

KUPNÍ SMLOUVA

uzavřená níže uvedeného dne, měsíce a roku

dle ustanovení § 2079 a násl. a § 2085 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

Čl. 1 Smluvní strany

Kupující: **město Sokolov**
Sídlo: Rokycanova 1929, 356 01 Sokolov
IČ: 00259586
DIČ: CZ00259586
Zastoupený:
Kontaktní osoba:

Bankovní spojení:

Číslo účtu:

jako kupující, na straně jedné
(dále jen „kupující“ nebo „zadavatel“)

a

Prodávající: **Aricoma Systems a. s.**
Sídlo: Hornopolská 3322/34, 702 00 Ostrava
IČ: 04308697
DIČ: CZ04308697

Zastoupený:
Kontaktní osoba:
Bankovní spojení:

Číslo účtu:

Zápis v OR: vedeném u Krajského soudu v Ostravě, spisová značka B 11012

jako prodávající na straně druhé
(dále jen „prodávající“ nebo „dodavatel“)

Čl. 2 Úvodní ustanovení

- 2.1. Tato smlouva je smlouvou na veřejnou zakázku s názvem „Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti“ (dále také jen „veřejná zakázka“), zadávanou kupujícím jakožto zadavatelem, a to na základě nabídky prodávajícího na plnění veřejné zakázky (dále také jen „Nabídka“), která tvoří přílohu č. 2 k této smlouvě.
- 2.2. Prodávající prohlašuje, že se seznámil se všemi podklady které určují předmět této smlouvy a že splňuje veškeré podmínky a požadavky podle této smlouvy, je dostatečně odborně způsobilý k plnění jejího předmětu, tj. je odborníkem ve smyslu § 5 a § 2950 občanského zákoníku, pokud jde o předmět smlouvy, a je oprávněn ji uzavřít a řádně plnit závazky v ní obsažené a k okamžiku uzavření této smlouvy nebyl na jeho majetek prohlášen konkurs, nedošlo k jeho zamítnutí pro nedostatek majetku ani k zamítnutí insolvenčního návrhu proto, že jeho majetek nepostačoval k úhradě nákladů insolvenčního řízení, není v likvidaci a nemá daňové nedoplatky na území České republiky ani v zemi sídla nebo místa podnikání či bydliště. Prodávající dále prohlašuje, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění podle této smlouvy a že má řádné vybavení, disponuje takovými kapacitami a odbornými znalostmi, schopnostmi a zkušenostmi, které jsou k řádnému a včasnému plnění této smlouvy nezbytné.

Čl. 3 Vlastnické vztahy

Prodávající prohlašuje, že

- 3.1. je výlučným vlastníkem části předmětu koupě, jak je níže specifikovaný odst. 4.1. písm. a) – g) , že na něm nevážnou žádná práva třetích osob a že neexistuje žádná právní ani faktická překážka, která by mu bránila s touto částí předmětu koupě podle této smlouvy nakládat; Pokud jde o část předmětu koupě, jak je níže specifikovaný odst. 4.1. písm. h) – j), pak prodávající prohlašuje, že je oprávněn udělit k němu kupujícímu právo tuto užít, jak je níže specifikováno v této smlouvě.
- 3.2. předmět koupě nemá žádné vady, které by bránily jeho použití k obvyklým účelům;
- 3.3. předmět koupě odpovídá požadavkům a podmínkám podle této smlouvy a vyhovuje veškerým požadavkům příslušných právních předpisů a technických norem platných a účinných na území České republiky ke dni odevzdání předmětu koupě kupujícímu.

Čl. 4 Předmět smlouvy

- 4.1. Prodávající se zavazuje odevzdat kupujícímu
- a) 2 ks Next Generation Firewall s příslušenstvím,
 - b) 2 ks páteřních přepínačů 48p s příslušenstvím,
 - c) 28 ks přístupových přepínačů 48p PoE s příslušenstvím,
 - d) 2 ks přístupových přepínačů 24p s příslušenstvím,
 - e) 300 ks autentizačních prostředků,
 - f) 150 ks klávesnic s integrovanou čtečkou karet, včetně ovladačů,
 - g) 150 ks samostatných USB čteček čipových karet, včetně ovladačů,
 - h) 1 ks licence k SW pro řízení přístupu do sítě založeného na protokolu 802.1x,
 - i) 1 ks licence k SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, systému PKI,
 - j) 1 ks licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM,

jejichž podrobné vymezení vč. jejich součástí a příslušenství je uvedeno v přílohách č. 1 a č. 2 k této smlouvě (dále společně také jen „předmět koupě“), a umožnit mu nabýt vlastnické právo či jiná níže specifikovaná práva k němu a současně závazek kupujícího předmět koupě převzít a zaplatit za něj prodávajícímu kupní cenu.

- 4.2. Prodávající se dále zavazuje poskytnout kupujícímu související plnění, kterým se rozumí zejména služby, činnosti a práce přímo související a nezbytné k řádnému uvedení předmětu koupě do provozu a k jeho řádnému užívání kupujícím, které jsou blíže specifikovány v příloze č. 1 k této smlouvě (dále také jen „související plnění“). Tyto služby budou poskytnuty a činnosti a práce provedeny za podmínek uvedených v příloze č. 1 k této smlouvě, není-li dále stanoveno jinak. Bez provedení těchto služeb a prací nebude možné považovat předmět koupě za řádně dodaný.
- 4.3. Spolu s Předmětem koupě předá prodávající kupujícímu zejména:
- 4.4. veškeré listiny, jichž je třeba k nakládání s předmětem koupě a k jeho řádnému užívání a údržbě v českém, slovenském nebo anglickém jazyce (zejména návod k použití a obsluze),
- 4.5. veškerou technickou či jinou dokumentaci vztahující se k předmětu koupě, z níž bude vyplývat zejména, že předmět koupě splňuje požadavky na jeho použití kupujícím k požadovanému účelu podle této smlouvy, právních předpisů a technických norem platných a účinných ke dni odevzdání předmětu koupě kupujícímu (zejména prohlášení o shodě apod.).
- 4.6. Prodávající je povinen postupovat při poskytování plnění podle této smlouvy podle harmonogramu, který je uveden v příloze č. 1 k této smlouvě, zejména dodržet lhůty v něm uvedené, jakož i podle ostatních ustanovení přílohy č. 1 k této smlouvě a splnit všechny povinnosti a požadavky v této příloze uvedené.
- 4.7. Plnění podle této smlouvy prodávající poskytne v rozsahu, způsobem, v jakosti a za podmínek stanovených:
- 4.8. touto smlouvou vč. přílohy č. 1 k ní,
- 4.9. Nabídkou,
- 4.10. obecně závaznými právními předpisy, normami ČSN a EN, metodikami výrobců, pokud neodporují právním předpisům a ČSN a EN, a veškerými písemnými pokyny a podklady předanými kupujícímu prodávajícímu podle této smlouvy a případnými pozdějšími změnami shora uvedené dokumentace, které byly vyvolány potřebami zjištěnými v průběhu plnění předmětu smlouvy, jeho kontroly či jinými okolnostmi smluvními stranami nepředvídanými, rozhodnutími, resp. vyjádřeními veřejnoprávních orgánů, výsledky kontrolních dnů a prováděných zkoušek s tím, že kupující je oprávněn upravit způsob plnění předmětu smlouvy,

přičemž platí, že v případě rozporů mezi výše uvedenými podklady platí, že předmět smlouvy je definován tak, aby vyhověl všem požadavkům na obdobné předměty a mohl být užíván ke svému účelu s tím, že pokud takový rozpor nebude zasahovat do možnosti řádného užívání předmětu koupě, má v případě rozporů větší váhu definice obsažená v podkladu podle výše uvedeného pořadí sestupně [nejvyšší váhu má písm. a)], to však neplatí, pokud Nabídka nabízí kupujícímu kvalitativně či kvantitativně jednoznačně výhodnější řešení.

Čl. 5 Licence

- 5.1. Prodávající v rámci plnění předmětu této smlouvy dodává software specifikovaný v čl. 4 odst. 4.1 písm. h) až j) podléhající ochraně podle zákona č. 121/2000 Sb. (autorský zákon), ve znění pozdějších předpisů, a ustanovení § 2358 a následujících občanského

zákoníku, proto poskytuje kupujícímu licenci k tomuto softwaru (tj. oprávnění k výkonu práva duševního vlastnictví (licenci) v ujednaném rozsahu), a to formou licenčního ujednání v této kupní smlouvě. Licence se poskytuje jako:

- a) nevýhradní k veškerým známým způsobům užití, a to v rozsahu minimálně nezbytném pro řádné užívání software kupujícími;
- b) neomezená územním či množstevním rozsahem (není-li v této smlouvě uvedeno jinak) a rovněž tak neomezená způsobem nebo rozsahem užití;
- c) na dobu určitou, a to po celou dobu trvání majetkových práv,
- d) převoditelná a postupitelná, tj. s právem postoupení licence třetí osobě.

5.2. Licence ve shora uvedeném rozsahu se vztahuje i na jakákoli rozšíření, upgrady, updaty, patche a další změny software.

5.3. Kupující není povinen poskytnutou licenci využít.

5.4. Licence se poskytuje v maximálním rozsahu povoleném platnými právními předpisy.

5.5. Prodávající prohlašuje, že odměna za poskytnutí licence je zcela zahrnuta v kupní ceně podle čl. 6 této smlouvy.

Čl. 6 Kupní cena a platební podmínky

6.1. Kupující se zavazuje zaplatit prodávajícímu za plnění vymezené v čl. 4 této smlouvy kupní cenu ve výši

9 778 662,00 Kč bez DPH,

tj. 11 832 181,02 Kč včetně DPH,

když DPH ve výši 21 % činí 2 053 519,02 Kč.

6.2. Kupní cena je stanovena jako cena konečná a úplná, zahrnuje veškeré dodávky a služby s dodávkami související a veškeré jiné náklady nezbytné pro řádnou a úplnou realizaci předmětu plnění této smlouvy včetně všech rizik a vlivů s plněním předmětu této smlouvy souvisejících. Kompletní skladba kupní ceny a její rozklad jsou uvedeny v příloze č. 3 k této smlouvě.

6.3. Prodávající není oprávněn požadovat po kupujícím poskytnutí zálohy.

6.4. Prodávající na sebe bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy. V případě, že dojde mezi dnem podpisu kupní smlouvy a dnem uskutečnění zdanitelného plnění ke změně sazby DPH podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, bude daň z přidané hodnoty připočtena ke kupní ceně ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

6.5. Kupní cenu zaplatí kupující prodávajícímu převodem na bankovní účet prodávajícího uvedený v článku 1 této smlouvy na základě daňového dokladu (faktury) vystaveného prodávajícím ke dni uskutečnění zdanitelného plnění, který je dnem podepsání předávacího protokolu na předmět plnění dle této smlouvy. Daňový doklad je považován za proplacený okamžikem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího.

6.6. Prodávající na základě svého práva vystavit daňový doklad (fakturu) vystaví samostatnou fakturu za předmět koupě dle této smlouvy. Prodávající je oprávněn vystavit fakturu a doručit ji kupujícímu až po odevzdání úplného předmětu koupě vč. jeho

součástí a příslušenství vč. listin podle čl. 4 odst. 4.3 a poskytnutí či provedení souvisejících plnění, potvrzených oboustranně podepsaným protokolem podle čl. 7 odst. 7.6.

- 6.7. Na daňovém dokladu (faktuře) bude uveden rozklad fakturované částky na jednotlivá zařízení, tak aby byla zřejmá cena jednotlivých zařízení, a tak aby bylo kupujícímu usnadněno zavedení do majetkové evidence. Součástí daňového dokladu rovněž musí být registrační číslo a název projektu „CZ.31.2.0/0.0/0.0/23_093/0009849 – Město Sokolov – Kybernetická bezpečnost“.
- 6.8. Splatnost daňového dokladu je 30 dnů ode dne jeho doručení kupujícímu.
- 6.9. Daňový doklad bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude mít náležitosti obchodní listiny dle § 435 občanského zákoníku. V případě, že daňový doklad takové náležitosti nebude splňovat, bude kupujícím vrácen do dne splatnosti daňového dokladu k opravení bez jeho proplacení. V takovém případě lhůta splatnosti počíná běžet znovu ode dne doručení opraveného či nového vyhotovení daňového dokladu.
- 6.10. Pro případ, že prodávající je, nebo se od data uzavření smlouvy do dne uskutečnění zdanitelného plnění stane na základě rozhodnutí správce daně „nespolehlivým plátcem“ ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, souhlasí prodávající s tím, že mu kupující uhradí cenu plnění bez DPH a DPH v příslušné výši odvede za nespolehlivého plátce přímo příslušnému správci daně. V souvislosti s tímto ujednáním nebude prodávající vymáhat od kupujícího část z ceny plnění rovnající se výši odvedeného DPH a souhlasí s tím, že tímto bude uhrazena část jeho pohledávky, kterou má vůči kupujícímu, a to ve výši rovnající se výši odvedené DPH.

Čl. 7 Předání a převzetí věci a vlastnické právo

- 7.1. Prodávající je povinen předat kupujícímu předmět koupě vč. všech jeho součástí a příslušenství a listiny a dokumenty podle čl. 4 odst. 4.3, poskytnout, resp. provést související plnění (podle čl. 4 odst. 4.2) a provést veškeré práce a činnosti, které jsou součástí plnění podle této smlouvy, do 120 dnů od nabytí účinnosti této smlouvy.
- 7.2. Místem dodání a předání předmětu plnění této smlouvy jsou technologické místnosti kupujícího v budově Městského úřadu Sokolov, Rokycanova 1929, 356 01 Sokolov.

Před dodávkou zařízení je prodávající povinen vyzvat kontaktní osobu kupujícího k potvrzení rozdělení jednotlivých dodávek mezi výše uvedené technologické místnosti.
- 7.3. Vlastnické právo k předmětu plnění přechází na kupujícího v okamžiku jeho předání prodávajícím a převzetí kupujícím potvrzeného na předávacím protokolu.
- 7.4. Nebezpečí nahodilé zkázy a nahodilého zhoršení vlastností předmětu plnění včetně užitku přechází na kupujícího současně s nabytím vlastnictví.
- 7.5. Náklady spojené s předáním předmětu plnění, zejména dopravu, nese prodávající a náklady spojené s převzetím nese kupující.
- 7.6. O předání a převzetí předmětu koupě, souvisejících plnění (podle čl. 4 odst. 4.2) a souvisejících dokladů podle čl. 4 odst. 4.3 bude sepsán předávací protokol podepsaný

zástupci obou smluvních stran. Za kupujícího je předávací protokol oprávněn podepsat a předmět plnění převzít kontaktní osoba kupujícího uvedená v článku 1. této smlouvy.

- 7.7. Pokud prodávající předmět plnění nedoručí vlastními prostředky, ale využije k tomu dopravce, považuje se za odevzdání věci kupujícímu až okamžik doručení takovým dopravcem. Ustanovení § 2090 a § 2091 občanského zákoníku se nepoužijí.
- 7.8. Kupující je oprávněn před samotným převzetím předmětu koupě, jeho součástí a příslušenství, listin podle čl. 4 odst. 4.3 a souvisejících plnění (podle čl. 4 odst. 4.2) vše zkontrolovat vč. kontroly funkčnosti a prodávající je povinen mu k tomu poskytnout nezbytnou součinnost.
- 7.9. Kupující je oprávněn odmítnout převzít předmět koupě vč. jeho součástí a příslušenství, listiny podle čl. 4 odst. 4.3 a související plnění (podle čl. 4 odst. 4.2) (resp. jejich výsledek), některé z nich či jejich část, bude-li se na nich či jejich části vyskytovat v době odevzdání či předání vada (vč. nedodělků); o odmítnutí převzetí se pořídí protokol.
- 7.10. Předmět koupě vč. jeho součástí a příslušenství, listiny podle čl. 4 odst. 4.3 a související plnění (podle čl. 4 odst. 4.2) (resp. jejich výsledek) se považují za odevzdané (popř. provedené) a povinnost prodávajícího odevzdat (popř. předat) je kupujícímu je splněna až okamžikem jejich převzetí kupujícím bez vad a nedodělků.
- 7.11. V případě, že se na předmětu koupě vč. jeho součástí a příslušenství, listinách podle čl. 4 odst. 4.3 a souvisejících plnění (podle čl. 4 odst. 4.2) (resp. jejich výsledku), některé z nich či jejich části bude vyskytovat vada anebo nedodělky, je kupující oprávněn, nikoli však povinen, je převzít, přičemž v protokolu podle odst. 7.6 uvede, že předmět koupě, listiny podle čl. 4 odst. 4.3 a související plnění (podle čl. 4 odst. 4.2) (resp. jejich výsledek) přebírá s vadami, které v protokolu konkretizuje, a stanoví prodávajícímu přiměřenou lhůtu k jejich odstranění, ve které je prodávající povinen vady vlastním nákladem odstranit. Strany výslovně sjednávají, že se v takovém případě nejedná o převzetí věci či prací nebo činností (resp. jejich výsledku), které jsou předmětem plnění podle této smlouvy, bez vad ve smyslu jiných ustanovení této smlouvy. Při odevzdání, resp. předání a převzetí po uplynutí lhůty k odstranění vad se podle tohoto článku postupuje obdobně.

Čl. 8 Součinnost

- 8.1. Součinnost kupujícího bude omezena na nezbytnou míru a bude se vztahovat především na schvalování výstupů prodávajícího v předem definovaných kontrolních dnech a na nezbytnou IT podporu nutnou k nasazení technologií.
- 8.2. Rozsah součinnosti bude odsouhlasen před zahájením implementačních a instalačních služeb, včetně termínů jejího poskytování.
- 8.3. V případě následného požadavku prodávajícího na součinnost nad dohodnutý rámec má kupující právo součinnost odmítnout, případně ji poskytnout v termínu a rozsahu dle svých možností, a to bez dopadu na harmonogram realizace a z něj vyplývající sankce za nedodržení termínů.
- 8.4. Neposkytnutí součinnosti jako důvod pro posun smluvních termínů bude akceptován pouze tam, kde byla součinnost kupujícím přislíbena při zahájení implementačních a instalačních prací.

Čl. 9 Projektový tým (seznam techniků)

9.1. Prodávající se zavazuje předmět plnění smlouvy realizovat prostřednictvím projektového týmu (techniků), kterým prokázal kvalifikaci v zadávacím řízení na veřejnou zakázku. Projektový tým (technici) prodávajícího je odpovědný za plnění této smlouvy.

9.2.

9.3.

9.4.

9.5.

9.6.

9.7. Změna konkrétní osoby na pozici člena projektového týmu prodávajícího je možná pouze za předpokladu prokázání potřebné kvalifikace novou osobou v rozsahu stanoveném pro danou pozici člena projektového týmu stanovenou v zadávací dokumentaci veřejné zakázky. Taková změna musí být prodávajícím řádně iniciována a písemně dokladována, jakož i prokázána kvalifikace nové osoby na pozici člena projektového týmu před jeho zapojením do realizace plnění dle této smlouvy (včetně všech souvisejících požadavků na projektový tým stanovený v zadávacích podmínkách, na jejichž základě je uzavřena tato smlouva, jako např. max. počet pozic obsazených jednou osobou apod.).

Čl. 10 Další práva a povinnosti smluvních stran

10.1. Prodávající se zavazuje zaslat kupujícímu seznam sériových čísel dodaných zařízení podle čl.4 odstavce 4.1 písmene a) až e) včetně MAC adres síťových karet, a to v elektronické podobě do datové schránky kupujícího nejpozději do 1 týdne od převzetí předmětu koupě stvrzeného protokolem podle článku 7.6 této smlouvy.

10.2. Prodávající se dále zavazuje předat kupujícímu listinné potvrzení dodaných licencí, které jsou předmětem koupě této kupní smlouvy, ve lhůtě definované ve čl.7 odstavci 7.1.

10.3. Prodávající je povinen uchovávat veškerou dokumentaci související s realizací projektu (předmětu plnění této smlouvy) včetně účetních dokladů minimálně do konce roku 2036.

10.4. Prodávající je povinen minimálně do konce roku 2036 poskytovat požadované informace a dokumentaci související s realizací projektu (předmětu plnění této smlouvy) zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu (předmětu plnění této smlouvy) a poskytnout jim při provádění kontroly součinnost.

10.5. Prodávající je v rámci plnění této smlouvy povinen:

- dodržovat lidská, sociální a pracovní práva osob, jež použije k plnění veřejné zakázky, vyplývající z obecně závazných právních předpisů;
- dodržovat veškeré povinnosti ohledně bezpečnosti práce a ochrany před vznikem nemoci z povolání, vyplývající z obecně závazných právních předpisů;
- dodržovat své povinnosti z hlediska zaměstnanosti a právních předpisů týkajících se zaměstnávání cizinců, vyplývající z obecně závazných právních předpisů;

- využívat práci osob znevýhodněných na trhu práce nebo dodávek sociálních podniků, pokud to bude možné;
- neznevýhodňovat malé a střední podniky jako své poddodavatele a plnit závazky k nim řádně a včas;
- dodržovat své povinnosti z hlediska ochrany životního prostředí, a to včetně povinností při nakládáním s odpady, vyplývající z obecně závazných právních předpisů, a
- využívat postupy a dodávky šetrné k životnímu prostředí – recyklace/znovu využití obalů, pokud je to možné.

Čl. 11 Práva z vadného plnění a smluvní záruka

- 11.1. Prodávající poskytuje kupujícímu záruku za jakost předmět koupě a všech jeho součástí a příslušenství s tím, že délka záruční doby je stanovena v příloze č. 1 k této smlouvě. Stanoví-li však prodávající v Nabídce, prohlášení o záruce či jinde delší záruční dobu anebo je delší záruční doba stanovena jinde (např. technické či výrobní dokumentaci), platí tato delší záruční doba. Prodávající odpovídá za vady zjevné, skryté i právní, které má předmět koupě v době jeho předání kupujícímu, a dále za ty, které se na zboží vyskytnou v záruční době.
- 11.2. Záruční doba na jednotlivá zařízení, která jsou předmětem plnění této smlouvy, počíná běžet dnem jejich předání kupujícímu na základě řádně oběma smluvními stranami podepsaného předávacího protokolu.
- 11.3. Prodávajícím poskytnutá záruka se vztahuje na funkčnost dodaného plnění, jakož i na jeho vlastnosti požadované kupujícím.
- 11.4. Délka záruční doby vztahující se na záruku na příslušenství a provedené implementační práce činí dva (2) roky, není-li uvedeno v příloze č. 1 této smlouvy jinak. V případě vad takového příslušenství se prodávající zavazuje provést opravu nebo věc nahradit novou do 30 kalendářních dnů ode dne nahlášení vady kupujícím v sídle kupujícího. V případě vady provedené implementační práce se prodávající zavazuje odstranit závadu do 14 kalendářních dnů ode dne nahlášení vady kupujícím.
- 11.5. Po celou záruční dobu na samotná zařízení podle této smlouvy prodávající garantuje kupujícímu přijmout od něj nahlášení poruchy a dle parametrů záruky pro jednotlivé zařízení dle specifikace uvedené v příloze č. 1 této smlouvy garantuje realizaci opravy technikem v místě dodávky.
- 11.6. Prodávající odpovídá kupujícímu za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání, stanovené v minimální konfiguraci v technické specifikaci kupujícího a v konečné konfiguraci ve specifikaci obsažené v Nabídce.
- 11.7. Prodávající odpovídá kupujícímu dále za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání a že je bez právních a faktických vad. Dále prodávající zaručuje, že na dodaném předmětu smlouvy nevážnou práva třetích osob.
- 11.8. Prodávající se zavazuje zajistit, že veškerá komunikace na základě této kupní smlouvy bude z jeho strany vedena v českém jazyce, a to včetně uplatňování a řešení závad a reklamací jednotlivých zařízení a licencí na základě této smlouvy.
- 11.9. Vady musí kupující uplatnit u prodávajícího bez zbytečného odkladu poté, co se o nich dozví.

- 11.10. Uplatněním práv z odpovědnosti za vadné plnění není dotčeno právo kupujícího na náhradu škody.
- 11.11. Ujednáními v tomto článku ani ujednáními týkajícími se záruky v příloze č. 1 k této smlouvě nejsou nijak dotčena další práva kupujícího plynoucí mu z titulu vad z obecně závazných právních předpisů (práva z vadného plnění).
- 11.12. Pokud prodávající jednostranně písemně oznámí, že může vady předmětu koupě (jeho jednotlivých částí) uplatnit i přímo u výrobců či jeho dodavatelů těchto jednotlivých součástí předmětu koupě, uplatněním vady u takové třetí osoby považuje se vada uplatněná i u prodávajícího. Právo kupujícího uplatňovat vady předmětu koupě přímo u prodávajícího tím není dotčeno.

Čl. 12 Smluvní pokuty

- 12.1. V případě prodlení prodávajícího s odevzdáním předmětu koupě, kterékoliv jeho části, příslušenství či listiny podle čl. 4 odst. 4.3 nebo prodlení s poskytnutím souvisejících plnění podle čl. 4. odst. 4.2 nebo prodlení s provedením jakékoliv činnosti či práce, které jsou součástí plnění podle této smlouvy, je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 5 000 Kč za každý den prodlení.
- 12.2. V případě prodlení prodávajícího s odstraněním vady ve lhůtě uvedené v čl. 11.5 smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 500 Kč za každou, i započatou, hodinu prodlení prodávajícího s odstraněním vady.
- 12.3. V případě prodlení prodávajícího s odstraněním vady příslušenství je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 200 Kč za každý celý kalendářní týden prodlení.
- 12.4. V případě prodlení prodávajícího s odstraněním vady v podobě provedených implementačních a konfiguračních prací je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 500 Kč za každý pracovní den prodlení.
- 12.5. V případě realizace předmětu plnění této smlouvy projektovým týmem prodávajícího v jiném složení, než které je uvedeno v článku 9.2 této smlouvy, je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 20 000 Kč za každý zjištěný případ.
- 12.6. Poruší-li nebo nesplní-li prodávající jakoukoliv jinou povinnost uvedenou v této smlouvě než povinnost podle odst. 12.1 až 12.5 a nezjedná-li nápravu v přiměřené lhůtě stanovené kupujícím, je povinen zaplatit kupujícímu smluvní pokutu ve výši 5 000 Kč za každý den prodlení a za každé nesplnění (porušení) povinnosti; není-li možné nápravu zjednat, výzva ke zjednání nápravy se nečiní.
- 12.7. Zaplacením smluvní pokuty nejsou dotčeny povinnost prodávajícího splnit dluh zajištěný smluvní pokutou ani právo na náhradu škody způsobené porušením povinnosti zajištěné smluvní pokutou.
- 12.8. Smluvní pokuta je splatná na základě písemné výzvy kupujícího do 10 dnů od doručení výzvy prodávajícímu převodem na účet uvedený v záhlaví této smlouvy.
- 12.9. Povinnost zaplatit smluvní pokutu může vzniknout i opakovaně a její celková výše není omezena.
- 12.10. Povinnost zaplatit smluvní pokutu trvá i po skončení této smlouvy či odstoupení od ní.

- 12.11. Prodávající považuje smluvní pokuty sjednané v tomto článku za přiměřené a vzdává se práva domáhat se u soudu jejich snížení.

Čl. 13 Odstoupení od smlouvy

- 13.1. Odstoupení od smlouvy se řídí ustanovením § 223 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a dále § 2001 a násl. občanského zákoníku.
- 13.2. Kupující je kromě důvodů pro odstoupení od smlouvy stanovených občanským zákoníkem oprávněn odstoupit od této smlouvy v případě, že:
- 13.3. prodávající je v prodlení s dodáním předmětu koupě, listin či dokumentů podle čl. 4 odst. 4.3 nebo s poskytnutím souvisejících plnění podle čl. 4. odst. 4.2 nebo provedením jiných prací či činností, které jsou součástí plnění podle této smlouvy, či kterékoli jejich části nebo s odstraněním jejich vad déle než 15 dnů,
- 13.4. proti prodávajícímu bude zahájeno insolvenční řízení, prodávající vstoupí do likvidace nebo proti němu bude zahájeno exekuční řízení, které bude ohrožovat nebo narušovat řádné plnění této smlouvy,
- 13.5. prodávající poruší nebo nesplní jinou povinnost podle této smlouvy než povinnosti podle písm. a) nebo b) a toto porušení neodstraní ani do 15 dnů od doručení výzvy kupujícího k odstranění,
- 13.6. prodávající uvedl v Nabídce informace nebo předložil doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výběr prodávajícího k uzavření této smlouvy coby smlouvy na veřejnou zakázku,
- 13.7. ukáže-li se jakékoliv prohlášení prodávajícího v této smlouvě jako nepravdivé či neodpovídající skutečnosti.
- 13.8. Prodávající je oprávněn od této smlouvy odstoupit, nebude-li uhrazena kupní cena do 60 dnů ode dne její splatnosti.
- 13.9. Právo odstoupit od této kupní smlouvy má kupující i tehdy, jestliže jej prodávající ujistil, že předmět plnění této smlouvy má určité vlastnosti, zejména vlastnosti kupujícím vymíněné, anebo prodávající kupujícího ujistil, že předmět plnění této smlouvy nemá žádné vady, a toto ujištění se ukáže být nepravdivým.

Čl. 14 Registr smluv – doložka

- 14.1. Prodávající uděluje souhlas kupujícímu k uveřejnění všech podkladů, údajů a informací uvedených v této smlouvě, k jejichž uveřejnění vyplývá pro kupujícího povinnost dle právních předpisů.
- 14.2. Prodávající je současně srozuměn s tím, že kupující je oprávněn zveřejnit obsah smlouvy (celý její obsah) a jejich případných změn (dodatků) a dalších dokumentů od této smlouvy odvozených včetně metadata požadovaných k uveřejnění dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.
- 14.3. Zaslání smlouvy k uveřejnění prostřednictvím registru smluv zajistí kupující.

Čl. 15 Závěrečná ustanovení

- 15.1. Smluvní strany se dohodly, že prodávající na sebe podle § 1765 odst. 2, jakož i podle § 2620 odst. 2 občanského zákoníku přebírá nebezpečí změny okolností.
- 15.2. Tato smlouva je vyhotovena v elektronickém originále, jež po podpisu zástupců obou smluvních stran obdrží obě smluvní strany.
- 15.3. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti uveřejněním prostřednictvím registru smluv.
- 15.4. Právní vztahy touto smlouvou výslovně neupravené a s ní související nebo z ní vyplývající se řídí ustanoveními občanského zákoníku.
- 15.5. Tato smlouva může být změněna pouze písemnou dohodou obou smluvních stran formou vzestupně číslovaných dodatků, schválených na straně kupujícího v souladu se zákonem č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů.
- 15.6. Nedílnými součástmi této smlouvy jsou:
- Příloha č. 1 – Technická dokumentace zadavatele (kupujícího),
 - Příloha č. 2 – Nabídka,
 - Příloha č. 3 – Cenová tabulka z nabídky prodávajícího.
- 15.7. Strany této smlouvy berou na vědomí, že kupující jako správce osobních údajů je oprávněn zpracovávat zde uvedené osobní údaje v souladu s článkem 6 odst. 1 písm. b) Obecného nařízení (toto zpracování je nezbytné pro splnění smlouvy) a písm. c) (toto zpracování je nezbytné pro splnění právní povinnosti správce zveřejnit smlouvu na profilu zadavatele dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, postupy podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím nebo na své úřední desce dle zákona č. 128/2000 Sb., o obcích).
- 15.8. V případě, že po podpisu této smlouvy na prodávajícího anebo jeho poddodavatele budou dopadat mezinárodní sankce podle zákona upravujícího provádění mezinárodních sankcí č. 69/2006 Sb. ve smyslu zákona č. 240/2022 Sb. účinného od 1. 9. 2022, je povinen to prodávající písemně oznámit kupujícímu. V případě, že oznámení neprovede a kupující zjistí, že na prodávajícího anebo jeho poddodavatele mezinárodní sankce dopadají, vyzve prodávajícího k vysvětlení nebo nápravě formou vyjmutí osoby ze sankčního seznamu. V případě že náprava není možná, odstoupí kupující od této smlouvy, přičemž účinnost odstoupení nastává doručením odstoupení prodávajícímu.
- 15.9. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují vlastnoruční podpisy na smlouvě.
- 15.10. Uzavření této smlouvy bylo schváleno usnesením Rady města Sokolova z 13. 11. 2025, č. 839/23RM/2025.



Příloha č. 4 Zadávací dokumentace – Technická dokumentace zadavatele

Příloha č. 1 Kupní smlouvy – Technická dokumentace kupujícího

Technická dokumentace

Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti

Verze 015 ze dne 30.07.2025

Obsah dokumentu

1. TECHNICKÁ SPECIFIKACE ZADAVATELE (KUPUJÍCÍHO)	3
1.1. NEXT GENERATION FIREWALL S PŘÍSLUŠENSTVÍM	5
1.2. PÁTEŘNÍ PŘEPÍNAČE 48P PŘÍSLUŠENSTVÍM	6
1.3. PŘÍSTUPOVÉ PŘEPÍNAČE 48P PoE PŘÍSLUŠENSTVÍM	7
1.4. PŘÍSTUPOVÉ PŘEPÍNAČE 24P PoE PŘÍSLUŠENSTVÍM	8
1.5. LICENCE SW PRO ŘÍZENÍ PŘÍSTUPU DO SÍTĚ ZALOŽENÉHO NA PROTOKOLU 802.1X	9
1.6. LICENCE SW APLIKACE PRO VÍCEFAKTOROVÉ OVĚŘOVÁNÍ UŽIVATELŮ A SPRÁVU AUTENTIZAČNÍCH PROSTŘEDKŮ A CERTIFIKÁTŮ, LICENCE SW SYSTÉMU PKI	11
1.7. AUTENTIZAČNÍ PROSTŘEDEK	12
1.8. KLÁVESNICE S INTEGROVANOU ČTEČKOU KARET, VČETNĚ OVLADAČŮ	13
1.9. SAMOSTATNÉ USB ČTEČKY ČÍPOVÝCH KARET, VČETNĚ OVLADAČŮ	13
1.10. LICENCE K NÁSTROJI PRO SPRÁVU PRIVILEGOVANÝCH ÚČTŮ SERVERŮ – PIM/PAM	13
2. POŽADAVKY NA INSTALAČNÍ A IMPLEMENTAČNÍ PRÁCE	16
2.1. SPECIFIKACE KONKRÉTNÍCH INSTALAČNÍCH A IMPLEMENTAČNÍCH POŽADAVKŮ	17
2.2. POŽADAVKY NA PŘEDIMPLEMENTAČNÍ ANALÝZU	18
2.3. POŽADAVKY NA ZPRACOVÁNÍ PROVÁDĚCÍ DOKUMENTACE	19
2.4. POŽADAVKY NA PROVOZNÍ DOKUMENTACI	19
2.5. POŽADAVKY NA ZAŠKOLENÍ	19
2.6. POŽADAVKY NA PROVEDENÍ ZKUŠEBNÍHO PROVOZU A AKCEPTAČNÍCH TESTŮ	19
2.7. DALŠÍ POŽADAVKY NA ZÁRUKY, ZÁRUČNÍ SERVIS A DALŠÍ PODMÍNKY V RÁMCI ZÁRUKY	20
3. HARMONOGRAM PLNĚNÍ	21

1. Technická specifikace zadavatele (kupujícího)

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Tyto důvody jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu veřejné správy zadavatele.

Propojení zařízení – SFP moduly a kabely

Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

Plnění jednotlivých komponent dle specifikace níže je požadováno v následujícím rozsahu, a to včetně příslušenství:

Položka plnění	Počet kusů
Next Generation Firewall s příslušenstvím	2
Pátevní přepínače 48p s příslušenstvím	2
Přístupové přepínače 48p PoE s příslušenstvím	28
Přístupové přepínače 24p s příslušenstvím	2
Licence SW pro řízení přístupu do sítě založeného na protokolu 802.1x	1
Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI	1
Autentizační prostředky	300
Klávesnice s integrovanou čtečkou karet, včetně ovladačů	150
Samostatné USB čtečky čipových karet, včetně ovladačů	150
Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM	1

1.1. Next Generation Firewall s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Pro montáž do 19" datového rozvaděče, včetně montážního materiálu
NGFW	Min. základní funkce Next-generation firewall – viz https://en.wikipedia.org/wiki/Next-generation_firewall – firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.
Porty	Min 2× 2.5GbE, 8x 1GbE a 2× 10GbE
Počet současných spojení	Min. 6 000 000.
Propustnost VPN	Min. 10 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 100 klientů.
Propustnost firewallu	Min. 18 Gbps pro pakety 1518 bytů a větší, provoz UDP.
Propustnost NGFW	Min. 15 Gbps při aktivní IPS.
Propustnost IPS	min. 15 Gbps pro provoz typu Enterprise mix.
Propustnost detekce škodlivého kódu	Min. 5 Gbps při zapnuté IPS.
Virtualizace	Podpora min 5 izolovaných virtuálních kontextů (virtuálních firewallů). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů.
Vysoká dostupnost	Režimy Active/Active se společnou konfigurací, včetně případných nezbytných licencí.
Dualstack	Podpora současného běhu IPv4 a IPv6.
VPN	Podpora IPSec, SSL VPN
Bezpečné DNS	Automatická blokáce přístupu k škodlivým doménám a IP adresám, definice součástí bezpečnostních aktualizací. Ochrana proti DNS tunelování.
Aplikační kontrola	Detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu.
Antivir	Integrovaný antivirus, podpora protokolu ICAP pro externí antivir
ZeroDay	Ochrana před ZeroDay útoky formou emulace neznámého kódu v bezpečném prostředí – Sandboxu
Kategorizace a blokáce provozu	Založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu
Antispam	Antispamová a antivirová a antiphishingová inspekce elektronické pošty. Transparentní (průchozí) kontrola i MTA režim.
Aktualizace	Automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení.
Ověřování uživatelů	LDAP, Active Directory, Radius, Ověřování na základě certifikátu.
Management a monitoring	HTTP/S, SSH, SNMP, syslog.

Centrální správa	Jednotná centrální správa samostatných boxů i clusteru, monitorování a aktualizace firmware z centrální grafické konzole. Lokální i cloudová správa s podporou spolupráce více správců (např. při řešení bezpečnostních událostí/incidentů) při zachování konzistence konfigurační nastavení.
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent (sFlow není ekvivalent).
Geolokace	Možnost nastavovat firewall politiky na základě geografických údajů IP adres
Standardní funkce	NAT, statické a dynamické routování (OSPFv3, BGP, RIP), publikace interních serverů, routování založené na politikách (policy based routing).
API	Integrované API rozhraní pro automatizaci a orchestraci
Napájení	Redundantní napájecí zdroje.
Záruční doba, podpora a záruční servis, technická podpora výrobce	Záruční doba, podpora a záruční servis min. 60 měsíců v režimu 8x5 poskytovaný výrobcem zařízení, odeslání náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a všech bezpečnostních funkcí – URL filtrace, DNS, IPS, antimalware, antispam, aplikační kontrola, sandbox, ZeroDay).

1.2. Páteří přepínače 48p příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní parametry	L2/L3 přepínač v rackovém provedení, 1U včetně montážního materiálu
Porty	min. 48x 10 Gb SFP+, 4x 100 Gb QSFP28 s podporou QSFP+
Propustnost	Neblokovaná architektura, přepínací kapacita je min. součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Agregace portů	Podpora LACP, min. 50 skupin, min. 8 portů ve fyzické agregační skupině, min. 16 portů ve virtuální agregační skupině při zapojení přepínačů do logického páru.
Směrování	Statické směrování (routování) včetně VLAN, dynamické směrování (min. RIP, OSPF, BGP), směrování založené na politikách, min. routovacích záznamů pro IPv4 24 000 a IPv6 12 000
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	Minimální přepínací výkon: 1,7 Tbps
VLAN	VLAN 802.1Q, MAC i založená na protokolu, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření, podpora IEEE 802.1ad (Q-in-Q), podpora statických a dynamických VXLAN, min. 1024 VLAN. Podpora privátních VLAN (PVLAN) pro izolaci klientů ve stejné VLAN (mikrosegmentace, dynamická segmentace)
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora min. 140 000 MAC adres.
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent. sFlow není ekvivalent.
Zrcadlení portů	Zrcadlení provozu (odchozího i příchozího) do lokálního i vzdáleného portu

Parametr	Popis minimální úrovně parametru
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST API a integrovaná podpora skriptů pro automatizaci. Interní detailní monitorování funkcí/služeb přepínače s možností konfigurovatelných automatických reakcí.
Nezávislý management	Vyhrazený LAN port pro správu (out-of-band management) - nezapočítává se do požadovaného počtu portů (viz Porty)
Napájení, chlazení	Integrované redundantní interní napájecí zdroje, zdroje i ventilátory vyměnitelné za provozu (hot-swap)
Centrální správa	Podpora stávajícím systém centrální správy
Stohování	Pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - např. technologie MLAG/MCLAG (Multi-Chassis Link Aggregation) nebo obdobná. Synchronizace konfigurací přepínačů ve stohu. Min. 32 portů v agregační skupině stohu. Kapacita stohovacího propojení: 400 Gbps
Záruční doba a záruční servis	Záruční doba a záruční servis min. 60 měsíců v režimu 24x7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace SW a aktualizace firmware.

Příslušenství pro páteřní přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství centrálních přepínačů	Pro celý komplet dodávaných centrálních přepínačů požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů: 92x SFP+ 10 Gbps modul, SM, 10 km, LC, DMI diagnostika pro nabízené přepínače 4x SFP+ 10GbE modul, RJ-45, DMI diagnostika pro nabízené přepínače 8x QSFP28 100GBASE-SR4, MM, 100 m 2x patch kabel MM OM3/4 MPOf-MPOf, překřížený, 1 m – pro propojení nabízených přepínačů 4x patch kabel MM OM4, MPOf – 8x LC (4 páry), 3 m 60x patch kabel SM LC-SC, 3 m 36x patch kabel SM LC-LC, 3 m Cena příslušenství musí být zohledněna v ceně samotných přepínačů. Záruční doba na příslušenství min. 36 měsíců
Licence pro centrální správu	Je požadováno dodání licencí pro začlenění dodávaných přepínačů do systému centrální správy kupujícího.

1.3. Přístupové přepínače 48p PoE příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	L2+ přepínač v rackovém provedení max. 1U; maximální hloubka přepínače 35 cm (z důvodu omezených rozměrů pobočkových rozvaděčů)
Porty	Min. 48x 1 GbE, 4x 10 Gb SFP+.
Propustnost	Neblokovaná architektura, přepínací kapacita je min. součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Power on Ethernet	Podpora PoE/PoE+ 802.3af/at na všech metalických portech, celkový PoE výkon min. 700 W.

Parametr	Popis minimální úrovně parametru
Agregace portů	Podpora LACP, min. 16 portů v agregační skupině, min. 20 skupin.
Směrování	Statické směrování (routování), min. 500 směrovacích cest pro IPv4 i IPv6
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	Minimální přepínací výkon 175 Gbps Minimální paketový výkon 120 Mpps
VLAN	VLAN 802.1Q, MAC i založená na protokolu, podpora zařazování do VLAN na základě 802.1X ověření.
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora min. 16 000 MAC adres.
Zrcadlení provozu	Zrcadlení příchozího i odchozího síťového provozu
Napájení	Interní napájecí zdroj.
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API a integrovaná podpora skriptů pro automatizaci
Nezávislý management	Vyhrazený LAN port pro správu (out-of-band management) - nezapočítává se do požadovaného počtu portů (viz Porty)
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent. sFlow není ekvivalent
Centrální správa	Podpora stávajícím systém centrální správy
Stohování	Pokročilé stohování po SFP+ portech s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - např. technologie MLAG/MCLAG (Multi-Chassis Link Aggregation) nebo obdobná. Synchronizace konfigurací přepínačů ve stohu. Podpora min. 4 členů ve stohu.
Záruční doba a záruční servis	Záruční doba a záruční servis min. 60 měsíců v režimu 24x7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace a aktualizace firmware.

Příslušenství pro přístupové přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství přístupových přepínačů	Pro celý komplet dodávaných přístupových přepínačů 48p PoE požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů: 112 ks 10 Gb SFP+ modul SM, min. 10 km, diagnostika, LC konektor 56 ks 2 m propojovacích SM kabelů LC-LC 56 ks 2 m propojovacích SM kabelů LC-SC Cena příslušenství musí být zohledněna v ceně samotných přepínačů. Záruční doba na příslušenství min. 36 měsíců
Licence pro centrální správu	Je požadováno dodání licencí pro začlenění dodávaných přepínačů do systému centrální správy kupujícího.

1.4. Přístupové přepínače 24p PoE příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	L2+ přepínač v rackovém provedení max. 1U
Porty	Min. 24× 1 GbE, 4× 10 Gb SFP+.
Propustnost	Neblokovaná architektura, přepínací kapacita je min. součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Agregace portů	Podpora LACP, min. 8 portů v agregační skupině, min. 8 skupin.
Směrování	Statické směrování (routování), min. 500 směrovacích cest pro IPv4 i IPv6
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	Minimální přepínací výkon 125 Gbps Minimální paketový výkon 90 Mpps
VLAN	VLAN 802.1Q, MAC i založená na protokolu, podpora zařazování do VLAN na základě 802.1X ověření.
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora min. 8000 MAC adres.
Zrcadlení provozu	Zrcadlení příchozího i odchozího síťového provozu
Napájení	Interní napájecí zdroj.
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST API pro automatizaci.
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent. sFlow není ekvivalent
Centrální správa	Podpora stávajícím systém centrální správy
Záruční doba a záruční servis	Záruční doba a záruční servis min. 60 měsíců v režimu 24×7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace a aktualizace firmware.

Příslušenství pro přístupové přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství přístupových přepínačů	Pro celý komplet dodávaných přístupových přepínačů 24p požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů: • 8 ks 10 Gb SFP+ modul SM, min. 10 km, diagnostika, LC konektor • 4 ks 2 m propojovacích SM kabelů LC-LC • 4 ks 2 m propojovacích SM kabelů LC-SC Cena příslušenství musí být zohledněna v ceně samotných přepínačů. Záruční doba na příslušenství min. 36 měsíců
Licence pro centrální správu	Je požadováno dodání licencí pro začlenění dodávaných přepínačů do systému centrální správy kupujícího.

1.5. Licence SW pro řízení přístupu do sítě založeného na protokolu 802.1x

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Software nebo softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení
Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém
Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN
Základní autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty
Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází – Active Directory, LDAP, ODBC
Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, autorizace proti externí SQL databázi
Rozšířená autentizace a autorizace	Podpora autentizace a autorizace min. LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth)
Kontextová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory
Externí identity	Podpora autentizace externími identitami - min. Microsoft, Google
Komplexní autorizace	Autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. pro omezení celkového času online či objemu přenesených dat za delší časové období
Dynamická autorizace	Podpora RADIUS CoA podle RFC3576. Možnost změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení
Profilování	Zjišťování doplňujících informací pro koncová zařízení (min. typ, výrobce, OS a pod.)
TACACS+	Podpora autentifikace a autorizace na síťové prvky protokolem TACACS+
Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)
Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení
Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu
Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (např. jen potvrzení uvítací/informační stránky)
Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem apod.
Ochrana identit	Veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované šifrované databázi, které bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES min. 128-bit.
Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, UPS, technologické prvky, IoT.

Parametr	Popis minimální úrovně parametru
Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru min. 2 appliance. Druhá appliance není součástí dodávky.
Licence	Trvalá licence pro min. 1000 současných (konkurenčních) koncových zařízení ověřených pomocí 802.1X bez omezení počtu uživatelů
Automatizace a integrace	REST-API rozhraní min. pro základní funkce AAA.
Kompatibilita	Software nebo appliance bude výrobcem podporována pro provoz v prostředí stávající serverové virtualizace
Podpora	Podpora výrobce 60 měsíců včetně nároku na nové verze a aktualizace software

1.6. Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Systém pro autentizaci uživatele identifikačním prostředkem vůči adresářové službě včetně nástrojů pro správu
Autentizace	Autentizace uživatele ve stávajících operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem (Microsoft) pomocí nabízených autentizačních médií
Obnova certifikátů	Automatické hlídání expirace osobních certifikátů a vyvolání uživatelského průvodce pro jeho jednoduchou uživatelskou obnovu podle nastavených politik. Včetně automatického odstranění neplatných certifikátů na základě politik.
Uživatelská správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK)
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu v operačním systému, testování integrity a použitelnosti
Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů vystavených veřejnými certifikačními autoritami (min. Postsignum) a vyvolání průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik
Správa prostředků	Evidence a správa životního cyklu identifikačních prostředků
Prostředky	Podpora kontaktních i hybridních identifikačních prostředků
Správa systému	Webové rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory
Evidence	Systém umožní evidovat minimálně - typ prostředku (kontaktní, bezkontaktní, hybridní) - druh prostředku (uživatelský, administrační, operátorský) - stav prostředku (používaný, k recyklaci, skartovaný) - historii prostředku (datum zavedení do evidence, vydání uživateli, recyklace) - držitele prostředku (aktuálního držitele i všechny předchozí držitele) - data uložená v prostředku (certifikáty a další data, včetně historie dat)

Parametr	Popis minimální úrovně parametru
Integrace	Napojení na Active Directory (zdroj dat o uživateli, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty)
Správa certifikátů	Správa certifikátů (doménových i kvalifikovaných): - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření a tisk protokolu o vystavení - odvolání certifikátu - vydávání "v zastoupení" - např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance
Obnova prostředků	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů
Personifikace	Integrované prostředí pro generování podkladů pro potisk identifikačních karet externím dodavatelem i na vlastní tiskárně
Ukládání dat	Centrální databázové úložiště údajů, podpora Microsoft SQL server (stávající hlavní databázové úložiště zadavatele)
Rozhraní	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování informací napojených systémům
Notifikace	E-mailové notifikace uživatelů i správců o blížící se expiraci certifikátů doménových i veřejných certifikačních autorit
PKI	Součástí dodávky bude vybudování kompletní kompatibilní infrastruktury PKI (public key infrastructure) pro zajištění celého životního cyklu osobních přihlašovacích certifikátů a jejich šablon, včetně dodávky potřebných licencí
Licence	Licence pro 300 uživatelů
Podpora	Podpora výrobce po dobu 60 měsíců včetně nároku na nové verze a aktualizace software

1.7. Autentizační prostředek

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Hybridní identifikační karta s kontaktní částí SmartCard a bezkontaktní částí čipem EM4102
Podporované certifikáty	Karta musí umožnit ukládání a používání vlastních certifikátů a certifikátů veřejných certifikačních autorit (I. CA, Postsignum, eidentity)
Identity	Karta musí umožnit ukládání více identit
Kvalifikovaný podpis	Karta musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku), viz https://www.dia.gov.cz/cs/legislativa/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/informace-pro-uzivatele/seznam-vydavanych-kvalifikovanych-prostredku-pro-vytvoreni-elektronickych-podpisu-v-ceske-republice
SW podpora	Součástí dodávky bude software a ovladače pro zpřístupnění jejich rozhraní v operačních systémech Windows, Linux, macOS a systému terminálových služeb Microsoft RDS včetně rozšířených funkcionalit, tzv. middleware.
Záruční doba	Záruční doba 2 roky včetně nároku na aktualizace middleware

1.8. Klávesnice s integrovanou čtečkou karet, včetně ovladačů

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Standardní PC klávesnice se samostatným numerickým blokem a integrovanou čtečkou čipových karet
Rozhraní	USB rozhraní
Čtečka	Kompatibilita s čipovou částí nabízených identifikačních prostředků a nabízeným SW pro vícefaktorové ověřování
Lokalizace	České (QWERTZ) rozložení kláves, české popisky
SW podpora	Součástí dodávky bude software a ovladače pro operační systémy Windows, Linux, macOS – nejsou-li ovladače standardní součástí operačních systémů.
Záruční doba	Záruční doba min. 2 roky

1.9. Samostatné USB čtečky čipových karet, včetně ovladačů

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Samostatná čtečka čipových karet
Rozhraní	USB rozhraní
Čtečka	Kompatibilita s čipovou částí nabízených identifikačních prostředků a nabízeným SW pro vícefaktorové ověřování
SW podpora	Součástí dodávky bude software a ovladače pro operační systémy Windows, Linux, macOS – nejsou-li ovladače standardní součástí operačních systémů.
Záruční doba	Záruční doba min. 2 roky

1.10. Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní funkce	Privilegovaný přístup na cílový systém bude zprostředkován prostřednictvím tzv. terminal/jump serveru zvoleným komunikačním protokolem tak, aby privilegovaný uživatel neměl přístup k přihlašovacím údajům cílového systému. Izolace přístupu bude možná až na úrovni aplikace (typu webový prohlížeč s konkrétním URL, MMC konzole s vybraným snap-in, konkrétní aplikace - např. MS SQL Management Studio, WinSCP atp.) a uživatel nebude mít možnost přistupovat k jiným službám či aplikacím v rámci dané relace. Ukončením aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI systému nebo pomocí standardních protokolů RDP a SSH a standardních klientů.
Bezpečná autentizace	Podpora vynucení silné autentizace pro připojení ke vzdálené relaci
SSH připojení	Privilegovaný přístup prostřednictvím SSH protokolu bude v rámci vzdálené relace prováděn přes ssh proxy, na které bude uživatel ověřen svými přihlašovacími údaji (s možností spárování s Active Directory). K cílovému systému bude uživatel připojen a přihlášen podle bezpečností politiky vybraným privilegovaným účtem bez zadávání hesla. Pro připojení

Parametr	Popis minimální úrovně parametru
	pomocí ssh proxy bude systém podporovat vynucení silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí ssh klíče).
Webové připojení	Systém umožní zprostředkovat privilegovanému uživateli bezpečné připojení v rámci vzdálené relace na vybrané webové aplikace, přístup do cloudu apod. pomocí webové proxy, na které bude uživatel ověřen neprivilegovaným účtem (s možností ověření vůči Active Directory). K cílovému systému bude uživatel připojen a přihlášen podle bezpečností politiky vybraným privilegovaným účtem bez zadávání hesla. Systém bude podporovat transparentní SSO (single-sign-on).
Nahrávání relace	Monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu a ve formátu screenshotů. Záznam relace musí být vytvářen kontinuálně. V nahrávkách bude možné zpětně vyhledávat podle metadat. Přehrávání musí být dostupné přímo z GUI systému běžným internetovým prohlížečem a nesmí vyžadovat instalaci komponent třetích stran (flash, java, codec apod.).
Metadata	Zaznamenávání rozšířených informací (metadat) o relacích, minimálně stisky kláves a odpovědi monitorovaných zařízení
Nahrávky	Ukládání nahrávek relací v optimalizované kvalitě s možností volby cílového úložiště.
Politiky	Logické zařazení napojených systémů do skupin či profilů, nad kterými bude možno nastavit a aplikovat společné politiky a nastavení.
Ukončení relací	Možnost okamžitého ukončení potenciálně nebezpečných relací administrátorem či operátorem systému.
Auditování	Integrovaný audit jednotlivých akcí uživatelů s privilegovanými účty – min. zobrazení hesla, změny uložených údajů, vytvoření relace. Export auditních záznamů.
Bezpečnost auditních záznamů	Nezpochybnitelná auditovatelnost jednotlivých operací, reportování a textových logů. Auditní záznamy musí být bezpečně uloženy tak, aby k nim měli přístup pouze oprávnění uživatelé.
Reportování	Integrovaný generátor reportu veškerých aktivit správce systému. Přístupu k reportům musí být možno nastavit pouze vybraným uživatelům.
Autentizace	Podpora minimálně LDAP/S, SAML2, RADIUS pro autentizaci, autorizaci a vícefaktorové ověřování
Workflow	Integrované workflow pro zadávání a schvalování žádostí o přístup. Funkční požadavky na workflow: - Zadávání požadavků uživatelů - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů
Změna privilegií	Podpora delegace a eskalace privilegií na bázi schvalovacího workflow.
Vícedoménová autentizace	Podpora současného napojení více Active Directory/LDAP domén současně.
API rozhraní	Integrované API s podporu REST, aktivované v rámci dodávky. Výrobce, resp. dodavatel musí poskytovat volně dostupný aktualizovaný popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací.
Integrace servicedesk	Podpora napojení a integrace na servicedeskové/tiketovací systémy.
Odolnost	Veškeré komponenty systémy musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště účtů, přihlašovacích údajů, nahrávek relací a auditních záznamů musí být zabezpečeno a odděleno od ostatních komponent řešení.

Parametr	Popis minimální úrovně parametru
Správa účtů	Integrované vyhledávání (discovery) a správa účtů v systémech Windows Server, Microsoft SQL Server, Active Directory.
Správa zařízení	Podpora automatického vyhledávání (discovery) zařízení a jimi používaných uživatelských účtů.
Správa privilegovaných účtů	Podpora vyhledávání (discovery) privilegovaných (administrátorských) účtů v Active Directory.
Automatický onboarding	Podpora automatického přidávání nalezených účtů a zařízení do vlastního bezpečného úložiště (onboarding účtů a zařízení)
Rotace hesel	Podpora automatické správy účtů a rotace hesel minimálně pro systémy Windows Server a Linux, síťová zařízení (např. aktivní prvky) a webové aplikace. Rotaci hesel musí být možné provádět na základě nastavitelných intervalů.
Komplexita hesel	Podpora stanovení požadavků na délku, složitost (komplexnost) a maximální stáří hesel.
Rotace ssh klíčů	Automatická správa a rotace ssh klíčů.
Kontrola shody	Automatická identifikace hesel, která neodpovídají nastaveným politikám a odepření jejich uložení.
Vytváření hesel	Generování náhodných hesel podle nastavených pravidel.
Role	Podpora model RBAC (Role-based User Access Control). Možnost nastavení a přidělování oprávnění na skupiny/role.
Politiky zařízení	Možnost nastavení přístupových politik na zařízení.
Logování	Zasílání bezpečnostních logů do nadřazených logovacích systémů centrálního logování – min. syslog
Automatické odhlášení	Automatické odhlášení z centrální konzole při nečinnosti
Sdílené účty	Podpora rozlišení jedinečných uživatelů pro sdílené účty
Nouzový přístup	Integrovaný mechanismus zobrazení přihlašovacích údajů v čitelné podobě v případě nedostupnosti síťového propojení na cílový systém.
Dočasný přístup	Podpora dočasného povolení k užívání přístupových údajů na základě žádosti (pro procesní opatření „čtyř očí“).
Notifikace	Integrovaný systém emailových upozornění/notifikací, s možností přímého prokliku k řešení notifikované události
Reporting	Integrovaný reportovací systém. Předdefinované reporty min.: • Seznam uživatelů a jejich oprávnění, včetně výpisu účtů, které mají k dispozici • Seznam všech spravovaných účtů, včetně přiřazených politik hesel a výčtu uživatelů, kteří mají k danému účtu přístup • Seznam aktivit nad účty (check out/in, přidělení účtů atp.) • Seznam automaticky vyhledaných nových uživatelských účtů a zařízení
Zálohování	Integrované nastavení a provádění pravidelných záloh.
Bezagentový systém	Podpora implementace bez potřeby instalace agentů na cílové systémy
Dokumentace	Dokumentace v českém jazyce poskytovaná a aktualizovaná výrobcem min. v rozsahu administrátorského a uživatelského manuálu včetně popisu konfigurace
Licence	Poskytnutá licence umožní nasazení a provoz pro 30 uživatelů a 300 napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace (počet a délka záznamů, velikost databází, počet reportů atd.).

Parametr	Popis minimální úrovně parametru
Podpora	Podpora výrobce po dobu 60 měsíců včetně nároku na nové verze a aktualizace software

2. Požadavky na instalační a implementační práce

Dodané řešení bude sloužit jako vysoce dostupná hyperkonvergovaná infrastruktura pro chod agendových IS kupujícího a jeho zálohování. Dodávka musí obsahovat kompletní instalaci a implementaci řešení, nad kterým pak bude v režii kupujícího se třetí stranou provedena implementace agendových systémů (virtuální databázové, aplikační a komunikační servery) a konfigurace úloh pro zálohování nově vytvořených virtuálních serverů s agendovými IS.

Implementace dodávaného řešení bude provedena po odsouhlasení zadavatelem a v souladu s „best practice“ a dle doporučení výrobců jednotlivých komponent dodávaného řešení k datu realizace plnění.

Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Dodavatel je povinen zahrnout (zohlednit do ceny) do nabídky i veškeré další činnosti a prostředky, které jsou nezbytné pro řádnou dodávku plnění v rozsahu doporučeném výrobcem a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

Popis stávajícího prostředí kupujícího vstupujícího do plnění podle této specifikace:

Firewall – Za účelem úvodní konfigurace nově nasazovaných firewallů zajistí prodávajícímu kupující přístup ke stávajícím firewallům typu CheckPoint QUANTUM 3800 SECURITY GATEWAY, ze kterých prodávající převezme aktuální bezpečnostní politiky a konfigurace a navrhne jejich přenesení a úpravu pro nově nasazované firewally. Aplikační firewall F5 BIG-IP.

Sekundární firewall Microsoft TMG (Microsoft Forefront Threat Management Gateway).

Serverové prostředí – Kupující provozuje serverové prostředí, které je virtualizované s využitím hypervisoru typu VMware ESX a v tomto prostředí provozuje jako majoritní serverový operační systém Windows server 2019 a v něm provozované doménové služby s MS Active Directory na OS MS Windows server 2012 (pro realizaci plnění podle této specifikace provede prodávající povýšení na verzi 2019 s využitím stávajících licencí kupujícího). Za účelem nasazení technologií v rámci plnění podle této specifikace umožní v rámci stávajícího hypervisoru užití přiděleného virtuálního stroje a dále užití licencí výše uvedeného serverového operačního systému. Pro implementaci služeb PKI a 802.1x bude prodávajícímu umožněn přístup do doménového prostředí kupujícího.

SIEM Qradar 7.5.

Přepínače – Ze stávajících páteřních přepínačů typu HP/HPE řad 2530, 5130, 5800, 6300, AP HP 425 řízené clusterem kontrolerů WLC MSM 760 a Centrální správy LAN a WiFi multi-vendor nástrojem IMC (Intelligent Management Center) požaduje kupující převzít a navrhnout rozšíření segmentace a konfigurace pravidel prodávajícím s návrhem lepší optimalizace a bezpečnosti provozu sítě. Za účelem plnění podle této specifikace umožní kupující prodávajícímu přístup ke konfiguraci těchto přepínačů a dále v rámci plnění bude požadovat jejich novou konfiguraci k plnění jim nově přidělených rolí v souvislosti s úpravou prostředí na základě plnění podle této specifikace.

Umístění dílčích nových přepínačů do stávajícího prostředí je dále omezeno velikostí pobočkových racků, která je pouze omezená a umožňuje osazení přepínačů pouze některých velikostí (nižší hloubka, která je promítnuta do požadavků na typová zařízení v rámci jejich specifikací v tomto dokumentu).

Pro propojení páteřních přepínačů jsou připraveny a instalovány stávající optická vlákna typu SM a dále pro napojení přístupových přepínačů budou užita stávající optická vlákna typu SM. Stávající optická vlákna jsou vždy zakončena konektory a není vyžadováno jejich navařování.

Kupující dále provozuje monitorování síťových toků Flowmon IDP-1000-CU.

2.1. Specifikace konkrétních instalačních a implementačních požadavků

V rámci předmětu plnění kupující požaduje provedení min. následujících služeb pro následující oblasti plnění:

Obecné požadavky
• dodávka požadovaného hardware a software, • doprava hardware do místa instalace, • montáž dodaných zařízení do stávajících datových rozvaděčů, • konfigurace portů pro správu a karet pro vzdálenou správu jednotlivých zařízení a jejich připojení do vyhrazené sítě pro správu, • aktualizace firmware v jednotlivých zařízeních a jejich komponentách na nejnovější doporučené verze, • zabezpečení přístupu ke správě jednotlivých zařízení, konfigurace synchronizace jejich času, konfigurace SNMP parametrů pro možnost vzdáleného dohledu, konfigurace SMTP pro zaslání e-mailové notifikace o stavu zařízení, • kompletní ověření funkčnosti celého řešení ○ simulovaný výpadek jednoho z páteřních přepínačů, ○ odpojení jednoho z propojů mezi páteřními přepínači, ○ otestování redundantního napájení jednotlivých zařízení střídavým odpojením jednoho z napájecích zdrojů, • propojení celého řešení do stávající síťové infrastruktury a vybudování služeb pro síťovou a serverovou infrastrukturu v rámci dodávaných technologií • ověření registrací zařízení a licencí u výrobců, aktivace licencí a služeb

Implementační služby

Next Generation Firewall s příslušenstvím
• analýza současného prostředí • návrh nové architektury, musí zahrnovat integraci se stávajícími firewally s možností jednotné správy a flexibilního využití (perimetrový/segmentační firewall, VPN koncentrátor apod.), převod role TMG do nového prostředí (a následné zrušení TMG), zachování a optimalizace role aplikačního firewallu. • migrace na nové firewally (export pravidel ze stávajících firewallů pro potřebu analýzy zajistí kupující) • optimalizace pravidel/politik včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) s využitím nových či vylepšených funkcionalit a začlenění firewallu do LAN prostředí. • související rekonfigurace stávajících zařízení

Páteřní přepínače a přístupové přepínače
• analýza stávajícího prostředí • návrh nové architektury včetně přeskupení a náhrady stávajících zařízení, bude zahrnovat i návrh segmentace LAN – tj. VLAN včetně adresace a řízení/filtrování provozu mezi nimi – předpokládaný počet VLAN jsou nižší desítky • sestavení stohů přepínačů a jejich propojení pro zajištění vysoké dostupnosti v co nejvyšším rozsahu • začlenění prvků do systému centrální správy a jeho rekonfigurace • konfigurace agregačních skupin (LACP) na přepínačích pro propojení přepínačů, připojení serverů • konfigurace VLAN, trunk portů a přístupových portů na jednotlivých přepínačích • vytvoření oddělených LAN a SAN komunikačních domén • nastavení exportu a zpracování NETFLOW/IPFIX • související rekonfigurace stávajících zařízení

Licence SW pro řízení přístupu do sítě 802.1X

- analýza současného prostředí
- návrh nové architektury, způsob autentizace jednotlivých typů klientů (počítače, mobilní zařízení, periferie, OT/IOT atd.) a identitní databáze (primárně Active Directory)
- implementace systému 802.1X
- začlenění přepínačů a WiFi přístupových bodů do systému 802.1X
- vytvoření a aplikování Connection Request Policy a Network Policy pro 802.1X
- vytvoření návodů pro zařazení běžných koncových zařízení do systému 802.1X (PC, notebook, chytrý telefon/tablet)
- související rekonfigurace stávajících zařízení

Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI

- analýza prostředí se zaměřením na zavedení vícefaktorové autentizace
- vybudování interní PKI (Public Key Infrastructure) včetně certifikační autority integrované s Active Directory
- vybudování systému vícefaktorové autentizace s využitím kontaktních identifikačních prostředků (karet, tokenů) pro systémy Windows a terminálové služby Microsoft RDS.
- Instalace klávesnic/čteček na koncová zařízení ani distribuce identifikačních medií uživatelům není součástí plnění
- návrh a vybudování systému pro správu kompletního životního cyklu identifikačních prostředků (karet a doménových i veřejných certifikátů) včetně uživatelské běžné správy a obnovy platnosti certifikátů
- návrh a realizace zálohování
- související rekonfigurace stávajících zařízení

Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM

- analýza ICT prostředí se zaměřením na vyhledání a inventarizaci privilegovaných účtů a systémů, u nichž bude činnost privilegovaných účtů monitorována
- návrh a vybudování systému pro správu a řízení privilegovaných účtů, včetně rotace hesel
- související rekonfigurace stávajících technologií
- Návrh a provedení akceptačních testů, musí prokázat minimálně funkčnost v obvyklých scénářích použití (přístup správce pomocí vzdálené plochy a příkazové řádky (ssh)), ukládání relací a rotaci hesel.

2.2. Požadavky na předimplementační analýzu

Dodavatel před implementací řešení zpracuje předimplementační analýzu, minimálně pro následující oblasti:

- způsob začlenění nabízeného řešení do stávajícího ICT prostředí,
- analýza požadavků na síťovou infrastrukturu,
- analýza požadavků na ukládání a zálohování dat, obnovu dat, toky a objemy dat,
- požadavky na rekonfigurace stávajících systémů ve vztahu k plánovanému využití,
- dopady implementace na dostupnost a funkčnost stávajících služeb,
- další podklady relevantní pro návrh řešení,
- požadovaná součinnost kupujícího,
- návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Výstupem předimplementační analýzy bude písemná zpráva podléhající schválení kupujícím.

2.3. Požadavky na zpracování prováděcí dokumentace

Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

Prováděcí dokumentace musí být před zahájením implementačních prací písemně schválena kupujícím.

Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:

- detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému,
- způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
- detailní návrh a popis postupu implementace předmětu plnění,
- detailní popis zajištění bezpečnosti informací,
- detailní harmonogram projektu včetně uvedení kritických milníků,
- návrh designu úložišť a virtuálních serverů a jeho konfigurace,
- návrh designu zálohování a jeho konfigurace,
- návrh designu síťového řešení a jeho konfigurace,
- návrh monitorování řešení monitorovacími nástroji,
- vazby na stávající systémy a jejich konfigurace,
- návrh akceptačních kritérií a akceptačních testů,
- detailní popis navrhovaných zaškolení administrátorů.

2.4. Požadavky na provozní dokumentaci

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat všechny dodané systémy.

2.5. Požadavky na zaškolení

Dodavatel zajistí zaškolení zaměstnanců Zadavatele – administrátorů – na zařízení a systémy, v rámci tohoto plnění, a to minimálně v rozsahu předávané provozní dokumentace.

- zaškolení zajistí seznámení specialistů IT kupujícího se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin,
- minimální rozsah zaškolení je 8 hodin,
- zaškolení bude probíhat v sídle kupujícího,
- předpokládá se účast 2 administrátorů,
- náklady na zaškolení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují.

2.6. Požadavky na provedení zkušebního provozu a akceptačních testů

Nabídne-li Dodavatel v rámci svého řešení HW, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje nižší záruční dobu, popř. podporu, požaduje kupující zahrnout do nabídky cenu povýšení záruční doby, popř. podpory na jím požadovanou úroveň.

Kupující požaduje přístup k aktualizacím software a firmware dodaného HW v kupní ceně minimálně po záruční dobu, záručního servisu a podpory.

Veškeré opravy v rámci záruční doby budou provedeny bez dalších nákladů pro kupujícího.

Není-li uvedeno u dané položky požadovaného HW jinak, požaduje zadavatel provedení opravy do deseti pracovních dnů.

2.7. Další požadavky na záruční dobu, záruční servis a další podmínky v rámci záruky

Nabídne-li Dodavatel v rámci svého řešení HW, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje nižší záruční dobu, popř. podporu, požaduje kupující zahrnout do nabídky cenu povýšení záruční doby, popř. podpory na jím požadovanou úroveň.

Kupující požaduje přístup k aktualizacím software a firmware dodaného HW v kupní ceně minimálně po záruční dobu, záručního servisu a podpory.

Veškeré opravy v rámci záruční doby budou provedeny bez dalších nákladů pro kupujícího.

Není-li uvedeno u dané položky požadovaného HW jinak, požaduje zadavatel provedení záruční opravy do deseti pracovních dnů.

3. Harmonogram plnění

Kupující požaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky. Údaj D značí datum nabytí účinnosti kupní smlouvy. Číslo značí počet kalendářních dnů.

Aktivita	Termín splnění
Nabytí účinnosti smlouvy (uveřejnění v registru smluv)	D
Předimplementační analýza – zpracování	D+21
Předimplementační analýza – připomínkové řízení, schválení	D+28
Prováděcí dokumentace – zpracování	D+42
Prováděcí dokumentace – připomínkové řízení, schválení	D+49
Realizace předmětu plnění	D+100
Školení administrátorů	D+110
Zkušební provoz	D+110
Akceptace předmětu plnění	D+120 dnů

Popis nabízeného technického řešení

Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti

1. Technická specifikace

Uchazeč navrhuje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v díle uvedené minimální specifikaci.

- Jedná se o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.
- Součástí dodávky níže uvedených technologií jsou i dále uvedené služby.
- Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.
- Nabízené zboží je standardní, běžně dostupné a určené k produkčnímu použití.
- Veškeré nabízené zboží je pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu bude možné kdykoliv vznést přímo na výrobce zařízení.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Propojení zařízení – SFP moduly a kabely

Všechny dodané technologie budou v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení budou dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet budou dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo je dodrženo stejně.

Plnění jednotlivých komponent dle specifikace níže je v následujícím rozsahu, a to včetně příslušenství:

Položka plnění	Počet kusů
Next Generation Firewall s příslušenstvím	2
Páteřní přepínače 48p s příslušenstvím	2
Přístupové přepínače 48p PoE s příslušenstvím	28
Přístupové přepínače 24p s příslušenstvím	2
Licence SW pro řízení přístupu do sítě založeného na protokolu 802.1x	1
Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI	1
Autentizační prostředky	300
Klávesnice s integrovanou čtečkou karet, včetně ovladačů	150
Samostatné USB čtečky čipových karet, včetně ovladačů	150
Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM	1

1.1. Next Generation Firewall s příslušenstvím

Parametr	Popis minimální úrovně parametru
Provedení	Pro montáž do 19" datového rozvaděče, včetně montážního materiálu – [REDACTED]
NGFW	Next-generation firewall – viz https://en.wikipedia.org/wiki/Next-generation_firewall – firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.
Porty	2x 2.5GbE, 8x 1GbE a 2x 10GbE
Počet současných spojení	7 200 000
Propustnost VPN	17,5 Gbps
Propustnost firewallu	20 Gbps pro pakety 1518 bytů a větší, provoz UDP.
Propustnost NGFW	16,2 Gbps při aktivní IPS.
Propustnost IPS	20 Gbps pro provoz typu Enterprise mix.
Propustnost detekce škodlivého kódu	5,5 Gbps při zapnuté IPS.
Virtualizace	Podpora 7 izolovaných virtuálních kontextů (virtuálních firewallů). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů.
Vysoká dostupnost	Režimy Active/Active se společnou konfigurací, včetně případných nezbytných licencí.
Dualstack	Podpora současného běhu IPv4 a IPv6.
VPN	Podpora IPSec, SSL VPN
Bezpečné DNS	Automatická blokáce přístupu k škodlivým doménám a IP adresám, definice součástí bezpečnostních aktualizací. Ochrana proti DNS tunelování.
Aplikační kontrola	Detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu.
Antivir	Integrovaný antivirus, podpora protokolu ICAP pro externí antivir
ZeroDay	Ochrana před ZeroDay útoky formou emulace neznámého kódu v bezpečném prostředí – Sandboxu
Kategorizace a blokáce provozu	Založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu
Antispam	Antispamová a antivirová a antiphishingová inspekce elektronické pošty. Transparentní (průchozí) kontrola i MTA režim.
Aktualizace	Automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení.
Ověřování uživatelů	LDAP, Active Directory, Radius, Ověřování na základě certifikátu.
Management a monitoring	HTTP/S, SSH, SNMP, syslog.
Centrální správa	Jednotná centrální správa samostatných boxů i clusteru, monitorování a aktualizace firmware z centrální grafické konzole. Lokální i cloudová správa s podporou spolupráce více správců (např. při řešení bezpečnostních událostí/incidentů) při zachování konzistence konfigurační nastavení.
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX https://sc1.checkpoint.com/documents/SMB_R80.20.35/CLI/Topics/netflow-collector.htm https://sc1.checkpoint.com/documents/Appliances/GSG_3900/EN/Content/Topics-GSG-3920-3950-3980/Configuring-Appliances.htm

Geolokace	Možnost nastavovat firewall politiky na základě geografických údajů IP adres
Standardní funkce	NAT, statické a dynamické routování (OSPFv3, BGP, RIP), publikace interních serverů, routování založené na politikách (policy based routing).
API	Integrované API rozhraní pro automatizaci a orchestraci
Napájení	Redundantní napájecí zdroje.
Záruční doba, podpora a záruční servis, technická podpora výrobce	Záruční doba, podpora a záruční servis 60 měsíců v režimu 8x5 poskytovaný výrobcem zařízení, odeslání náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a všech bezpečnostních funkcí – URL filtrace, DNS, IPS, antimalware, antispam, aplikační kontrola, sandbox, ZeroDay).

1.2. Páteří přepínače 48p příslušenstvím

Parametr	Popis minimální úrovně parametru
Základní parametry	L2/L3 přepínač v rackovém provedení, 1U včetně montážního materiálu
Porty	48x 10 Gb SFP+, 4x 40/100 Gb QSFP28 s podporou QSFP+/QSFP28
Propustnost	Neblokovaná architektura, přepínací kapacita je součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Agregace portů	Podpora LACP, 50 skupin, 8 portů ve fyzické agregační skupině, 16 portů ve virtuální agregační skupině při zapojení přepínačů do logického páru.
Směrování	Statické směrování (routování) včetně VLAN, dynamické směrování (RIP, OSPF, BGP), směrování založené na politikách routovacích záznamů pro IPv4 24 576 a IPv6 12 288
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	Přepínací výkon: 1,76 Tbps
VLAN	VLAN 802.1Q, MAC i založené na protokolu, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření, podpora IEEE 802.1ad (Q-in-Q), podpora statických a dynamických VXLAN, 1024 VLAN. Podpora privátních VLAN (PVLAN) pro izolaci klientů ve stejné VLAN (mikrosegmentace, dynamická segmentace)
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora 147 456 MAC adres.
Síťové toky	Plný přímý export síťových toků – IPFIX
Zrcadlení portů	Zrcadlení provozu (odchozího i příchozího) do lokálního i vzdáleného portu
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST API a integrovaná podpora skriptů pro automatizaci. Interní detailní monitorování funkcí/služeb přepínače s možností konfigurovatelných automatických reakcí.
Nezávislý management	Vyhrazený LAN port pro správu (out-of-band management) - nezapočítává se do požadovaného počtu portů (viz Porty)
Napájení, chlazení	Integrované redundantní interní napájecí zdroje, zdroje i ventilátory vyměnitelné za provozu (hot-swap)
Centrální správa	Podpora stávajícím systém centrální správy

Stohování	Pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - technologie MC-LAG (Multichassis Link Aggregation). Synchronizace konfigurací přepínačů ve stohu. 32 portů v agregační skupině stohu. Kapacita stohovacího propojení: 400 Gbps
Záruční doba a záruční servis	Záruční doba a záruční servis více jak 60 měsíců (60 měsíců po ukončení prodeje) v režimu 24x7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace SW a aktualizace firmware.

Příslušenství pro páteří přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství centrálních přepínačů	Pro celý komplet dodávaných centrálních přepínačů je v dodávce následující celkový počet příslušenství v podobě SFP modulů a kabelů: • 92x SFP+ 10 Gbps modul, SM, 10 km, LC, DMI diagnostika pro nabízené přepínače • 4x SFP+ 10GbE modul, RJ-45, DMI diagnostika pro nabízené přepínače • 8x QSFP28 100GBASE-SR4, MM, 100 m • 2x patch kabel MM OM3/4 MPOf-MPOf, překřížený, 1 m – pro propojení nabízených přepínačů • 4x patch kabel MM OM4, MPOf – 8x LC (4 páry), 3 m • 60x patch kabel SM LC-SC, 3 m • 36x patch kabel SM LC-LC, 3 m Záruční doba na příslušenství 36 měsíců
Licence pro centrální správu	

1.3. Přístupové přepínače 48p PoE příslušenstvím

Parametr	Popis minimální úrovně parametru
Provedení	dení 1U; hloubka přepínače 32,66 cm
Porty	48x 1 GbE, 4x 10 Gb SFP+.
Propustnost	Neblokovaná architektura, přepínací kapacita je součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Power on Ethernet	Podpora PoE/PoE+ 802.3af/at na všech metalických portech, celkový PoE výkon 740 W.
Agregace portů	Podpora LACP, 16 portů v agregační skupině, 20 skupin.
Směrování	Statické směrování (routování), 500 směrovacích cest pro IPv4 i IPv6
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	přepínací výkon 176 Gbps paketový výkon 130,9 Mpps
VLAN	VLAN 802.1Q, MAC i založená na protokolu, podpora zařazování do VLAN na základě 802.1X ověření.
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora 32 768 MAC adres.

Zrcadlení provozu	Zrcadlení příchozího i odchozího síťového provozu
Napájení	Interní napájecí zdroj.
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API a integrovaná podpora skriptů pro automatizaci
Nezávislý management	Vyhrazený LAN port pro správu (out-of-band management) - nezapočítává se do požadovaného počtu portů (viz Porty)
Síťové toky	Plný přímý export síťových toků – IPFIX
Centrální správa	Podpora stávajícím systém centrální správy
Stohování	Pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - technologie MC-LAG (Multichassis Link Aggregation). Synchronizace konfigurací přepínačů ve stohu. Podpora 4 členů ve stohu.
Záruční doba a záruční servis	Záruční doba a záruční servis více jak 60 měsíců (60 měsíců po ukončení prodeje) v režimu 24x7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace SW a aktualizace firmware.

Příslušenství pro přístupové přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství přístupových přepínačů	Pro celý komplet dodávaných přístupových přepínačů 48p PoE požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů: 112 ks 10 Gb SFP+ modul SM, 10 km, diagnostika, LC konektor 56 ks 2 m propojovacích SM kabelů LC-LC 56 ks 2 m propojovacích SM kabelů LC-SC Záruční doba na příslušenství 36 měsíců
Licence pro centrální správu	

1.4. Přístupové přepínače 24p PoE příslušenstvím

Parametr	Popis minimální úrovně parametru
Provedení	L2+ přepínač v rackovém provedení 1U
Porty	24x 1 GbE, 4x 10 Gb SFP+.
Propustnost	Neblokovaná architektura, přepínací kapacita je součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Agregace portů	Podpora LACP, 8 portů v agregační skupině, 8 skupin.
Směrování	Statické směrování (routování), 500 směrovacích cest pro IPv4 i IPv6
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	přepínací výkon 128 Gbps paketový výkon 95,2 Mpps
VLAN	VLAN 802.1Q, MAC i založená na protokolu, podpora zařazování do VLAN na základě 802.1X ověření.
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora 8 192 MAC adres.
Zrcadlení provozu	Zrcadlení příchozího i odchozího síťového provozu
Napájení	Interní napájecí zdroj.

Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST API pro automatizaci.
Síťové toky	Plný přímý export síťových toků – IPFIX [REDACTED]
Centrální správa	Podpora stávajícím systém centrální správy
Záruční doba a záruční servis	Záruční doba a záruční servis více jak 60 měsíců (60 měsíců po ukončení prodeje) v režimu 24x7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace SW a aktualizace firmware [REDACTED]

Příslušenství pro přístupové přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství přístupových přepínačů	Pro celý komplet dodávaných přístupových přepínačů 24p požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů: 8 ks 10 Gb SFP+ modul SM, 10 km, diagnostika, LC konektor 4 ks 2 m propojovacích SM kabelů LC-LC 4 ks 2 m propojovacích SM kabelů LC-SC Záruční doba na příslušenství 36 měsíců
Licence pro centrální správu	[REDACTED]

1.5. Licence SW pro řízení přístupu do sítě založeného na protokolu 802.1x

Parametr	Popis minimální úrovně parametru
Provedení	Software nebo softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení [REDACTED]
Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik pomocí přiřazení VLAN, ACL. Atributy pro definici politik. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém
Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN
Základní autentizační metody	PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty
Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází – Active Directory, LDAP, ODBC
Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, autorizace proti externí SQL databázi
Rozšířená autentizace a autorizace	Podpora autentizace a autorizace LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (SAML 2+ IdP a SP, OAuth)
Kontextová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory
Externí identity	Podpora autentizace externími identitami – Microsoft, Google

Komplexní autorizace	Autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. pro omezení celkového času online či objemu přenesených dat za delší časové období
Dynamická autorizace	Podpora RADIUS CoA podle RFC3576. Možnost změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení
Profilování	Zjišťování doplňujících informací pro koncová zařízení (. typ, výrobce, OS a pod.)
TACACS+	Podpora autentifikace a autorizace na síťové prvky protokolem TACACS+
Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)
Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení
Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu
Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (např. jen potvrzení uvítací/informační) stránky [REDACTED]
Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem apod.
Ochrana identit	Veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované šifrované databázi, které bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES 256-bit. [REDACTED]
Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, UPS, technologické prvky, IoT.
Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru 2 appliance. Druhá appliance není součástí dodávky.
Licence	Trvalá licence pro 1000 současných (konkurenčních) koncových zařízení ověřených pomocí 802.1X bez omezení počtu uživatelů
Automatizace a integrace	REST-API rozhraní pro základní funkce AAA.
Kompatibilita	Software nebo appliance bude výrobcem podporována pro provoz v prostředí stávající serverové virtualizace
Podpora	Podpora výrobce 60 měsíců včetně nároku na nové verze a aktualizace software

1.6. Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI

Systém bude sestavený z komponent systému **ProID+ CMS**, **Kartové centrum**, **Správce karty**, **ACEX a NTF Mail** a bude využívat technologii **Windows Hello**. Infrastruktura PKI bude vybudována na technologii **Microsoft Active Directory Certificate Services**

Parametr	Popis minimální úrovně parametru
Provedení	Systém pro autentizaci uživatele identifikačním prostředkem vůči adresářové službě včetně nástrojů pro správu Datasheety: ProID+CMS.pdf, ProID+KartoveCentrum.pdf,

	ProID+ACEx.pdf, ProID+NTFMail.pdf, ProID+SpravceKarty.pdf, ProID+Q.pdf, WindowsServerSmartCard.pdf, AD PKI.pdf
Autentizace	Autentizace uživatele ve stávajících operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem (Microsoft) pomocí nabízených autentizačních médií
Obnova certifikátů	Automatické hlídání expirace osobních certifikátů a vyvolání uživatelského průvodce pro jeho jednoduchou uživatelskou obnovu podle nastavených politik. Včetně automatického odstranění neplatných certifikátů na základě politik.
Uživatelská správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK)
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu v operačním systému, testování integrity a použitelnosti
Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů vystavených veřejnými certifikačními autoritami (Postsignum) a vyvolání průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik
Správa prostředků	Evidence a správa životního cyklu identifikačních prostředků
Prostředky	Podpora kontaktních i hybridních identifikačních prostředků
Správa systému	Webové rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory
Evidence	Systém umožní evidovat - typ prostředku (kontaktní, bezkontaktní, hybridní) - druh prostředku (uživatelský, administrační, operátorský) - stav prostředku (používaný, k recyklaci, skartovaný) - historii prostředku (datum zavedení do evidence, vydání uživateli, recyklace) - držitele prostředku (aktuálního držitele i všechny předchozí držitele) - data uložená v prostředku (certifikáty a další data, včetně historie dat)
Integrace	Napojení na Active Directory (zdroj dat o uživateli, autentizace uživatele, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty)
Správa certifikátů	Správa certifikátů (doménových i kvalifikovaných): - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření a tisk protokolu o vystavení - odvolání certifikátu - vydávání "v zastoupení" - např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance
Obnova prostředků	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (l vzdálené), tisk protokolů
Personifikace	Integrované prostředí pro generování podkladů pro potisk identifikačních karet externím dodavatelem i na vlastní tiskárně
Ukládání dat	Centrální databázové úložiště údajů, podpora Microsoft SQL server (stávající hlavní databázové úložiště zadavatele)
Rozhraní	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování informací napojených systémům

Notifikace	E-mailové notifikace uživatelů i správců o blížící se expiraci certifikátů doménových i veřejných certifikačních autority
PKI	Součástí dodávky bude vybudování kompletní kompatibilní infrastruktury PKI (public key infrastructure) pro zajištění celého životního cyklu osobních přihlašovacích certifikátů a jejich šablon, včetně dodávky potřebných licencí
Licence	Licence pro 300 uživatelů
Podpora	Podpora výrobce po dobu 60 měsíců včetně nároku na nové verze a aktualizace software

1.7. Autentizační prostředek

ProID-Q Hybridní identifikační karta

Parametr	Popis minimální úrovně parametru
Provedení	Hybridní identifikační karta s kontaktní částí SmartCard a bezkontaktní částí čipem EM4102 ProID+Q.pdf
Podporované certifikáty	Karta musí umožnit ukládání a používání vlastních certifikátů a certifikátů veřejných certifikačních autorit (I. CA, Postsignum, eidentity)
Identity	Karta musí umožnit ukládání více identit
Kvalifikovaný podpis	Karta musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku), viz https://www.dia.gov.cz/cs/legislativa/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/informace-pro-uzivatele/seznam-vydavanych-kvalifikovanych-prostredku-pro-vytvoreni-elektronickych-podpisu-v-ceske-republice
SW podpora	Součástí dodávky bude software a ovladače pro zpřístupnění jejich rozhraní v operačních systémech Windows, Linux, macOS a systému terminálových služeb Microsoft RDS včetně rozšířených funkcionalit, tzv. middleware.
Záruční doba	Záruční doba 2 roky včetně nároku na aktualizace middleware

1.8. Klávesnice s integrovanou čtečkou karet, včetně ovladačů

HP USB Business Slim Smartcard Keyboard Z9H48AA

Parametr	Popis minimální úrovně parametru
Provedení	Standardní PC klávesnice se samostatným numerickým blokem a integrovanou čtečkou čipových karet HP USB Business Slim Smartcard.pdf
Rozhraní	USB rozhraní
Čtečka	Kompatibilita s čipovou částí nabízených identifikačních prostředků a nabízeným SW pro vícefaktorové ověřování
Lokalizace	České (QWERTZ) rozložení kláves, české popisky
SW podpora	Součástí dodávky bude software a ovladače pro operační systémy Windows, Linux, macOS – nejsou-li ovladače standardní součástí operačních systémů.
Záruční doba	Záruční doba 2 roky

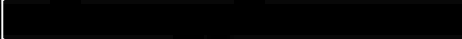
1.9. Samostatné USB čtečky čipových karet, včetně ovladačů

IDBridge_CT30

Parametr	Popis minimální úrovně parametru
Provedení	Samostatná čtečka čipových karet IDBridge_CT30.pdf
Rozhraní	USB rozhraní
Čtečka	Kompatibilita s čipovou částí nabízených identifikačních prostředků a nabízeným SW pro vícefaktorové ověřování
SW podpora	Součástí dodávky bude software a ovladače pro operační systémy Windows, Linux, macOS – nejsou-li ovladače standardní součástí operačních systémů.
Záruční doba	Záruční doba 2 roky

1.10. Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM



Parametr	Popis minimální úrovně parametru
Základní funkce	Privilegovaný přístup na cílový systém bude zprostředkován prostřednictvím tzv. terminal/jump serveru zvoleným komunikačním protokolem tak, aby privilegovaný uživatel neměl přístup k přihlašovacím údajům cílového systému. Izolace přístupu bude možná až na úroveň aplikace (typu webový prohlížeč s konkrétním URL, MMC konzole s vybraným snap-in, konkrétní aplikace - např. MS SQL Management Studio, WinSCP atp.) a uživatel nebude mít možnost přistupovat k jiným službám či aplikacím v rámci dané relace. Ukončením aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI systému nebo pomocí standardních protokolů RDP a SSH a standardních klientů. 
Bezpečná autentizace	Podpora vynucení silné autentizace pro připojení ke vzdálené relaci
SSH připojení	Privilegovaný přístup prostřednictvím SSH protokolu bude v rámci vzdálené relace prováděn přes ssh proxy, na které bude uživatel ověřen svými přihlašovacími údaji (s možností spárování s Active Directory). K cílovému systému bude uživatel připojen a přihlášen podle bezpečností politiky vybraným privilegovaným účtem bez zadávání hesla. Pro připojení pomocí ssh proxy bude systém podporovat vynucení silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí ssh klíče).
Webové připojení	Systém umožní zprostředkovat privilegovanému uživateli bezpečné připojení v rámci vzdálené relace na vybrané webové aplikace, přístup do cloudu apod. pomocí webové proxy, na které bude uživatel ověřen neprivilegovaným účtem (s možností ověření vůči Active Directory). K cílovému systému bude uživatel připojen a přihlášen podle bezpečností politiky vybraným privilegovaným účtem bez zadávání hesla. Systém bude podporovat transparentní SSO (single-sign-on).
Nahrávání relace	Monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu a ve formátu screenshotů. Záznam relace musí být vytvářen kontinuálně. V nahrávkách bude možné zpětně vyhledávat podle metadat. Přehrávání musí být dostupné přímo z GUI systému běžným internetovým prohlížečem a nesmí vyžadovat instalaci komponent třetích stran (flash, java, codec apod.).
Metadata	Zaznamenávání rozšířených informací (metadat) o relacích, minimálně stisky kláves a odpovědi monitorovaných zařízení
Nahrávky	Ukládání nahrávek relací v optimalizované kvalitě s možností volby cílového úložiště.
Politiky	Logické zařazení napojených systémů do skupin či profilů, nad kterými bude možno nastavit a aplikovat společné politiky a nastavení.

Ukončení relací	Možnost okamžitého ukončení potenciálně nebezpečných relací administrátorem či operátorem systému.
Auditování	Integrovaný audit jednotlivých akcí uživatelů s privilegovanými účty –zobrazení hesla, změny uložených údajů, vytvoření relace. Export auditních záznamů.
Bezpečnost auditních záznamů	Nezpochybnitelná auditovatelnost jednotlivých operací, reportování a textových logů. Auditní záznamy musí být bezpečně uloženy tak, aby k nim měli přístup pouze oprávnění uživatelé.
Reportování	Integrovaný generátor reportu veškerých aktivit správce systému. Přístupu k reportům musí být možno nastavit pouze vybraným uživatelům.
Autentizace	Podpora LDAP/S, SAML2, RADIUS pro autentizaci, autorizaci a vícefaktorové ověřování
Workflow	Integrované workflow pro zadávání a schvalování žádostí o přístup. Funkční požadavky na workflow: - Zadávání požadavků uživatelů - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů
Změna privilegií	Podpora delegace a eskalace privilegií na bázi schvalovacího workflow.
Vícedoménová autentizace	Podpora současného napojení více Active Directory/LDAP domén současně.
API rozhraní	Integrované API s podporu REST, aktivované v rámci dodávky. Výrobce, resp. dodavatel musí poskytovat volně dostupný aktualizovaný popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací.
Integrace servicedesk	Podpora napojení a integrace na servicedeskové/tiketovací systémy.
Odolnost	Veškeré komponenty systému musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště účtů, přihlašovacích údajů, nahrávek relací a auditních záznamů musí být zabezpečeno a odděleno od ostatních komponent řešení.
Správa účtů	Integrované vyhledávání (discovery) a správa účtů v systémech Windows Server, Microsoft SQL Server, Active Directory.
Správa zařízení	Podpora automatického vyhledávání (discovery) zařízení a jimi používaných uživatelských účtů.
Správa privilegovaných účtů	Podpora vyhledávání (discovery) privilegovaných (administrátorských) účtů v Active Directory.
Automatický onboarding	Podpora automatického přidávání nalezených účtů a zařízení do vlastního bezpečného úložiště (onboarding účtů a zařízení)
Rotace hesel	Podpora automatické správy účtů a rotace hesel pro systémy Windows Server a Linux, síťová zařízení (např. aktivní prvky) a webové aplikace. Rotaci hesel musí být možné provádět na základě nastavitelných intervalů.
Komplexita hesel	Podpora stanovení požadavků na délku, složitost (komplexnost) a maximální stáří hesel.
Rotace ssh klíčů	Automatická správa a rotace ssh klíčů.
Kontrola shody	Automatická identifikace hesel, která neodpovídají nastaveným politikám a odepření jejich uložení.
Vytváření hesel	Generování náhodných hesel podle nastavených pravidel.
Role	Podpora model RBAC (Role-based User Access Control). Možnost nastavení a přidělování oprávnění na skupiny/role.
Politiky zařízení	Možnost nastavení přístupových politik na zařízení.
Logování	Zasílání bezpečnostních logů do nadřazených logovacích systémů centrálního logování – syslog
Automatické odhlášení	Automatické odhlášení z centrální konzole při nečinnosti
Sdílené účty	Podpora rozlišení jedinečných uživatelů pro sdílené účty

Nouzový přístup	Integrovaný mechanismus zobrazení přihlašovacích údajů v čitelné podobě v případě nedostupnosti síťového propojení na cílový systém.
Dočasný přístup	Podpora dočasného povolení k užívání přístupových údajů na základě žádosti (pro procesní opatření „čtyř očí“).
Notifikace	Integrovaný systém emailových upozornění/notifikací, s možností přímého prokliku k řešení notifikované události
Reporting	Integrovaný reportovací systém. Předdefinované reporty: • Seznam uživatelů a jejich oprávnění, včetně výpisu účtů, které mají k dispozici • Seznam všech spravovaných účtů, včetně přiřazených politik hesel a výčtu uživatelů, kteří mají k danému účtu přístup • Seznam aktivit nad účty (check out/in, přidělení účtů atp.) • Seznam automaticky vyhledaných nových uživatelských účtů a zařízení
Zálohování	Integrované nastavení a provádění pravidelných záloh.
Bezagentový systém	Podpora implementace bez potřeby instalace agentů na cílové systémy
Dokumentace	Dokumentace v českém jazyce poskytovaná a aktualizovaná výrobcem v rozsahu administrátorského a uživatelského manuálu včetně popisu konfigurace
Licence	Poskytnutá licence umožní nasazení a provoz pro 30 uživatelů a 300 napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace (počet a délka záznamů, velikost databází, počet reportů atd.).
Podpora	Podpora výrobce po dobu 60 měsíců včetně nároku na nové verze a aktualizace software

2. Instalační a implementační práce

Dodané řešení bude sloužit jako vysoce dostupná hyperkonvergovaná infrastruktura pro chod agendových IS kupujícího a jeho zálohování. Dodávka obsahuje kompletní instalaci a implementaci řešení, nad kterým pak bude v režii kupujícího se třetí stranou provedena implementace agendových systémů (virtuální databázové, aplikační a komunikační servery) a konfigurace úloh pro zálohování nově vytvořených virtuálních serverů s agendovými IS.

Implementace dodávaného řešení bude provedena po odsouhlasení zadavatelem a v souladu s „best practice“ a dle doporučení výrobců jednotlivých komponent dodávaného řešení k datu realizace plnění.

Popis stávajícího prostředí kupujícího vstupujícího do plnění podle této specifikace:

- Firewall – Za účelem úvodní konfigurace nově nasazovaných firewallů zajistí prodávajícímu kupující přístup ke stávajícím firewallům typu CheckPoint QUANTUM 3800 SECURITY GATEWAY, ze kterých prodávající převezme aktuální bezpečnostní politiky a konfigurace a navrhne jejich přenesení a úpravu pro nově nasazované firewally.
- Aplikační firewall F5 BIG-IP.
- Sekundární firewall Microsoft TMG (Microsoft Forefront Threat Management Gateway).
- Serverové prostředí – Kupující provozuje serverové prostředí, které je virtualizované s využitím hypervisoru typu VMware ESX a v tomto prostředí provozuje jako majoritní serverový operační systém Windows server 2019 a v něm provozované doménové služby s MS Active Directory na OS MS Windows server 2012 (pro realizaci plnění podle této specifikace provede prodávající povýšení na verzi 2019 s využitím stávajících licencí kupujícího). Za účelem nasazení technologií v rámci plnění podle této specifikace umožní v rámci stávajícího hypervisoru užití přiděleného virtuálního stroje a dále užití licencí výše uvedeného serverového operačního systému. Pro implementaci služeb PKI a 802.1x bude prodávajícímu umožněn přístup do doménového prostředí kupujícího.
- SIEM Qradar 7.5.
- Přepínače – Ze stávajících páteřních přepínačů typu HP/HPE řad 2530, 5130, 5800, 6300, AP HP 425 řízené clusterem kontrolerů WLC MSM 760 a Centrální správy LAN a WiFi multi-vendor nástrojem IMC (Intelligent Management Center) požaduje kupující převzít a navrhnout rozšíření segmentace a konfigurace pravidel prodávajícím s návrhem lepší optimalizace a bezpečnosti provozu sítě. Za účelem plnění podle této specifikace umožní kupující prodávajícímu přístup ke konfiguraci těchto přepínačů a dále v rámci plnění bude požadovat jejich novou konfiguraci k plnění jim nově přidělených rolí v souvislosti s úpravou prostředí na základě plnění podle této specifikace.
- Umístění dílčích nových přepínačů do stávajícího prostředí je dále omezeno velikostí pobočkových racků, která je pouze omezená a umožňuje osazení přepínačů pouze některých velikostí (nižší hloubka, která je promítnuta do požadavků na typová zařízení v rámci jejich specifikací v tomto dokumentu).
- Pro propojení páteřních přepínačů jsou připraveny a instalovány stávající optická vlákna typu SM a dále pro napojení přístupových přepínačů budou užita stávající optická vlákna typu SM. Stávající optická vlákna jsou vždy zakončena konektory a není vyžadováno jejich navařování.
- Kupující dále provozuje monitorování síťových toků Flowmon IDP-1000-CU.

2.1. Specifikace konkrétních instalačních a implementačních požadavků

V rámci předmětu plnění budou provedeny následující služby pro následující oblasti plnění:

Obecné požadavky
• dodávka požadovaného hardware a software, • doprava hardware do místa instalace, • montáž dodaných zařízení do stávajících datových rozvaděčů, • konfigurace portů pro správu a karet pro vzdálenou správu jednotlivých zařízení a jejich připojení do vyhrazené sítě pro správu, • aktualizace firmware v jednotlivých zařízeních a jejich komponentách na nejnovější doporučené verze, • zabezpečení přístupu ke správě jednotlivých zařízení, konfigurace synchronizace jejich času, konfigurace SNMP parametrů pro možnost vzdáleného dohledu, konfigurace SMTP pro zasílání e-mailové notifikace o stavu zařízení, • kompletní ověření funkčnosti celého řešení o simulovaný výpadek jednoho z páteřních přepínačů, ○ odpojení jednoho z propojů mezi páteřními přepínači, ○ otestování redundantního napájení jednotlivých zařízení střídavým odpojením jednoho z napájecích zdrojů, • propojení celého řešení do stávající síťové infrastruktury a vybudování služeb pro síťovou a serverovou infrastrukturu v rámci dodávaných technologií • ověření registrací zařízení a licencí u výrobců, aktivace licencí a služeb

Implementační služby

Next Generation Firewall s příslušenstvím
• analýza současného prostředí • návrh nové architektury, musí zahrnovat integraci se stávajícími firewally s možností jednotné správy a flexibilního využití (perimetrový/segmentační firewall, VPN koncentrátor apod.), převod role TMG do nového prostředí (a následně zrušení TMG), zachování a optimalizace role aplikačního firewallu. • migrace na nové firewally (export pravidel ze stávajících firewallů pro potřebu analýzy zajistí kupující) • optimalizace pravidel/politik včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) s využitím nových či vylepšených funkcionalit a začlenění firewallu do LAN prostředí. • související rekonfigurace stávajících zařízení
Páteřní přepínače a přístupové přepínače
• analýza stávajícího prostředí • návrh nové architektury včetně přeskupení a náhrady stávajících zařízení, bude zahrnovat i návrh segmentace LAN – tj. VLAN včetně adresace a řízení/filtrování provozu mezi nimi – předpokládaný počet VLAN jsou nižší desítky • sestavení stohů přepínačů a jejich propojení pro zajištění vysoké dostupnosti v co nejvyšším rozsahu • začlenění prvků do systému centrální správy a jeho rekonfigurace • konfigurace agregačních skupin (LACP) na přepínačích pro propojení přepínačů, připojení serverů • konfigurace VLAN, trunk portů a přístupových portů na jednotlivých přepínačích • vytvoření oddělených LAN a SAN komunikačních domén • nastavení exportu a zpracování IPFIX • související rekonfigurace stávajících zařízení

Licence SW pro řízení přístupu do sítě 802.1X
• analýza současného prostředí • návrh nové architektury, způsob autentizace jednotlivých typů klientů (počítače, mobilní zařízení, periferie, OT/IOT atd.) a identitní databáze (primárně Active Directory) • implementace systému 802.1X • začlenění přepínačů a WiFi přístupových bodů do systému 802.1X • vytvoření a aplikování Connection Request Policy a Network Policy pro 802.1X • vytvoření návodů pro zařazení běžných koncových zařízení do systému 802.1X (PC, notebook, chytrý telefon/tablet) • související rekonfigurace stávajících zařízení
Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI
• analýza prostředí se zaměřením na zavedení vícefaktorové autentizace • vybudování interní PKI (Public Key Infrastructure) včetně certifikační autority integrované s Active Directory • vybudování systému vícefaktorové autentizace s využitím kontaktních identifikačních prostředků (karet, tokenů) pro systémy Windows a terminálové služby Microsoft RDS. • Instalace klávesnic/čteček na koncová zařízení ani distribuce identifikačních medií uživatelům není součástí plnění • návrh a vybudování systému pro správu kompletního životního cyklu identifikačních prostředků (karet a doménových i veřejných certifikátů) včetně uživatelské běžné správy a obnovy platnosti certifikátů • návrh a realizace zálohování • související rekonfigurace stávajících zařízení
Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM
• analýza ICT prostředí se zaměřením na vyhledání a inventarizaci privilegovaných účtů a systémů, u nichž bude činnost privilegovaných účtů monitorována • návrh a vybudování systému pro správu a řízení privilegovaných účtů, včetně rotace hesel • související rekonfigurace stávajících technologií • Návrh a provedení akceptačních testů, musí prokázat minimálně funkčnost v obvyklých scénářích použití (přístup správce pomocí vzdálené plochy a příkazové řádky (ssh)), ukládání relací a rotaci hesel.

2.2. Předimplementační analýza

Před implementací řešení bude zpracována předimplementační analýza, pro následující oblasti:

- způsob začlenění nabízeného řešení do stávajícího ICT prostředí,
- analýza požadavků na síťovou infrastrukturu,
- analýza požadavků na ukládání a zálohování dat, obnovu dat, toky a objemy dat,
- požadavky na rekonfigurace stávajících systémů ve vztahu k plánovanému využití,
- dopady implementace na dostupnost a funkčnost stávajících služeb,
- další podklady relevantní pro návrh řešení,
- požadovaná součinnost kupujícího,
- návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Výstupem předimplementační analýzy bude písemná zpráva podléhající schválení kupujícím.

2.3. Zpracování prováděcí dokumentace

Před zahájením implementačních prací bude zpracována prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

Prováděcí dokumentace bude před zahájením implementačních prací písemně schválena kupujícím.

Prováděcí dokumentace zohlední podmínky stávajícího stavu, požadavky cílového stavu a bude obsahovat tyto části:

- detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému,
- způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
- detailní návrh a popis postupu implementace předmětu plnění,
- detailní popis zajištění bezpečnosti informací,
- detailní harmonogram projektu včetně uvedení kritických milníků,
- návrh designu úložišť a virtuálních serverů a jeho konfigurace,
- návrh designu zálohování a jeho konfigurace,
- návrh designu síťového řešení a jeho konfigurace,
- návrh monitorování řešení monitorovacími nástroji,
- vazby na stávající systémy a jejich konfigurace,
- návrh akceptačních kritérií a akceptačních testů,
- detailní popis navrhovaných zaškolení administrátorů.

2.4. Provozní dokumentace

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat všechny dodané systémy.

2.5. Zaškolení

Dodavatel zajistí zaškolení zaměstnanců Zadavatele – administrátorů – na zařízení a systémy, v rámci tohoto plnění, a to v rozsahu předávané provozní dokumentace.

- zaškolení zajistí seznámení specialistů IT kupujícího se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin,
- rozsah zaškolení je 8 hodin,
- zaškolení bude probíhat v sídle kupujícího,
- předpokládá se účast 2 administrátorů,

2.6. Provedení zkušebního provozu a akceptačních testů

Zkušební provoz je navržen v harmonogramu plnění

Návrh a způsob provedení akceptačních testů bude upřesněn v rámci prováděcí dokumentace

2.7. Další požadavky na záruční dobu, záruční servis a další podmínky v rámci záruky

Kupující bude mít přístup k aktualizacím software a firmware dodaného HW v kupní ceně po záruční dobu, záručního servisu a podpory.

Veškeré opravy v rámci záruční doby budou provedeny bez dalších nákladů pro kupujícího.

Provedení záruční opravy do deseti pracovních dnů.

3. Harmonogram plnění

harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky.

Údaj D značí datum nabytí účinnosti kupní smlouvy. Číslo značí počet kalendářních dnů.

Aktivita	Termín splnění
Nabytí účinnosti smlouvy (uveřejnění v registru smluv)	D
Předimplementační analýza – zpracování	D+21
Předimplementační analýza – připomínkové řízení, schválení	D+28
Prováděcí dokumentace – zpracování	D+42
Prováděcí dokumentace – připomínkové řízení, schválení	D+49
Realizace předmětu plnění	D+100
Školení administrátorů	D+110
Zkušební provoz	D+110
Akceptace předmětu plnění	D+120 dnů

Cenová tabulka veřejné zakázky s názvem Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti

1. Účastník zadávacího řízení cenou tabulku vyplní a cenu vypočte pouze v buňkách označených

2. Účastník vyplní do tabulky jednotlivé ceny dodávek a služeb včetně jejich příslušenství

3. Pro stanovení nabídkové ceny do ceny zařízení dodavatele zaneše cenu standardní záruky, která je k zařízení dodávána. Nadstandardní záruku, záruční servis a podporu dodavatel nacení samostatně do příslušné položky k zařízení v tabulce níže. Podpora zařízení a podpora software za předpokladu, že první rok podpory je součástí dodávky licence nebo zařízení může být součástí ceny zařízení a licence, každý další rok musí být naceněn samostatně ve sloupečku E této tabulky, jako samostatná podpora, není-li v technické dokumentaci uvedeno jinak.

4. Náklady na implementační služby budou zohledněny v ceně dodávek zařízení.

Název dodavatele:		Aricoma Systems a.s.		
Položka	Počet	Celková cena za uvedený Počet [Kč bez DPH]	Cena za prodlouženou záruku a záruční servis k zařízení dle specifikace [Kč bez DPH]	Tech. podpora po dobu celkem 5 let (maintenance, bezpečnostní update, patche, subskripce, nároky na aktualizací balíčky dat atd.) [Kč bez DPH]
Next Generation Firewall s příslušenstvím	2	1 252 800 Kč	295 254 Kč	321 748 Kč
Páteřní přepínače 48p s příslušenstvím	2	585 760 Kč	48 000 Kč	---
Přístupové přepínače 48p PoE s příslušenstvím	28	2 508 814 Kč	112 000 Kč	---
Přístupové přepínače 24p s příslušenstvím	2	357 518 Kč	16 000 Kč	---
Licence SW pro řízení přístupu do sítě založeného na protokolu 802.1x	1	1110 291 Kč	---	181 465 Kč
Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI	1	922 244 Kč	---	88 000 Kč
Autentizační prostředky	300	340 244 Kč	---	---
Klávesnice s integrovanou čtečkou karet, včetně ovladačů	150	125 756 Kč	---	---
Samostatné USB čtečky čipových karet, včetně ovladačů	150	57 158 Kč	---	---
Nástroj pro správu privilegovaných účtů serverů – PIM/PAM	1	1 269 610 Kč	---	186 000 Kč
			Nabídková cena celkem v Kč bez DPH	9 778 662,00 Kč
			DPH ve výši 21 %	2 053 519,02 Kč
			Nabídková cena celkem v Kč včetně DPH	11 832 181,02 Kč

V Karlových Varech dne dle el. podpisu

Podpis osoby oprávněné za účastníka zadávacího řízení