SPRÁVA ŽELEZNIČNÍ
DOPRAVNÍ CESTY

Smlouva o dílo

Číslo smlouvy objednatele. 43087/2019-SŽDC-GŘ-O8
Číslo smlouvy zhotovitele. ---

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

Objednatel: **Správa železniční dopravní cesty, státní organizace**
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384
Praha 1 - Nové Město, Dlážděná 1003/7, PSČ 110 00
IČO 70994234, DIČ CZ70994234
zastoupená Bc. Jiřím Svobodou, MBA, generálním ředitelem

Zhotovitel: **Dimension Data Czech Republic s.r.o.**
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. C 77064
Sídlo: Milevská 2095/5, 140 00 Praha 4
IČO 26175738, DIČ CZ26175738
Bankovní spojení: XXX
Číslo účtu: XXX
Zastoupená Ing. Petrem Hüblem, jednatelem

Tato smlouva je uzavřena na základě výsledků zadávacího řízení veřejné zakázky s názvem „**82100 – Implementace Privileged Account Managementu**", č. j. veřejné zakázky: 29906/2019-SŽDC-GŘ-O8 (dále jen „veřejná zakázka"). Jednotlivá ustanovení této Smlouvy tak budou vykládána v souladu se zadávacími podmínkami veřejné zakázky.

1 Dílo

1.1 Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro Objednatele Dílo, jež zahrnuje zhotovení Předmětu díla, poskytnutí všech Souvisejících plnění a předání Dokladů.

2 Předmět díla

2.1 Předmětem díla je Implementace Privileged Account Managementu v prostředí SŽDC, s.o. dle legislativních požadavků zákona č. 181/2014 Sb., tzv. „Zákon o kybernetické bezpečnosti" a jeho prováděcích předpisů zejména vyhlášky 82/2018, § 12, § 19 a § 20. Dále je předmětem nasazení na systémy a prvky v prostředí infrastruktury SŽDC, s.o. Cílem projektu je správa a zabezpečení přístupů privilegovaných uživatelů k administrovaným systémům.
2.2 Bližší specifikace předmětu plnění (technická specifikace) je přílohou č. 1 této smlouvy.
2.3 Požadavky na projektové řízení jsou specifikovány v příloze č. 2 této Smlouvy.
2.4 Objednatel požaduje dodání harmonogramu projektu, který bude členěný na milníky uvedené v příloze č. 2 této Smlouvy. Harmonogram bude Zhotovitelem předložen při prvním zahajovacím zasedání Řídícího výboru, který jej schválí, nejpozději však musí být Zhotovitelem předložen do pěti pracovních dnů od nabytí účinnosti této smlouvy. Objednatel požaduje, aby dodaný harmonogram projektu obsahoval nejméně tyto neměnné akceptovatelné části:

- Iniciace (start projektu, tým, nastavení)
- Analýza (komplexní analýza řešení)
- Návrh řešení (kompletní zadávací dokumentace pro řešení)
- Implementace (detailní rozpis jednotlivých kroků implementace)
- Fat (Funkční akceptační test)
- Uat (Uživatelské akceptační)
- Nasazení (Nasazení do ostrého provozu)
- Dokončení (finalizace projektu, odevzdání dokumentace, zdrojových kódů apod.)

2.5 Veškeré podmínky pro provedení Předmětu díla jsou uvedeny v Příloze č. 1 této Smlouvy.

3 Cena díla

3.1	Cena bez DPH	11 323 000,- Kč.
3.2	Výše DPH 21%	2 377 830,- Kč.
3.3	Cena včetně DPH	13 700 830,- Kč.

3.4 Fakturace bude provedena po dokončení celého Předmětu díla na základě faktury vystavené Zhotovitelem a předáním předmětu díla v rámci akceptačního řízení, na základě akceptačního protokolu, podepsaného oběma smluvními stranami. Průběh akceptačního řízení a náležitosti akceptačního protokolu jsou uvedeny v příloze č. 2 této Smlouvy.

4 Místo a doba plnění

4.1 Místem plnění je sídlo SŽDC, Dlážděná 1003/7, 110 00 Praha 1 – Nové Město a jednotlivé organizační složky SŽDC na území ČR.

4.2 Zahájení plnění Předmětu díla je od účinnosti této Smlouvy.

4.3 Zahájení akceptačního řízení Implementační analýzy: do 3 měsíců od účinnosti této Smlouvy

4.4 Zhotovitel je povinen provést Dílo nejpozději do 9 měsíců od akceptace Implementační analýzy.

4.5 Objednatel je oprávněn v průběhu doby plnění, vždy po dokončení jednotlivých fází Předmětu díla, danou dokončenou část Předmětu díla řádně otestovat. Po úspěšně provedeném testu (v případě, že byl proveden), Objednatel v rámci akceptačního řízení dokončenou část Předmětu díla schválí. Průběh testování a akceptačního řízení je uveden v Příloze č. 1 a Příloze č. 2 této Smlouvy. Zhotovitel je povinen k výše uvedenému poskytnout Objednateli veškerou součinnost.

5 Záruční doba

5.1 Záruční doba činí 24 měsíců.

6 Poddodavatelé a realizační tým

6.1 Na provedení Díla se budou podílet poddodavatelé uvedení v příloze č. 3 této Smlouvy.

7 Licenční podmínky

7.1. V případě, že výsledkem činnosti dle uzavřené Smlouvy bude Dílo podléhající režimu zákona číslo 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským
a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „autorský zákon"), uděluje Zhotovitel Objednateli licenci k tomuto Dílu dle ustanovení Občanského zákoníku.

7.2. Zhotovitel poskytuje Objednateli převoditelnou, nevýhradní, teritoriálně a co do množství neomezenou licenci na celou dobu trvání autorských a majetkových práv. Ve stejném rozsahu poskytuje Zhotovitel Objednateli licenci i k části Díla, lze-li část Díla užít samostatně. Objednatel není povinen licenci využívat.

7.3. Zhotovitel poskytuje tuto licenci bezúplatně. Tato licence opravňuje Objednatele k tomu, aby:

a) bez omezení využíval Dílo v rámci své podnikatelské činnosti,

b) si pořídil neomezený počet kopií Díla pro vlastní potřebu,

c) aby sám nebo prostřednictvím třetích osob měnil, rozšiřoval a jinak upravoval Dílo v souladu se svými potřebami, to však jen s předchozím písemným souhlasem Zhotovitele.

7.4. Objednatel je oprávněn převést licenci na třetí osoby pouze v případě předchozí písemné dohody Objednatele se Zhotovitelem.

7.5. Při uplatnění práv třetí osobou na autorská práva nese následky případných sporů Zhotovitel.

7.6. Zhotovitel prohlašuje, že je oprávněn poskytnout výše uvedenou licenci, že má s autorem Díla vypořádána autorská práva. V případě porušení tohoto odstavce, se Zhotovitel zavazuje zaplatit smluvní pokutu Objednateli ve výši 2.000.000,-- Kč. Právo na náhradu škody přesahující smluvní pokutu není ujednáním o smluvní pokutě dotčeno.

7.7. Není-li Zhotovitel na výzvu Objednatele ochoten uzavřít Smlouvu na další přiměřený rozvoj softwarového Díla dle požadavků Objednatele a na údržbu softwarového Díla za přiměřených podmínek a obvyklých cen ve lhůtě 2 měsíců od doručení výzvy Objednatelem, je povinen předat Objednateli zdrojové kódy aktuální verze softwarového Díla, a to do 90 dnů od marného uplynutí lhůty k uzavření Smlouvy.

7.8. Body 7.1. - 7.7. této Smlouvy plně nahrazují body 165-170 Obchodních podmínek.

8 Další ujednání

8.1 Zhotovitel prohlašuje, že je způsobilý k řádnému a včasnému provedení Díla a že disponuje takovými kapacitami a odbornými znalostmi, které jsou třeba k řádnému provedení Díla.

8.2 Kontaktními osobami smluvních stran jsou

8.2.1 za Objednatele XXX, tel. XXX, email: XXX,
za Zhotovitele XXX, tel. XXX, email: XXX.

8.3 Smluvní strany berou na vědomí, že tato Smlouva podléhá uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „ZRS"), a současně souhlasí se zveřejněním údajů o identifikaci Smluvních stran, předmětu Smlouvy, jeho ceně či hodnotě a datu uzavření této Smlouvy.

8.4 Zaslání Smlouvy správci registru smluv k uveřejnění v registru smluv zajišťuje obvykle Objednatel. Nebude-li tato Smlouva zaslána k uveřejnění a/nebo uveřejněna prostřednictvím registru smluv, není žádná ze Smluvních stran oprávněna požadovat po druhé Smluvní straně náhradu škody ani jiné újmy, která by jí v této souvislosti vznikla nebo vzniknout mohla.

8.5 Smluvní strany výslovně prohlašují, že údaje a další skutečnosti uvedené v této Smlouvě, vyjma částí označených ve smyslu následujícího odstavce této Smlouvy, nepovažují za obchodní tajemství ve smyslu ustanovení § 504 Občanského zákoníku (dále jen „obchodní tajemství"), a že se nejedná ani o informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS.

8.6 Jestliže Smluvní strana označí za své obchodní tajemství část obsahu Smlouvy, která v důsledku toho bude pro účely uveřejnění Smlouvy v registru smluv znečitelněna, nese tato Smluvní strana odpovědnost, pokud by Smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, která ze stran Smlouvu v registru smluv uveřejnila. S částmi Smlouvy, které druhá Smluvní strana neoznačí za své obchodní tajemství před uzavřením této Smlouvy, nebude Objednatel jako s obchodním tajemstvím nakládat a ani odpovídat za případnou škodu či jinou újmu takovým postupem vzniklou. Označením obchodního tajemství ve smyslu předchozí věty se rozumí doručení písemného oznámení druhé Smluvní strany Objednateli obsahujícího přesnou identifikaci dotčených částí Smlouvy včetně odůvodnění, proč jsou za obchodní tajemství považovány. Druhá Smluvní strana je povinna výslovně uvést, že informace, které označila jako své obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504 občanského zákoníku, a zavazuje se neprodleně písemně sdělit Objednateli skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

8.7 Osoby uzavírající tuto Smlouvu za Smluvní strany souhlasí s uveřejněním svých osobních údajů, které jsou uvedeny v této Smlouvě, spolu se Smlouvou v registru smluv. Tento souhlas je udělen na dobu neurčitou.

8.8 V případě poskytnutí osobních údajů v rámci plnění Smluvního vztahu se zhotovitel zavazuje přijmout vhodná technická a organizační opatření podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně

fyzických osob v souvislosti se zpracováním osobních údajů, které se na něj jako na zhotovitele vztahují a plnění těchto povinností na vyžádání doložit objednateli.

9 Závěrečná ujednání

9.1 Tato Smlouva se řídí Obchodními podmínkami ke Smlouvě o dílo (dále jen „Obchodní podmínky"). Odchylná ujednání ve Smlouvě o dílo mají před zněním Obchodních podmínek přednost.

9.2 Zhotovitel prohlašuje, že

9.2.1 se zněním Obchodních podmínek se před podpisem této Smlouvy seznámil,

9.2.2 v dostatečném rozsahu se seznámil s veškerými požadavky Objednatele dle této Smlouvy, přičemž si není vědom žádných překážek, které by mu bránily v poskytnutí sjednaného plnění v souladu s touto Smlouvou.

9.3 Tato Smlouva je sepsána ve třech vyhotoveních, přičemž jedno vyhotovení obdrží Zhotovitel a dvě vyhotovení Objednatel.

9.4 Veškerá práva a povinnosti Smluvních stran vyplývající ze Smlouvy o dílo a Obchodních podmínek se řídí českým právním řádem.

9.5 Smluvní vztahy neupravené Smlouvou o dílo a Obchodními podmínkami se řídí Občanským zákoníkem a dalšími právními předpisy.

9.6 Všechny spory vznikající ze Smlouvy o dílo a v souvislosti s ní budou dle vůle Smluvních stran rozhodovány soudy České republiky, jakožto soudy výlučně příslušnými.

9.7 Smlouvu o dílo lze měnit pouze písemnými dodatky.

9.8 Poté, co Zhotovitel poprvé obdrží spolu se Smlouvou o dílo i Obchodní podmínky v písemné formě, postačí pro veškeré další případy Smluv o dílo mezi Smluvními stranami pro to, aby se Smlouva o dílo řídila Obchodními podmínkami, pokud Smlouva o dílo na Obchodní podmínky pouze odkáže, aniž by bylo třeba Obchodní podmínky činit fyzickou součástí vyhotovení Smlouvy o dílo, neboť Zhotoviteli již bude obsah Obchodních podmínek známý.

9.9 Pokud některá ustanovení Obchodních podmínek nebo jejich část nelze vzhledem k povaze Díla objektivně a zcela zřejmě použít, pak z takových ustanovení nebo jejich částí práva ani povinnosti Smluvním stranám nevznikají.

9.10 Zvláštní podmínky, na které odkazuje Smlouva o dílo, mají přednost před zněním Obchodních podmínek, Obchodní podmínky se užijí v rozsahu, v jakém nejsou v rozporu s takovými zvláštními podmínkami.

9.11 Tato Smlouva nabývá platnosti okamžikem podpisu poslední ze Smluvních stran. Je-li Smlouva uveřejňována v registru smluv, nabývá účinnosti dnem uveřejnění v registru smluv, jinak je účinná od okamžiku uzavření.

Přílohy

1. Bližší specifikace předmětu díla (Technická specifikace)
2. Požadavky na projektové řízení
3. Seznam poddodavatelů

V Praze dne 15. 8. 2019

Bc. Jiří Svoboda, MBA v. r.

Za Objednatele
Bc. Jiří Svoboda, MBA
generální ředitel

V Praze dne 21. 8. 2019

Ing. Petr Hübl v. r.

Za Zhotovitele
Ing. Petr Hübl
jednatel

Tato Smlouva byla uveřejněna prostřednictvím registru smluv dne …

SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY

Příloha č. 1 Smlouvy o dílo

PAM
Privileged Account Management

Technická specifikace

Obsah

1 Obecná specifikace

Široké využívání stále rozsáhlejších informačních systémů, virtualizace a cloudu, a neustále rostoucí dynamika dnešních výpočetních prostředí zvyšují jak důležitost, tak i složitost dlouho známého problému: zabezpečení a audit přístupu uživatelů k privilegovaným účtům včetně efektivní správy a ochrany hesel. Řízení přístupu k privilegovaným účtům vytváří v rámci současné heterogenní informační infrastruktury (síťové prvky, servery, aplikace, databáze, koncové stanice atd.) dlouhodobý problém z hlediska bezpečnosti a shody s předpisy (zejména zákon č. 181/2014 Sb., tzv. „Zákon o kybernetické bezpečnosti") a jeho prováděcích předpisů.

IT prvky kritické infrastruktury jsou spravovány přes privilegované (správcovské) účty. Správci se přes ně dokáží přihlásit a provádět dohled, údržbu, měnit nastavení nebo odstraňovat technické závady. Pokud však privilegované přístupy nejsou zabezpečeny, jejich zneužití představuje velké riziko - útočník nebo insider může přes ně vyřadit systémy nebo převzít nad nimi kontrolu a tak vystavit organizaci velkým ztrátám.

Proto zabezpečení privilegovaných přístupů k IT prvkům kritické infrastruktury patří ke klíčovým bezpečnostním strategiím. Z těchto důvodů je třeba řídit přístupy a kontrolovat aktivity na privilegovaných účtech, provedené interními lidmi nebo dodavatelem.

Cílem veřejné zakázky je implementace Privileged Account Managementu v prostředí SŽDC, s.o. dle legislativních požadavků vyhlášky 82/2018, § 12, 19 a 20, zákona č. 181/2014 Sb a normy ČSN ISO/IEC 27001. Dále je předmětem veřejné zakázky nasazení na systémy a prvky v prostředí infrastruktury SŽDC, s.o. s cílem správy a zabezpečení přístupů privilegovaných uživatelů k administrovaným systémům.

1.1 Obecný popis přínosů po zavedení PAM:

Řešení musí umět poskytnout:

- **Ověření uživatelů** - všechny uživatele přistupující do IT infrastruktury musí být možné jednoznačně ověřit a každý přístup musí být personalizovaný konkrétní osobě. Uživatele je třeba ověřit dvěma faktory - např. heslem a tokenem nebo čipovou kartou.
- **Řízení přístupových práv** - definice přístupových oprávnění, tzn . jaký uživatel může přistupovat ke kterým systémům, za jakých okolností a na základě jakého pověření. Je nutná pravidelná revize oprávnění. Při ukončení důvodu oprávnění k přístupu, je nutné okamžitě odejmout přístupová oprávnění.
- **Schvalování přístupu** - pokud je vyžádán vzdálený přístup, je nutné ho ohraničit časem a zadat důvod přístupu. Odpovědná osoba (např. Bezpečnostní manažer nebo supervizor, vlastník systému) musí přístup schválit nebo zamítnout. Workflow by mělo být automatizované přes e-mail nebo manuálně přes web.
- **Řízení hesel** - pro prvky v IT infrastruktuře je třeba vynucovat dodržování bezpečnostních politik pro přihlašovací údaje k privilegovaným účtům (komplexnost hesla, periodicita výměny hesel, unikátnost). Výměny hesel by měly být zautomatizované pro zamezení chybovosti. Hesla k privilegovaným účtům jsou bezpečně uloženy a poskytovány pouze pověřeným osobám.
- **Izolace připojení** - počítače správců jsou často připojeny na internet a tak představují riziko, že na nich může být škodlivý kód. Proto pro připojení k IT infrastruktuře je třeba využít bezpečný skok přes tzv. jump server. Ten je důsledně chráněn a plně pod kontrolou organizace. Jump server ověří uživatele a bezpečně ho přihlásí na prvek IT infrastruktury bez toho, aby uživatel zadával heslo. Jediná data, která "protékají" z přistupujícího systému uživatele jsou pouze data periferii jako pohyb myši nebo stisky kláves na klávesnici. Výsledkem je plná izolace přistupujícího systému a tedy zamezení možnosti případné kompromitace cílového systému škodlivým kódem z přistupujícího systému a ukradení hesel.

- **Auditních stopa a záznam aktivit** - Všechny přístupy, schválení, udělení oprávnění musí být nezpochybnitelně zaznamenány. Aktivity správců na prvcích IT infrastruktury jsou nahrávány ve video formátu a s textovými přepisy pro kontrolu změn. Systém umožňuje i živé sledování aktivit - pro případnou kontrolu čtyř očí. Zároveň systém by měl upozorňovat na podezřelé aktivity a zneužití oprávnění v prvcích kritické infrastruktury.
- **Naplnění podmínky zákona o kybernetické bezpečnosti** - zákon č. 181/2014 Sb a normy ČSN ISO/IEC 27001.

1.2 Zkratky a pojmy

SŽDC	Správa železniční dopravní cesty, státní organizace
PAM	Privileged Account Management
MS AD, AD	Adresářová služba Microsoft Active Directory
WS	Webová služba
VPN	Virtuální privátní síť, prostředek k propojení několika počítačů prostřednictvím nedůvěryhodné počítačové sítě.
OTP	One-time password, jednorázové heslo, je heslo, které je platné pouze pro jedno přihlášení nebo pro nějakou transakci.
Hypervizor	Virtual Machine Monitor, Virtual Machine Manager, VMM je v informatice označení pro jednu z technik virtualizace hardwaru počítače, která umožňuje na jednom počítači spustit zároveň více operačních systémů.
PKI	PKI je v kryptografii označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie. PKI umožňuje pomocí přenosu důvěry používat cizí veřejné klíče a ověřovat jimi elektronické podpisy bez nutnosti jejich individuální kontroly.
Jump server	Způsob řízení privilegovaného přístupu, ze kterých je prováděna veškerá správa IT externími dodavateli nebo i interními administrátory.
Autentizace	Autentizace znamená potvrzení, že uživatel požadující služby je platným uživatelem poskytovaných síťových služeb. Autentizace je dosažena pomocí představení identity a jistého pověření nebo tajemství. Mezi různé typy tajemství patří například hesla, pověření na jedno použití, digitální certifikáty nebo telefonní čísla (ať už volající nebo volaná).
Autorizace	Autorizace znamená udělení specifického typu služby (včetně „žádné služby“) uživateli, na základě jeho autentizace, služeb, které požaduje a aktuálního stavu systému. Autorizace může být založena na omezeních, například omezení na určité hodiny v rámci dne, nebo omezení na fyzickou polohu, nebo omezení vícenásobného přihlášení jednoho uživatele. Autorizace určuje povahu služby, která je poskytnuta uživateli. Typy služeb jsou například: filtrování IP adres, přidělení adresy, přidělení cesty, QoS, řízení šířky pásma/řízení toku, tunelování do konkrétního koncového bodu, nebo šifrování.
RBAC, Role-Based Access Control	Model, ve kterém jsou uživateli přiřazeny role, které mu dávají určitý stupeň přístupu ke zdroji. Přiřazení role garantuje uživateli definovanou sadu entitlementů (nároků na oprávnění), které jsou přiřazeny buď automaticky, nebo po splnění určité podmínky, nebo na základě schválení odpovědnými osobami. Výhodou modelu RBAC je opětovná použitelnost přidělených rolí a možnost definování atributů role – např. popis.
HSM	Hardware security modul
SSO	Single Sign On

1.3 Systémové požadavky

- Podpora operačního systému Windows nebo Unix.
- Centrální zabezpečené úložiště dat (trezor)
- Řešení, které podporuje skriptovací jazyk.
- Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC.
- Řešení podporuje kódování UTF-8 i UTF-16.

1.4 Licence a další požadavky

- Zadavatel požaduje, aby počet licencí byl do budoucna bez omezení ve všech těchto aspektech:
  1. Oddělení testovacího, vývojového a produkčního prostředí
  2. Podpora až 10 000 uživatelů
  3. Neomezené počty koncových systémů
  4. Neomezené počty jump serverů,
  5. Neomezené počty procesorových jader, velikost paměti a jiných hardwarových, softwarových či aplikačních parametrů.

- Zadavatel požaduje možnost připojení budoucích nových systémů a vložení jejich přístupových rolí a logiky do systému PAM bez dodatečných licenčních nákladů.
- Dodavatel se zaručuje, že v dodávce jsou zahrnuty licence třetích stran (např. licence Microsoft RDS nebo podobné) a používání díla jako celku nevyžaduje žádné další dodatečné náklady.
- Dodavatel se zaručuje, že při používání systému PAM v souladu s licenčními podmínkami, pokud dojde k uplatnění práv třetí osobou na autorská práva nese následky případných sporů dodavatel.

- Licence opravňuje zadavatele k tomu, aby:
  1. Bez omezení využíval dílo v rámci své podnikatelské činnosti
  2. Pořídil si počet kopií díla pro vlastní potřebu dle zakoupené licence

2 Technické požadavky

2.1 Obecné požadavky na uživatelské rozhraní v PAM

Nabízené řešení musí mít Webové rozhraní pro administrátory i pro koncové uživatele.

2.2 Autoritativní zdroje dat

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

- Zdroj pro komunity: interní a externí uživatelé, apod.
- Možnosti napojení: např. CSV import, LDIF import, webové služby, Rest API
- Z bezpečnostních důvodů nepředpokládáme přímý přístup do DB
-

2.3 Active Directory

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

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

2.4 Určení typu privilegovaných uživatelů podle způsobu jejich přístupu

Vzhledem k tomu, že k privilegovaným účtům v rámci sítí SŽDC přistupují jak interní uživatelé, tak uživatelé externí (přes VPN), musí být řešení schopno obě tyto varianty pokrýt.

2.4.1 Externí přístup (VPN, atd.)

Externí přístup musí být řešením podporován minimálně na úrovni VPN, a to tak, že VPN spojení umožní externím privilegovaným uživatelům přístup pouze k PAM řešení, a nikoliv přímo k privilegovaným účtům ve spravovaných systémech. Tím se zajistí, že všechny uživatelské relace spojené s privilegovanými účty budou procházet přes PAM řešení, a bude tak možné je auditovat a monitorovat. PAM řešení musí být distribuované co nejblíže k požadovaným systémům, aby případná nekryptovaná komunikace probíhala po co nejkratší trase/lince.

2.4.2 Přístup z interní sítě

Pro přístup k řešení PAM z interní sítě je vyžadována podpora webového klienta případně doplněná klientskou aplikací podporující běžné operační systémy, tedy Windows, Linux/Unix, MacOS. PAM řešení musí umožnit instalaci klientské aplikace, včetně jejích různých verzí, do tohoto řešení a přístup uživatele přes takto instalovanou aplikaci.

2.4.3 Autentizace uživatelů ke jmenným účtům

Pro přístup do PAM řešení musí být zajištěna podpora minimálně dvoufaktorové autentizace na bázi jednorázových hesel (OTP) a digitálních certifikátů (PKI). Preferovaná je také možnost rozšíření autentizace o tzv. „risk-based" autentizaci, tedy o analýzu rizika autentizace každého uživatele na bázi kontextu (čas, lokalita, rychlost, atd.)

Ve všech případech musí být řešení schopno autentizovat uživatele vůči záznamům v několika, do PAM řešení připojených, MS Active Directory doménách. Jednotlivé „sejfy" pro hesla musí být

logicky odděleny tak, aby byla zajištěna segregace rolí. Systém musí generovat detailní auditní logy o přístupu k sejfům, heslům či dalším údajům uloženým v sytému.

2.4.4 Analýza rizika

S ohledem na vysokou citlivost a kritičnost systémů v rámci sítě SŽDC musí řešení také podporovat rizikovou analýzu chování uživatele během celé uživatelské relace, a v případě detekce nestandardního chování buď upozornit odpovědnou osobu, nebo přímo danou relaci vynuceně ukončit.

2.5 Oblasti pokrytí

Správa železniční dopravní cesty provozuje dva typy sítí – uživatelskou (administrační) a technologickou. Do obou sítí jsou připojeny standardní systémy, jako jsou síťové a bezpečnostní prvky, servery s aplikacemi a databázemi, síťová úložiště, uživatelské stanice (desktopy), apod. Technická síť navíc obsahuje specifické řídicí systémy, ke kterým existuje administrátorský přístup pomocí klientských aplikací.

Cílem nasazení řešení PAM je zabezpečení privilegovaného / administrátorského přístupu a jeho audit a monitoring na obou zmíněných sítích. V případě uživatelské (administrační) sítě je do systému třeba integrovat přibližně 300 systémů a 300 uživatelských stanic, v případě technické sítě více než 10 000 prvků.

S ohledem na integraci do obou sítí musí řešení PAM podporovat řízení přístupu k privilegovaným účtům na systémech a síťových prvcích používaných v rámci SŽDC, zejména:

- Windows
- Unix / Linux
- Cisco (lokální či TACACS ověřování)
- Oracle
- MS SQL

Z pohledu komunikačních protokolů a typů připojení se jedná o podporu:

- SSH
- Telnet
- RDP, RDP Application
- HTTP/S
- Tlustého klienta

2.5.1 Uživatelská / administrační síť

V této síti nyní pracuje přibližně 300 privilegovaných uživatelů přistupujících z interní sítě a zhruba dalších 300 externích uživatelů přistupujících přes VPN. Celkové množství budoucích privilegovaných uživatelů této sítě je tedy 600 s tím, že v rámci aktuální poptávky Zadavatele bude licenčně pokryto 75 uživatelů.

2.5.2 Technologické sítě

S ohledem na velké množství řídicích systémů zapojených do této sítě, a s ohledem na jejich specifičnost a nestandardní způsoby přístupu, předpokládá SŽDC připojení těchto systémů do řešení PAM pomocí několika tzv. „jump serverů". Tyto „jump servery" budou přímo integrovány s řešením PAM, a jejich prostřednictvím budou uživatelé přistupovat k cílovým řídicím systémům v technické síti. Vzhledem k potřebě rozložení přístupu v rámci ČR bude potřeba do budoucna vybudovat několik desítek kusů těchto „jump serverů".

Zmíněné „jump servery" budou založeny na OS Windows nebo Linux/Unix, a na nich bude po přihlášení konkrétního uživatele spuštěna klientská aplikace, pro přístup k cílovým systémům. Pro

připojení uživatele k Windows „jump serverům" předpokládá SŽDC připojení pomocí protokolu RDP či SSH, a z „jump serverů" k cílovým systémům protokolem využívaným danou klientskou aplikací. Pro připojení uživatele k Linux/Unix „jump serverům" předpokládá SŽDC připojení pomocí protokolu ssh, a z „jump serverů" k cílovým řídicím systémům primárně pomocí protokolu ssh, ale v odůvodněných případech je přípustný Telnet.

Celkové množství budoucích privilegovaných uživatelů technologických sítí (vč. externích organizací) je cca 600 s tím, že v rámci aktuální poptávky Zadavatele bude licenčně pokryto 75 uživatelů.

2.6 Privilegované účty a požadavky na jejich pokrytí jednotlivými funkcemi

2.6.1 Centralizované úložiště přihlašovacích údajů

Implementované řešení musí do budoucna umožňovat zavedení více centralizovaných šifrovaných úložišť přihlašovacích údajů pro systémy a privilegované účty, a to pro několik na sobě nezávislých sítí, či pro každý její izolovaný segment. Úložiště musí být jediným místem k ukládání, auditovanému využívání, a řízení životního cyklu přihlašovacích údajů. To je naprosto zásadní pro okamžitou eleminaci nebezpečných metod ukládání hesel (jako jsou například tabulky aplikace Excel), které usnadňují jejich sdílení a případné zneužití. „Trezor hesel", jak se také občas takové úložiště nazývá, musí být zabezpečeno silným šifrováním. Výhodou je shoda s bezpečnostním standardem FIPS 140-2, případně možnost připojení HSM (hardware security modulu) pro bezpečné uložení šifrovacích klíčů a tím povýšení na maximální možnou úroveň bezpečnosti.

S ohledem na ochranu šifrovacích klíčů je vhodné, aby řešení umělo kryptograficky ochránit šifrovací klíče v době, kdy se používají (tj. v paměti), což zabrání útočníkům v zachycení a poskládání klíčů při monitorování standardních rozhraní a paměti. Tato metoda je výrazně účinnější než slabší alternativy založené např. na dělení klíčů a jejich jednoduchém maskování.

2.6.2 Řízení životního cyklu hesel a SSH klíčů

Řešení musí nabízet automatizované a na pravidlech založené vytváření, používání a pravidelnou obměnu hesel a SSH klíčů, a tím eliminovat vytváření slabých hesel nebo jejich opakované používání. Měla by být možnost flexibilně nastavit politiky a vynutit tak dostatečnou složitost hesel podle bezpečnostní politiky a možností vybraných koncových systémů, implementovat automatické obnovování hesel – například v závislosti na čase (např. každý den nebo každý týden) nebo v reakci na určitou událost (např. po každém použití) – a řídit jejich používání (např. povolit přístup pouze v určených časových oknech nebo vyžadovat dvojité či vícenásobné ověřování při přístupu k heslům). Politiky by mělo být možné používat na celé skupiny koncových systémů najednou s tím, že přidáním systému do skupiny se na něj automaticky tyto politiky aplikují.

Ačkoli SSH klíče nejsou hesly v tradičním smyslu, fungují velmi podobně a jsou vystaveny také podobným rizikům a hrozbám, jako jsou kopírování, sdílení, nechtěné prozrazení a neauditovaná zadní vrátka. Protože se tyto klíče často vkládají přímo do kódu nebo jsou používány transparentně, aby uživatelé nebyli zatěžováni jejich relativní složitostí, jsou také více ohroženy zastaráním nebo zcizením. Je proto logické na tyto klíče uplatnit stejné postupy, které se používají pro správu a ochranu hesel. Mezi doporučené postupy pro odvrácení souvisejících rizik proto patří:

- přesunutí autorizovaných klíčů do chráněného úložiště,
- pravidelná výměna klíčů (pro zajištění ukončení přístupu v případě vyzrazeného klíče),

Za tím účelem by mělo řešení podporovat ověřování pomocí klíčů SSH a řízení jejich životního cyklu. Jinými slovy musí být možné tyto klíče bezpečně uložit, rotovat a určovat pro ně pravidla použití. Tím SŽDC zajistí, že i přihlašovací klíče lze získat a použít pouze způsobem, který minimalizuje rizika jejich odcizení nebo prozrazení.

2.6.3 Vyzvedávání hesel

Uložení privilegovaných přihlašovacích údajů do „trezoru hesel" je zbytečné, pokud neexistuje způsob jejich získání a použití. Prvním krokem tohoto procesu musí být silné ověření entity (ať už osoby, aplikace nebo skriptu), která se snaží uložené přihlašovací údaje použít. V tomto ohledu musí být řešení schopno využít existující autentizační infrastrukturu zadavatele včetně integrace adresářových služeb MS Active Directory. Pro budoucí integraci je nutné, aby řešení podporovalo standardizované autentizační protokoly (např. RADIUS a TACACS+) a podporovalo dvoufaktorovou autentizaci, digitální certifikáty, atd.

Po autentizaci a pouze v politikou jasně definovaných případech (např. havarijní stav) si může uživatel vyzvednout aktuálně platné heslo ke konkrétnímu účtu, a tímto heslem se k účtu přihlásit. S ohledem na bezpečnost a jednoznačnou osobní zodpovědnost musí PAM systém umožnit vygenerování a změnu hesla k takovému účtu buď před jeho vyzvednutím uživatelem a/nebo po jeho navrácení.

Každé vyzvednutí/vrácení hesla k účtu musí být zaznamenáno v auditním logu.

2.6.4 Automatické přihlašování uživatelů k privilegovaným účtům

V preferovaném provozním režimu předá systém přihlašovací údaje oprávněné entity (uživatele nebo aplikace) ze svého zabezpečeného úložiště přímo cílovému systému a automaticky ho tak autentizuje. Tento přístup s sebou nese několik bezpečnostních výhod. Za prvé, oproti běžným a výše popsaným řešením typu uložit/vyzvednout uživatel v tomto případě svá hesla vůbec neuvidí ani nezíská. Tím se výrazně snižuje riziko jejich vyzrazení. Navíc, protože ověření na cílovém systému je plně automatické a uživatelé si tedy nemusí pamatovat ani přepisovat svá hesla, je možné nastavit politiky s výrazně vyššími požadavky na složitost hesel. Protože pak veškerý přístup k cílovým systémům probíhá prostřednictvím systému, je možné zajistit dokonalou kontrolu nad aktivitami privilegovaných uživatelů, a to i pro sdílené privilegované účty typu „root" nebo „administrator".

A pro úplnost ještě dodejme, že veškerá síťová komunikace musí být šifrována, např. pomocí SSL.

Řešení musí umožňovat vývoj vlastních konektorů. Tím bude zajištěno automatické přihlašování k privilegovaným účtům pomocí tlustých klientů.

2.6.5 Nahrávání uživatelských relací a jejich metadat

Nahrávání uživatelských relací musí být nedílnou součástí řešení, a musí pokrývat všechny běžné protokoly a způsoby připojení k cílovým systémům, minimálně:

- SSH
- Telnet
- RDP
- Web

Nahrávky relací musí obsahovat také metadata o čase, uživateli, systému, privilegovaném účtu, případně další komentáře popisující videonahrávku, aby v nich bylo možno vyhledávat a filtrovat je podle potřebných kritérií. Textové (CLI) relace, zejména SSH a Telnet, musí umožňovat také vyhledávání dle zadaných příkazů a odpovědí systému, tedy tzv. „fulltext" vyhledávání. Výhodou může být řešení podporující vyhledávání dle metadat a komentářů v nahrávkách grafických relací, a to s realizací bez instalací agentů na koncové systémy. Případná hesla zadávaná uživateli v nahrávaných relacích nesmí být v nahrávkách viditelná.

Přístup k nahrávkám musí mít pouze oprávnění uživatelé, kteří mohou nahrávky prohlížet. Export musí být, jako důkazní materiál v trestním řízení či jako doklady pro správní orgán (NÚKIB), umožněn určeným osobám.

Nahrávky musí být zabezpečeny proti cílenému či náhodnému smazání, a musí mít možnost nastavení jejich řízeného vymazání z úložiště po uplynutí doby potřebné pro jejich úschovu.

2.6.6 Automatické vyzvedávání hesel pro technické účty

Lidé nejsou jedinými uživateli privilegovaných účtů. Ve většině organizací mají k citlivým prostředkům, například aplikacím nebo databázím, přístup také různé aplikace a skripty. To se typicky realizuje vestavěním příslušných přihlašovacích údajů přímo do kódu příslušné aplikace nebo jejich zpřístupněním za běhu prostřednictvím konfiguračních souborů a skriptů – ani jeden způsob ovšem není nijak zvlášť bezpečný. Proto musí řešení nabízet „privilegovaným aplikacím" dynamické získávání hesel stejně, jako to poskytuje klasickým uživatelům, a to minimálně na platformách Windows a Unix/Linux, tedy tam, kde se aplikace a skripty provozují.

V rámci zjednodušení integrace do prostředí SŽDC by měl PAM systém v této oblasti přímo podporovat alespoň Perl, PHP, Python a UNIX Shell skripty, Java aplikace, a případně další. Z tohoto důvodu preferujeme architekturu na bázi agentů na systémy s těmito skripty či aplikacemi, které vyzvedávání aktuálních hesel k technickým účtům bezpečně zprostředkují. Tyto agenti musí podléhat stejné politice pro získávání a implementaci opravných balíčků a nových verzí, jako jim podléhá vlastní PAM systém.

2.7 Integrace s dalšími částmi informačního systému

Řešení PAM musí být z důvodu maximální efektivity a bezpečnosti provozu schopno úzké integrace do informačního systému SŽDC, a to na několika níže uvedených úrovních.

2.7.1 HSM

Vzhledem k vysoké citlivosti dat zašifrovaných a uložených v „trezoru hesel" počítá SŽDC s uložením šifrovacích klíčů mimo vlastní PAM systémy, a to v externích HSM („hardware security modulech"), a to pro každou síť či její oddělený segment. Tím bude zajištěna maximální možná ochrana šifrovacích klíčů a potažmo tak přihlašovacích údajů k privilegovaným účtům v systémech.

Řešení PAM musí být integrovatelné s běžnými HSM systémy, případně takový systém přímo obsahovat.

2.7.2 SIEM

V rámci centralizace bezpečnostních událostí a incidentů z celého prostředí SŽDC pro jejich snadnější analýzu a korelaci bude řešení PAM v budoucnu integrováno do SIEM řešení („security information and event management"), ideálně pomocí standardního formátu syslog, a při zabezpečení této komunikace (např. pomocí IPsec). Řešení PAM musí být schopno logovat a zasílat všechny události spojené s administrací systému i s aktivitami jednotlivých privilegovaných uživatelů. Výhodou je možnost logovat a zasílat do SIEMu také všechny příkazy (a případně i odpovědi systémů) v rámci uživatelských relací.

2.7.3 Service Desk

U kritických systémů uvažuje SŽDC o povolení přístupu k privilegovanému účtu až na základě schválení tzv. „service ticketu", tedy žádosti o provedení servisního zásahu. Vzhledem k tomu, že se budou tyto žádosti zpracovávat mimo řešení PAM v servisní aplikaci („service desk"), je do budoucna žádoucí řešení PAM se service deskem integrovat. Tím bude umožněno automatické povolení přístupu uživatele k účtu v rámci řešení PAM ihned po schválení odpovědným pracovníkem service desku.

2.8 Architektura, způsob nasazení a provozu

2.8.1 Vysoká dostupnost

Správa přístupu k privilegovaným účtům je kritickým prvkem IT infrastruktury každé organizace. A platí to dvojnásob, když se implementace rozšíří o scénáře „aplikace-aplikace", které pracují zcela automatickým způsobem. Za tím účelem musí řešení PAM nabízet klastrování (ideálně „active-active") a rozdělování zátěže, aby bylo schopné se plně vyrovnat s požadavky na vysokou dostupnost a možnosti škálování i v náročném prostředí SŽDC. Tyto klastry by mělo být možné konfigurovat jako plně redundantní i v rámci geograficky rozdělených datových center.

Z důvodu požadavků SŽDC na budoucí pokrytí až 64 oddělených sítí bude nutné všechny tyto sítě vybavit potřebným počtem jump serverů.

2.8.2 Řešení havarijních stavů

Pro rychlé a efektivní řešení různých havarijních stavů musí být řešení PAM schopno pracovat nejen v módu vysoké dostupnosti, ale musí mít také možnost pravidelného automatického zálohování dat s možností jejich rychlé obnovy, tedy tzv. DR („data recovery").

2.8.3 Testovací prostředí

Pro možnost testování nových politik či jiných nastavení systému zadavatel požaduje oddělené testovací prostředí, aby při špatné konfiguraci či jiném zásahu nemohlo dojít k narušení funkčnosti a integrity produkčního prostředí. Testovací prostředí by mělo být navrženo v minimální variantě, napojené na testovací infrastrukturu SŽDC a pracující s testovacími účty.

2.8.4 Lidské zdroje

Řešení PAM se stane kritickou bezpečnostní bránou k celé informační a řídící infrastruktuře SŽDC, a musí proto být samo maximálně zabezpečeno z pohledu jeho uživatelů. Požadavkem na řešení PAM je takzvaný „role-based access control" (RBAC), ve kterém jsou přístupová oprávnění navázána na jednotlivé role (např. uživatel, administrátor, auditor), a uživatelé či jejich skupiny jsou na tyto role navázány. Přidáním uživatele do systému a přidělení role tak automaticky nastaví potřebná oprávnění, která pak není třeba zadávat ručně s rizikem neúmyslné či úmyslné chyby.

2.8.5 Uživatelé

Uživateli se v oblasti PAM rozumí administrátoři a jiné identity přistupující k privilegovaným účtům. V prostředí SŽDC se jedná celkem o 600 identit. Tato skupina může být dále dělena na skupiny uživatelů podle jejich zaměření (sítě, operační systémy, databáze, bezpečnost) a/nebo podle jejich oprávnění ke skupinám cílových systémů (Windows, Unix/Linux, Oracle, MS SQL, řídící prvky, atd.)

Uživatelé by obecně neměli mít oprávnění k administračním ani konfiguračním funkcím PAM systému, stejně jako by neměli mít oprávnění k přístupu k auditním údajům.

2.8.6 Administrace systému

Administraci a konfiguraci systému PAM bude v prostředí SŽDC provádět pouze omezené množství administrátorů (v řádu jednotek až desítek) s potřebnými znalostmi a oprávněními. Tito

administrátoři by neměli mít přístup k produkčním privilegovaným účtům na cílových systémech, a měli by v případě potřeby pracovat pouze s testovacími systémy a/nebo účty.

2.8.7 Audit relací, investigace incidentů

Auditní funkce, jako je prohlížení logů, videonahrávek relací apod., musí být přístupny pouze oprávněným uživatelům v rámci informační bezpečnosti a případně auditu.

2.9 Firemní pravidla

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

2.9.1 Politiky hesla

Nabízené řešení musí umožnit konfiguraci politiky hesel tak, aby byla v souladu s politikou hesel na SŽDC. Nastavení politiky hesel musí být plně konfigurovatelné.

Aktuální politika hesel je:

- Heslo má minimální délku 12 znaků, u privilegovaných účtů 19 znaků
- Password Complexity ve Windows 2012 R2/2016, popř. vyšší:
  - Heslo obsahuje alespoň tři z následujících čtyř požadavků:
    - nejméně jedno velké písmeno (A – Z),
    - nejméně jedno malé písmeno (a – z),
    - nejméně jednu číslici (0 – 9) nebo
    - nejméně jeden nealfanumerický znak (t.j. ~!@ #$%^&*_-+=`|\(){}[]:;"'<>,.?/).
  - Heslo nesmí obsahovat řetězec vlastního samAccountName (účtu), je-li jeho délka 3 a více znaků, bez ohledu na velká či malá písmena.
  - Heslo nesmí obsahovat název účtu (displayName, fullName), a to bez ohledu na velká či malá písmena. Všechny části názvu účtu oddělené mezerou nebo oddělovacími znaménky a delší než dva znaky se posuzují zvlášť.

2.10 Emailové notifikace

Nabízené řešení musí podporovat:

- Možnost definice šablon emailů s podporou vícejazyčnosti a HTML
- Možnost konfigurace parametrů odesílání zpráv (SMTP server apod.)
- Odesílání pomocí SMS gateway zadavatele, která je přístupná přes e-mail routing
- Vkládání hypertextových odkazů na konkrétní odkazované záznamy

2.11 Požadavky na dokumentaci

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

2.11.1 Dokumentace jádra systému

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

2.11.2 Příručka administrátora PAM

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

2.11.3 Uživatelská příručka

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

3 Další požadavky

3.1 GDPR

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

4 Rozsah dodávky poptávané Zadavatelem

Zadavatel požaduje dodat dílo v níže uvedeném rozsahu. Dodávka se tak skládá z dodávky licencí potřebných pro provoz řešení, HW pro instalaci komponent a implementace řešení tak, aby splňovalo uvedené požadavky. Tyto části dodávky díla jsou detailně rozepsané níže.

4.1 Licence pro užívání řešení

Zadavatel požaduje dodávku licencí dle následujících požadavků

- 150 uživatelských licencí
- Neomezený počet řízených hesel/systémů
- Bezpečné úložiště hesel v režimu vysoké dostupnosti (aktivní a záložní)
- Neomezený počet jump serverů
- Záruka (maintenance a support) na celé řešení po dobu 2 let (bez SLA)

pozn. Licence pro operační systémy zajišťuje Zadavatel

4.1.1 Dodávka HW

Je požadována dodávka HW pro následující komponenty řešení

- 2x centrální bezpečné úložiště v režimu vysoké dostupnosti (aktivní a záložní)
- 1x centrální webové rozhraní pro přístup uživatelů a administraci řešení + komponenta pro automatické vyhodnocování privilegovaných relací
- 2x jump server pro přístup k cílovým systémům ve 4 síťových prostředích

- 2x jump server s podporou přímého SSH spojení pro přístup k cílovým SSH/Telnet systémům ve 4 síťových prostředích
- 2x komponenta pro řízení hesel k cílovým systémům ve 4 síťových prostředích

Minimální požadavky HW serverů

Počet	Min. požadavky na HW Serveru
2ks	1288H V5, 2x Intel Xeon Silver 4110(2.1GHz/8-core/11MB/85W); 32GB RAM; 2x 300GB SAS hotswappable drives (15K RPM); RAID Controller; 2x Network adapter (1Gb); Out-Of-Band management; DVD ROM; 4x 1TB RAID 6 additional storage for PSM recordings;
1ks	1288H V5, 2x Intel Xeon Silver 4116(2.1GHz/12-core/16.5MB/85W); 64GB RAM; 2X 600GB; SAS hotswappable drives; RAID Controller; 4x Network adapter (1Gb); Out-Of-Band management
2ks	1288H V5, 2x Intel Xeon Silver 4112(2.6GHz/4-core/8.25MB/85W); 16GB RAM; 2X 300GB; SAS hotswappable drives; RAID Controller; 2x Network adapter (1Gb); Out-Of-Band management
2ks	1288H V5, 2x Intel Xeon Gold 6130(2.1GHz/16-core/22MB/125W); 32GB RAM; 2X 300GB SATA/SAS hotswappable drives (15K RPM); RAID Controller; 2x Network adapter (1Gb); Out-Of-Band management
2ks	1288H V5, 2x Intel Xeon Silver 4110(2.1GHz/8-core/11MB/85W); 32GB RAM; 2X 300GB SATA/SAS hot-swappable drives; RAID Controller; 2x Network adapter (1Gb); Out-Of-Band management

Pro dodané servery je požadována podpora na tři roky na místě instalace se SLA next business day, 4 hodiny.

pozn. HW pro ostatní komponenty nyní poptávaného řešení (tj. min. 6 serverů) zajišťuje Zadavatel

4.1.2 Implementace

Výsledkem implementace musí být řešení splňující požadavky na architekturu, kapacitní parametry a integrace se systémy zadavatele, uvedené v kapitole 4.1.2.1. a v Implementačním projektu. Implementační projekt musí současně splňovat náležitosti uvedené v kapitole 4.1.2.2

4.1.2.1 Požadavky na implementované řešení

- Architektura řešení
  - 2x centrální bezpečné úložiště v režimu vysoké dostupnosti (aktivní a záložní)
  - 1x centrální webové rozhraní pro přístup uživatelů a administraci řešení
  - 1x komponenta pro automatické vyhodnocování privilegovaných relací
  - 4x jump server pro přístup k cílovým systémům ve 4 síťových prostředích
  - 4x SSH jump server pro přístup k cílovým systémům ve 4 síťových prostředích
  - 4x komponenta pro řízení hesel k cílovým systémům ve 4 síťových prostředích

- Integrace na existující systémy zadavatele:
  - Active Directory pro autentizaci a autorizaci uživatelů
  - SMTP server pro zasílání emailových notifikací

- Integrace na následující typy cílových systémů (tj. schopnost automatického přihlášení a řízení hesel):

Oblast	Typ systému	Klientská aplikace	Komunikační protokol
Servery	MS windows	RDP klient	RDP
Servery	Unix/Linux	SSH klient	SSH

Databáze	Oracle	SQL Plus, TOAD	Oracle NET
Databáze	MSSQL	SQL Server Management Studio	TCP
Dálková diagnostika traťových systémů	Integrační server	Webový prohlížeč	HTTPS
Elektrodispečink	Inženýrská stanice	RDP klient	RDP
Diagnostika jedoucích kolejových vozidel	Kamerový systém I (Bosch)	Webový prohlížeč	HTTPS
Diagnostika jedoucích kolejových vozidel	Kamerový systém II (iVision)	Webový prohlížeč	HTTPS
Diagnostika jedoucích kolejových vozidel	Zapojovače	Webový prohlížeč	HTTPS
Diagnostika jedoucích kolejových vozidel	Rozhlasové ústředny	Webový prohlížeč	HTTPS
Infrastruktura	Cisco	SSH klient	SSH
Infrastruktura	Cisco	Telnet klient	Telnet

Kapacitní parametry poptávaného řešení:

- Řízení až 100 000 hesel v cílových systémech
- Provoz až 50 současných relací na jednom jump serveru
- Provoz až 200 současných relací na jednom jump serveru pro SSH
- Uložení nahrávek relací v objemu 300 hodin za den
- Uchování nahrávaných relací a auditních záznamů po dobu jednoho roku

4.1.2.2 Požadavky na implementační projekt

Implementační projekt musí obsahovat minimálně tyto neměnné akceptovatelné části

- Iniciace projektu
- Analýza
  - Identifikace požadavků na nasazení a používání řešení
- Návrh řešení
  - Architektura, umístění komponent, adresace
  - Síťové prostupy
    - Komunikační matice
  - Zabezpečení
    - Šifrování
    - Hardening
    - Řízení přístupů
    - Zálohování
  - Integrace na interní systémy zadavatele
    - LDAP pro autentizaci a autorizaci
    - SMTP pro emailové notifikace
  - Integrace na cílové systémy zadavatele
    - Identifikace klientských aplikací a jejich specifik
  - Způsoby použití
- Implementace
  - Instalace a konfigurace řešení dle schváleného návrhu
  - Vytvoření prototypů pro integraci na cílové systémy
  - Časový plán implementace a Termíny plnění (začíná běžet po schválení vypracovaného Implementačního plánu Zadavatelem)
- Fat (funkční akceptační test)
  - Testování jádra systému a integrací
- Uat (uživatelský akceptační test)
  - Testování integrací na cílové systémy

    - Testování způsobů užití
- Školení
    - Koncoví uživatelé (připojení ke koncovým systémům) v rozsahu 2 MD
    - Auditoři (ověření souladu, nahrávky, auditní záznamy) v rozsahu 2 MD
    - Administrátoři sejfů (správa hesel) v rozsahu 2 MD
- Nasazení (nasazení do ostrého provozu)
    - Podpora při zavedení hesel do systému
- Dokončení (finalizace projektu, odevzdání dokumentace apod.)

SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY

Příloha č. 2 Smlouvy o dílo

Požadavky na projektové řízení

1. Požadavky na projektové řízení

1.1. Zhotovitel se zavazuje, že dodávka díla bude řešena jako projekt a budou použity zásady řízení standardů projektového řízení, jako např.:

- Vytvoření komunikační matice a struktury řízení projektu;
- Jasně stanovené SMART cíle;
- Plánování pomocí projektového plánu a hierarchické struktury prací (WBS);
- Součástí harmonogramu jsou požadovány minimálně tyto milníky:
  - Analýza,
  - Kompletní návrh řešení,
  - Akceptace kompletního návrhu řešení,
  - Realizace;
- Změny pouze v rámci Změnového řízení s jasnými pravidly.

2. Požadavky na řízení a realizaci projektu

2.1. Řízení a realizace projektu budou zajištěny za pomoci:

2.1.1. **Koordinátora projektu (Objednatel)** – je pracovník jmenovaný Objednatelem, který je odpovědný za zajištění dohodnuté součinnosti Objednatele, zejména zajištění zdrojů a kapacit Objednatele potřebných pro řádné plnění projektu. Je odpovědný za aktivní spolupráci zaměstnanců Objednatele ve společných pracovních týmech a celkově řídí a spravuje procesy zajišťující plnění povinností Objednatele.

2.1.2. **Projektového manažera (Zhotovitel)** – je pracovník jmenovaný Zhotovitelem, který řídí práce na projektu. Je odpovědný za detailní plánování, koordinaci a kontrolu všech činností prováděných v rámci projektu. Zajišťuje administrativu spojenou s činností Řídicího výboru.

2.1.3. **Řídící výbor** – je vrcholný, rozhodovací a řídící orgán projektu. Členy Řídícího výboru jsou oprávněné osoby a další smluvními stranami jmenované osoby vybavené potřebnými kompetencemi rozhodovat v zásadních otázkách projektu a tato rozhodnutí prosadit v rámci své smluvní strany. Řádná zasedání Řídícího výboru se konají pravidelně, zpravidla jednou měsíčně. Předseda Řídícího výboru (sponzor projektu Objednatele) má v případě potřeby nebo na žádost kteréhokoli člena Řídícího výboru možnost svolat i mimořádné zasedání Řídícího výboru.

2.1.4. **Pracovní tým** – je výkonný orgán projektu. Je podřízen Řídícímu výboru, řízen je Projektovým manažerem, jehož rozhodnutí jsou závazná pro všechny členy, odpovídá za přípravu výstupů projektu, plánování, kontrolu plnění schváleného harmonogramu a další z něho vyplývající úkoly. Členy jsou Projektový manažer, Koordinátor projektu, klíčoví uživatelé, experti odboru Informatiky, Bezpečnosti a dalších dotčených odborů.

3. Požadavky na implementační analýzu

3.1. Objednatel požaduje implementační analýzu prostředí Objednatele a požadavků odboru Informatiky a klíčových uživatelů. Zpracována bude Zhotovitelem a předložena Projektovým manažerem Řídicímu výboru ke schválení. Obsahovat bude:

- cíle a požadavky (včetně metrik a jejich hodnot) projektu, rozsah projektu včetně hranic,
- organizační struktury projektu,
- složení pracovních týmů projektu,
- pravidla vedení dokumentace,
- matici odpovědností, vazeb a informačních toků v rámci organizace projektu,
- návrh postupu realizace včetně harmonogramu projektu, členění na samostatně akceptovatelné části,
- plán řízení rizik,

- analýzu bezpečnosti s ohledem na Zákon o kybernetické bezpečnosti,
- popis změnového řízení,
- popis projektové metodiky,
- popis akceptačního řízení.

4. Požadavky na akceptaci projektu nebo jeho ucelených částí

4.1. Akceptace projektu či jeho ucelených částí bude probíhat v rámci Akceptačního řízení:

4.1.1. **Akceptační řízení** je proces posouzení výstupů/plnění dle Akceptačních kritérií. Zahájeno je na základě žádosti Zhotovitele, který doloží Řídicímu výboru podklady pro posouzení. Výsledkem Akceptačního řízení je Akceptační protokol (s výhradou či bez výhrad) podepsaný oběma smluvními stranami. Akceptační protokol bude obsahovat i doložku o možnosti fakturovat zakceptované dílo.

4.1.2. V případě, že Objednatel v Akceptačním řízení zjistí jakoukoliv závadu zásadně bránící plnění funkce plnění, bude vyhotoven protokol s vytknutými vadami. Objednatel poskytne Zhotoviteli přiměřenou dobu na odstranění této vady. Po tuto dobu je přerušeno Akceptační řízení a dílo se považuje za nepřevzaté.

4.1.3. V Případě prodlení na straně Objednatele s poskytnutím vyjádření k výstupům/plnění v rámci Akceptačního řízení o více než 3 dny, se termín ukončení plnění díla prodlužuje o stejný počet dnů, o který nebyl Akceptační protokol (s výhradou či bez výhrad) ze strany Objednatele poskytnutý Zhotoviteli.

4.1.4. **Akceptační kritéria** jsou definicí měřitelných charakteristik díla předem dohodnutá smluvními stranami na úrovni Řídicího výboru či Implementační analýzy. Akceptačním kritériem je provedení akceptačních testů. Způsob a metodiku testování k zajištění bezproblémové implementace včetně dokumentace vypracuje Zhotovitel.

4.2. Objednatel požaduje provedení Akceptačního řízení minimálně těchto ucelených částí projektu:

4.2.1. Harmonogram – Akceptace detailního harmonogramu projektu minimálně v bodech:
- Iniciace (start projektu, tým, nastavení)
- Analýza (komplexní analýza řešení)
- návrh řešení (kompletní zadávací dokumentace pro řešení)
- implementace (detailní rozpis jednotlivých kroků implementace)
- fat (Funkční akceptační test)
- uat (Uživatelské akceptační)
- nasazení (Nasazení do ostrého provozu)
- dokončení (finalizace projektu, odevzdání dokumentace, zdrojových kódů apod.)

4.2.2. Implementační analýza – detailní požadavky a cíle na základě komunikace se zákazníkem, komplexní analýza řešení.

4.2.3. Návrh řešení - kompletní zadávací dokumentace pro řešení.

4.2.4. testy FAT – Funkční akceptační testy, testování musí obsahovat všechny testovací scénáře použité pro testy FAT.

4.2.5. testy UAT – uživatelské akceptační testy, testování musí obsahovat všechny testovací scénáře použité pro testy UAT

4.2.6. Nasazení do provozu - nasazení do ostrého provozu, najíždění agendy.

4.2.7. Dokončení - Akceptace projektu - fakturační milník

4.3. Objednatel požaduje, aby předmět plnění byl Zhotovitelem dle harmonogramu řádně otestován. Harmonogram bude Zhotovitelem předložen při prvním zahajovacím zasedání Řídícího výboru, který jej schválí.

SPRÁVA ŽELEZNIČNÍ
DOPRAVNÍ CESTY

Příloha č. 3 Smlouvy o dílo

Seznam poddodavatelů:

Název poddodavatele: **Clarystone s.r.o.**
Sídlo: Rostovská 1481/2a, Vršovice, 101 00 Praha 10
Spisová značka: C 206322 vedená u Městského soudu v Praze
IČO: 27745422
Statutární orgán: Mgr. Petr Koch, jednatel
David Šíbl, jednatel
Prokura: Mgr. Martin Píštěk
Části předmětu plnění, které bude plnit: Dodávka HW a projektové řízení

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Doložka číslo: 379205

Původní datový formát: application/pdf

UUID původní komponenty: a5e4fb36-e4f7-45ed-b543-e9921b218b79

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:

Systém ERMS (zpracovatel dokumentu Dana NOVOSVĚTSKÁ)

Subjekt, který změnu formátu provedl: Správa železniční dopravní cesty, státní organizace

Datum vyhotovení ověřovací doložky: 28.08.2019 09:03:04