky uvedené v příloze 2.
   - Akceptační testy jsou ukončeny nahlášením výsledku a předáním seznamu nalezených vad. Po odstranění podstatných vad budou akceptační testy celé opakovány a ověří tak kvalitu předávaného SW řešení nebo jeho části. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

   Podstatné vady jsou vady, které způsobují tak závažné problémy, že objednatel nemůže produkt nebo jeho klíčovou část používat, ovládat nebo není zajištěna jeho základní funkce v souladu s dokumentací.

2. Objednatel převezme SW řešení podpisem závěrečného akceptačního protokolu dle čl. IV.

Článek III
Lhůty plnění

1. Poskytovatel poskytne objednateli plnění dle článku I odst. 1 a 2 do 8 týdnů ode dne podpisu smlouvy.
2. Poskytovatel se zavazuje dokončit a uzavřít jednotlivé etapy v následujících lhůtách:
   a) 1. etapu do 2 týdnů od podpisu smlouvy,
   b) 2. etapu do 5 týdnů od podpisu smlouvy,
   c) 3. etapu do 3 týdnů od ukončení druhé etapy.
3. Lhůty uvedené v odstavci 2 tohoto článku mohou být na základě dohody objednatele a poskytovatele prodlouženy formou zápisu podepsaného pověřenými osobami objednatele a poskytovatele. Zápis bude mít účinky dodatku ke smlouvě. V zápisu bude rovněž uvedeno, zda a o jakou dobu se prodloužením lhůty pro danou etapu prodlužuje lhůta pro celé plnění stanovená v odstavci 1 tohoto článku.
4. Pověřenými osobami jsou:
   a) za objednatele:

      Luboš Minár, tel. č.: 22441 2606, e-mail: lubos.minar@cnb.cz, nebo
      Robert Lederer, tel. č.: 22441 2669, e-mail: robert.lederer@cnb.cz.

   b) za poskytovatele:

      Ing. Marián Svetlík, tel. č.: 221 628 400, e-mail: svetlik@rac.cz, nebo
      Ing. Jiří Hološka, Ph.D.,tel. č.: 221 628 400, e-mail: holoska@rac.cz.
5. Smluvní strany se zavazují ohlástit změnu pověřených osob nebo kontaktních údajů podle tohoto článku nebo podle článku VI odst. 6 nejpozději následující pracovní den po provedení změny na e-mailové adresy pověřených osob.

Článek IV
Akceptace předmětu plnění smlouvy

1. Po ukončení první a druhé etapy předloží poskytovatel výsledek jím provedených prací k posouzení a odsouhlasení objednateli v akceptačním řízení. O výsledku akceptačního řízení bude sepsán akceptační protokol zhotovený objednatelem. Každá etapa bude považována za úspěšně ukončenou pouze, pokud bude výsledek prací prostý vad, nerozhodne-li objednatel jinak.
2. K akceptačnímu protokolu vyhotovenému objednatelem vyjádří poskytovatel své stanovisko vždy nejpozději do 2 pracovních dnů od jeho obdržení. Pokud tak neučiní, má se za to, že s uvedeným závěrem souhlasí.
3. Pokud objednatel pro vady neodsouhlasí předmět prací provedený v dané etapě, připomínky sdělí poskytovateli do 2 pracovních dnů od převzetí výsledků provedených prací. V takovém případě není poskytovatel oprávněn pokračovat v navazující etapě, dokud nebudou vady odstraněny a objednatel předmět prací neodsouhlasí bez výhrad a nebo pokud se objednatel nerozhodne odsouhlasit předmět prací s výhradami. V takovém případě budou jednotlivé výhrady zaznamenány v akceptačním protokolu a poskytovatel je oprávněn pokračovat v navazující etapě.

4. Objednatel převezme SW řešení pouze tehdy, pokud:
   - byly odsouhlaseny všechny dílčí etapy a případné vady byly odstraněny,
   - poskytovatel dodal kompletní SW řešení prosté vad a včetně požadované dokumentace,
   - poskytovatel poskytl veškeré potřebné licence pro provoz SW řešení,
   - poskytovatel předal v elektronické podobě na sjednaném datovém médiu (např. CD, DVD) veškeré podklady a dokumenty potřebné ke správě, údržbě.
5. Převzetí SW řešení bude uskutečněno podpisem závěrečného akceptačního protokolu. Tím je plnění předáno objednateli k běžnému provoznímu využití.

Článek V
Ceny plnění, množství a platební podmínky

1. Cena za plnění dle článku I odst. 1 a 2 byla stanovena dohodou smluvních stran a činí celkem **650 533,75 Kč** bez DPH. Z toho cena dodávky včetně dokumentace činí 550 533, 75 Kč a cena implementace včetně instalační dokumentace činí 100 000 Kč. V ceně dodávky je zahrnuta i cena licencí a zaškolení.
2. Cena za roční podporu provozu dle čl. I odst. 4 je zahrnuta v ceně za podporu licencí dle čl. I odst. 5.
3. Cena za roční podporu licencí dle čl. I odst 5 ode dne podpisu závěrečného akceptačního protokolu byla stanovena dohodou smluvních stran ve výši **86 866,56 Kč** bez DPH.
4. K cenám uvedeným v odst. 1, 2 a 3 bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění. Ceny uvedené v odst. 1, 2 a 3 zahrnují veškeré náklady poskytovatele spojené s plněním podle této smlouvy.
5. Úhrada ceny dle odst. 1 bude provedena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve v den podpisu závěrečného akceptačního protokolu.
6. Úhrada ceny dle odst. 2 a 3 bude prováděna vždy ročně předem, a to na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve 30 dnů před začátkem období, na které se platí.
7. Daňový doklad bude vedle náležitostí stanovených zákonem o DPH a § 13a obchodního zákoníku obsahovat i evidenční číslo smlouvy objednatele. V případě, že daňový doklad bude postrádat některou z těchto náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn vrátit vadný daňový doklad poskytovateli. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného daňového dokladu. Daňový doklad zašle poskytovatel na adresu:

   Česká národní banka
   sekce rozpočtu a účetnictví
   odbor centrální účtárna
   Na Příkopě 28
   115 03 Praha 1.
8. Splatnost daňového dokladu je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

Článek VI
Podpora

1. Poskytovatel ručí za to, že SW řešení bude funkční a schopné použití v prostředí objednatele a bude odpovídat požadavkům objednatele uvedeným v příloze č. 2 a vlastnostem a parametrům deklarovaným v příloze č. 1 a v dokumentaci.
2. Poskytovatel bude v rámci poskytování podpory provozu odstraňovat závady. Podpora bude poskytována jen v pracovní dny v pracovní době objednatele v době od 8.00 hod. do 16.30 hod.
3. Poskytovatel zahájí odstraňování závady nejpozději do 6 pracovních hodin od ohlášení závady objednatelem, nedohodnou-li se pověřené osoby smluvních stran v konkrétním případě jinak.
4. V odstraňování závady bude poskytovatel pokračovat bez neodůvodněného přerušení až do odstranění závady. Poskytovatel odstraní podstatnou vadu vymezenou v čl. II odst. 1 písm. c) do 1 pracovního dne od jejího nahlášení v souladu s odst. 5 tohoto článku. Ostatní vady poskytovatel odstraní do 15 kalendářních dnů, nedohodnou-li se pověřené osoby smluvních stran v konkrétním případě jinak.
5. Potřebu podpory provozu ohlašuje objednatel poskytovateli telefonicky na telefonní číslo poskytovatele 221 628 400 v době od 8:00 do 17:00 hod. s následným písemným potvrzením e-mailem na e-mailovou adresu holoska@rac.cz nebo potřebu podpory objednatel nahlašuje e-mailem na mailovou adresu poskytovatele uvedenou v tomto odstavci.
6. Poskytovatel je povinen potvrdit přijetí oznámení učiněné v pracovní dny od 8:00 do 16:30 do 2 hodin od doručení. Oznámení učiněná po 16:30 hod. se považují za oznámené v 8:00 hod. následující pracovní den.
7. Poskytovatel poskytne objednateli aktualizace SW bez zbytečného odkladu, nejpozději do 30 dnů od uvedení SW výrobcem na evropský trh. Aktualizací SW je míněna jakákoliv aktualizace vyvolaná aktualizací sw. prostředí (aplikační server, DB, firewall atd.), a dále vlastním rozvojem dodávaného systému.
8. Poskytovatel je srozuměn s tím, že veškerá komunikace při plnění této smlouvy bude mezi objednatelem a pracovníky poskytovatele probíhat v českém jazyce.

Článek VII
Licenční ujednání

1. Pro SW je poskytována nevýhradní, nepřevoditelná, nedělitelná, časově a územně neomezená multilicence, tj. právo užití pro 500 koncových zařízení objednatele 30 uživatelů a aplikací (systém bude využívat 25 administrátorů a 5 aplikací, koncová zařízení: 80 unix/linux serverů, 70 DB, 200 windows serverů, 130 síťových prvků a 20 ostatních zařízení). Právo užívání SW dle této smlouvy přechází na objednatele dnem podpisu závěrečného akceptačního protokolu
2. Objednatel není povinen licenci využít.
3. Součástí licence je příslušná dokumentace v elektronické podobě.

4. Poskytovatel prohlašuje, že práva, která touto smlouvou poskytuje, mu náleží bez jakéhokoliv omezení, a odpovídá za škodu, která by objednateli vznikla, pokud by toto prohlášení bylo nepravdivé.
5. Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace (tj. update/upgrade/patch/hotfix atd.).

Článek VIII
Mlčenlivost, bezpečnostní požadavky objednatele

1. Poskytovatel se zavazuje zajistit, že jeho pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí, a které nejsou veřejně známy. Povinnost mlčenlivosti není časově omezena.
2. Poskytovatel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky objednatele, které jsou uvedeny v příloze č. 3 této smlouvy.
3. Dle § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „ZOOU"), strany sjednaly:
   a) Zpracování veškerých osobních údajů objednatelem, který je ve smyslu ZOOU zpracovatelem, probíhá podle ZOOU, zejména je zpracovatel povinen ve smyslu § 7 ZOOU splnit obdobně všechny povinnosti stanovené v § 5 ZOOU pro správce osobních údajů.
   b) Toto ujednání o zpracování osobních údajů se uzavírá za účelem zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB způsobem, v rozsahu a postupem dle smlouvy, jejímž je toto ujednání dle § 6 ZOOU součástí. Rozsah zpracování osobních údajů bude odpovídat účelu zpracování, tedy bude obsahovat identifikační osobní údaje (jméno, příjmení a číslo průkazu totožnosti zaměstnanců poskytovatele). Zpracování osobních údajů podle tohoto ujednání se sjednává na dobu existence závazkového vztahu vzniklého ze smlouvy, jejíž součástí je toto ujednání, nejpozději do likvidace posledního osobního údaje zpracovatelem ve smyslu povinnosti zlikvidovat osobní údaje podle ZOOU.
   c) Objednatel poskytuje poskytovateli následující záruky technického a organizačního zabezpečení ochrany osobních údajů:
      - veškeré materiály s osobními údaji jsou zajištěny v uzamykatelném nábytku v uzamčených prostorách v sídle objednatele,
      - všechny osobní údaje jsou následně zpracovávány na PC, která jsou zabezpečena heslem, a jsou přístupné pouze vybraným zaměstnancům objednatele,
      - organizace a povinnosti zaměstnanců objednatele ohledně ochrany osobních údajů, jsou stanoveny ve vnitřním předpisu objednatele.

Článek IX
Uveřejnění smlouvy, výše skutečně uhrazené ceny a seznamu subdodavatelů

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků, výši skutečně uhrazené ceny za plnění této smlouvy a seznam subdodavatelů, kterým poskytovatel za plnění subdodávky uhradil více než 10 % z ceny za plnění dle této smlouvy.

2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „ZVZ") uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je www.vhodne-uverejneni.cz.
3. Poskytovatel je povinen dle § 147a odst. 4 ZVZ předložit objednateli vždy nejpozději do 28. února následujícího kalendářního roku seznam subdodavatelů, jimž za plnění subdodávky uhradil více než 10 % z části ceny uhrazené objednatelem poskytovateli za plnění dle této smlouvy. Poskytovatel zašle seznam objednateli na adresu:

   Česká národní banka
   sekce správní
   odbor obchodní
   Na Příkopě 28
   115 03 Praha 1.
4. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 147a ZVZ a uveřejňování bude prováděno dle ZVZ a příslušného prováděcího předpisu ZVZ.

Článek X
Smluvní pokuty, úrok z prodlení

1. V případě, že se v průběhu plnění podle článku II prokáže, že nebyl poskytovatelem splněn jakýkoliv požadavek objednatele uvedený v příloze č. 2 má objednatel právo požadovat smluvní pokutu ve výši 1 000 Kč za každý případ nedodržení požadavku. Tím není dotčeno právo na odstoupení od smlouvy ani na náhradu vzniklé škody.
2. V případě, že poskytovatel nedodrží závaznou lhůtu pro předání plnění dle čl. III odst. 1 nebo pro úspěšné ukončení příslušné etapy dle čl. III odst. 2, případně prodlouženou podle čl. III odst. 3, uhradí objednateli smluvní pokutu ve výši 1 000 Kč za každý den prodlení. To neplatí, pokud k prodlení poskytovatele došlo z důvodů na straně objednatele.
3. V případě prodlení poskytovatele ve lhůtě pro zahájení odstranění závady podle článku VI odst. 3 je objednatel oprávněn požadovat smluvní pokutu ve výši Kč 200 za každou pracovní hodinu prodlení.
4. V případě prodlení poskytovatele ve kterékoli lhůtě podle článku VI odst. 4 je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
5. V případě prodlení poskytovatele ve lhůtě podle článku VI odst. 7 je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
6. V případě prodlení objednatele s úhradou daňového dokladu má poskytovatel právo požadovat úrok z prodlení podle příslušných ustanovení předpisů občanského práva.
7. Smluvní pokuta a úrok z prodlení jsou splatné do 14 dnů ode dne doručení platebního dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
8. Smluvní pokutou není dotčen nárok na náhradu škody.
9. Smluvní strany se ve smyslu ustanovení § 364 obchodního zákoníku dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelm, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelm, ať splatné či nesplatné.

Článek XI
Doba trvání smlouvy, výpověď, odstoupení od smlouvy

1. Smlouva se v části poskytování provozní podpory a podpory licencí uzavírá na dobu neurčitou.
2. Smlouvu lze v části provozní podpory a podpory licencí ukončit písemnou výpovědí, která musí být doručena druhé smluvní straně nejpozději 3 měsíce přede dnem uplynutí předplacené doby provozní podpory nebo podpory licencí s tím, že závazky týkající se poskytování provozní podpory nebo podpory licencí zanikají uplynutím posledního dne předplacené doby podpory.
3. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele vypovědět tuto smlouvu v části týkající se poskytování podpory, a to ve 14 denní výpověďní lhůtě, která počíná běžet dnem následujícím po doručení písemné výpovědi poskytovateli. V případě, že účinnost smlouvy skončí před koncem účtovacího období, vrátí poskytovatel objednateli alikvotní část předplacené ceny plnění.
4. Poruší-li kterákoliv strana podstatným způsobem závazky vyplývající z této smlouvy, má druhá strana právo odstoupit od smlouvy, a to prostřednictvím písemného odstoupení. Takové odstoupení bude platné a nabude účinnosti dnem jeho doručení druhé smluvní straně.
5. Za podstatné porušení smlouvy strany považují zejména tyto případy:
   a) objednatel neuhradí poskytovateli cenu ve lhůtě 30 dnů po dni její splatnosti ani po písemném oznámení poskytovatele,
   b) dodané SW řešení, nebo některá jeho komponenta, nebude splňovat veškeré požadavky dle této smlouvy,
   c) systém není způsobilý pracovat v rámci systémového prostředí ČNB - např. není plně kompatibilní s operačními systémy (jejich verzemi), databázemi (jejich verzemi) a aplikacemi (jejich verzemi),
   d) poskytovatel bude v prodlení s předáním plněním nebo kterékoliv etapy plnění delším než 30 dnů.
6. Odstoupení od smlouvy je účinné doručením písemného oznámení o odstoupení poskytovateli.

Článek XII
Ostatní ujednání

Poskytovatel tímto prohlašuje, že je ke dni uzavření této smlouvy pojištěn pro případ vzniku odpovědnosti za škodu způsobenou třetí osobě v souvislosti s plněním této smlouvy, a to s pojistným plněním ve výši nejméně 2 000 000 Kč a jeho spoluúčast nepřevyšuje 5%. Poskytovatel se zavazuje, že pojištění v uvedené výši a rozsahu zůstane účinné po celou dobu účinnosti této smlouvy, a do pěti pracovních dnů od výzvy objednatele je poskytovatel povinen toto objednateli prokázat.

Článek XIII
Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami.

2. Smlouva může být měněna a doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oběma smluvními stranami, není-li ve smlouvě stanoveno jinak.
3. Smluvní strany se dohodly, že závazkový vztah založený touto smlouvou, se řídí zákonem č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů předpisů a zákonem č. 121/2000 Sb., autorský zákon,ve znění pozdějších předpisů.
4. Tato smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak
5. Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
6. Smlouva je vyhotovena ve třech vyhotoveních s platností originálu, z nichž objednatel obdrží dvě a poskytovatel jedno vyhotovení.

Přílohy: č. 1 – Technická specifikace produktu
č. 2 - Technické požadavky objednatele
č. 3 - Bezpečnostní požadavky objednatele

V Praze dne: 25. 10. 2012

Za objednatele:

.....
Ing. Vladimír Mojžíšek
ředitel sekce informatiky

.....
Ing. Zdeněk Virius
ředitel sekce správní

V Praze dne: 22. 10. 2012

Za poskytovatele:

.....
Ing. Michal Žipaj, MBA

RAC
Risk Analysis Consultants, s.r.o.
Konviktská 24, 110 00 Praha 1
Tel.: 221 628 400, Fax: 221 628 401
DIČ: CZ63672774

[redacted]

Příloha č. 1

RISK ANALYSIS CONSULTANTS

Technická specifikace

D135.02.07-1-NAB

Automatická správa privilegovaných účtů

pro

ČNB

The First Czech Company
NATO BOA Partner

MEMBER OF ITIC GROUP

Tato stránka je vynechána úmyslně

Obsah

Základní informace o uchazeči

Kapitola obsahuje identifikaci nabídky, společnosti RAC a kontaktní osoby pro tuto nabídku.

Identifikace dokumentu

Klasifikace:	N135.02.07-1-NAB
Název:	Nabídka na Cyber-Ark PIM
Verze a stav:	verze 1.0
Datum verze:	17. září 2012
Verze šablony:	šablona NAB v.3.0
Vytvořil:	Jiří Hološka, Marián Svetlík, Zbyněk Marx
Schválil:	Michal Žipaj

Základní údaje o společnosti

Název společnosti:	Risk Analysis Consultants, s.r.o.
Sídlo společnosti:	Konviktská 291/24, 110 00 Praha 1
Kanceláře společnosti:	Španělská 2, 120 00 Praha 2
Právní forma:	společnost s ručením omezeným
Identifikační čísla:	IČO: 63672774, DIČ: CZ63672774
Jednatelé společnosti:	Ing. Michal Žipaj, MBA, CISSP Martin Másílko
Bankovní spojení:	ČSOB Praha 576 900 263 / 0300

Kontaktní osoba pro tuto nabídku

Marián Svetlík
tel. 221 628 400
mobil 602 231 780
fax 221 628 401
svetlik@rac.cz

Antonín Šmíd
tel. 221 628 400
mobil 606 628 877
fax 221 628 401
smid@rac.cz

OCHRANA INFORMACÍ

Ochrana vzájemně poskytnutých informací může být provedena uzavřením Smlouvy o ochraně obchodních informací, případně, bude-li uzavírána smlouva o dílo, uvedením pasáže obsahující ustanovení směřující k ochraně informací.

ŘEŠENÍ CYBER-ARK PIM

PIM je základním řešením nabízeným firmou Cyber-Ark. Jedná se o „state of art" řešení na správu a řízení sdílených privilegovaných účtů.

Základem systému je zabezpečené úložiště Vault neboli datový trezor pro ukládání dokumentů, hesel k privilegovaným účtům, video záznamů sezení a logů událostí.

Pomocí modulu Application Identity Management (AIM), lze základní funkcionalitu rozšířit o správu aplikačních hesel. Aplikační hesla jsou koncipována jako jednorázová hesla a nahrazují hesla, která se běžně vyskytují v čitelné formě v různých konfiguračních souborech zejména u webových aplikací.

Cyber-Ark umožňuje vyjma řízení hesel a prosazovaní politik pro životní cykly privilegovaných i aplikačních hesel také řízení uživatelských přístupů k jednotlivým spravovaným administrátorským identitám.

Z uživatelského pohledu jde o centralizovanou databázi dostupných administrátorských identit dostupných skrze webovou aplikaci.

Úroveň oprávnění administrátorských účtů na systémech Microsoft Windows a GNU/Linux lze centralizovaně řídit pomocí modulu On-demand-Privileges (OPM). Modul OPM umožňuje definovat různým uživatelům využívat jen specifické privilegované operace, které pokrývají jejich běžnou pracovní náplň. Veškeré pokusy o přístup k neautorizovaným operacím jsou bezpečně zaznamenány v datovém trezoru, kde lze zamezit pokusům o úpravy nebo odstranění těchto záznamů.

Pokud záznamy o událostech z modulu pro řízení přístupů k privilegovaným identitám nejsou dostatečně průkazné, nebo jsou vyžadovány detailnější informace o provedených operacích v rámci aktivních sezení, je možné pro potřeby auditů vytvářet modulem Privilege Session Management (PSM) záznamy aktivních sezení. Záznamy aktivních sezení obsahují na systémech Windows video záznam celé obrazovky a lze tak bezpečně určit jaké operace administrátor na systému prováděl. Záznam ze systému GNU/Linux nebo Unix navíc obsahuje i přepis příkazů zadaných do terminálu v textové podobě. Oba druhy záznamů jsou uloženy v trezoru, obsah záznamů je zpřístupněn pouze uživatelům s oprávněním „Auditor".

Systémové výpadky na hardwarové, softwarové nebo síťové úrovni lze zabezpečit pomocí modulů High Availability a Disaster recovery, zajišťující záložní řešení pro případ nečekaného výpadku.

Detailní informace o produktu lze získat z přehledového dokumentu „PIM SOLUTION OVERVIEW 2012" od firmy Cyber-Ark.

An Integrated Approach to Privileged Identity Management: Solution Overview

June 2012

1. The Challenges of Managing Privileged Identities

In today"s environment, organizations spend a lot of time and money building a sophisticated infrastructure to ensure the security of their enterprise and seamless business continuity. A typical infrastructure is comprised of many components, such as servers, firewalls, databases and network devices, all of which are controlled using a variety of privileged and elevated accounts, also known as break-glass, emergency or fire IDs. These accounts have full access and authorizations on the infrastructure and are the most powerful in the organization. There are often hundreds, if not thousands, of these powerful accounts in a typical environment. It is very common practice to properly manage all system accounts, and have every user's password reset every few weeks or months. Ironically, privileged accounts and their passwords, which are the most powerful in the organization, are often neglected, remain unmanaged, and rarely changed and is further made complex with the need to monitor their session activities.
In some cases, these accounts are required, not only by internal IT personnel, but also by external 3rd party vendors and, thus, require extra care, such as secure remote access and secure session initiation without exposing the credentials. Powerful passwords are also often hard coded inside applications, scripts and parameter files, leaving them unsecured, rarely changed and visible to the world.
Privileged accounts are the keys to every asset in the enterprise, and therefore, mismanagement of privileged accounts imposes great risks to the organization:

Audit failures – Leaving passwords unchanged and unaudited compromises compliance regulations (such as Sarbanes Oxley, PCI and Basel II) which require organizations to provide accountability about who accessed shared accounts, what was done, and whether passwords were protected and updated according to policy.

Security risk – Traditionally the risk of the **insider threat** has been a major driver for a PIM solution, where employees can harm the organization they work for when no one expects them to do so. They are able to do so because they know the root password of all servers (which is also identical across all servers), and there was no way to prove it was a specific individual because all administrators know the password as well. **External targeted attacks** have also become common occurrences and are becoming more sophisticated, better planned and targeted. Such attacks, on the most part, go after vulnerabilities that

result in gaining privileged access or hard-coded application passwords that can do significant damage to an organization's bottom line and reputation

Loss of productivity – A password that was manually reset by one of the IT people who did not inform his team members, may cause hours of delay in recovering from an IT failure and thus leave hundreds of users unproductive and information inaccessible. With hundreds of network devices, privileged identities can be extremely time-consuming to manually update and report on, and more prone to human errors.

Organizations need to gain control over their privileged and shared identities and create accountability for their usage by specific individuals. The ability to granularly track any activity related to these accounts would greatly mitigate security risks, meet regulatory compliance and ensure business continuity.

2. Cyber-Ark's Privileged Identity Management Suite

Cyber-Ark's Privileged Identity Management (PIM) Suite, a full lifecycle solution for centrally managing privileged and shared identities, as well as embedded passwords found in applications and scripts. The PIM Suite is an enterprise-class, unified policy-based solution that secures, manages and monitors all privileged accounts and activities associated with datacenter management whether on-premise or in the cloud.

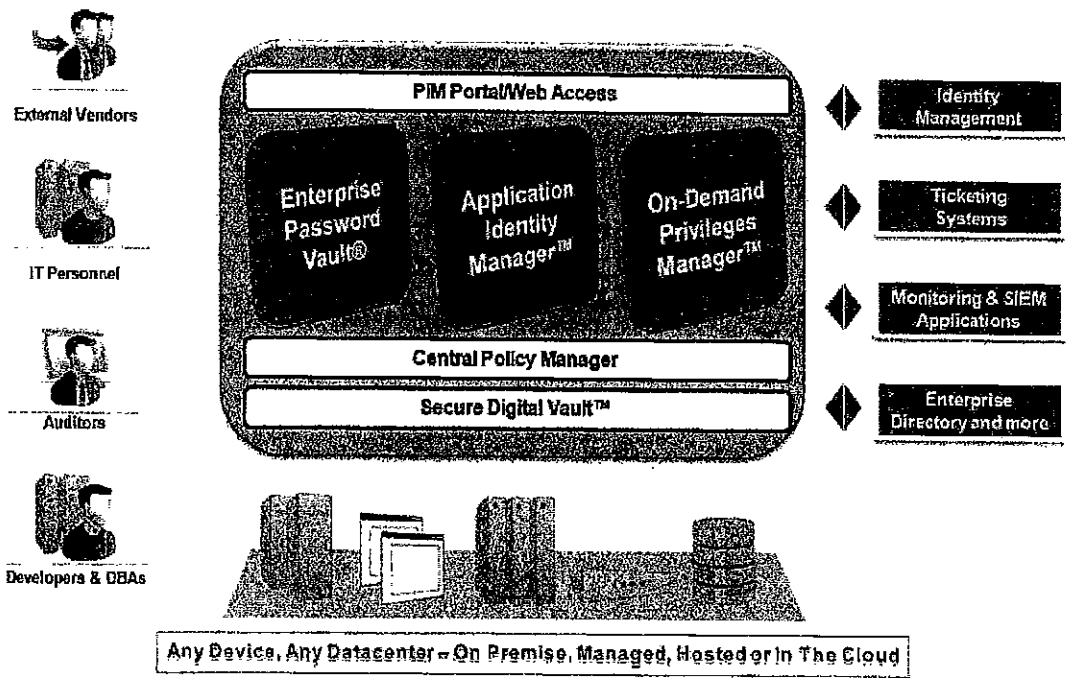


Figure 1: PIM Suite Diagram

Privileged accounts, as well as the audit information associated with using them, must be protected according to the highest security standards. The Cyber-Ark PIM Suite utilizes the Patented Digital Vault®, validated as highly secure by independent security evaluators (such as ICSA Labs). This core technology is the heart of the PIM Suite and was designed to meet

the highest security requirements for controlling the "keys to the kingdom." The Digital Vault provides numerous underlying security capabilities for authentication, encryption, tamper-proof audit and data protection.
The Cyber-Ark PIM Suite includes the following products:
Enterprise Password Vault ® – Cyber-Ark"s award winning Enterprise Password Vault (EPV) enables organizations to enforce an enterprise policy that protects your most critical systems, managing the entire lifecycle of shared and privileged accounts across data centers.
Application Identity Manager™ – Cyber-Ark"s market leading Application Identity Manager (AIM) fully addresses the challenges of hard-coded App2App credentials and encryption keys. The solution eliminates the need to store App2App credentials in applications, scripts or configuration files, and allows these highly-sensitive credentials to be centrally stored, audited and managed within Cyber-Ark"s patented Digital Vault.

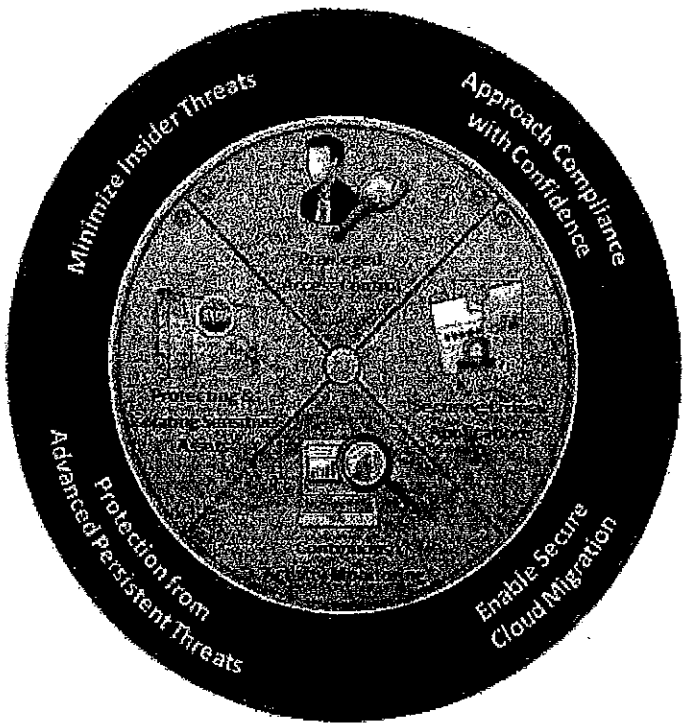


Figure 2: Improving Your Security Posture with a Preventative Approach

3. THE PIM SUITE ARCHITECTURE

The Cyber-Ark PIM Suite provides a „Safe Haven" within your enterprise, where all your privileged identities can be securely archived, transferred, automatically managed and shared by either human authorized users, such as IT staff, on-call administrators, DBAs, and local administrators in remote locations or by unattended services such as business/IT applications, scripts, jobs and more. The PIM Suite basic infrastructure is comprised of the following components and entities:

Vault Server – Highly Secure Repository

The solution is based on Cyber-Ark"s patented Digital Vault technology, which includes a FIPS 140-2 validated cryptography module (with AES-256 encryption), and is proven to meet security and industry regulations such as PCI, NERC, FERC, SOX, HIPAA, GLB, etc. The multiple and tightly coupled security layers (including Firewall, VPN, Authentication, Access Control, Encryption, and more) that are at the core of the PIM Suite provide you with a proven, highly secure solution for storing and sharing credentials in an enterprise environment. The Vault server can be delivered either as software, VM image or as a hardware appliance.

Central Policy Manager – Enforces Enterprise Policies

The PIM Suite allows enterprises to define policies based on their specific workflows and needs that will control how privileged identities are accessed and managed. Some examples include:

- The type of account indicates the rule that applies to the password's strength, such as the minimum number of characters required for the password, the type of characters, etc.
- The frequency of the password change indicates whether the password must be changed at regular intervals, or if it is a „one-time" password that must be changed after having been accessed.
- Additional automation parameters determine whether passwords should be automatically verified to check if they are synchronized with the real passwords on the remote devices, what to do in case a synchronization problem occurs, and more.

The PIM Suite supports as many policies as necessary to meet organizational requirements. A policy might apply to individual accounts or to a group of accounts.
Policies can be managed by the security or risk teams separately from the daily management of privileged accounts which can be delegated to the teams who own them e.g. UNIX/Windows teams etc.
Cyber-Ark"s Privileged Identity Management (PIM) Suite is designed and developed using an extensible architecture approach, which provides great flexibility to dynamically support additional managed devices.
As a component of PIM, the Central Policy Manager (CPM) enforces the enterprise policy and automates password management. The CPM is designed and developed using an extensible architecture approach, which provides great flexibility to dynamically support a wide array of enterprise platforms, systems and target devices as operating systems, applications, databases,network devices, security appliances, etc. The PIM suite includes out-of-box support for hundreds of target devices. Cyber-Ark constantly releases CPM plug-ins for new platforms as part of and between official releases of the PIM Suite. PIM V7 opens a new world of access to include support for managing web-based application credentials e.g. the Corporate Facebook account, ERP/CRM web-based applications, web-based firewall configuration interfaces etc.

Password Vault Web Access (PVWA) – Intuitive PIM Portal

The Password Vault Web Access (PVWA) is a fully featured pure web Portal that provides a single console for requesting, accessing and managing privileged passwords as well as transparently connecting[1] to managed devices throughout the enterprise by both end users, administrators and auditors with almost no training.

Viewing accounts is very user friendly where the Accounts Page allows a quick way to display, sort and access your accounts. Predefined and dynamic views enable you to display accounts according to predetermined criteria, e.g. account and operation status, as well as define new views based on common search operations.

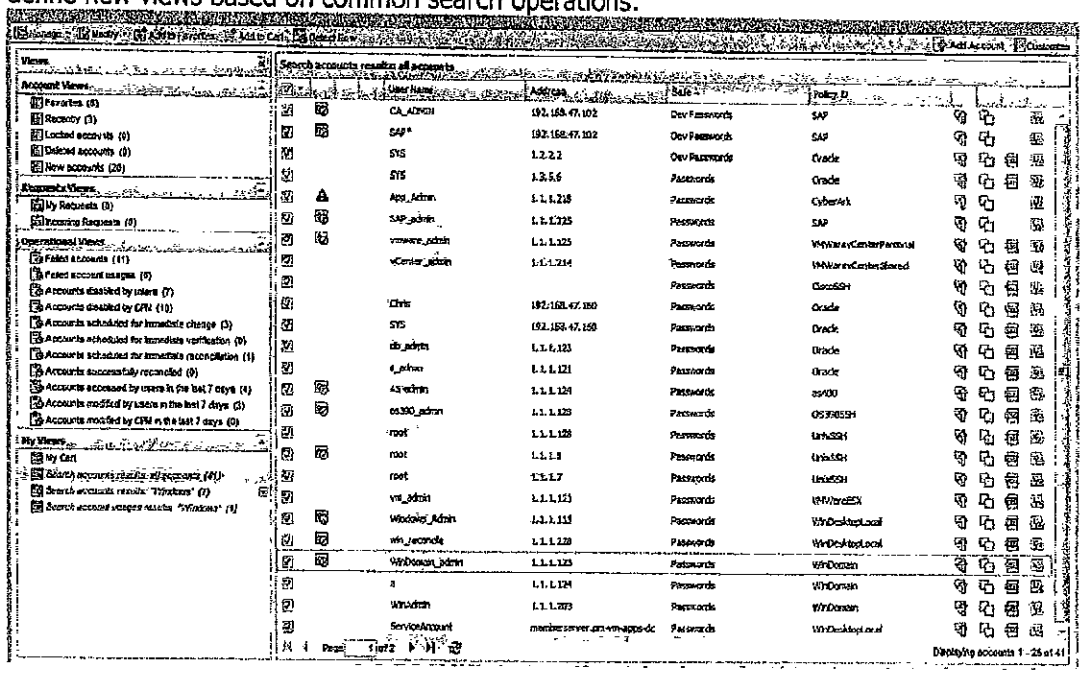


Figure 3: Accounts Page View

The PIM Suite enables the IT Administrators to access privileged accounts in various workflows depending on the enterprise requirements, either from a desktop browser or from their mobile devices, such as BlackBerry, iPhone or Android. Customized workflows can be defined, including enforcing users to enter an open and valid ticket ID whenever requesting a password, while the system will validate this ticket ID against the relevant Ticketing System.

---

1 Transparent connection to remote devices is done through a "Connect" button or from a desktop shortcut, and can optionally be done without divulging the password to the end user

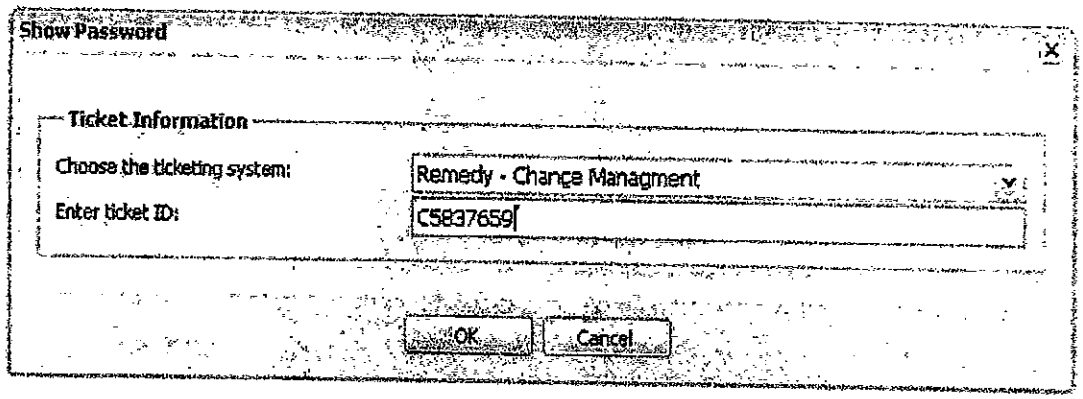


Figure 4: Enforce entering a valid Ticket ID when accessing a privileged account

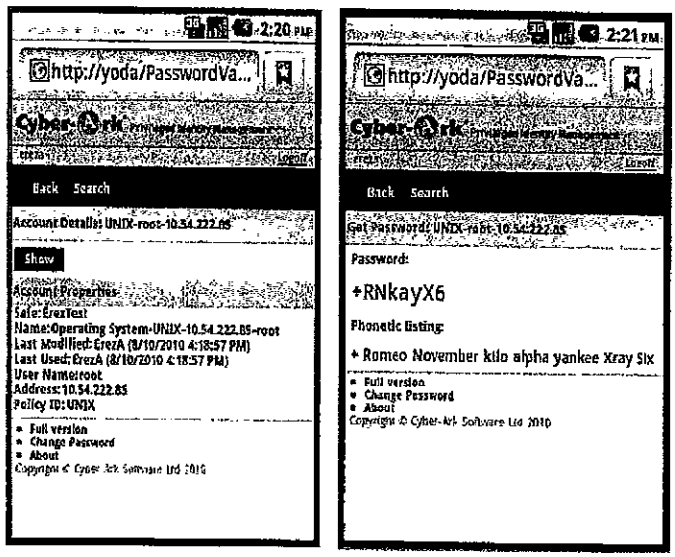
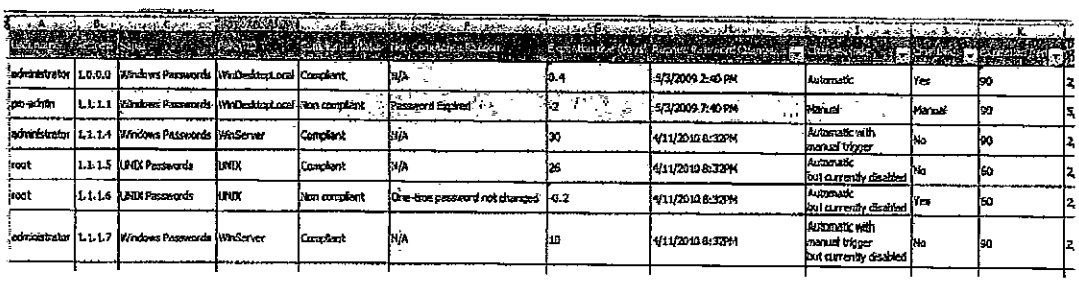


Figure 5: Access privileged accounts anywhere from your mobile device

The PIM Portal allows managers and auditors to gain insight on privileged activities via a unique dashboard, which offers a bird's-eye view of the status of privileged account management. In addition, scheduled or ad-hoc compliance and activity reports can be generated via the PIM Portal. These reports give insight as to who has access to which privileged accounts, when they were last accessed or changed and by whom, to what extent an account is compliant with the current policy etc.



administrator	1.0.0.0	Windows Passwords	WinDesktopLocal	Compliant	N/A	0.4	5/3/2009 2:40 PM	Automatic	Yes	90
pw-admin	1.1.1.1	Windows Passwords	WinDesktopLocal	Non compliant	Password Expired	42	5/3/2009 7:40 PM	Manual	Manual	90
administrator	1.1.1.4	Windows Passwords	WinServer	Compliant	N/A	30	4/11/2010 8:32PM	Automatic with manual trigger	No	90
root	1.1.1.5	UNIX Passwords	UNIX	Compliant	N/A	26	4/11/2010 8:32PM	Automatic but currently disabled	No	60
root	1.1.1.6	UNIX Passwords	UNIX	Non compliant	One-time password not changed	0.2	4/11/2010 8:32PM	Automatic but currently disabled	Yes	60
administrator	1.1.1.7	Windows Passwords	WinServer	Compliant	N/A	10	4/11/2010 8:32PM	Automatic with manual trigger but currently disabled	No	90

Figure 6: Easily understand which accounts meet compliance guidelines

The following diagram shows a typical PIM Suite environment, with different privileged account access workflows.

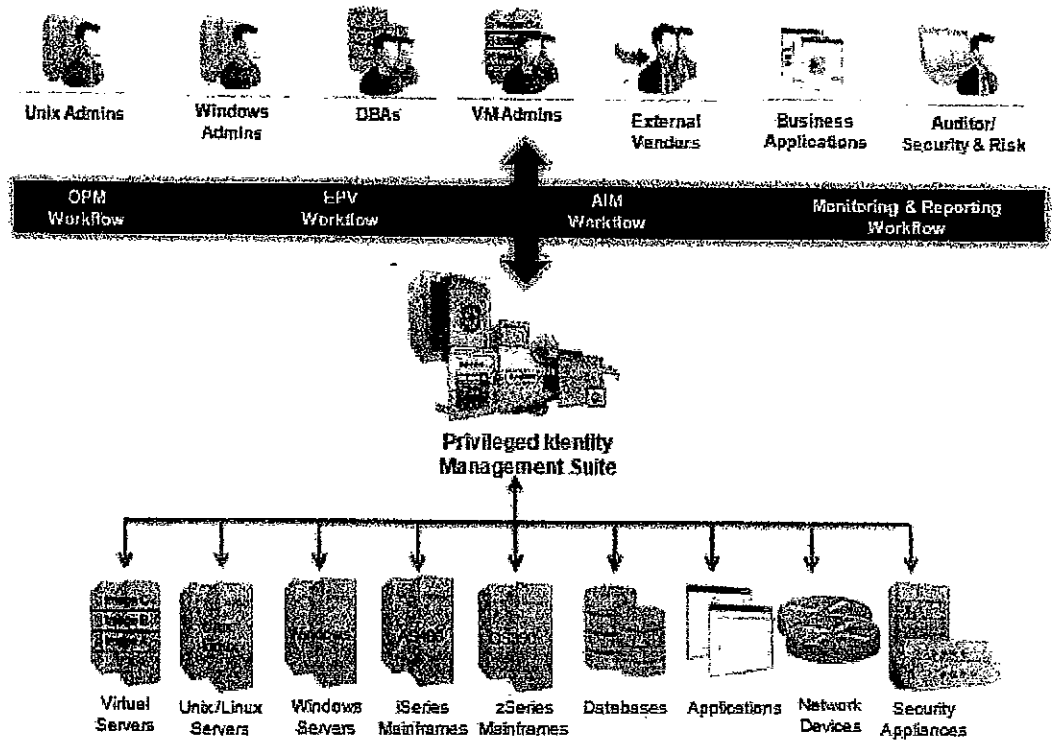


Figure 7: Unified policies for all privileged accounts access workflows

As the first step in managing privileged accounts, an authorized user defines them in the Vault and determines which users will be able to access them and according to which privileges.
Once they are in the Vault, authorized users, such as IT personnel, can access passwords and use them according to their permissions on a variety of platforms and devices.
Passwords can be retrieved and used in any of the following workflows:

- **EPV** – Users retrieve passwords and use them directly from the PVWA or connect to target systems without knowing the password.

- **AIM** - applications or scripts that need to connect to databases or any other network resource using embedded credentials.

At any time, auditors can view activities that took place in the Vault by generating reports or viewing recordings.
The PIM Suite portal is available in various languages, including French, German, Spanish, Russian, Japanese and Simplified Chinese.

An Enterprise Ready Solution

To eliminate administrative overhead and ensure compliance with enterprise IT practices, the PIM Suite delivers the highest level of enterprise class integration with a wide range of enterprise systems, including:

Managing Extensive Amounts of Target Systems using the PIM Suite - large enterprises usually manage tens and even hundreds of thousands of devices. The PIM Suite leads market solutions by ensuring that performance requirements are addressed in this type of environment, providing a robust infrastructure backend management engine and end user UI.

Transparent user management through enterprise Directories

The PIM Suite transparently communicates with LDAP compliant Directory servers to obtain user identification and security information. When using the PIM Suite, customers can continue using their Directory as a single point for managing users and groups, and are not required to duplicate definitions of users and groups in the privileged account management solution.

Automatic discovery of privileged accounts

The PIM Suite provides a unique solution for automatically discovering and provisioning privileged accounts from different Directories, which assist enterprises to streamline the process of on-boarding privileged accounts and automatically managing them, as well as eliminating the need to manually reflect any changes in the environment. By automatically managing privileged accounts, security of volatile environments is dramatically improved. Automatic detection is currently supported for Microsoft Active Directory and VMware vCenter private clouds.

The automatic detection provides the following functionality:

- Automatic provisioning of ESX host machines – automatically manage the root accounts of the ESX host machines. The PIM Suite will automatically detect any new ESX host that is added to the vCenter and delete any machine that was removed from it. The ESX CPM plug-in that uses VMWare tools can automatically verify or change root account passwords, based on the enterprise policy, without the need to open SSH.
- Automatic provisioning of Linux/UNIX machines – automatically manage the Linux/UNIX root or other privileged/shared accounts based on predefined templates. Once provisioned in the Vault, those accounts can be automatically managed based on the enterprise policy.
- Automatic Provisioning of Windows machines - automatically manage Administrator or other privileged/shared accounts based on predefined templates. Once provisioned in the Vault, those accounts can be automatically managed based on the enterprise policy.
- Automatic Detection and Provisioning of Windows service accounts – automatically detect and manage privileged account usages used within Windows services, scheduled Tasks, COM+, IIS setting, etc. This ensures that automatic change of these passwords will not disrupt any process, as the password will be automatically updated wherever it is used.
- Report on local Administrators group member - Enterprises can generate reports listing all local Administrators group member for each machine.

- Alert on unmanaged accounts - Enterprises can receive email alerts when detecting privileged accounts that are currently not managed within the PIM Suite. For example, a privileged account used within a Windows Service and is not managed in the Vault. This helps ensure compliance with organizational policy for service accounts as well as reducing the security risks of unmanaged accounts.

- The unique automatic detection capability completely eliminates administrative overhead while allowing a scalable solution to easily manage tens of thousands of privileged accounts such as Windows local Administrators across the enterprise.

Enhanced authentication options
A major advantage of Cyber-Ark's Enterprise Password Vault has always been its ability for seamless integration with enterprise authentication schemes and the ability to leverage many types and formats of enterprise authentication. The PIM Suite supports a variety of authentication methods for end users including: LDAP, PKI, RADIUS, RSA SecurID, Windows authentication, Oracle SSO and a robust infrastructure for integrating with most Web SSO or OTP solutions.

Integration with enterprise Ticketing Systems
As many organizations use enterprise ticketing systems to control troubleshooting and emergency access to privileged accounts, the PIM Suite introduces an open approach to integrating the password retrieval workflow to inputs and verifications from ticketing systems e.g. whether a valid ticket exists.

Monitoring and SIEM Integration
The PIM suite provides out-of-box support for SIEM solutions. A simple configuration setting enables the PIM suite to send audit records to the SIEM system, and allows users to define very detailed customization of the log record format that is best suited to the SIEM system. In addition, the solution provides standard means, such as allowing customers to monitor the product using standard enterprise monitoring tools, including SNMP notifications, writing to EventLog, a robust built-in email notification mechanism, and more.

Backup – the PIM Suite backup solution can seamlessly integrate with all leading backup products and is designed to protect against data loss due to human errors or hardware problems. The solution provides a thorough backup solution that supports both incremental and full backup, and enables the Vault data to be exported into a backup medium in an encrypted, secure way.

Supported Managed Devices

Operating systems: Windows, Linux/Unix, OS390, OS400, OVMS, HP Tandem, Mac OS X

Windows Applications Service accounts: Scheduled Tasks, IIS Application Pools, COM+, IIS Anonymous Access

Databases: Oracle, MSSQL, DB2, Informix, Sybase, any ODBC compliant database

Security Appliances: CheckPoint, Nokia, Juniper, Cisco, Blue Coat, IBM, TippingPoint, SourceFire, Fortinet, WatchGuard

Directories: Microsoft, Sun, Novell, Unix vendors

Remote Control and Monitoring: IBM, HP iLO, SUN, Dell DRAC, Digi, Cyclades

Generic Interfaces: any SSH/Telnet device, Windows registry

4. Eliminating Hard Coded Passwords with the Application Identity Manager (AIM)

In today"s complex IT environments, multiple scripts, processes and applications, need to access multi-platform resources, to retrieve and store sensitive information. Such applications are granted use of dedicated accounts, usually allowing unlimited access to sensitive information stored in corporate databases, the enterprise"s most sensitive assets. As a result they are often the victim of ongoing targeted attacks. Indeed, many of the recent sophisticated attacks reported stemmed from the compromise of hard-coded privileged credentials.

Hard coded passwords are not only a local problem. They exist everywhere and are usually embedded inside the application code, scripts, services, application server data sources, configuration files, databases, 3rd party products, and more.

Despite the sensitivity of privileged accounts in applications, many fear to manage them due to the operational consequences such as recompiling, testing and redeployment. Others don"t manage them due to lack of knowledge on the possible consequences and the potential downtime to systems. As a result, up to 42% of enterprises report that they never change hard-coded and embedded passwords for application IDs, testing scripts and batch jobs. This imposes great risk to enterprises, including:

Failed audits – regulations such as PCI DSS specifically instruct enterprises to develop secure applications/systems, remove hard coded credentials and enforce strong access control and authorization.

Lack of accountability – with visible hard coded credentials, enterprises have very limited audit around who accessed an application account

Security risks – static and clear text hard coded credentials become known to a wide variety of employees overtime, including also ex-employees and even external vendors. Compromising these accounts may lead to severe damage to the enterprise.

In order to successfully eliminate and manage hard coded application credentials, a robust app2app solution must meet the following requirements:

High availability and survivability – Requesting applications cannot afford any downtime. Credentials should always be available to them, independent of network failures or storage unavailability. This also includes the ability to work in complex and distributed environments, where local branches do not always have access to the main data center.

Robust Application authentication – Applications requesting credentials must be strongly authenticated to ensure sensitive passwords are returned only to authorized applications.

Strong Access Control - A strong access control mechanism must be enforced on password usage to enable granular control over who can access the password, down to the application level.

Periodic and automatic password changes – Passwords should be changed periodically based on enterprise policy in order to adhere to the appropriate regulatory compliance rules, with no interruption or downtime to business applications.
Broad platform support – Be able to support a wide variety of systems, applications, scripts and more, which are common in today's enterprise environments.

Comprehensive audit - Allow easy tracking of any access to passwords, by both applications (unattended services) and human users.
Simple and flexible integration – The process of changing applications to eliminate the use of hard-coded passwords should be as simple and intuitive as possible for ease of deployment.

The Application Identity Management Solution

Cyber-Ark's Application Identity Management eliminates the need to store application passwords embedded in applications, scripts or configuration files, and allows these highly-sensitive passwords to be centrally stored, logged and managed within the Vault. This unique approach enables organizations to comply with internal and regulatory compliance such as PCI Data Security, which specifically instructs enterprises to develop and maintain secure systems and applications, remove any hard-coded custom usernames, passwords or connection strings from applications, periodically replace passwords, and monitor privileged access across all systems, databases and applications.
The PIM Suite provides applications with easy-to-use tools to access the application credentials using a single function call in a command line interface (CLI) or native API for Java, .Net, C/C++, and COM on a variety of platforms.
For example, the following "hard coded" password is used inside a script:

```
With Pass
.Address = "192.168.1.1"
.UserName = "DBA"
.Content = "Pass123"
conn.Open driver={SQL Server};server=" & .Address & ";uid=" &
.Username & ";pwd=" & .Content & ";"
End With
```

Using the Application Password SDK, the password, as well as the account's address and username can be removed from the script, replacing them with a simple function call that will securely retrieve the password and its properties:

```
With PassReq
.Safe = "Passwords"
.Folder = "Root"
.Object = "App1"
.Reason = "Billing application - connect to DB2"
End With
Set Pass = sdk.GetPassword(PassReq)
With Pass
conn.Open driver={SQL Server};server=" & .Address & ";uid=" &
.Username & ";pwd=" & .Content & ";"
End With
```

The AIM solution utilizes the **Cyber-Ark PIM Provider,** which is installed on every machine running applications, manages and protects application credentials in a secure local cache, providing the highest availability to applications, and greatest performance. The Provider authenticates applications that request credentials, based on their path, machine address or OS user. In addition, a unique signature based application authentication, provides organizations with tamper proof protection to their applications code
The Cyber-Ark PIM Provider also synchronizes password replacement against the Central Policy Manager, so that passwords are constantly accurate. It provides immediate availability to passwords, even with no network connectivity to the Vault, and provides millisecond response time independent of network performance.

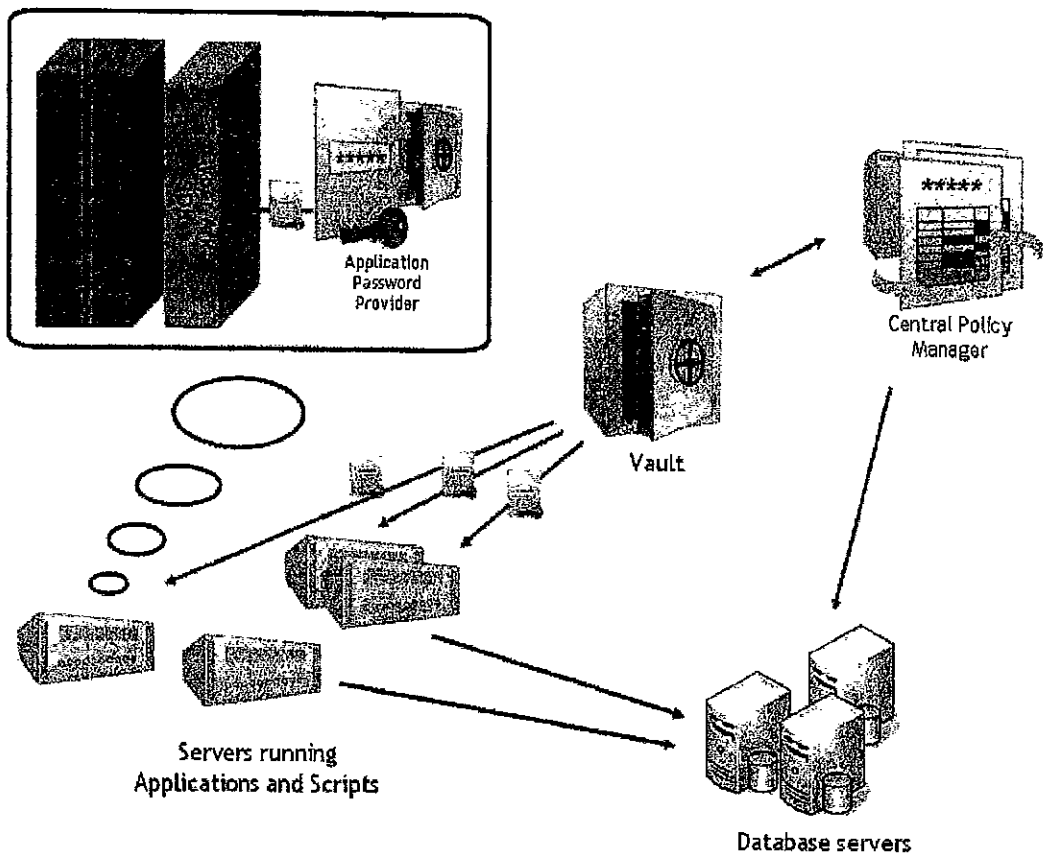


Figure 8: Application Identity Manager™ Architecture

The Application Identity Management Solution supports the following platforms and environments:

Supported Platforms

Windows
UNIX:

- o Solaris
- o Linux (RHEL, SUSE zLinux, SUSE Intel, Fedora)
- o AIX
- o HP-UX*

Supported Environments

- o C/C++
- o Java
- o CLI
- o .NET, VisualBasic
- o VBS (COM)

5. Privileged Identity Management Solution Benefits

With Cyber-Ark"s Privileged Identity Management Suite (PIM), enterprises can easily:

Eliminate Internal and External Threats

PIM manages, protects and controls access to all privileged accounts and makes hard-coded application credentials invisible to developers, database administrators, external vendors and IT staff.

Meet Compliance and Audit Requirements with Confidence

The PIM Suite creates easy to use, unified audit reports required by Sarbanes-Oxley, PCI DSS, NIST 800-53 and more. It allows enterprises to enforce corporate security policies to ensure compliance with regulatory needs and security best practices related to access and usage of privileged accounts for both human and application access, including:

Managing and Protecting all Privileged Accounts – The PIM Suite utilizes a secure Digital Vault in order to store, protect, manage and control access to Privileged Accounts at a centralized point using a robust policy management engine. Cyber-Ark"s patented Vaulting Technology® utilizes a fully integrated model of critical security layers, interwoven to meet the highest security needs.

Controlling Access to Privileged Accounts – PIM Suite offers a simple access control interface that easily pinpoints who is entitled to use privileged accounts, when and why.

In-depth UNIX security - enhance access control to a more granular level and determine who can run which commands within the UNIX environment and elevate to 'root' only when needed. With a unified solution for shared and super user accounts, reporting becomes easy with a single, correlated view.

Managing application and service credentials – PIM provides sophisticated and transparent solutions for securing and managing critical applications as well as Application Server accounts, and eliminating the use of hard-coded and embedded passwords, making them invisible to developers and support staff.

Reduce IT Overhead with More Efficient Control and Less Human Error

PIM eliminates manual administration with extremely reliable and uninterrupted service. Minimal administrator overhead results in increased productivity and is less prone to human errors.

Enterprise-ready

With industry leading performance, scalability and robustness, proven in hundreds of large enterprises, PIM can protect and manage up to hundreds of thousands of privileged accounts across a highly heterogeneous IT environment, with complex and distributed network architectures. PIM can leverage existing enterprise infrastructure and integrate with core corporate systems.

Příloha č. 2

Technické požadavky kupujícího

Preambule

Zadavatel požaduje dodávku komplexního systému pro automatickou správu hesel privilegovaných účtů v prostředí ČNB. Prostředí ČNB se skládá z fyzických serverů a virtuálních serverů na platformě VMware vSphere 4.1, z fyzických pracovních stanic IBM-PC kompatibilních, virtuálních pracovních stanic a síťových prvků HP a Cisco.
Virtuální pracovní stanice jako publikovaný desktop hostovaný na terminálových serverech s operačním systémem MS Windows Server 2008 R2 Standard Edition a Citrix XenApp 6.5.
Proces sestavení jednotlivých terminálových serverů je řízen prostřednictvím Provisioning Services platformy Citrix – jednotlivý terminálový server je každý den vytvářen z master (golden) image.
Zadavatel provozuje cca 90 unix/linux serverů, 80 DB, 200 windows serverů, 130 síťových prvků, 20 ostatních zařízení.
Systém bude využívat cca 25 administrátorů a 5 aplikací a bude v něm uloženo cca 1000 hesel

1. Systém automatické správy hesel privilegovaných účtů splňuje:

1.1. Všechny komponenty systému jsou spustitelné na virtuálním serveru Windows 2008 R2.
1.2. Žádnou z komponent nebude nutné instalovat na koncová zařízení
1.3. Všechny komponenty systému jsou dostupné v českém nebo anglickém jazyce.
1.4. Všechny požadované funkce se spravují a využívají přes společnou řídící konzoli, která je přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím Internet exploreru 8.0 a novějších.
1.5. Systém k přihlášení využívá doménové účty s využitím SSO (web SSO) včetně přihlášení pomocí čipové karty ČNB a také lokální účty.
1.6. Přístup uživatelů je řízen oddělenými rolemi. Budou definované min. následující role:
administrátor - nastavuje a konfiguruje systém, zakládá uživatele a přiděluje oprávnění, definuje a přiřazuje politiky hesel, atd. (Nemá přístup k uloženým heslům a nemůže měnit ani mazat auditní logy.)
auditor - má přístup pouze k auditním logům
operátor složky - zakládá a spravuje složky pro ukládání hesel a přiděluje přístupová oprávnění k těmto složkám
user - má přístup k heslům dle nastavených oprávnění
1.7. Systém vyhledává dle klíčových slov (řetězců) v názvech účtů, v politikách a v auditních lozích.
1.8. Systém zaznamenává veškeré auditní logy o využívání uložených hesel a užívání vlastního systému. Logy jsou v systému uloženy po nastavitelnou dobu a zároveň pravidelně odesílány protokolem syslog do systému SCOM (System Center Operations Manager).
1.9. Systém v nastavitelnou dobu pravidelně zálohuje uložená data (hesla) do kryptovaného souboru na určené diskové úložiště.
1.10. Systém vytváří reporty ve formátech PDF a CSV, popř. dalších. Reporty jsou generovány z předdefinovaných šablon, které lze vytvářet a editovat. Pro všechny

reporty lze nastavit automatické spouštění v definovaném čase a ukládání na síťové úložiště nebo odesílání emailem. V rámci implementace budou vytvořeny následující šablony reportů:
- výpis použití definovaného hesla z auditního logu za dané období
- seznam všech účtů hesel uložených v el. trezoru

1.11. Systém zasílá emaily s upozorněním (notifikací) v případě, že nastane definovaná událost dle definovatelných parametrů. Pro odesílání notifikací je požadováno využití protokolu SMTP s možností konfigurace přijímacího MTA (message Transfer Agent) uzlu. V rámci implementace budou vytvořeny následující notifikace:
- pokud heslo uložené v trezoru neodpovídá heslu spravovaného OS, DB
- pokud v systému nastala kritická chyba

1.12. Existuje mechanismus bezpečného přístupu k heslům uložených v systému v případě jeho nedostupnosti.

1.13. Systém umožňuje rozšíření o modul nahrávání videozáznamů činností uživatelů ve spravovaných systémech v případě přístupu z dodaného systému.

1.14. Systém umožňuje rozšíření o modul ekvivalentní náhrady příkazu SUDO v OS Unix/Linux tak, aby správa a logování bylo zajištěno dodaným systémem

1.15. Systém podporuje instalaci do clusteru pro zajištění maximální dostupnosti služeb

1.16. Systém zvládá správu systému i pomocí přenosových cest se sníženou propustností (WAN, DSL, VPN)

1.17. Systém používá šifrovací mechanismy v souladu se standardem FISP 140-2

2. Automatická správa hesel splňuje následující požadavky:

2.1. Hesla privilegovaných účtů (dále jen hesla) jsou uložena v oddělených složkách. Pro každou složku lze nastavit rozdílnou politiku a oprávnění uživatele.

2.2. Lze definovat oprávnění uživatele k danné složce, zejména:
- zobrazit hesla ve složce
- použít hesla ve složce, bez možnosti je zobrazit
- vynutit změnu hesla nebo ručně zadat nové heslo
- vkládat nová hesla
- prohlížet auditní logy
- definovat oprávnění uživatele k danné složce

2.3. Politiky hesel umožňují k dané složce nastavit:
- maximální dobu platnosti hesla a dobu platnosti hesla po jeho použití
- minimální délku hesla
- znakové sady pro vytváření hesel

2.4. Systém podporuje definování centrální politiky pro nastavení hesel všech podporovaných platforem

2.5. Systém umožňuje nastavit pro daná hesla jejich automatickou změnu po ukončení jejich platnosti, jak ve vlastní složce, tak ve spravovaném systému.

2.6. Lze ručně zadat heslo pro jednotlivé účty i pro definovatelnou skupinu účtů.

2.7. Před použitím hesla z definované složky, je do logu zapsán důvod použití administrátorem spravovaného systému.

2.8. Před použitím hesla z definované složky, je nutné schválení alespoň jedním dalším uživatelem z definované skupiny (schvalovací proces). Schvalování je možné i z mobilních zařízeních s OS Blackberry 6.0 a vyšší a iPhone OS ve verzi 4.0 a vyšší.

2.9. Systém kontroluje platnost hesla vůči heslu ve spravovaném systému v nastavitelném intervalu s možností emailové notifikace v případě rozdílů.

3. Funkcionality vůči spravovaným systémům

3.1. Systém podporuje automatickou správu hesel následujících systémů:
- Windows 2003 a Windows 2008 R2, které jsou nebo nejsou součástí MS domény
- RedHat Linux 5.7 a vyšší , Solaris 5.10, HP-UX B.11.31, Linux Debian
- DB Oracle 8.1.7.4.1 a vyšší, DB MSSQL 2005 a vyšší
- HPILO, DellDRAC
- VMware ESX/ESXi 4.1 a vyšší

3.2. Systém, s využitím uloženého hesla, připojí oprávněného uživatele:
- k OS Unix/Linux protokolem SSH, otevřením terminálového okna a aplikace Putty
- k OS Unix/Linux s využitím aplikace WinSCP
- k OS Windows protokolem RDP otevřením vzdálené plochy spravovaného systému. Takto vytvořené připojení má přístup k lokálním úložištím klientského zařízení (HDD, CD, Flash, atd.)
- k DB s využitím aplikace SQL Plus
- k HPILO pomocí protokolu HTTPS otevřením webového prohlížeče IE 8.0
- k DellDRAC pomocí protokolu HTTPS otevřením webového prohlížeče IE 8.0
- k VMware vCenter a ESX/ESXi 4.1

3.3. Systém dále musí umět:
- použít heslo pro oprávněného uživatele při nastavovování naplánované úlohy (Scheduled Tasks) v OS Windows
-

3.4. Systém zajišťuje, prostřednictvím API, bezpečný přístup aplikací do systému dle nastavených oprávnění s možností vyzvednutí hesla. API je dodáno pro programovací jazyky:
- Java
- C/C++
- Bash shell skripty

Příloha č. 3

Bezpečnostní požadavky objednatele

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB") budou vstupovat nebo vjíždět pouze jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu, schváleném ČNB (dále jen „seznam"). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam poskytovatel předloží ČNB nejpozději v den podpisu smlouvy.

2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti pracovníků poskytovatele. Součástí seznamu je „Prohlášení o získání souhlasu subjektů osobních údajů se zpracováním osobních údajů v ČNB ve smyslu zákona č.101/2000 Sb., o ochraně osobních údajů". Poskytovatel v něm prohlásí a nese odpovědnost za to, že jeho zaměstnanci uvedení v seznamu vydali souhlas se zpracováním osobních údajů Českou národní bankou v rozsahu: jméno, příjmení a číslo průkazu totožnosti. Důvodem předání těchto osobních údajů je zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB.

3. Požadavky na případné doplňky a změny schváleného seznamu pracovníků poskytovatele je nutno neprodleně oznámit ČNB. Případné doplňky a změny podléhají schválení ČNB. Osoby neschválené ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.

4. Při příchodu do objektů ČNB zaměstnanci poskytovatele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny na seznamu, nebudou do objektu ČNB vpuštěny.

5. Schválení pracovníci poskytovatele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci poskytovatele budou do prostorů ČNB vstupovat a v těchto prostorách se pohybovat v režimu návštěv, to znamená vždy pouze v doprovodu zaměstnance ČNB nebo zaměstnance referátu bankovní policie ČNB. Pracovníci poskytovatele se budou v rámci objektů ČNB pohybovat pouze v pracovním oděvu s viditelným a nesnímatelným označením („logem") poskytovatele.

6. V případě mimořádné události se pracovníci zaměstnanci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícím zaměstnancem ČNB a dále instrukcemi vyhlašovanými vnitřním rozhlasem.

7. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom co je a není nebezpečný předmět rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.

8. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.

9. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.

10. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací, dozorujícího zaměstnance ČNB. Dále se pracovníci poskytovatele musí zdržet poškozování či zcizení

majetku ČNB, a dále zdržet se nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.

11. Pracovníci poskytovatele uvedení na seznamu se musí před započetím výkonu práce v objektech ČNB prokazatelně seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifikami daných objektů ČNB (např. způsob vyhlášení požárního poplachu, určení ohlašovny požáru, seznámení s únikovými cestami, poplachovými směrnicemi, evakuačním plánem, umístěním věcných prostředků požární ochrany apod.). ČNB je oprávněna kdykoliv podrobit kontrole kterékoliv pracovníka poskytovatele uvedeného na seznamu z dodržování těchto předpisů a ustanovení.