číslo odběratele: 192/2020
číslo dodavatele:

ICZ 648903 / 1

Smlouva o poskytnutí řešení
„Správa a monitoring privilegovaných účtů – PAM“

Smluvní strany:

1. Česká republika – Ministerstvo vnitra

Se sídlem:	Nad Štolou 936/3, 170 34 Praha 7
IČO:	00007064
DIČ:	CZ00007064
Zastoupená:	**Ministerstvo vnitra-generálním ředitelstvím Hasičského záchranného sboru České republiky** (dále jen „MV-GŘ HZS ČR“)
Právně jednající:	plk. Ing. Radek Jančík, ředitel odboru KIS
Doručovací adresa:	MV-GŘ HZS ČR, Kloknerova 26, 148 01 Praha 414
ID datové schránky:	84taiur
Bankovní spojení:	ČNB Praha 1
Číslo účtu:	8908-881/0710

dále jen „odběratel“

a

2. ICZ a.s.

Zapsán:	OR u Městského soudu v Praze, sp.zn. B 4840
Se sídlem:	Na hřebenech II 1718/10, Nusle, 140 00 Praha 4
IČO:	25145444
DIČ:	CZ699000372
Právně jednající:	[redacted]
Bankovní spojení:	
Číslo účtu:	
Kontaktní osoba:	
- ve věcech smluvních:	
- ve věcech technických:	

dále jen „dodavatel“

uzavírají v souladu s ustanovením § 1746 odst. 2 ve spojení s § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále „občanský zákoník“), tuto *Smlouvu o poskytnutí řešení „Správa a monitoring privilegovaných účtů – PAM“* (dále jen „smlouva“):

ZÁKLADNÍ USTANOVENÍ

Podkladem pro uzavření této smlouvy je nabídka dodavatele ze dne 1. 10. 2020, která byla pro účely zadání veřejné zakázky malého rozsahu zveřejněna pod číslem N006/20/V00017772 prostřednictvím národního elektronického nástroje a byla vybrána jako nejvýhodnější (dále jen „veřejná zakázka“).

I.
Předmět smlouvy

1. Předmětem této smlouvy je povinnost dodavatele odběrateli:

   a) dodat návrh technického řešení a uvedení do provozuschopného stavu PAM řešení na IT technologie v prostředí odběratele, realizovat základní seznámení včetně poskytnutí časově neomezené licence k užívání PAM řešení v minimálním počtu 20 ks a provést další činnosti specifikované v této smlouvě a její příloze č. 1, kterou tvoří Technická specifikace veřejné zakázky (dále jen poskytnutí **„PAM řešení“**);

   b) dodat 2 ks provozních serverů typ HPE DL360 Gen10 8SFF CTO Server(včetně podpory – extensive support po dobu 36 měsíců ode dne podpisu oboustranně schváleného *konečného předávacího protokolu* /viz. čl. II. odst. 4 této smlouvy/) nezbytných pro provoz navrhovaného PAM řešení včetně dodávky operačních systémů specifikovaných v příloze č. 1 této smlouvy (dále jen **„zboží“**);

   c) dodávat podporu uvedenou v části 2. Technické specifikace, která tvoří přílohu č. 1 této smlouvy, po dobu 36 měsíců od dne podpisu oboustranně schváleného *konečného předávacího protokolu* /viz. čl. II. odst. 4 této smlouvy/ (dále jen **„podpora“**)

dle níže uvedených podmínek a popisu a dále povinnost odběratele uhradit po dodání předmětu smlouvy dodavateli ujednanou cenu.

2. Dodavatel se zavazuje v rámci plnění podle této smlouvy nainstalovat nejnovější, výrobcem otestovanou a doporučenou plnou verzi programových prostředků, která bude výrobcem v době podpisu konečného předávacího protokolu uvedena na trh, a následně v době poskytování podpory.

3. Legislativní požadavky, specifikace, podmínky a konkretizace předmětu smlouvy a další požadavky odběratele jsou uvedeny v zadávací dokumentaci veřejné zakázky a příloze č. 1 této smlouvy.

II.
Lhůta dodání, místo plnění, předání a převzetí předmětu smlouvy

1. Dodavatel je povinen dodat předmět smlouvy uvedený v čl. I. odst. 1 písm. a) a b) **nejpozději do 6 týdnů** ode dne nabytí účinnosti této smlouvy (viz. čl. VIII odst. 2 této smlouvy). Předmět smlouvy uvedený v čl. I. odst. 1 písm. c) bude dodáván po dobu 36 měsíců ode dne podpisu oboustranně schváleného *konečného předávacího protokolu* viz. čl. II. odst. 4 této smlouvy.

2. Dodání předmětu smlouvy bude provedeno v pracovní dny v době od 8:00 do 16:00 hod., konkrétní termíny dodání budou dohodnuty s kontaktní osobou odběratele v součinnosti s kontaktní osobou dodavatele, která oznámí termín alespoň 3 pracovní dny předem. Místem plnění je doručovací adresa odběratele: MV-GŘ HZS ČR, Kloknerova 26, 148 01 Praha 414.

3. Po uplynutí lhůty dodání může dodavatel dodat předmět smlouvy jen po předchozím písemném souhlasu odběratele. Právo na uplatnění smluvní pokuty je zachováno.

4. Dodavatel se zavazuje předat předmět smlouvy v rozsahu uvedeném v čl. I. odst. 1 písm. a) a b) této smlouvy řádně a ve sjednaném termínu, prostý jakýchkoliv vad a nedodělků, a to na základě oboustranně schváleného *konečného předávacího protokolu*, v kvalitě a v rozsahu odpovídajícím požadavku odběratele a zákonné úpravě a při dodržení podmínek v této smlouvě. Součástí *konečného předávacího protokolu* je rovněž zajištění a předání všech dokladů potřebných k řádnému užívání předmětu smlouvy v souladu s obecně platnými právními předpisy, příslušnými technickými normami a povinnost předání návodů, schémat a poučení (informace). Tento *konečný předávací protokol* bude podepsán kontaktními osobami smluvních stran, přičemž zástupce odběratele v něm výslovně uvede, že předmět smlouvy přebírá bez výhrad nebo přebírá s výhradami s uvedením důvodů, vad a s uvedením lhůt jejich odstranění, případně nepřebírá s uvedením důvodů. *Konečný předávací protokol* bude vyhotoven ve třech výtiscích – jeden pro odběratele, jeden pro dodavatele, třetí se přiloží k vystavené faktuře podle čl. III. odst. 3.

5. **Kontaktní osobou odběratele** ve věcech technických a kontroly poskytování a převzetí (podpisy protokolů) PAM řešení, je: [redacted]

6. **Kontaktní osobou dodavatele** ve věcech technických, který je oprávněn k podpisům protokolů, je: [redacted]

III.
Cena a platební podmínky

1. Cena byla stanovena na základě nabídky dodavatele v rámci veřejné zakázky č. N006/20/V00017772, která byla vybrána jako nejvýhodnější, takto:

Položka č.	Předmět smlouvy		Cena v Kč bez DPH	Sazba DPH v %	Výše DPH v Kč	Cena v Kč s DPH
1.	PAM řešení - viz. čl. I. odst. 1 písm. a):	- technického řešení:	614 300,00	21	129 003,00	743 303,00
		- uvedení do provozuschopného stavu	142 000,00	21	29 820,00	171 820,00
2.	Zboží - viz. čl. I. odst. 1písm. b)		395 866,00	21	83 131,86	478 997,86 zaokrouhleno - 0,86 Kč celkem k úhradě 478 997 Kč
3.	Podpora za 36 měsíců - viz. čl. I. odst. 1 písm. c)		383 220,00	21	80 476,20	463 696,20
3.1	Cena podpory za prvních 12 měsíců		110 574,00	21	23 220,54	133 794,54
3.2.	Cena podpora za 12 měsíců ve druhém a třetím roce		136 323,00	21	28 627.83	164 950,83

Celková nabídková cena (součet položek 1., 2. a 3.)	**1 535 386,00**	**21**	**322 431,06**	**1 857 816,20**

2. V případě změny právních předpisů týkajících se výše sazby DPH bude tato stanovena v souladu s platnými právními předpisy. Tato cena je konečná a zahrnuje veškeré náklady spojené s úplnou realizací předmětu smlouvy včetně dopravy a zajištění licenčních oprávnění.

3. Cena za položky uvedené v odst. 1 pod č. 1, č. 2 a č. 3.1 (prvních 12 měsíců poskytování podpory) tohoto článku bude zaplacena na základě faktury vystavené dodavatelem. Faktura bude vystavena a zaslána dodavatelem na adresu uvedenou v odst. 6 tohoto článku a to max. do 10 dnů od podpisu *konečného předávacího protokolu* odběratelem. Vlastnické právo k předmětu smlouvy přejde na odběratele v momentě uhrazení ceny uvedené v odst. 1 pod položkou č. 1 a č. 2 této smlouvy. Po dobu dodání předmětu smlouvy nese odpovědnost za případné škody na předmětu smlouvy dodavatel.

4. Faktura (daňový doklad) musí splňovat náležitosti daňového dokladu dle stávajících platných právních předpisů, a její přílohou bude oboustranně podepsaný originál *konečného předávacího protokolu*.

5. Cena za podporu uvedenou v odst. 1 pod položkou č. 3 tohoto článku je splatná po částech jednou ročně na základě faktury vystavené dodavatelem. Faktura musí být vystavena do 31. 10. 2021 resp. do 31. 10. 2022 a zaslána dodavatelem na adresu uvedenou v odst. 6 tohoto článku a musí obsahovat náležitosti daňového dokladu dle stávajících platných právních předpisů.

6. Fakturace se uskuteční na adresu:

MV-GŘ HZS ČR pošt. přihr. 69
Kloknerova 26
148 01 Praha 414

Na faktuře bude jako identifikace odběratele uvedeno:

ČR – Ministerstvo vnitra
Nad Štolou 936/3
170 34 Praha 7

Zastoupené – doručovací adresa:

MV-GŘ HZS ČR
Kloknerova 26
pošt. přihr. 69
148 01 Praha 414

7. Odběratel je povinen zaplatit fakturu do 21 dnů ode dne doručení na adresu odběratele uvedenou v záhlaví této smlouvy.

8. Za den uskutečnění platby se považuje den, kdy byla cena odepsána z účtu odběratele.

9. Odběratel je oprávněn fakturu do data splatnosti vrátit, pokud obsahuje nesprávné cenové údaje nebo neobsahuje některou z dohodnutých náležitostí dle odst. 4 tohoto článku. Do doby doručení

opravené faktury se odběratel nenachází v prodlení s placením dlužné částky. Po doručení opravené faktury odběrateli počíná běžet nová lhůta její splatnosti 21 dnů.

10. Odběratel nebude poskytovat dodavateli jakékoliv zálohy na úhradu ceny předmětu smlouvy.

11. Pokud odběratel uplatní nárok na odstranění vady předmětu smlouvy dle čl. VI. odst. 1. ve lhůtě splatnosti faktury, není odběratel povinen až do odstranění vady předmětu smlouvy cenu uhradit.

IV.
Rozsah poskytovaných uživatelských oprávnění

1. Dodavatel prohlašuje, že je oprávněn poskytnout odběrateli veškerá plnění sjednaná touto smlouvou včetně udělení nebo zprostředkování práva k užití PAM řešení, zboží a podpory, zavazuje se poskytnout tyto v souladu s dotčenými licenčními oprávněními a zajistit, aby tyto nebyly poskytovány bez nedořešených práv v oblasti duševního vlastnictví. V případě, že se toto prohlášení ukáže nepravdivým, zavazuje se dodavatel uhradit odběrateli, jakož i třetím osobám, veškerou újmu, která by jim v této souvislosti vznikla, jakož i smluvní pokutu ve výši všech sankcí, které budou odběrateli uložené ze strany mezinárodních či jakýchkoliv státních orgánů, včetně orgánů činných v trestním řízení.

2. Dodavatel zodpovídá za seznámení odběratele se všemi závazky a omezeními vyplývajícími z jednostranně stanovených licenčních podmínek užívání případného programového vybavení nebo jiného předmětu ochrany duševního vlastnictví tvořícího součást PAM řešení, zboží nebo podpory, které je odběratel povinen dodržovat a jež jsou stanoveny oprávněným původcem příslušného programového vybavení nebo jiného předmětu ochrany duševního vlastnictví a to nejpozději ke dni příslušné aktivace PAM řešení, dodání zboží resp. poskytnutí podpory.

3. Právo užívání PAM řešení, zboží a podpory a všech jeho součástí včetně příslušných licenčních oprávnění a odpovědnost za eventuální škodu přechází na odběratele okamžikem jeho aktivace (případně převzetí, je-li to třeba s ohledem na jeho povahu) nebo jeho prvního poskytnutí, nelze-li toto s ohledem na jeho povahu poskytnout již při aktivaci PAM řešení nebo dodání zboží (např. upgrade softwaru poskytnutého za trvání smlouvy).

4. V případě, že k užívání PAM řešení, zboží nebo podpory je třeba licenční oprávnění poskytované dodavatelem jako k tomu příslušnou osobou, dodavatel touto smlouvu uděluje odběrateli právo k jeho užívání a to v rozsahu a k takovým způsobům užití, aby bylo možné dosáhnout účelu této smlouvy. V případě, že k užívání součástí PAM řešení, zboží nebo podpory bude s ohledem na jeho povahu nezbytné získat obdobné oprávnění v době poskytování podpory podle této smlouvy (např. upgrade software), zavazuje se dodavatel udělit odběrateli vždy současně příslušná oprávnění nejméně v rozsahu podle věty první.

V.
Mlčenlivost

1. Dodavatel se zavazuje zachovávat ve vztahu ke třetím osobám mlčenlivost o informacích, které při realizaci této smlouvy získá od odběratele nebo o odběrateli či jeho zaměstnancích a spolupracovnících a nesmí je zpřístupnit bez písemného souhlasu odběratele žádné třetí osobě ani je použít v rozporu s účelem této smlouvy, ledaže se jedná:

- o informace, které jsou veřejně přístupné;

- o případ, kdy je zpřístupnění informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu.

2. Dodavatel je povinen zavázat povinností mlčenlivosti podle odst. 1 tohoto čl. všechny osoby, které se budou podílet na poskytování předmětu plnění podle této smlouvy.

3. Za porušení povinnosti mlčenlivosti osobami, které se budou podílet na poskytování předmětu plnění podle této smlouvy, odpovídá dodavatel jako by povinnost porušil sám.

4. Povinnost mlčenlivosti trvá i po ukončení účinnosti této smlouvy.

VI.
Záruka, odpovědnost za vady a reklamace

1. Dodavatel se zavazuje vždy předat předmět smlouvy řádně a včas, prostý jakýchkoliv vad a nedodělků, tzn. v kvalitě a v rozsahu odpovídajícím požadavku odběratele, v rozsahu odpovídajícím požadavku zákonné úpravy, množství, druhu, ve sjednaném termínu a ve sjednaném místě plnění, při dodržení podmínek v této smlouvě a příloze č. 1 této smlouvy.

2. Dodavatel odpovídá za vady, které má předmět smlouvy v době jeho předání odběrateli, a za vady, které se vyskytnou v níže uvedené záruční době.

3. Dodavatel poskytuje odběrateli záruku za jakost na předmět smlouvy v délce 24, resp. 36 měsíců v závislosti na typu zařízení, a to od data předání odběrateli na základě *konečného předávacího protokolu*. Záruční doba počíná běžet dnem podpisu oběma smluvními stranami (v protokolu je nutné uvést výrobky a materiály vyloučené ze záruky, resp. s kratší záruční dobou. Dále je nutno uvést podmínky údržby a zacházení s výrobky a materiály, jejichž nedodržení vylučuje odpovědnost za výskyt vady v záruční době).

4. Vadou předmětu smlouvy se rozumí porušení povinnosti dle čl. VI. odst. 1 smlouvy jakož i odchylka v parametrech s technickými normami, právními předpisy a přílohou č. 1 této smlouvy.

5. Odběratel je oprávněn odmítnout převzetí zboží, pokud nebude dodáno v souladu s ustanovením čl. VI. odst. 1 této smlouvy a to při předání a převzetí zboží v místě plnění, kdy zboží bude zjevně poškozeno.

6. Smluvní strany se dohodly, že v případě výskytu vady předmětu smlouvy v záruční době má odběratel právo požadovat a dodavatel povinnost bezplatně vady odstranit.

7. Odběratel se zavazuje, že případnou reklamaci vady po jejím zjištění písemně uplatní bez zbytečného odkladu.

8. V případě, že u dodavatele bude ze strany odběratele písemně (elektronicky na e-mail [redacted] reklamována vada, zavazuje se dodavatel zahájit její odstraňování v co nejkratší technicky možné lhůtě od jejího uplatnění, nejpozději do 6 hodin ode dne jejího uplatnění a odstraní nebo navrhne způsob jejího odstranění nejpozději do 24 hodin obojí v rámci pracovních dnů v době 9:00 – 16:00. V případě, že bude uplatňována vada provozních serverů, tak bude odstraněna dodáním funkčního HW nejpozději následující pracovní den (viz. extensive support vymezený v příloze č. 1 této smlouvy.

9. Záruční doba neběží v době, po kterou odběratel nemůže užívat zboží pro jeho vady, za které odpovídá dodavatel.

10. Není-li výše stanoveno jinak, použijí se při stanovení práv a povinností z odpovědnosti za vady, kryté zárukou za jakost, příslušná ustanovení občanského zákoníku. Sjednáním záruky za jakost nejsou dotčena práva odběratele plynoucí z odpovědnosti za vady stanovené občanským zákoníkem.

VII.
Smluvní pokuta a úrok z prodlení

1. Nedodá-li dodavatel předmět smlouvy uvedený v čl. I. odst. 1. písm. a) nebo b) ani do 15 dnů po uplynutí lhůty dodání, zaplatí odběrateli smluvní pokutu ve výši 0,05 % z celkové ceny včetně DPH za každý i započatý den prodlení od marného uplynutí lhůty dodání uvedené v čl. II. odst. 1 této smlouvy až do řádného dodání tohoto předmětu smlouvy.

2. Odběratel je oprávněn uplatnit smluvní pokutu ve výši 1000,- Kč za každý den prodlení s odstraňováním reklamovaných vad, a to za každou zvlášť uplatněnou vadu.

3. Odběratel je dále oprávněn uplatnit smluvní pokuty ve výši 1000,- Kč za každé porušení mlčenlivosti dle čl. V. této smlouvy.

4. Zaplacením smluvní pokuty není dotčen nárok odběratele na náhradu škody.

5. Odběratel je povinen zaplatit dodavateli úrok z prodlení ve výši 0,05 % z oprávněně fakturované částky bez DPH za každý i započatý den prodlení v případě nezaplacení ceny včas.

6. Smluvní pokuta a úrok z prodlení jsou splatné do 30 kalendářních dnů od obdržení písemné výzvy k jejich uhrazení.

VIII.
Vznik, trvání a ukončení smlouvy

1. Tato smlouva je uzavřena a nabývá platnosti dnem jejího podpisu poslední smluvní stranou.

2. Tato smlouva nabývá účinnosti dnem jejího uveřejnění prostřednictvím registru smluv podle § 6 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů. Zveřejnění smlouvy zajistí odběratel.

3. Tato smlouva se uzavírá na dobu určitou a skončí uplynutím 36 měsíců ode dne podpisu oboustranně schváleného *konečného předávacího protokolu* (viz. čl. II. odst. 4 této smlouvy).

4. Všechny změny nebo doplnění smlouvy jsou platné pouze v podobě písemných vzestupně číslovaných dodatků ke smlouvě podepsaných osobami k tomu oprávněnými.

5. Smlouva může být předčasně ukončena písemnou dohodou obou smluvních stran, odstoupením jedné ze smluvních stran nebo výpovědí.

6. Obě smluvní strany jsou oprávněny od této smlouvy jednostranně odstoupit v případě, že druhá smluvní strana opakovaně (min. 3x) v průběhu 6ti měsíců poruší své povinnosti z této smlouvy pro ni vyplývající, pokud povinná smluvní strana neprovede, ani po předchozím písemném upozornění strany oprávněné, účinná opatření směřující k nápravě, což smluvní strany považují za podstatné porušení smluvních povinností.

7. Odstoupit od této smlouvy je dále oprávněn:

a) dodavatel v případě, že odběratel bude v prodlení s úhradou ceny za předmět smlouvy po dobu delší 60 kalendářních dnů.

b) odběratel
- v případě, že dodavatel bude v prodlení s dodáním předmětu smlouvy uvedeném v čl. I. odst. 1. písm. a) nebo b) delším než 15 kalendářních dnů.
- v případě, že dodavatel neodstraní reklamované vady ve lhůtě stanovené v čl. VI., odst.8. této smlouvy.

8. Smluvní strany jsou dále oprávněny od této smlouvy odstoupit ze zákonných důvodů.

9. Oznámení o odstoupení od smlouvy musí být učiněno písemně a doručeno druhé smluvní straně. Odstoupením od smlouvy není dotčen případný nárok na náhradu škody ani úhradu smluvních pokut.

10. Obě smluvní strany jsou oprávněny tuto smlouvu ukončit výpovědí bez udání důvodu s tří měsíční výpovědní lhůtou, která počíná běžet prvním dnem kalendářního měsíce následujícího po měsíci, ve kterém byla výpověď doručena.

11. Smluvní strany berou na vědomí, že po ukončení smlouvy jsou povinny plnit své povinnosti pro ně vyplývající z čl. V. této smlouvy. Rovněž ta ustanovení smlouvy, která z povahy věci přesahují účinnost smlouvy, zůstávají nedotčená až do jejich naplnění.

12. Smluvní strany se zavazují vzájemně vyrovnat své závazky a pohledávky do 21 dnů od ukončení této smlouvy.

IX.
Závěrečná ustanovení

1. Ve věcech touto smlouvou neupravených se smluvní strany řídí právním řádem České republiky.

2. Smluvní strany jsou povinny bez zbytečného odkladu oznámit druhé smluvní straně změnu základních identifikačních údajů uvedených v záhlaví této smlouvy.

3. Dodavatel je povinen dokumenty související s poskytováním předmětu smlouvy podle této smlouvy uchovávat nejméně po dobu deseti (10) let od konce účetního období, ve kterém došlo k zaplacení posledního zdanitelného plnění dle této smlouvy, a to zejména pro účely kontroly oprávněnými kontrolními orgány.

4. Dodavatel je povinen umožnit kontrolu dokumentů souvisejících s poskytováním podpory dle této smlouvy ze strany odběratele a jiných orgánů oprávněných k provádění kontroly, a to zejména ze strany Ministerstva vnitra ČR, Ministerstva financí ČR a případně dalších orgánů oprávněných k výkonu kontroly a ze strany třetích osob, které tyto orgány ke kontrole pověří nebo zmocní.

5. Dodavatel je ve smyslu ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

6. Dodavatel je povinen upozornit odběratele písemně na existující či hrozící střet zájmů bezodkladně poté, co střet zájmů vznikne nebo vyjde najevo, pokud dodavatel i při vynaložení veškeré odborné péče nemohl střet zájmů zjistit před uzavřením této smlouvy.

7. Dodavatel není bez předchozího písemného souhlasu odběratele oprávněn postoupit práva a povinnosti z této smlouvy na třetí osobu.

8. Dodavatel podpisem této smlouvy uděluje souhlas se zpracováním údajů uvedených ve smlouvě a to po dobu její platnosti a po dobu stanovenou pro archivaci. Dodavatel bez jakýchkoliv výhrad souhlasí se zveřejněním své identifikace a dalších údajů uvedených ve smlouvě včetně ceny v registru smluv. Osobní údaje stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

9. Smluvní strany uzavírají tuto smlouvu v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, a podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

10. Smluvní strany se zavázaly řešit spory nejprve smírně. Nebude-li smírného řešení dosaženo, budou spory řešeny v soudním řízení. Veškeré spory vzniklé z této smlouvy se řídí platným českým právem.

11. Tato smlouva je vyhotovena ve dvou stejnopisech, každý s platností originálu, z nichž každá smluvní strana obdrží jedno vyhotovení.

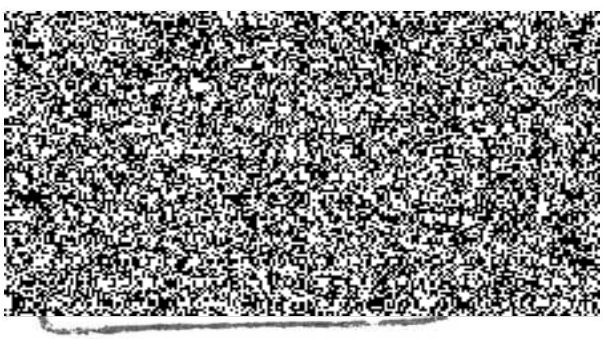
12. Smluvní strany prohlašují, že smlouva nebyla uzavřena v tísni ani za jednostranně nevýhodných podmínek, s ustanoveními této smlouvy souhlasí a na důkaz toho připojují své podpisy.

13. Nedílnou součástí této smlouvy jsou tyto přílohy:

1. Technická specifikace – správa a monitoring privilegovaných účtů

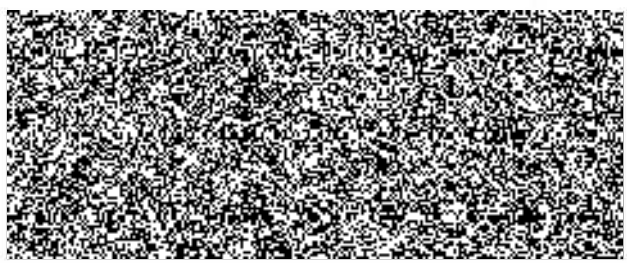
V Praze dne 3. 11. 2020

Za odběratele:



V Praze dne

Za dodavatele: 2. 11. 2020



106
ICZ a.s.
Na hřebenech II 1718/10
140 00 Praha 4
IČO: 25145444

Příloha č. 1 k č.j. **MV-112044-1/PO-KIS-2020**

SPRÁVA A MONITORING PRIVILEGOVANÝCH ÚČTŮ

Technická specifikace

1. ÚČEL DOKUMENTU

Tento dokument je součástí zadávací dokumentace veřejné zakázky malého rozsahu „**Správa a monitoring privilegovaných účtů**“, č. zakázky N006/20/V00017772, popisuje technické a funkční požadavky ***na řešení pro řízení privilegovaných účtů*** používanými administrátory Generálního ředitelství hasičského záchranného sboru a administrátory dalších subjektů pro správu technických a programových prostředků tvořících informační systémy GŘ HZS a dále obsahuje představení požadovaného konceptu řešení, jeho základní popis a požadavky závazné pro všechny potenciální uchazeče o zajištění realizace zakázky.

2. POUŽITÉ ZKRATKY

Termín	**Význam**
GŘ HZS = zadavatel	Generální ředitelství hasičského záchranného sboru
DB	Databáze
DC	Datové centrum
Dodavatel	Subjekt, který dodává řešení popsané v této technické specifikaci
HA	High Availability – režim vysoké dostupnosti (např. redundance)
Koncový systém	Komponenta informačního systému spravovaná provozovatelem (OS, DB, webový portál, síťové zařízení, apod.)
LDAP	Lightweight Directory Access Protocol
OS	Operační Systém
PAM	Privileged Account Management – řízení privilegovaných účtů
Privilegovaný účet	Uživatelský účet s širokou nebo neomezenou množinou administrátorských oprávnění
Provozovatel informačního systému (zadavatel)	Subjekt zajišťující funkčnost technických a programových prostředků tvořících informační systém
PuTTY	Klient protokolů SSH, Telnet, rlogin a holého TCP
RDP	Remote Desktop Protocol – protokol na přenos vzdálené plochy

SSO	Single sign on - systém jednotného přihlášení
SW	Software
TS	Terminálový server
WMI	Windows Management Instrumentation

3. ZÁKLADNÍ CÍLE

GŘ HZS spravuje velké množství informačních systémů, na jejichž chodu je závislý provoz samotné organizace, i části systémů, jež využívají a které zároveň obsahují citlivé informace, ke kterým je nutné patřičně zabezpečit přístup. Jelikož oprávnění účtů administrátorů provozovatelů umožňují z povahy jejich činností neomezený přístup ke zdrojům a datům informačních systémů, představují tyto privilegované účty potencionální bezpečnostní riziko. Toto riziko se vztahuje na všechny technické a programové prostředky informačních systémů, počínaje servery, operačními systémy, databázemi, až po komplexní aplikační část informačních systémů distribuovaných jako produkt nebo vyvinuté na míru. Ať už přímo nebo nepřímo se tak problém možného zneužití privilegovaných účtů dotýká všech informačních systémů, včetně systémů, jež v budoucnu mohou díky své povaze nabýt statusu „Významný informační systém" v rámci zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti, ve znění pozdějších předpisů, dále jen „zákon o kybernetické bezpečnosti".

K minimalizaci rizika kompromitace informačních systémů a k zajištění auditní stopy privilegovaných operací a přístupů na systémy s citlivými informacemi, a v neposlední řadě k zajištění plnění povinností definovaných zákonem o kybernetické bezpečnosti a příslušnými vyhláškami, je nutné zavést správu přístupu k těmto účtům a jejich monitoring. V rámci zadávacího řízení poptává zadavatel řešení pro správu privilegovaných účtů a monitoring jejich použití (dále též jako „systém PAM"). Základní popis a požadavky kladené na toto řešení jsou definovány v tomto dokumentu.

4. POPIS PROSTŘEDÍ

Informační systémy zadavatele jsou provozovány v datových centrech GŘ HZS. Zadavatel sám nebo prostřednictvím subdodavatelů spravuje kompletní zdroje a infrastrukturu informačních systémů, tedy jak fyzický či virtuální server, tak i operační systémy a aplikační komponenty – databázové servery, webové servery, aplikační servery apod. informačních systémů.

5. POŽADOVANÝ CÍLOVÝ STAV

Obecné požadavky na PAM řešení

Pomocí PAM řešení musí být možné zajistit následující funkční požadavky:

1. Centrální správa účtů a jejich hesel v rámci zabezpečeného úložiště se správou přístupů k těmto účtům **(Password Management)**

2. Zaznamenávání aktivit privilegovaných účtů v rámci relací navázaných přes PAM včetně nahrávek obrazovek a stisků kláves **(Session Recording)**

3. Řízení oprávnění v rámci operačního systému, detekce a ochrana prostředků systému na základě definovaných politik **(Access Control)**. **Tato funkcionalita není vyžadována v rámci dodávky.** PAM však musí být možné o tuto funkcionalitu v rámci produktu v případě potřeby snadno rozšířit.

4. Detekce podezřelých uživatelských aktivit s klasifikací jejich závažnosti a s možností automatického přerušení této aktivity **(Threat Analysis)**.

Z důvodu urychlení nasazení řešení rizik je požadováno implementovat oblast Password Management, Session Recording a Threat Analysis, které pokryjí většinu identifikovatelných rizik a zároveň umožní naplnit nařízení v rámci návrhu zákona o kybernetické bezpečnosti, konkrétně:

Technická opatření:

- *Nástroj pro ověřování identity uživatelů*
- *Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců*

Řešení PAM musí licenčně a výkonově zajistit přístup a nahrávání relací min. pro 20 administrátorů zadavatele, zajistit uložení nahraných relací pro on-line analýzu po dobu min. 1 roku s možností přístupu ke starším nahrávkám v archivu/off-line záloze stejným způsobem jako v případě přístupu k on-line nahrávkám (např. zpětnou obnovou do PAM řešení) a umožnit integraci přibližně 800 koncových systémů bez omezení počtu integrovaných účtů.

Zároveň musí dodaná licence umožnit nasadit a provozovat řešení dle této technické specifikace tak, jak je popsáno v požadavcích na cílový stav a zároveň PAM řešení musí splnit všechny funkční požadavky uvedené v Části 1. této Technické specifikace – Funkční požadavky. Zadavatel si vyhrazuje právo ověření si splnění těchto funkčních požadavků, kdy Uchazeč musí na žádost Zadavatele předložit potřebné doklady či záruky jednoznačně prokazující naplnění daného požadavku.

Všechny licence nutné pro provoz PAM řešení dle této technické specifikace musí být součástí dodávky.

2 ks provozních serverů (včetně podpory – extensive support*) pro PAM řešení musí být součástí dodávky a musí plně odpovídat HW/SW požadavkům výrobce PAM řešení pro provoz dle požadovaného rozsahu (minimálně 20 administrátorů/800 integrovaných zařízení).

* minimální požadavky na extensive support jsou:

- v případě poruchy dodání HW nejpozději následující pracovní den,

- přístup k updatum firmware,

- možnost řešení problémů s výrobcem HW.

Minimální technická specifikace dodávaných serverů :

Dvousoketový server o velikosti maximálně 1U včetně rackmount kitu
Osazený min 1x CPU, každé CPU minimálně 16 jader / CPU , velikost cache min 16 MB / CPU, nominální frekvence min. 2,3 GHz
Min. 24x DIMM slotů (min. 12 dostupných slotů s 1x CPU) možností osazeni až 3TB (1,5TB s 1x CPU)
Velikost osazené RAM minimálně 32GB pomocí DIMM modulů DDR4 2933 MT/s
Dva za chodu vyměnitelné napájecí zdroje s příkonem maximálně 500W a účinností min. 94 %
Větráky v serveru musí být vyměnitelné za provozu a redundantní
Minimálně 1x 4-portovou 1Gb síťovou kartu nezabírající místo v PCI-e slotech
Minimálně 1x 1Gb LAN port pro servisní procesor

Požadavky na architekturu

Dodané PAM řešení musí být možné nasadit v režimu vysoké dostupnosti s geograficky oddělenými komponentami sloužícími pro přístup na koncové systémy, aby se minimalizovaly požadavky na síťovou komunikaci přes spojovací LAN linky.

Databázová komponenta PAM řešení, obsahující data o účtech, nahrávkách, auditní logy apod., bude provozována na samostatných provozních (fyzických) serverech, které musí být součástí dodávky. V případě ostatních komponent Zadavatel umožní vytvořit virtuální servery ve vlastní virtuální infrastruktuře založené na produktu VMware vSphere. Součástí dodávky však musí být veškeré licence OS nutné pro provoz komponent PAM řešení.

Integrované systémy

V rámci integrace koncových systémů do PAM řešení je požadována integrace účtů operačních systémů Windows a Linux, účtů databázových systémů MS SQL, DB Oracle, účtů infrastrukturních řešení Cisco, HP, Alcatel, které slouží k přihlašování administrátorů na tyto typy koncových systémů k zajištění provozu softwarových komponent informačních systémů. **Instalace a integrace aplikačních nebo servisních účtů není v rámci této dodávky vyžadována.** Integrace musí zajistit možnost přihlášení administrátorů pomocí osobních i sdílených privilegovaných účtů na koncové systémy v rámci nahrávané uživatelské relace bez požadavku na zadání hesla a tedy jeho znalosti (SSO). PAM řešení musí zároveň zajistit

periodickou změnu hesel těchto integrovaných účtů v souladu s definovanou politikou zadavatele.

Rovněž samotné PAM řešení bude zaintegrováno stejným způsobem jako výše uvedené systémy. To znamená, že veškerá správa PAM řešení bude probíhat přes PAM, a to v rámci nahrávané relace. Tímto způsobem budou integrovány všechny účty mající administrátorskou či auditorskou roli v PAM řešení.

Správa aplikačních komponent informačních systémů bude probíhat současným způsobem, kdy administrátor bude při přihlašování zadávat heslo. Tato správa se však bude odehrávat v rámci nahrávané relace, aby byla zajištěna auditní stopa provedených činností. Integrace aplikačních komponent do PAM řešení bude následovat v další fázi rozvoje.

Uživatelské role PAM řešení

PAM řešení musí minimálně umožnit definovat níže uvedené uživatelské role, které budou sloužit k segregaci administrátorských oprávnění v rámci PAM řešení.

1. **Uživatel**
   Tato role je určena pro administrátory informačních systémů, kteří budou PAM řešení používat pro přístup na komponenty těchto informačních systémů. Role umožní každému jednotlivému uživateli přístup pouze k takovým účtům, které daný uživatel potřebuje pro výkon činností plynoucích např. ze smlouvy pro provoz informačního systému. Použití přístupu a veškerá činnost provedená v rámci administrátorské relace bude nahrávána k zajištění nepopiratelnosti a auditní stopy. Přihlášení k jiným systémům, než pro které byla uživateli nastavena oprávnění, nebude na úrovni PAM řešení možné.
2. **Administrátor organizační jednotky**
   Tato role bude sloužit k delegaci částí administrátorských oprávnění v rámci PAM řešení na externí subjekt/organizační jednotku, která tak bude na základě tohoto oprávnění schopna sama spravovat (přidávat, odebírat, upravovat) účty provozovaných systémů. Administrátoři různých organizačních jednotek nebudou mít žádnou možnost přístupu a správy účtů definovaných jinou jednotkou.
3. **Auditor PAM**
   Role auditora bude sloužit k přístupu k logům o používání účtů a přístupů v rámci PAM řešení, bude disponovat oprávněním pro vytváření reportů o používání účtů a reportů o nastavení oprávnění nad účty v rámci PAM. Zároveň bude mít tato role přístup k nahrávkám všech uživatelských relací navázaných přes PAM řešení a tyto nahrávky bude moci exportovat.
4. **Administrátor PAM**
   Administrátor PAM bude nejvyšší role, která bude mít oprávnění konfigurovat celé PAM řešení a definovat společnou politiku, jež bude následně využívána administrátory PAM.

Nouzový přístup

Nabízené PAM řešení musí umožnit přístup na všechny integrované systémy, jejichž správa probíhá přes PAM i v případě nouzových situací, jako je částečná či úplná nedostupnost PAM řešení. Nedostupnost PAM řešení tak nesmí znemožnit možnost správy informačních systémů a jejich podpůrných komponent. Proces nouzového přístupu musí zohlednit standardní bezpečnostní principy a požadavky definované zadavatelem, tak i legislativou. Použití nouzového přístupu musí být detekovatelné více v části - Integrace na centrální logovací nástroj.

Integrace na centrální logovací nástroj

Zadavatel ve svém prostředí provozuje logovací nástroj, ve kterém centralizuje veškeré logy z vnitřních systémů a provozovaných informačních systémů za účelem centrálního vyhodnocování, reportingu a nezávislého uložení logů pro potřeby auditu.

Řešení PAM musí umožňovat logování do tohoto centrálního logovacího nástroje pomocí standardních metod (např. syslog), a to na všech komponentách PAM řešení, které logy generují a to minimálně v následujících situacích:

1. Detekce přihlášení na koncový systém mimo PAM řešení,
2. Detekce přístupu na koncový systém za použití nouzového přístupu, více v části – Nouzový přístup

PODPORA

Zadavatel požaduje dodat podporu uchazeče na PAM řešení v základní délce 36 měsíců a parametrech viz část:

Požadavky na podporu PAM řešení jsou shrnuty v Části 2. této technické specifikace.

ČÁST 1. TECHNICKÉ SPECIFIKACE – SPRÁVA A MONITORING PRIVILEGOVANÝCH ÚČTŮ

5. FUNKČNÍ POŽADAVKY NA SYSTÉM

Tabulka níže obsahuje funkční požadavky, které musí dodané řešení pro správu a monitoring privilegovaných účtů splňovat (PAM řešení):

Funkční požadavek	**Splňuje ANO / NE**
Řešení obsahuje bezpečné úložiště. Veškeré informace o účtech, heslech, vlastnících, přístupech a veškeré nahrávky a logy budou uložené v centrálním zabezpečeném úložišti, které musí být chráněné alespoň těmito mechanismy: • firewall nakonfigurovaný tak, aby se systémem mohly komunikovat pouze autorizované komponenty řešení • restriktivní konfigurace systému - tzv. hardening • silný mechanismus řízení přístupů "ACL" - na úrovni bezpečného úložiště, a to až na úroveň jednotlivých objektů • řízení vzdáleného přístupu • integrace silné autorizace	ANO
Řešení umožňuje nasazení v režimu vysoké dostupnosti. Každou komponentu řešení musí být možné nainstalovat ve dvou samostatných instancích v režimech active/active nebo active/passive. Řízení vysoké dostupnosti musí být plně automatické. V případě vzniku nedostupnosti některé z komponent řešení za běžného bezporuchového stavu tak musí dojít k automatickému přepnutí provozu/aktivaci druhé nebo záložní komponenty (failover). Řešení, které vyžaduje manuální zásah je nepřípustné a řešení se nesmí spoléhat na zajištění vysoké dostupnosti pomocí virtualizačních funkcí. Po sjednání opravy komponenty je však přípustné provést její aktivaci (failback) manuálně. Bezpečné úložiště musí být instalovatelné na fyzický – nevirtualizovaný – hardware, aby byla zajištěna možnost přístupu k zabezpečeným datům i v případě nedostupnosti virtuálního prostředí. Ostatní komponenty řešení musí být nainstalované z bezpečnostních a provozních důvodů na jiném systému, než je bezpečné úložiště.	ANO
Úložiště privilegovaných účtů a jejich přihlašovacích údajů, a nastavení řešení je možné pravidelně zálohovat, aby byla zaručená jeho dostupnost. Zálohy jsou zabezpečené šifrováním proti neoprávněnému přístupu. Je implementovaný proces zajišťující bezpečný přístup k heslům uloženým v systému v případě částečné, nebo úplné nedostupnosti systému.	ANO

Funkční požadavek	Splňuje ANO / NE
Uživatelské prostředí poskytující funkce uživatelům je přístupné přes webové rozhraní s plnou podporou následujících prohlížečů v OS Windows, Mac, a Linux: • Internet Explorer • Edge • Chrome • Firefox • Safari	ANO
Auditní záznamy a logy veškerých aktivit v zabezpečeném úložišti jsou chráněné proti změnám a vymazání všemi uživateli (včetně administrátora řešení).	ANO
Data a objekty jako hesla, SSH klíče, video nahrávky, logy, definice přístupových oprávnění jsou uložené v zabezpečeném úložišti a zašifrované. Přístup k nim má pouze vlastník a jím určené osoby. Administrátor zabezpečeného úložiště ani jiný nepověřený uživatel, nemá práva přístupu ke čtení, používání, modifikace, nebo smazání.	ANO
Řešení podporuje integraci s LDAP pro správu uživatelů. Nabízené řešení musí podporovat synchronizaci změn a aktualizovat záznamy. Například uživatel přidaný/odebraný ze správy LDAP – řešení automaticky propaguje/odstraní uživatele ze systému správy.	ANO
Nabízené řešení podporuje dotazy a řízení přístupu k heslům i pro "vnořené" globální skupiny, podporuje komplexní Active Directory infrastruktury - geografické lokality, sofistikované prohledávání LDAP.	ANO
Autentizace a autorizace uživatelského přístupu k veškerým komponentám je řízená pomocí LDAP, Radius a Active Directory.	ANO
Pro autentizaci uživatele je možné využít automatické přihlášení (SSO) na základě přihlášení k doméně AD Integrated Windows Authentication. Řešení také podporuje dvoufaktorovou autentizaci PKI, OTP a LDAPS.	ANO
V rámci řešení jsou definovatelné minimálně tyto role: a) administrátor řešení – má možnost spravovat systém, přidávat uživatele a řídit povolené objekty b) auditor - má přístup k auditním informacím a nahrávkám c) uživatel - má umožněný přístup k řešení a jeho běžné užívání	ANO
Řešení musí logovat auditní záznamy o administrátorských a uživatelských aktivitách. Minimálně musí logovat následující typy událostí vykonaných v rozhraní aplikace: • úspěšné a neúspěšné (pokusy o) přihlášení a odhlášení • konfigurační změny (musí být zřejmé, kdo provedl, jakou konfigurační změnu) • získání hesla • přístup k nahrané session	ANO
Řešení podporuje zasílání notifikací pomocí emailu pro definované události, a to minimálně při následujících akcích: • použití účtu • požadavek na heslo a schválení požadavku	ANO

Funkční požadavek	Splňuje ANO / NE
Řešení disponuje vlastními předdefinovanými reporty o aktivitách uživatelů a auditech používání spravovaných přihlašovacích údajů. Podporuje plánování automatického generování těchto reportů: • oprávnění uživatelů • aktivity uživatelů • přehled privilegovaných účtů • přehled činností konkrétního uživatele	ANO
Řešení je možné integrovat s externím ticketovacím systémem a zároveň má integrovaný vlastní interní ticketing systém pro schvalování požadavků na přístup k objektům (privilegované účty, záznamy, logy).	ANO
Řešení je možné napojit na logovací systém a přenáší data v reálném čase a pomocí alespoň jednoho z těchto formátů: • Syslog • SNMP Trap • Textový soubor • JDBC • CEF nebo LEEF • Microsoft Event Log	ANO
Řešení PAM umožňuje komplexní centrální evidenci a správu privilegovaných osobních, sdílených, servisních a aplikačních účtů	ANO
Řešení PAM umožňuje definovat, kterým uživatelům mají být k dispozici jaké privilegované účty, na kterých systémech, jakým způsobem se mají uživatelé k vybraným privilegovaným účtům moci připojit.	ANO
Uživatel se do systému autentizuje přes webové rozhraní a po přihlášení je uživateli zobrazen seznam jenom těch privilegovaných účtů, ke kterým má přidělen přístup. Veškeré ostatní privilegované účty zůstávají v systému pro uživatele skryté a nedostupné.	ANO
Řešení PAM se připojuje k spravovaným systémům a umožňuje změnu hesel privilegovaných účtů na koncových systémech bez instalace agenta atp. Připojení probíhá tak, aby minimálně zatěžovalo spravovaný systém a je možné plánovat čas připojení.	ANO
Řešení PAM umožňuje také evidovat hesla pro nespravované privilegované účty. Změna hesel u takových účtů se provádí manuálně.	ANO
Řešení PAM podporuje proces pro automatické vyhledávání „discovery" nespravovaných účtů na cílových systémech. Takovéto účty jsou v rámci navrhovaného procesu zařazeny do systému řízení PAM. Výsledky Discovery jsou zaznamenány a jsou dostupné v přehledném a interaktivním zobrazení.	ANO
Řešení PAM umožňuje automaticky vyhledávat a přidávat nové privilegované účty do správy PAM. Řešení dle charakteristiky privilegovaného účtu automaticky přiřazuje definovanou bezpečnostní politiku.	ANO
Řešení PAM umožňuje definovat vlastnosti hesel pro jednotlivé privilegované účty, nebo skupiny privilegovaných účtů: • nastavení komplexnosti hesel – počet znaků a podpora různých znakových sad a kombinace znaků • periodicita výměny hesla na cílových systémech	ANO

Funkční požadavek	Splňuje ANO / NE
• nastavení doby platnosti hesla • definování unikátnosti hesla v definovaném počtu posledních výměn	ANO
PAM Řešení musí poskytovat možnost změny jednoho nebo skupiny hesel: • automaticky po skončení doby platnosti hesla • manuálně uživatelem • automaticky, pokud heslo v bezpečném úložišti nesouhlasí s heslem na spravovaném systému	ANO
Řešení PAM umožňuje definovat vlastnosti přístupů k přihlašovacím údajům pro jednotlivé privilegované účty a pro skupiny privilegovaných účtů: • přístup bez omezení – uživatel si může heslo zobrazit, zkopírovat a přímo se transparentně připojit k cílovému systému s využitím privilegovaného účtu • dvojí kontrola – heslo nebo připojení je uživateli poskytnuto až po schválení přístupu schvalovatelem. Pro přístup k heslu se vytvoří žádost, generuje se automaticky emailová notifikace pro schvalovatele, nebo skupině schvalovatelů, kteří musí přístup/y schválit • exkluzivní přístup – umožňuje využít privilegovaný účet pouze jedinou osobou v jeden čas – ostatní uživatelé nemají možnost přístupu k heslu • jednorázový přístup (one time password) – po použití přístupu PAM vymění heslo privilegovanému účtu	ANO
Řešení PAM pro jednotlivé privilegované účty, nebo skupiny privilegovaných účtů ověřuje shodu hesla uloženého v bezpečném úložišti a na spravovaném systému (může být například změněno lokálně administrátorem): • PAM řešení je schopné ověřit, zda je heslo uložené v bezpečném úložišti stejné jako na koncovém systému • v případě, že je heslo na koncovém systému jiné, než v bezpečném úložišti, musí být řešení schopné danou událost zalogovat, vytvořit notifikaci a zajistit automatickou změnu hesla za heslo uložené v bezpečném úložišti	ANO
Řešení zaznamenává a uchovává historii hesel (například poslední tři hesla, nebo podle časového období) a umožňuje jednoduchý přístup k historii přes webové rozhraní.	ANO
Systém podporuje Single Sign On (SSO) pro privilegované účty, tedy možnost automaticky se přihlásit ke koncovému systému prostřednictvím privilegovaného účtu bez nutnosti zadávání hesla. Podporované jsou minimálně následující aplikace/protokoly: • Windows RDP • SSH (např. PuTTY) • HTTP(s)/Web aplikace • SQL Developer • SQL Server Management Studio • Libovolný "tlustý klient pro aplikace instalované ve Windows	ANO

Funkční požadavek	Splňuje ANO / NE
prostředí	
Během SSO je heslo automaticky zadané do aplikace na pozadí bez možnosti jeho odhalení.	ANO
Existuje mechanismus zajišťující bezpečný přístup k heslům uloženým v systému i v případě jeho částečné, nebo úplné nedostupnosti.	ANO
Řešení umožňuje měnit hesla, bez instalace agenta na koncový bod, pro privilegované účty v následujících systémech: • Windows desktopové systémy od verze Windows 7 a vyšší • Windows serverové systémy Windows Server 2008 a vyšší • Linux - Red Hat, Ubuntu, Fedora, CentOS, Novell SUSE, Debian, BSD • VMware - ESX, ESXi Server • Microsoft Active Directory • Azure Active Directory Podporováno je řízení lokálních, doménových a adresářových účtů prostřednictvím protokolů: • WMI • SSH • remote PowerShell • ODBC • JDBC	ANO
Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Windows aplikacích bez nutnosti instalace agenta na koncový bod: • Windows Services • Windows Scheduled Tasks • IIS Application Pool • IIS Directory Security • Cluster Service	ANO
Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Aplikacích bez nutnosti instalace agenta na koncový bod: • SAP Application Server • IBM Websphere, Tivoli Storage Manager • BEA Weblogic • JBOSS • Oracle Application ERP, PeopleSoft, GridControl, Application Server • Tomcat • Apache, nginx	ANO
Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících databázových systémech bez nutnosti instalace agenta na koncový bod: : • Oracle • Microsoft SQL Server	ANO

6. ČÁST 2. TECHNICKÉ SPECIFIKACE – SPRÁVA A MONITORING PRIVILEGOVANÝCH ÚČTŮ

7. SPECIFIKACE PODPORY

Níže jsou popsány vyžadované parametry podpory uchazeče pro nabízené PAM řešení, které mají za úkol pomoci instalaci, implementaci či řešení incidentů.

Portál podpory

Uchazeč musí poskytnout servisní portál, který sjednotí veškeré výstupy podpory v jednotném bezpečném prostředí, čímž poskytne platformu pro efektivnější získání, uložení či výměnu zabezpečených informací, mezi něž patří např.:

- Balíček instalačních procesů softwaru
- Dokumentace týkající se instalací SIM, PAS a EPM včetně Implementačních návodů
- Platforma, kde mohou být uloženy veškeré citlivé informace, které jsou v řešení s týmem podpory
- Místo, kde jsou uloženy licenční podmínky společnosti

Technické zázemí

Technické zázemí zajišťuje platformu, na které může Zadavatel efektivně komunikovat s týmem podpory, a navíc také mít neomezený přístup k potřebným technickým informacím.

Technické zázemí musí pracovníkům Zadavatele umožňovat plně řešit technické incidenty, účastnit se diskuzí, nahlédnout řešení problémů, zakládat požadavky na zlepšení systému.

Releasy, opravy a bezpečnostní oznámení

Funkční požadavek	Splňuje ANO / NE
• IBM DB 2 a Informix • Sybase Database • MySQL • FireBird • PostgreSQL • všechny ODBC kompatibilní databáze	ANO
Automatické řízení privilegovaných účtů v těchto systémech musí být dodáno v rámci implementace a podporováno po dobu platnosti zakoupené licence řešení	ANO
Řešení podporuje reporting o stavu SSH klíče, jako je jeho platnost, délka klíče apod. Zároveň identifikuje nesoulad s politikou.	ANO
Řešení musí bezpečně uchovávat SSH klíče v centrálním zabezpečeném úložišti a zároveň kontrolovat a řídit přístupy k těmto klíčům.	ANO
Řešení musí podporovat automatickou výměnu klíčů. Podporuje také rotaci páru SSH klíčů (výměnu privátního a veřejného klíče na cílovém zařízení).	ANO
Řešení musí spravovat a chránit SSH klíče, které jsou používané aplikacemi pro autentizaci.	ANO
Řešení umí posílat notifikace při použití vybraného SSH klíče.	ANO
Řešení zabezpečuje správu SSH klíčů a je integrováno do stejné infrastruktury jako zabezpečení privilegovaných účtů a hesel.	ANO
Nástroj umožňuje nahrávání privilegovaných relací v rámci celého počtu licencí. Minimálně ve formě: a) textové relace (např. SSH, telnet) b) relace prostřednictvím vzdálené plochy (např. RDP, VNC)	ANO
Řešení umožňuje vyhledávat v nahraných relacích dle zadaných slov.	ANO
Řešení umožňuje během privilegovaného přístupu oddělit prostředí klienta od cílového systému, pro zvýšení zabezpečení a minimalizaci rizika nákazy. Stejně tak je možné znemožnit kopírování informací a dat z cílového systému na klienta.	ANO
Nástroj umožňuje monitorovat aktivní relace jinou osobou, např. bezpečnostními správci, auditory apod. Včetně možnosti do aktivní relace zasáhnout.	ANO
Řešení umožňuje detekovat podezřelé uživatelské aktivity s klasifikací jejich závažnosti a možností automatického přerušení této aktivity.	ANO

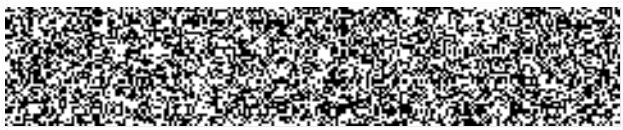
Uchazeč na svém portálu musí umožnit přístup k SW aktualizacím a záplatám systému PAM.

Součástí technické podpory uchazeče musí být též informační služba - oznámení, která obsahují důležité updaty týkající se blížících se releasů, nasazených oprav či bezpečnostních oznámeních.

Hot-line

Uchazeč musí umožnit kontaktovat vlastní Hot-Line technické podpory minimálně v pracovních dnech v době 9:00 - 16:00.

Přístup na Hot-Line:



Odezva na požadavek vznesený v rámci Hot-line:

Uchazeč potvrdí registraci požadavku na Hot-line do 2 hodin ode dne jeho nahlášení na tel. linku nebo zaslání na e-mail a to elektronicky na e-mail kontaktní osoby odběratele ve věcech technických a kontroly uvedený ve Smlouvě o poskytnutí řešení „Správa a monitoring privilegovaných účtů – PAM".

Uchazeč započne práce na požadavku do 6 hodin od potvrzení jeho registrace v rámci pracovních dnů v době od 9:00 – 16:00.

Požadavek bude odstraněn, případně bude navržen způsob jeho odstranění, nejpozději do 24 hodin v rámci pracovních dnů v době od 9:00 – 16:00.

PLNÁ MOC

ICZ a.s., IČO: 251 45 444, se sídlem Praha 4 - Nusle, Na hřebenech II 1718/10, PSČ 147 00, Česká republika, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 4840 (dále „**Zmocnitel**"),

tímto zmocňuje

[redacted]

aby za Zmocnitele činil veškerá právní jednání a jiné úkony v **obchodních vztazích** (včetně vztahů týkajících se veřejných zakázek ve smyslu ustanovení zákona č. 134/2016 Sb., zákon o zadávání veřejných zakázek, ve znění pozdějších předpisů), v nichž cena předmětu plnění vyjádřená peněžní částkou nepřesáhne částku **13.000.000,-Kč** (slovy třináct miliónů korun českých) s tím, že půjde-li o opakující se plnění, je základem pro výpočet tohoto limitu součet ceny všech opakujících se plnění bez DPH.

Tato plná moc nezahrnuje oprávnění Zmocněnce nakupovat a zcizovat cenné papíry, obchodní podíly, uzavírat smlouvy o prodeji části nebo celého podniku, zprostředkovatelské smlouvy, smlouvy o sdružení, smlouvy příkazní či mandátní, smlouvy nájemní, podnájemní či leasingové, přijímat a poskytovat úvěry, sjednávat odstupné, podepisovat směnky, zcizovat nemovitosti a zatěžovat je právními závazky. Zmocněnec dále není na základě této plné moci oprávněn uzavírat jakákoli narovnání a zavazovat Zmocnitele jakýmikoli ručitelskými závazky.

Tato plná moc se uděluje na dobu neurčitou s účinností od 1.1.2019.

V Praze dne 18. prosince 2018

[redacted]

[redacted]

MĚSTSKÁ ČÁST PRAHA 4
126

OVĚŘOVACÍ DOLOŽKA PRO VIDIMACI
Podle ověřovací knihy Úřad městské části Praha 4
poř.č. vidimace **III/5201/2020**
tato úplná kopie obsahující 1 stranu
souhlasí doslovně s předloženou listinou, z níž byla pořízena,
a tato listina je prvopisem obsahujícím 1 stranu.
Listina, z níž je vidimovaná listina pořízena, neobsahuje viditelný zajišťovací prvek.

MĚSTSKÁ ČÁST PRAHA 4
126

V Praze 4 dne 9.10.2020

[redacted]