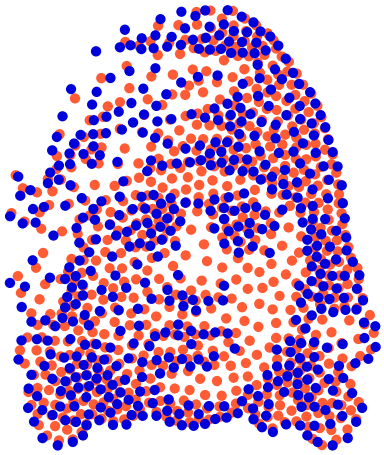

Státní tiskárna cenin, s. p.
se sídlem Růžová 943/6, Nové Město, 110 00 Praha 1
zapsaný v OR vedeném Městským soudem v Praze, oddíl ALX, vložka 296

Statutární orgán:
Mgr. Marek Šimandl, MPA
generální ředitel

Státní tiskárna cenin, s. p. je držitelem certifikátu ISO 14298 (Systém řízení bezpečnostního tisku), ISO/IEC 27001 (Systém managementu bezpečnosti informací), ISO 9001 (Systém managementu kvality), ISO 14001 (Systém environmentálního managementu), ISO 45001 (Systém managementu bezpečnosti a ochrany zdraví při práci)

Zadávací dokumentace

(dále jen „tato ZD“)

pro zpracování nabídky k veřejné zakázce na dodávky zadávané v otevřeném nadlimitním řízení dle ustanovení § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon“)

Služby poskytování implementace a podpory IDM a PAM

(dále jen „veřejná zakázka“ nebo „tato veřejná zakázka“)

1. IDENTIFIKAČNÍ ÚDAJE ZADAVATELE

Zadavatel	**Státní tiskárna cenin, s. p.**
Sídlo	Růžová 943/6, Nové Město, 110 00 Praha 1
IČO	00001279
Statutární orgán	Mgr. Marek Šimandl, MPA generální ředitel
Kontaktní osoba zadavatele	Šárka Kadlecová
E-mail	kadlecova.sarka2@stc.cz
Profil zadavatele	https://mfcr.ezak.cz/profile_display_53.html
Identifikátor datové schránky	hqe39ah

(dále jen „**zadavatel**“ nebo „**objednatel**“)

Zadavatel tímto prohlašuje, že je povinnou osobou – poskytovatelem regulované služby v režimu vyšších povinností ve smyslu zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“), zákona č. 266/2025 Sb., o kritické infrastruktuře a vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „Vyhláška na řízení dodavatelů“).

Název regulované služby – digitální infrastruktura a služby – poskytování řízené služby.

Zadavatel tímto informuje Účastníky zadávacího řízení, že vybraný dodavatel bude ve smyslu § 9 – Řízení dodavatelů Vyhlášky na řízení dodavatelů identifikován a evidován jako významný dodavatel.

2. ZPŮSOB A TERMÍN ZAHÁJENÍ VEŘEJNÉ ZAKÁZKY

Zadavatel zahajuje otevřené řízení v souladu s § 56 odst. 1 zákona odesláním oznámení o zahájení zadávacího řízení k uveřejnění způsobem podle § 212 zákona, kterým vyzývá neomezený počet dodavatelů k podání nabídky.

3. PŘEDMĚT VEŘEJNÉ ZAKÁZKY

3.1 Předmětem plnění této veřejné zakázky je:

3.1.1 dodání a provozování systému Identity Management – správy uživatelských účtů (dále jen „**IdM**“) a systému Privileged Access Management – systému pro řízení privilegovaných účtů (dále jen „**PAM**“) v prostředí zadavatele, zajišťující dlouhodobou koncepci řízení privilegovaných účtů, řízení identit a přístupových oprávnění (IdM A PAM také společně jako „**systémy**“).

3.1.2 implementace těchto systémů umožňující centralizovanou, bezpečnou a efektivní správu identit (uživatelských účtů a přístupových práv), automatizace procesů spojených s přidělováním a odnímáním přístupů a monitorování aktivit privilegovaných uživatelů a

3.1.3 dodání řešení, které bude možné provozovat jak prostřednictvím dodavatele, tak jiným externím subjektem nebo samotným zadavatelem.

3.2 Detailní popis předmětu plnění je vymezen v návrhu smlouvy uvedené příloze č. 1 této ZD (výše a dále jen „**Návrh smlouvy**“), zejména v:

3.2.1 příloze č. 1a Návrhu smlouvy (Technické požadavky) a v příloze č. 1b Návrhu smlouvy (Koncové systémy a počet uživatelů), které jsou nedílnou součástí Návrhu smlouvy.

3.2.2 čl. VI odst. 10 a čl. VII Návrhu smlouvy, který upravuje licenční podmínky.

3.3 Předmět plnění je rozdělen na níže uvedené dílčí etapy, které jsou blíže vymezeny v příloze č. 1 Návrhu smlouvy.

3.3.1 Etapu 1: Implementace IdM a jeho napojení na aktiva definovaná v Tabulce A přílohy č. 1b Návrhu smlouvy,

3.3.2 Etapu 2: Implementace PAM a a jeho napojení na aktiva definovaná v Tabulce D přílohy č. 1b Návrhu smlouvy,

3.3.3 Etapu 3: Napojení dalších aktiv definovaných v Tabulce B přílohy č. 1b Návrhu smlouvy na IdM.

3.4 Činnosti (Fáze) pro jednotlivé Etapy:

Pro Etapu 1:

3.4.1 Provedení předimplementační analýzy v rozsahu dle podkapitoly 5.1 přílohy č. 1a Návrhu smlouvy; Výstupy z této části plnění podléhají akceptační proceduře obdobně dle čl. VI odst. 4 až 7 Návrhu smlouvy (dále také jako „**předimplementační analýza**“);

3.4.2 Implementace a integrace IdM v rozsahu dle podkapitoly 5.2 přílohy č. 1a Návrhu smlouvy v souladu se zadavatelem akceptovanou předimplementační analýzou;

3.4.3 Předání dokumentace vztahující se k systému IdM v rozsahu dle podkapitoly 5.3 přílohy č. 1a Návrhu smlouvy;

3.4.4 Zajištění školení v rozsahu dle podkapitoly 5.4 přílohy č. 1a Návrhu smlouvy;

3.4.5 Poskytnutí licencí k systému IdM v rozsahu dle čl. VI odst. 10 a čl. VII Návrhu smlouvy;

3.4.6 Testovací provoz v rozsahu dle podkapitoly 5.5 přílohy č. 1a Návrhu smlouvy a akceptační řízení dle čl. VI odst. 4 až 7 Návrhu smlouvy včetně akceptačních testů.

Provedení akceptační procedury je nezbytné k předání a převzetí celého systému IdM a souvisejícího plnění a uvedení IdM do produkčního provozu (Go-live).

Pro Etapu 2:

3.4.7 Aktualizace a doplnění předimplementační analýzy pro Etapu 2 v rozsahu dle podkapitoly 6.1 přílohy č. 1a Návrhu smlouvy;

3.4.8 Implementace a integrace PAM v rozsahu dle podkapitoly 6.2 přílohy č. 1a Návrhu smlouvy v souladu se zadavatelem akceptovanou předimplementační analýzou;

3.4.9 Předání dokumentace vztahující se k systému PAM v rozsahu dle podkapitoly 6.3 přílohy č. 1a Návrhu smlouvy;

3.4.10 Zajištění školení v rozsahu dle podkapitoly 6.4 přílohy č. 1a Návrhu smlouvy;

3.4.11 Dodání HW včetně poskytnutí záruky v rozsahu dle čl. IX Návrhu smlouvy, pokud bude součástí dodávaného řešení dodavatele dle přílohy č. 2b Návrhu smlouvy;

3.4.12 Poskytnutí licencí k systému PAM v rozsahu dle čl. VI odst. 10 a čl. VII Návrhu smlouvy;

3.4.13 Testovací provoz v rozsahu dle podkapitoly 6.5 přílohy č. 1a Návrhu smlouvy a akceptační řízení dle čl. VI odst. 4 až 7 Návrhu smlouvy včetně akceptačních testů.

Provedení akceptační procedury je nezbytné k předání a převzetí celého systému PAM a souvisejícího plnění a uvedení PAM do produkčního provozu (Go-live).

Pro Etapu 3:

3.4.14 Aktualizace a doplnění předimplementační analýzy pro Etapu 3 v rozsahu dle podkapitoly 7.1 přílohy č. 1a Návrhu smlouvy;

3.4.15 Integrace IdM na systémy v rozsahu dle podkapitoly 7.2 přílohy č. 1a Návrhu smlouvy v souladu se zadavatelem akceptovanou předimplementační analýzou;

3.4.16 Předání dokumentace v rozsahu dle podkapitoly 7.3 přílohy č. 1a Návrhu smlouvy;

3.4.17 Zajištění školení v rozsahu dle podkapitoly 7.4 přílohy č. 1a Návrhu smlouvy;

3.4.18 Testovací provoz v rozsahu dle podkapitoly 7.5 přílohy č. 1a Návrhu smlouvy a akceptační řízení dle čl. VI odst. 4 až 7 Návrhu smlouvy včetně akceptačních testů.

Provedení akceptační procedury je nezbytné k předání a převzetí předmětného plnění a uvedení do produkčního provozu (Go-live).

3.5 Dále je součástí předmětu plnění poskytování technické podpory pro systém IdM a PAM spočívající v zajišťování Monitoringu (servisní podpora v režimu 24/7 u systému PAM a 8x5 u systému IdM, včetně garance SLA), možnosti neomezeného řešení incidentů (Incident Management), provádění servisních zásahů, služby podpory produktů (maintenance) a konzultací, a to v rozsahu dle podkapitoly 7.6 přílohy č. 1a Návrhu smlouvy pro systém IdM a podkapitoly 7.7 přílohy č. 1a Návrhu smlouvy pro systém PAM a v souladu s požadavky na provoz řešení a SLA stanovených v příloze č. 5 Návrhu smlouvy (dále také jako „**Služby podpory**“).

3.6 Dále jsou součástí předmětu plnění služby na vyžádání na provedení úprav dodaných systémů IdM a PAM a jejich rozvoj, dalších rozvojových integrací systémů IdM a další nezbytné činnosti v maximálním celkovém rozsahu 1000 člověkodnů (dále jen „**MD**“) za dobu trvání smlouvy (dále jen „**ad hoc služby**“) v rozsahu dle podkapitoly 7.8 přílohy č. 1a Návrhu smlouvy.

3.7 Zadavatel si ve smyslu § 100 odst. 1 ZZVZ **vyhrazuje právo na uplatnění vyhrazené změny závazku** zajišťující splnění požadavků ZoKB a Vyhlášky na řízení dodavatelů související s předmětem plnění a Návrhem smlouvy. Podrobnosti o této vyhrazené změně závazku jsou uvedeny v čl. II. odst. 10 Návrhu smlouvy. Pro vyloučení jakýchkoliv pochybností smluvní strany uvádějí, že Zadavatel je oprávněn, nikoli však povinen, uplatnit vyhrazenou změnu závazku dle tohoto čl. II. odst. 10 Návrhu smlouvy. Účastník je povinen vyhovět této změně, pokud je v souladu s podmínkami Návrhu smlouvy.

3.8 Zadavatel uvádí v souladu s § 36 odst. 4 zákona, že část ZD, konkrétně Technickou specifikaci zakázky jako přílohu č. 1 Návrhu smlouvy, vypracovala ve spolupráci se zadavatelem osoba odlišná od zadavatele, a to dodavatel **ICZ a.s., se sídlem: Na hřebenech II 1718/10, Nusle (Praha 4), 140 00 Praha, IČO: 25145444**. Dále se na dílčích zadávacích podmínkách podílel dodavatel **Deepview s.r.o., se sídlem: Všehrdova 560/2, 118 00 Praha 1 – Malá Strana, IČO: 24734462.**

3.9 Zadavatel v souladu s ustanovením § 36 odst. 4 zákona uvádí, že v rámci přípravy zadávacího řízení provedl průzkum trhu, jehož součástí byla i předběžná tržní konzultace (dále jen „PTK“), které se zúčastnil dodavatel: **AMI Praha a. s., se sídlem Hanusova 29, 140 00 Praha, IČO: 25715909**. Zadavatel v souladu s § 36 odst. 4 zákona označil všechny informace, které zahrnul na základě PTK do zadávacích podmínek, konkrétně se jedná o červený text označený *PTK v příloze č. 1a Návrhu smlouvy (Technické požadavky).

3.10 **Aspekty sociálně odpovědného zadávání**

V souladu s ustanovením § 6 odst. 4 zákona je zadavatel povinen při vytváření zadávacích podmínek, hodnocení nabídek a výběru dodavatele dodržovat principy a zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací za předpokladu, že to bude vzhledem k povaze a smyslu veřejné zakázky vhodné. Zadavatel zohlednil tuto povinnost v rámci přípravy této ZD.

4. KLASIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY

Kód CPV	Předmět veřejné zakázky
72261000-2	Informační systémy

5. PŘEDPOKLÁDANÁ HODNOTA, MAXIMÁLNÍ NABÍDKOVÁ CENA

5.1 Zadavatel stanovil předpokládanou hodnotu veřejné zakázky řádně s ohledem na rozsah předmětu plnění a další aspekty veřejné zakázky a pro účely této veřejné zakázky předpokládanou hodnotu neuvádí.

5.2 Zadavatel stanovil požadavek na maximální povolenou výši celkové nabídkové ceny, která nesmí být vyšší než **48 000 000 Kč bez DPH za celý předmět plnění této veřejné zakázky**.

5.3 Zadavatel dále uvádí, že nabídková cena za 1 člověkoden (dále jen „MD“, uvedeno v čl. II, odst. 5 bod 5.3 Návrhu smlouvy) **nesmí překročit částku 18.000, - Kč bez DPH/1 MD**.

V případě, že účastník ve své nabídce předloží celkovou nabídkou cenu vyšší, než je zadavatelem stanovena maximální výše celkové nabídkové ceny, jedná se o nesplnění zadávacích podmínek a důvod pro vyloučení nabídky účastníka ze zadávacího řízení. Obdobně bude postupováno v případě překročení stanoveného cenového limitu pro dílčí část nabídkové ceny, a to ceny za 1 MD.

6. POŽADAVKY NA VARIANTY

Zadavatel nepřipouští variantní řešení.

7. MÍSTO PLNĚNÍ VEŘEJNÉ ZAKÁZKY

7.1 Místem plnění této veřejné zakázky je sídlo zadavatele a výrobní závody zadavatele:

- **Výrobní závod I – Růžová 943/6, Nové Město, 110 00 Praha 1;**
- **Výrobní závod II – Za Viaduktem 8, 170 00 Praha 7,**

pokud z povahy konkrétní činnosti nutné k plnění předmětu zakázky nevyplývá něco jiného (např. vzdálený přístup k systému prostřednictvím VPN).

8. DOBA PLNĚNÍ VEŘEJNÉ ZAKÁZKY

8.1 Předpokládaný termín uzavření smlouvy: **ihned po výběru dodavatele, tj. předběžně červenec 2026.**

8.2 Termín plnění předmětu veřejné zakázky je uveden **v čl. III Návrhu smlouvy.**

9. POŽADAVKY NA JEDNOTNÝ ZPŮSOB ZPRACOVÁNÍ NABÍDKOVÉ CENY

9.1 Účastník zadávacího řízení (dále jen „účastník“) je povinen v rámci své nabídky vyplnit své dílčí nabídkové ceny v Kč bez DPH do přílohy č. 3 této ZD („Stanovení nabídkové ceny“), v souladu se všemi požadavky zadavatele a ve struktuře požadované dle této přílohy (bližší pokyny pro vyplnění jsou součástí této přílohy). Účastník je povinen vyplnit v rámci své nabídky přílohu č. 3 této ZD konkrétně listy „Celkem“, „Podpora“, „Licence IdM“, „Licence PAM“ a „HW“, následně bude v rámci finalizace smlouvy před jejím podpisem zadavatelem přiložena celá příloha č. 3 ZD, jako příloha č. 4 Návrhu smlouvy. Příslušné nabídkové ceny, resp. jejich totožné výše, budou zadavatelem uvedeny do odpovídajících ustanovení Návrhu smlouvy **v rámci finalizace smlouvy** před jejím uzavřením (výše a dále také jako „Celková nabídková cena“).

9.2 Jednotlivé dílčí nabídkové ceny budou stanoveny jako ceny nejvýše přípustné a musí v nich být zahrnuty veškeré náklady dodavatele, spojené s realizací předmětu veřejné zakázky, a to i v souladu s čl. IV odst. 11 Návrhu smlouvy.

9.3 Účastník není oprávněn podmínit jím navrhovanou Celkovou nabídkovou cenu, ani žádnou z jejích částí, další podmínkou. Podmínění nebo uvedení několika rozdílných hodnot dílčích nabídkových cen na různých místech v nabídce je důvodem pro vyloučení dodavatele ze zadávacího řízení.

9.4 Celková nabídková cena, popřípadě kterákoliv její součást, uvedená v nabídce na základě ZD, musí mít kladnou hodnotu. Zadavatel připouští nulovou cenu u těchto dílčích položek: open-source licence (FOSS) a HW. Nulová cena může být uvedena pouze z důvodu při využití bezplatných open-source licencí (FOSS) a v případě volitelnosti dodávky HW v rámci systému PAM (Etapy č. 2). Dodavatel není povinen dodat HW, pokud jeho dodání není nezbytné pro řádné plnění předmětu veřejné zakázky. V případě, že HW nebude v rámci plnění dodáván, může být příslušná položka oceněna nulovou hodnotou. Celková nabídková cena, popřípadě kterákoliv její součást, bude stanovena s přesností na dvě desetinná místa.

10. KVALIFIKACE DODAVATELE

10.1 **Splnění kvalifikace**

Kvalifikaci splní účastník, který prokáže splnění:

- základní způsobilosti ve smyslu ustanovení § 74 zákona podle ustanovení § 75 zákona,
- profesní způsobilosti podle ustanovení § 77 zákona,
- technické kvalifikace podle ustanovení § 79 zákona,
- ekonomická kvalifikace podle ustanovení § 78 zákona.

Dodavatel může pro účely podání nabídky v souladu s ustanovením § 86 odst. 2 zákona nahradit doklady požadované v rámci základní způsobilosti podle ustanovení § 74 zákona písemným čestným prohlášením. Dodavatel může využít vzor prohlášení v příloze č. 2 této ZD (Krycí list nabídky). Před podpisem smlouvy je vybraný dodavatel povinen předložit jednotlivé požadované doklady k základní způsobilosti dle § 75 zákona.

Doklady požadované v rámci profesní způsobilosti podle ustanovení § 77 odst. 1 zákona a technické kvalifikace podle ustanovení § 79 zákona je dodavatel povinen předložit dle požadavků zadavatele v této ZD.

Dle ustanovení § 87 zákona lze prokázat splnění kvalifikace také jednotným evropským osvědčením pro veřejné zakázky.

Zadavatel si může v průběhu tohoto zadávacího řízení vyžádat předložení originálů nebo úředně ověřených kopií dokladů o kvalifikaci.

Doklady prokazující základní způsobilost podle § 74 zákona musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců PŘEDE DNEM ZAHÁJENÍ TOHOTO ZADÁVACÍHO ŘÍZENÍ.

10.2 **Základní způsobilost**

10.2.1 **Způsobilým není dodavatel, který**:

a) byl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 k zákonu nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží; jde-li o právnickou osobu, musí tento předpoklad splňovat jak tato právnická osoba, tak zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí výše uvedené podmínky splňovat jak tato právnická osoba, tak každý člen statutárního orgánu této právnické osoby a také osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

   Podává-li nabídku či žádost o účast pobočka závodu zahraniční právnické osoby, musí výše uvedené podmínky splňovat tato právnická osoba a vedoucí pobočky závodu,

   Podává-li nabídku či žádost o účast pobočka závodu české právnické osoby, musí výše uvedené podmínky splňovat vedle výše uvedených osob (tj. jak tato právnická osoba, tak zároveň každý člen statutárního orgánu, a je-li členem statutárního orgánu dodavatele právnická osoba, musí výše uvedené podmínky splňovat jak tato právnická osoba, tak každý člen statutárního orgánu této právnické osoby a také osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele) rovněž vedoucí pobočky;

b) má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,

c) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,

d) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,

e) je v likvidaci, nebylo proti němu vydáno rozhodnutí o úpadku, nebyla vůči němu nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.

10.2.2 **Prokázání splnění základní způsobilosti dodavatelem se sídlem v České republice**

Dodavatel se sídlem v České republice prokazuje splnění podmínek základní způsobilosti předložením:

a) výpisu z evidence Rejstříku trestů ve vztahu k 10.2.1 písm. a) této ZD,

b) potvrzení příslušného finančního úřadu ve vztahu k 10.2.1 písm. b) této ZD,
c) písemného čestného prohlášení ve vztahu ke spotřební dani ve vztahu k 10.2.1 písm. b) této ZD,
d) písemného čestného prohlášení ve vztahu k 10.2.1 písm. c) této ZD,
e) potvrzení příslušné okresní správy sociálního zabezpečení ve vztahu k 10.2.1 písm. d) této ZD,
f) výpisu z obchodního rejstříku, nebo předložením písemného čestného prohlášení v případě, že není v obchodním rejstříku zapsán, ve vztahu k 10.2.1 písm. e) této ZD.

10.2.3 **Prokázání splnění základní způsobilosti dodavatelem se sídlem mimo Českou republiku**

Dodavatel se sídlem mimo Českou republiku prokazuje splnění podmínek základní způsobilosti předložením:

ve vztahu k České republice

a) potvrzení příslušného českého finančního úřadu ve vztahu k 10.2.1 písm. b) této ZD,
b) písemného čestného prohlášení ve vztahu ke spotřební dani ve vztahu k 10.2.1 písm. b) této ZD,
c) písemného čestného prohlášení ve vztahu k 10.2.1 písm. c) této ZD,
d) potvrzení příslušné české okresní správy sociálního zabezpečení ve vztahu k 10.2.1 písm. d) této ZD,
e) výpisu z českého obchodního rejstříku, nebo předložením písemného čestného prohlášení v případě, že není v obchodním rejstříku zapsán, ve vztahu k 10.2.1 písm. e) této ZD.

a zároveň

ve vztahu k zemi svého sídla:

a) dodavatel prokazuje splnění podmínek základní způsobilosti **ve vztahu k zemi svého sídla** v souladu s ustanovením § 81 zákona doklady vydanými podle právního řádu země, ve které byla kvalifikace získána, a to v rozsahu požadovaném zadavatelem.
b) V rámci základní způsobilosti je zahraniční dodavatel povinen prokázat **ve vztahu k zemi svého sídla** skutečnosti dle k 10.2.1 písm. a), b), c), d) a e) této ZD.
c) Pokud se podle příslušného právního řádu požadovaný doklad nevydává, může být v souladu s ustanovením § 45 odst. 3 zákona nahrazen **písemným čestným prohlášením**.

10.3 **Profesní způsobilost**

Dle § 77 odst. 1 zákona výpis z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

10.4 **Seznam kvalifikovaných dodavatelů**

Předloží-li dodavatel ve své nabídce výpis ze seznamu kvalifikovaných dodavatelů v souladu s § 228 zákona, tento výpis nahrazuje doklady prokazující kvalifikaci dle čl. 10.2. a 10.3. této ZD v tom rozsahu, v jakém údaje ve výpisu ze seznamu kvalifikovaných dodavatelů prokazují splnění kritérií profesní způsobilost. Výpis ze seznamu kvalifikovaných dodavatelů nesmí být k poslednímu dni, ke kterému má být prokázána základní způsobilost nebo profesní způsobilost, starší než 3 měsíce.

10.5 **Technická kvalifikace**

10.5.1 K prokázání technické kvalifikace zadavatel požaduje podle ustanovení § 79 odst. 2 písm. b) zákona **předložení seznamu významných zakázek poskytnutých za poslední 3 roky před dnem zahájením zadávacího řízení** včetně uvedení ceny a doby jejich poskytnutí a identifikace objednatele.

Minimální požadovaná úroveň této kvalifikace:

Dodavatel splňuje kvalifikaci, pokud realizoval

- **min. 3 významné zakázky** obdobného předmětu jako je předmět této veřejné zakázky, tj. jejichž předmětem byla dodávka a implementace nástroje pro správu a zabezpečení privilegovaných účtů (PAM) a nástroje pro správu uživatelských účtů (IdM) v rozsahu obdobném funkčním požadavkům této ZD, vždy včetně poskytnuté služby podpory v délce minimálně 6 měsíců, přičemž:
    - alespoň jedna z významných dodávek musí obsahovat **dodávku IdM** systému v minimálním objemu **5 000 000 Kč bez DPH,** přičemž do uvedeného finančního objemu se nezapočítává hodnota dodaného HW a implementovaný systém musí rozsahem řídit přístupy alespoň 300 identit,
    - alespoň jedna z významných dodávek musí obsahovat **dodávku PAM** systému v minimálním objemu **5 000 000 Kč bez DPH,** přičemž do tohoto objemu se nezapočítává hodnota dodaného HW.

Účastník tento seznam významných dodávek předloží ve své nabídce ve formě čestného prohlášení, které tvoří přílohu č. 4 této ZD, kde musí být strukturovaně uvedeny u každé z těchto významných zakázek údaje rozhodné pro prokázání dané kvalifikace, minimálně však následující údaje:

- identifikace dodavatele, který dané plnění poskytl a jeho role při plnění zakázky;
- identifikace objednatele, kterému bylo dané plnění poskytnuto;
- doba plnění s přesností na kalendářní měsíce;
- stručný popis předmětu plnění;
- finanční objem (celkovou cenu v Kč bez DPH);
- kontaktní osoba objednatele pro účely ověření uvedených informací (jméno, telefon a e-mail).

10.5.2 K prokázání technické kvalifikace zadavatel požaduje v souladu s § 79, odst. 2, písm. c) **Seznam členů řešitelského týmu,** kteří se budou podílet na plnění veřejné zakázky, včetně dokladů prokazujících jejich odbornou způsobilost, a to v minimálním rozsahu:

- 1 osoba na pozici Expert IdM,
- 1 osoba na pozici Expert PAM,
- 1 osoba na pozici Architekt řešení,
- 1 osoba na pozici Senior Project manager,
- 1 osoba na pozici Bezpečnostní expert,
- 1 osoba na pozici Integrátror IdM/PAM,

Zadavatel nepřipouští kumulaci rolí u jedné osoby. **Výjimku tvoří Expert IdM**

a Expert PAM, tyto dvě role mohu být prokazovány jednou osobou.

Jednotliví členové týmu musí splňovat minimálně tyto požadavky:

Expert IdM:

- Minimálně 5 let zkušeností z oblasti implementace systémů IdM v obdobné roli,
- Předložení minimálně 3 stále probíhajících nebo ukončených referenčních projektů za období posledních 10let před vyhlášením této veřejné zakázky, kdy se tato osoba na těchto referenčních projektech podílela v pozici experta IdM nebo materiálně obdobné pozici a jejichž předmětem byla implementace systému IdM, implementace musí být u každého z těchto projektů ukončena nasazením do produkce. V případě stále probíhajících referenčních projektů, musí být řešení ke dni vyhlášení této veřejné zakázky plně nasazeno do provozu a akceptováno a probíhá pouze následná podpora.

Expert PAM:

- Minimálně 5 let zkušeností z oblasti implementace systémů PAM v obdobné roli,
- Předložení minimálně 3 stále probíhajících nebo ukončených referenčních projektů za období posledních 10let před vyhlášením této veřejné zakázky, kdy se tato osoba na těchto referenčních projektech podílela v pozici experta PAM nebo materiálně obdobné pozici a jejichž předmětem byla implementace systému PAM, implementace musí být u každého z těchto projektů ukončena nasazením do produkce. V případě stále probíhajících referenčních projektů, musí být řešení ke dni vyhlášení této veřejné zakázky plně nasazeno do provozu a akceptováno a probíhá pouze následná podpora.

Architekt řešení:

- Minimálně 2 roky zkušeností s tvorbou architektury pro implementaci IdM a/nebo PAM v obdobné roli,
- Minimálně 5 let zkušeností s tvorbou architektury v souvislosti se zavedením systémů pro kybernetickou bezpečnost.

Senior Project Manager:

- Minimálně 5 let zkušeností z oblasti řízení projektů týkajících se implementace softwarových řešení v obdobné roli,
- Předložení minimálně 1 referenčního projektu implementace systému IdM nebo PAM, na kterém se tato osoba podílela na pozici Senior project managera nebo materiálně obdobné pozici, dokončeného v posledních 5 letech před zahájením této veřejné zakázky, a to vč. nasazení do produkce,
- Certifikace PRINCE2 Practitioner či jiný obdobný certifikát prokazující stejnou či vyšší úroveň znalostí.

Bezpečnostní expert:

- Minimálně 5 let zkušeností z oblasti kybernetické bezpečnosti v obdobné roli,

- Předložení minimálně 1 referenčního projektu implementace systému IdM nebo PAM, na kterém se tato osoba podílela na pozici bezpečnostního experta nebo materiálně obdobné pozici, dokončeného v posledních 5 letech před zahájením této veřejné zakázky, a to vč. nasazení do produkce,
- Certifikace minimálně v rozsahu některého z těchto certifikátů: CISSP nebo CISM nebo CompTIA Security+ +

Integrátor (IdM/PAM):

- Předložení minimálně 3 úspěšně realizovaných referenčních projektů implementace systému IdM nebo PAM, dokončených v posledních 5 letech před zahájením této veřejné zakázky, a to vč. nasazení do produkce, kdy osoba v roli Integrátor (Idm/PAM) nebo materiálně obdobné pozici musela nést odpovědnost minimálně za tyto části projektů:
  - napojení alespoň 5 koncových systémů na IdM,
  - napojení alespoň 5 koncových systémů na PAM,
  - integrace HR systému jako zdrojového systému na IdM a,
  - integrace IdM na AD nebo MS Entra.

  Účastník prokáže splnění této kvalifikace předložením Seznamu členů realizačního týmu, jehož vzor tvoří přílohu č. 4 této ZD.

10.5.3 K prokázání technické kvalifikace zadavatel požaduje podle ustanovení § 79 odst. 2 písm. e) zákona prokázání že má účastník implementovány bezpečnostní postupy k zajištění bezpečnosti informací v rámci plnění předmětu veřejné zakázky **v minimální úrovni dle normy „ISO/IEC 27001 Systém řízení bezpečnosti informací“**.

Účastník tuto část technické kvalifikace naplní předložením prosté kopie platného akreditovaného certifikátu **„ISO/IEC 27001 Systém řízení bezpečnosti informací“**, přičemž **předmět certifikace musí odpovídat předmětu plnění veřejné zakázky,** nebo potvrzením certifikačního orgánu o úspěšném provedení certifikace a o přípravě vydání nového certifikátu.

10.6 **Ekonomická kvalifikace**

Ekonomickou kvalifikaci splní dodavatel, který doloží:

• výši svého obratu dosaženého s ohledem na předmět zakázky za 3 bezprostředně předcházející účetní období v hodnotě minimálně 20 mil. Kč bez DPH za každé účetní období. Obratem s ohledem na předmět zakázky je míněn obrat dosažený v oblasti dodávek IT a non-IT technologií.

Jestliže dodavatel vznikl později, předkládá údaje o svém obratu v požadované výši za všechna účetní období od svého vzniku.

10.6.1 **Způsob prokázání splnění ekonomické kvalifikace:**

Dodavatel prokáže obrat výkazy zisků a ztrát dodavatele nebo obdobnými doklady podle právního řádu země sídla dodavatele a současně čestným prohlášením podepsaným osobou oprávněnou jednat jménem nebo za dodavatele, ve kterém specifikuje obrat v požadované oblasti.

10.7 **Prokázání kvalifikace získané v zahraničí**

V případě, že byla kvalifikace jak dodavatele se sídlem v České republice, tak zahraničního dodavatele, získána v zahraničí, prokazuje se dle ustanovení § 81 zákona doklady vydanými podle právního řádu země, ve které byla získána, a to v rozsahu požadovaném zadavatelem.

Pokud se podle příslušného právního řádu požadovaný doklad nevydává, může být v souladu s ustanovením § 45 odst. 3 zákona nahrazen písemným čestným prohlášením. To platí jednak v situacích, kdy požadovaný doklad nemá v právním řádu země, kde byla kvalifikace získána, ekvivalent (tj. požadovaný doklad v zahraničním právním řadu neexistuje), a jednak v situacích, kdy v zahraničním právním řádu vůbec neexistuje povinnost, jejíž splnění zadavatel požaduje prokázat předložením dokladu. Ve druhém z uvedených případů dodavatel učiní čestné prohlášení o neexistenci povinnosti, jejíž splnění zadavatel požaduje prokázat.

10.8 **Prokázání kvalifikace prostřednictvím jiné osoby**

V souladu s § 83 odst. 1 zákona může dodavatel ekonomickou kvalifikaci, technickou kvalifikaci nebo profesní způsobilost s výjimkou kritéria podle § 77 odst. 1 zákona požadovanou zadavatelem prokázat prostřednictvím jiných osob.

Dodavatel je v takovém případě povinen zadavateli předložit:

a) doklady prokazující splnění profesní způsobilosti podle ustanovení § 77 odst. 1 zákona (obchodní rejstřík) touto jinou osobou,

b) doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,

c) doklady prokazující splnění úplné základní způsobilosti podle ustanovení § 74 odst. 1 zákona touto jinou osobou,

d) smlouvu nebo jinou osobou podepsané potvrzení o její existenci, jejímž obsahem je závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat při plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.

Prokazuje-li dodavatel prostřednictvím jiné osoby kvalifikaci a předkládá doklady podle § 79 odst. 2 písm. a), b) nebo d) zákona vztahující se k takové osobě, musí ze smlouvy nebo potvrzení o její existenci podle § 83 odst. 1 písm. d) zákona vyplývat závazek, že jiná osoba bude vykonávat stavební práce či služby, ke kterým se prokazované kritérium kvalifikace vztahuje.

Má se za to, že požadavek podle § 83 odst. 1 písm. d) zákona je splněn, pokud z obsahu smlouvy nebo potvrzení o její existenci podle § 83 odst. 1 písm. d) zákona vyplývá závazek jiné osoby plnit veřejnou zakázku společně a nerozdílně s dodavatelem; to neplatí, pokud smlouva nebo potvrzení o její existenci podle § 83 odst. 1 písm. d) zákona musí splňovat požadavky podle § 83 odst. 2 zákona.

10.9 **Prokázání kvalifikace v případě společné nabídky**

Má-li být předmět veřejné zakázky plněn ve smyslu ustanovení § 82 zákona několika dodavateli společně a za tímto účelem podávají či hodlají podat společnou nabídku, je každý z dodavatelů povinen prokázat splnění základní způsobilosti podle ustanovení § 74 a profesní způsobilosti podle ustanovení § 77 odst. 1 zákona samostatně v plném rozsahu.

Zadavatel v souladu s § 103 odst. 1 písm. f) zákona vyžaduje, aby odpovědnost vůči zadavateli nesli všichni dodavatelé podávající společnou nabídku společně a nerozdílně.

10.10 **Požadavek na uvedení poddodavatelů**

V souladu s ustanovením § 105 odst. 1 zákona zadavatel požaduje, aby účastník ve své nabídce specifikoval části veřejné zakázky, které má v úmyslu zadat jednomu či více poddodavatelům.

Účastník ve své nabídce předloží seznam poddodavatelů spolu s uvedením, jaká část této veřejné zakázky bude realizována poddodavatelem – s uvedením druhu dodávek, služeb nebo stavebních prací a s uvedením procentuálního (%) finančního podílu na veřejné zakázce (příloha č. této 5 této ZD).

Pokud účastník nemá v úmyslu zadat žádnou část veřejné zakázky poddodavateli, je rovněž povinen předložit čestné prohlášení o této skutečnosti v rámci své nabídky (příloha č. 5 této ZD).

10.11 **Účastník může podat v zadávacím řízení jen jednu nabídku**.

Dodavatel, který podal nabídku v zadávacím řízení, nesmí být současně osobou, jejímž prostřednictvím jiný dodavatel v tomtéž zadávacím řízení prokazuje kvalifikaci.

Zadavatel vyloučí účastníka, který podal více nabídek samostatně nebo společně s jinými dodavateli, nebo podal nabídku a současně je osobou, jejímž prostřednictvím jiný účastník v tomtéž zadávacím řízení prokazuje kvalifikaci.

11. HODNOCENÍ NABÍDEK

11.1 **Kritéria hodnocení**

Základním kritériem hodnocení pro zadání této veřejné zakázky je v souladu s ustanovením § 114 odst. 1 zákona ekonomická výhodnost nabídky.

Ekonomická výhodnost nabídky bude hodnocena podle **nejnižší Celkové nabídkové ceny v Kč bez DPH zpracované dle této ZD.**

11.2 **Způsob hodnocení**

Nabídky budou seřazeny vzestupně podle **výše Celkové nabídkové ceny v Kč bez DPH**. Jako ekonomicky nejvýhodnější bude vybrána nabídka s nejnižší Celkovou nabídkovou cenou v Kč bez DPH.

11.3 Zadavatel neprovede hodnocení nabídek, pokud by měl hodnotit nabídku pouze jednoho dodavatele.

11.4 Dodavatel není oprávněn podmínit jim navrhované hodnoty (údaje), které jsou předmětem hodnocení, další podmínkou. Podmínění nebo uvedení několika rozdílných hodnot, které jsou předmětem hodnocení, je důvodem pro vyřazení nabídky a následné vyloučení dodavatele ze zadávacího řízení. Obdobně bude zadavatel postupovat v případě, že dojde k uvedení hodnoty, která je předmětem hodnocení, v jiné veličině či formě, než zadavatel požaduje.

12. OBCHODNÍ A PLATEBNÍ PODMÍNKY

12.1 Platební a obchodní podmínky jsou stanoveny v **závazném** Návrhu smlouvy, který tvoří přílohu č. 1 této ZD.

12.2 Účastník není povinen v nabídce předložit Návrh smlouvy. Návrh smlouvy bude vyplněn a doplněn zadavatelem před uzavřením smlouvy s vybraným dodavatelem a zadavatelem. **Účastník je však povinen v nabídce předložit písemné čestné prohlášení o tom, že Návrh smlouvy plně a bezvýhradně akceptuje a dále uvést údaje požadované pro kompletaci Návrhu smlouvy před jejím oboustranným podpisem v rozsahu přílohy č. 2 této ZD**.

12.3 V případě společné nabídky musí být v Krycím listě nabídky (příloha č. 2 této ZD) uvedeny osoby oprávněné jednat za každého účastníka a bude uveden zmocněnec k podepisování společné nabídky a součástí bude prostá kopie této plné moci.

13. POSKYTNUTÍ ZADÁVACÍ DOKUMENTACE

13.1 Kompletní zadávací dokumentace, s výjimkou přílohy č. 6 této zadávací dokumentace podle následujícího bodu, je uveřejněna na profilu zadavatele, a to minimálně po celou dobu běhu lhůty pro podání nabídek.

13.2 Zadavatel upozorňuje, že příloha č. 6 této ZD – Konfigurace systémů obsahuje důvěrné informace, a proto tato část ZD bude poskytnuta dodavatelům výhradně na základě jejich písemné žádosti a oproti podpisu prohlášení o zachování mlčenlivosti, jehož vzor tvoří přílohu č. 7 této ZD (dále jen „Prohlášení“).

13.3 Prohlášení předložené dodavatelem musí plně korespondovat s textací Prohlášení, které tvoří Přílohu č. 7 ZD (pole k doplnění dodavatelem jsou označena jako [DOPLNÍ DODAVATEL]). Prohlášení musí být **elektronicky** (platným kvalifikovaným elektronickým podpisem) podepsané osobou/osobami oprávněnými zastupovat dodavatele. Pokud Prohlášení bude na základě zmocnění podepsáno jinou osobou než statutárním orgánem, musí být prostá kopie tohoto zmocnění předložena společně s Prohlášením. **Za písemnou žádost dodavatele dle § 96 odst. 2 ZZVZ bude zadavatel považovat až předání podepsaného Prohlášení ve výše uvedeném smyslu.**

13.4 Žádost o zpřístupnění přílohy č. 6 této ZD dle § 96 odst. 2 ZZVZ včetně podepsaného Prohlášení musí být dodavatelem zaslána prostřednictvím elektronického nástroje (profilu) zadavatele.

13.5 Na základě písemné žádosti a podepsaného Prohlášení podle předchozího bodu zpřístupní zadavatel dožadujícímu dodavateli Přílohu č. 6 této ZD – Konfigurace systémů. Soubor zip bude dožadujícímu se dodavateli zaslán prostřednictvím elektronického nástroje (profilu) zadavatele, a to soukromou zprávou.

14. ŽÁDOST O VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE, KOMUNIKACE V PRŮBĚHU ZADÁVACÍHO ŘÍZENÍ

14.1 Dodavatel je ve smyslu ustanovení § 98 odst. 3 zákona oprávněn písemně požadovat po zadavateli vysvětlení této ZD, a to prostřednictvím datové schránky zadavatele, elektronicky e-mailem na adrese: **kadlecova.sarka2@stc.cz** nebo prostřednictvím elektronického nástroje.

14.2 Zadavatel uveřejní písemné vysvětlení této ZD včetně přesného znění dotazu bez identifikace dodavatele, případně související dokumenty, nejpozději do 3 pracovních dnů ode dne doručení žádosti dodavatele, a to na svém profilu zadavatele / elektronickém nástroji.

14.3 Zadavatel může poskytnout účastníkům písemné vysvětlení této ZD i bez předchozí žádosti.

14.4 V rámci dodržení principu rovného zacházení se všemi účastníky nemohou být případná vysvětlení, změny či doplnění zadávací dokumentace poskytována telefonicky. **Dodavateli je doporučeno pravidelně sledovat profil zadavatele / elektronický nástroj https://mfcr.ezak.cz/profile_display_53.html**.

14.5 Zadavatel zdůrazňuje, že v souladu s ustanovením § 4 odst. 1 vyhlášky č. 260/2016 Sb., o stanovení podrobnějších podmínek týkajících se elektronických nástrojů, elektronických úkonů při zadávání veřejných zakázek a certifikátu shody, při komunikaci uskutečňované prostřednictvím **elektronického nástroje** je dokument doručen již okamžikem **přijetí datové zprávy na elektronickou adresu adresáta datové zprávy v elektronickém nástroji**.

14.6 Zadavatel dále zdůrazňuje, že v souladu s ustanovením § 211 odst. 9 zákona při komunikaci uskutečňované prostřednictvím **datové schránky** je dokument doručen **dodáním do datové schránky adresáta**.

14.7 Zadavatel tímto vyzývá dodavatele, aby případné výhrady k Návrhu smlouvy či jiným zadávacím podmínkám zaslal postupem uvedeným v tomto článku, tj. písemně do konce lhůty pro podání nabídek uvedené v čl. 18.1 této ZD. Zadavateli bude tímto poskytnuta možnost posoudit takovou výhradu a zvolit odpovídající postup (tj. návrh odmítnout, či částečně nebo zcela akceptovat a případně přiměřeně prodloužit lhůtu pro podání nabídek,

bude-li třeba).

15. DALŠÍ ZADÁVACÍ PODMÍNKY ZADAVATELE

15.1 Tato ZD je pro dodavatele závazná.

15.2 **Právní forma dodavatele**

Zadavatel je povinen ve smyslu ustanovení § 48 odst. 9 zákona vyloučit vybraného účastníka z účasti v zadávacím řízení, pokud zjistí, že jsou naplněny důvody pro vyloučení dle ustanovení § 48 odst. 7 zákona, to znamená, že **vybraný účastník, který je akciovou společností nebo má právní formu obdobnou akciové společnosti nemá vydány <u>výlučně zaknihované akcie</u>.**

15.3 **Střet zájmů**

Obchodní společnost, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů, nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, se nesmí účastnit zadávacích řízení dle ZZVZ jako účastník zadávacího řízení nebo jako poddodavatel, prostřednictvím kterého účastník zadávacího řízení prokazuje kvalifikaci.

Účastník je povinen předložit o této skutečnosti čestné prohlášení v rámci své nabídky (příloha č. 2 této ZD).

15.4 **Sankce v souvislosti s ruskou agresí na území Ukrajiny**

V souvislosti zejména s:

- nařízením Rady (EU) Rady (EU) č. 833/2014 ze dne 31. července 2014, o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění nařízení Rady (EU) č. 2022/576 ze dne 8. dubna 2022;
- a nařízením Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, v platném znění, nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014, o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, v platném znění, nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006, o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska, v platném znění, včetně aktuálních příloh těchto všech nařízení;

je dodavatel povinen předložit o této skutečnosti čestné prohlášení v rámci své nabídky (příloha č. 2 této ZD).

15.5 **Popis technického řešení, technická dokumentace**

Zadavatel požaduje, aby nabídka účastníka obsahovala následující specifikaci a dokumentaci nabízeného technického řešení a dalších součástí, **<u>které musí být v souladu se všemi požadavky zadavatele v této veřejné zakázce</u>**, jako součást stanovených technických podmínek účasti:

15.5.1 Vyplněná příloha č. 1a Návrhu smlouvy „Technická specifikace"

Účastník je povinen vyplnit žlutě vyznačené buňky v dané příloze. **Pro splnění zadávacích podmínek musí dodavatel v každé položce vyplnit "*Splněno*".** Pokud bude v některé z položek vyplněno "*Nesplněno*", jedná se o nesplnění

zadávacích podmínek.

15.5.2 Návrh architektury IdM a PAM řešení, obsahující výčet veškerých navrhovaných komponent

Účastník ve své nabídce uvede základní popis řešení, informace o architektuře nabízeného řešení a výčet všech potřebných zdrojů pro provoz IdM a PAM v požadované specifikaci dle technické specifikace, která tvoří přílohu č. 1 Návrhu smlouvy, a této ZD.

15.5.3 Položkový seznam navrhovaných SW komponent včetně uvedení jejich licence (příloha č. 3 ZD – Stanovení nabídkové ceny)

Dodavatel ve své nabídce stanoví a položkově uvede veškeré potřebné licence vlastního IdM a PAM řešení, jakož i případných jiných komponent, které shledá potřebnými pro jím navržené řešení, splňující veškeré požadavky dle technické specifikace, která tvoří přílohu č. 1 Návrh smlouvy, a této ZD.

15.5.4 Položkový seznam navrhovaných HW komponent včetně jejich technických sizing parametrů (příloha č. 3 ZD – Stanovení nabídkové ceny)

Dodavatel ve své nabídce stanoví a položkově uvede úplnou specifikaci hardware vlastního IdM a PAM řešení, splňující veškeré požadavky dle technické specifikace, která tvoří přílohu č. 1 Návrh smlouvy, a této ZD.

Zadavatel předpokládá a **preferuje virtuální nasazení**, avšak pokud dodavatel pro dosažení požadovaných parametrů uzná za vhodné použít HW appliance, uvede to v nabídce.

Dodavatel navrhne parametry HW, potřebného pro běh všech navržených SW komponent řešení, a to formou přehledové tabulky parametrů s uvedením, zda se musí jednat o dedikovaný HW či virtuální nasazení a popisem funkčnosti daného HW.

Výše uvedený podklad dle čl. 15.5.1 výše bude tvořit přílohu č. 1a závazného Návrhu smlouvy.

Výše uvedené podklady dle čl. 15.5.2, 15.5.3. a 15.5.4 budou jako specifikace navrženého řešení dodavatele tvořit přílohu č. 2 závazného Návrhu smlouvy (2a pro systém IdM a 2b pro systém PAM).

16. SOUČINNOST PŘED UZAVŘENÍM SMLOUVY (PRO VYBRANÉHO DODAVATELE)

16.1 **Pojistná smlouva**

Vybraný dodavatel je povinen v souladu s ustanovením § 104 písm. a) zákona před podpisem smlouvy předložit **prostou kopii pojistné smlouvy v souladu s čl. VIII odst. 1 Návrhu smlouvy**. Rovnocenným dokladem pro prokázání tohoto požadavku je také prostá kopie pojistného certifikátu nebo prostá kopie potvrzení o uzavření pojistné smlouvy vystaveného pojistitelem.

16.2 **Skuteční majitelé**

16.2.1 Účastník, který je českou právnickou osobou

Nelze-li zjistit údaje o skutečném majiteli vybraného dodavatele, který je **českou** právnickou

osobou, postupem dle ustanovení § 122 odst. 5 zákona, má zadavatel povinnost vybraného dodavatele vyloučit z další účasti v zadávacím řízení dle § 122 odst. 8 písm. a) zákona.

K zápisu zpřístupněnému v evidenci skutečných majitelů po odeslání oznámení o vyloučení dodavatele zadavatel dle § 122 odst. 8 písm. a) zákona nepřihlíží.

Povinnost vyloučení se nevztahuje na právnické osoby, které skutečného majitele nemají ve smyslu ustanovení § 7 zákona č. 37/2021 Sb., o evidenci skutečných majitelů.

16.2.2 Účastník, který je zahraniční právnickou osobou

Vybraného dodavatele, je-li zahraniční právnickou osobou, zadavatel vyzve k předložení výpisu ze zahraniční evidence obdobné evidenci skutečných majitelů nebo, není-li takové evidence:

a) ke sdělení identifikačních údajů všech osob, které jsou jeho skutečným majitelem, a

b) k předložení dokladů, z nichž vyplývá vztah všech osob podle písmene a) k dodavateli; těmito doklady jsou zejména:
   1. výpis ze zahraniční evidence obdobné veřejnému rejstříku,
   2. seznam akcionářů,
   3. rozhodnutí statutárního orgánu o vyplacení podílu na zisku,
   4. společenská smlouva, zakladatelská listina nebo stanovy.

Veškeré doklady je dodavatel povinen předložit v jazyce požadovaném zadavatelem dle této ZD.

V případě, že vybraný dodavatel nepředloží požadované informace a doklady, je zadavatel v souladu s ustanovením § 122 odst. 8 písm. b) zákona povinen vybraného dodavatele vyloučit z další účasti v zadávacím řízení.

16.3 Spolehlivost plátce DPH

16.3.1 V souladu s ustanovením § 6 odst. 4 zákona zadavatel požaduje, aby vybraný dodavatel, který je tuzemským plátcem DPH v České republice, byl spolehlivým plátcem daně podle § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. V souladu s ustanovením § 104 odst. e) zákona je vybraný dodavatel, který je tuzemským plátcem DPH, před podpisem smlouvy povinen předložit prostou kopii výpisu / printscreenu obrazovky z databáze zveřejněné správcem daně způsobem umožňujícím dálkový přístup tzv. „Registr plátců DPH“. Číslo účtu, vyplněné dodavatelem v nabídce, v souladu s požadavkem uvedeném v čl. 12.2 této ZD, musí být shodné s číslem účtu uvedeném v registru plátců DPH.

16.3.2 Vzhledem k současné právní úpravě a skutečnosti, že zadavatel nenese odpovědnost za DPH dodavatele, který není tuzemským plátcem DPH (v České republice), požadavek stanovený v čl. 16.3.1 této ZD se nevztahuje na dodavatele, který není tuzemským plátcem DPH (v České republice).

16.4 Bankovní účet

Vybraný dodavatel, **který není plátcem DPH v České republice**, je povinen v souladu s ustanovením § 104 písm. e) zákona před podpisem smlouvy předložit prostou kopii potvrzení či prohlášení banky, že bankovní účet uvedený vybraným dodavatelem v nabídce patří vybranému dodavateli.

17. PODMÍNKY PRO PODÁNÍ NABÍDKY

17.1 Zadavatel nepožaduje po účastníkovi, aby veškeré doklady či prohlášení byly podepsány statutárním orgánem účastníka nebo osobou oprávněnou jednat jménem či za účastníka. **Účastník podáním nabídky prostřednictvím elektronického nástroje stvrzuje, že nabídku podala osoba oprávněná činit tyto úkony a podáním nabídky zároveň účastník souhlasí se zadávacími podmínkami stanovenými zadavatelem a zákonem.**

17.2 Nabídka bude podána v **českém jazyce, pokud v této ZD není stanoveno jinak. Použití anglického jazyka je možné ve smyslu použití požadované přílohy č. 3 této ZD v nabídce a obdobně vyplněné přílohy č. 1 Návrhu smlouvy č. 1a „Technická specifikace" či jiných podkladů dle čl. 15.5. této ZD, které mohou obsahovat anglické názvy a termíny obvyklé pro předmět plnění této VZ.** Pokud bude jakákoli část nabídky v jiném než povoleném jazyce, může si zadavatel vyžádat od dodavatele překlad (prostý překlad) do povoleného jazyka.

17.3 Podaná nabídka musí obsahovat veškeré dokumenty požadované zákonem a zadavatelem, včetně požadovaných dokladů a informací.

17.4 Veškeré části nabídky musí být dobře čitelné. Žádná část nabídky nesmí obsahovat opravy a přepisy, které by zadavatele mohly uvést v omyl.

18. FORMÁLNÍ POŽADAVKY NA ZPRACOVÁNÍ NABÍDKY

18.1 **Lhůta pro podání nabídek končí dne 28. 5. 2026 v 09:00 hod.**

18.2 Nabídku dodavatel zpracuje **písemně v elektronické podobě.**

18.3 **Podání nabídek v elektronické podobě:**

- Nabídka bude podána prostřednictvím elektronického nástroje E-ZAK dostupného na internetové adrese:

  https://mfcr.ezak.cz/profile_display_53.html.

- Veškeré části nabídky musí být dobře čitelné. Žádná část nabídky nesmí obsahovat opravy a přepisy, které by zadavatele mohly uvést v omyl.

- **Dodavatel je za účelem podání nabídky povinen se registrovat v elektronickém nástroji (respektive do jeho propojených databází „CDD“ a „FEN“).**

- ***Registrace dodavatele do elektronického nástroje:***

  - Další informace ohledně registrace do databáze FEN a ověření identity jsou dostupné na:

    https://sites.google.com/fen.cz/napovedafen/

    Před zahájením registrace dodavatele se ujistěte, že máte k dispozici:

    - doklad prokazující subjektivitu organizace (např. výpis z obchodního rejstříku nebo jiný relevantní dokument),
    - plnou moc k jednání jménem či za organizaci (v případě, kdy jste zároveň statutárním zástupcem nebo budete registraci provádět s využitím datové schránky, plnou moc nepotřebujete),
    - elektronický podpis založený na kvalifikovaném certifikátu (pro elektronický způsob ověření dodavatele).

    Pokud dodavatel nedisponuje odpovídající kvalitou elektronického podpisu, který je požadován v průběhu proces ověření identity, je možné ověřit identitu „Mimo systém“, což obnáší stažení odpovídající žádosti, která musí být

v listinné podobě podepsána a spolu s dalšími dokumenty zaslána poštou technickému provozovateli. Následujte instrukcí v uvedených manuálech.

- **Proces registrace dodavatele může trvat několik dnů.**

- Systémové požadavky na PC pro podání nabídek jsou k dispozici na internetové adrese:

https://ezak.cz/manualy/pozadavky-na-provoz-systemu-e-zak .

- Test nastavení prohlížeče a systému je možno provést na internetové adrese:

https://ezak.cz/manualy/test-nastaveni-prohlizece-a-testovaci-nabidka-manual .

- Podrobné instrukce elektronického nástroje se nacházejí v „uživatelské příručce“ na internetové adrese:

https://ezak.cz/manualy/pruvodce-podanim-nabidky-dodavatelem-v-e-zaku .

18.4 Zadavatel doporučuje níže uvedené řazení nabídky:

- Obsah nabídky;
- Krycí list nabídky včetně ČP k základní způsobilosti, ČP o střetu zájmů a ČP k aplikovaným sankcím (příloha č. 2 této ZD);
- Vyplněná příloha č. 3 této ZD („Stanovení nabídkové ceny“)
- Doklady prokazující splnění kvalifikace, a to v tomto řazení:
  - profesní způsobilost
  - technická kvalifikace (příloha č. 4 této ZD, včetně kopií příslušných certifikátů, kopie certifikátu ISO/IEC 27 001)
  - ekonomická kvalifikace;
- Seznam poddodavatelů (příloha č. 5 této ZD).

18.5 V případě, že zadavatel v rámci této ZD požaduje předložení dokumentů, které jsou zároveň jako povinná součást Návrhu smlouvy, postačí, když účastník do své nabídky tyto dokumenty předloží v 1 vyhotovení.

18.6 Za obsahovou úplnost nabídky odpovídá výhradně účastník – výčet dokumentů obsažený v tomto článku ZD slouží pouze pro usnadnění orientace účastníka při kompletaci nabídky – pokud v tomto výčtu nebude uveden dokument, povinnost, jehož doložení do nabídky by event. vyplývala ze zadávacích podmínek nebo ze zákona, nemůže se účastník zbavit odpovědnosti za obsahovou neúplnost nabídky poukazem na tento výčet dokumentů.

19. OTEVÍRÁNÍ NABÍDEK

Otevírání nabídek proběhne bez zbytečného odkladu po uplynutí lhůty pro podání nabídek, a to bez přítomnosti veřejnosti. Pokud o to účastník zadávacího řízení po skončení lhůty pro podání nabídek písemně požádá, zadavatel do 5 pracovních dnů od doručení této žádosti odešle všem účastníkům zadávacího řízení, nebo uveřejní na profilu zadavatele údaje z nabídek odpovídající číselně vyjádřitelným kritériím hodnocení, a to bez identifikačních údajů účastníků zadávacího řízení, dle § 109 odst. 3 zákona.

20. OSTATNÍ UJEDNÁNÍ

20.1 Zadavatel nehradí účastníkům náklady vzniklé z účasti v řízení.

20.2 Podáním nabídky účastník bere na vědomí, že zadavatel je jako povinný subjekt dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) povinen po uzavření smlouvy s vybraným dodavatelem tuto smlouvu uveřejnit v registru smluv. Uveřejnění smlouvy v registru smluv je obligatorní podmínkou účinnosti smlouvy. Zadavatel upozorňuje, že některá práva a povinnosti ze smlouvy, resp. s nimi související lhůty mohou být vázány na toto uveřejnění.

20.3 Po uzavření smlouvy s vybraným dodavatelem je zadavatel povinen ve smyslu ustanovení § 219 zákona zveřejnit na svém profilu zadavatele, resp. v registru smluv text uzavřené smlouvy s vybraným dodavatelem, včetně jejích případných změn a dodatků.

20.4 Zadavatel si vyhrazuje právo před rozhodnutím o výběru dodavatele ověřit, případně vyjasnit informace deklarované účastníky v nabídkách.

20.5 Nabídky ani jednotlivé součásti nabídek účastníků či vyloučených účastníků nebudou vráceny.

- **PŘÍLOHY**

  - Příloha č. 1 – Návrh smlouvy včetně příloh
  - Příloha č. 2 – Krycí list nabídky (včetně čestných prohlášení)
  - Příloha č. 3 – Stanovení nabídkové ceny
  - Příloha č. 4 – Seznam významných zakázek
  - Příloha č. 5 – Seznam poddodavatelů
  - Příloha č. 6 – Konfigurace systémů (neveřejná příloha)
  - Příloha č. 7 – Prohlášení o zachování mlčenlivosti

V Praze dne *dle elektronického podpisu*

Marek Šimandl
Digitálně podepsal Marek Šimandl
Datum: 2026.04.13 14:53:53 +02'00'

.....

Mgr. Marek Šimandl, MPA
generální ředitel
Státní tiskárna cenin, s. p

Č.j.: STC/018412/ÚSDS/2025
JID: R_STCSPS_0113359

SMLOUVA NA DODÁVKU, IMPLEMENTACI A PODPORU SYSTÉMU PRO SPRÁVU IDENTIT (IdM) A SYSTÉMU PRO ŘÍZENÍ PRIVILEGOVANÝCH ÚČTŮ (PAM)

evidovaná u objednatele pod č. 074/OS/2025
evidovaná u dodavatele pod č. **[zadavatel doplní před podpisem smlouvy a v souladu s Nabídkou evidenční číslo smlouvy u účastníka, pokud bude v Nabídce uvedeno]**

uzavřená v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ“),
a
v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „Autorský zákon“),
a
v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“)

(dále jen „**tato smlouva**“)

mezi:

Státní tiskárna cenin, s. p.
se sídlem Růžová 943/6, Nové Město, 110 00 Praha 1
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, oddíl ALX, vložka 296
IČO: 00001279
DIČ: CZ00001279
zastoupený: **Mgr. Markem Šimandlem, MPA, generálním ředitelem**
bankovní spojení: Česká národní banka
číslo účtu: 1602011/0710
(dále jen „**objednatel**“ nebo „**STC**“)

a

[zadavatel doplní identifikační údaje vybraného dodavatele dle nabídky]
se sídlem **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**
zapsaný v obchodním rejstříku vedeném **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**
zastoupený: **[zadavatel doplní jméno osoby oprávněné za vybraného dodavatele jednat; dle nabídky]**
IČO: **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**
DIČ: **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**
bank. spojení: **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**

číslo účtu: **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**
(dále jen „**dodavatel**")

(„objednatel" a „dodavatel" dále společně jen jako „**smluvní strany**")

Zmocněnci pro jednání smluvní a ekonomická:

za objednatele: **Mgr. Marek Šimandl, MPA,** generální ředitel

za dodavatele: **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**

Zmocněnci pro jednání věcná a technická:

za objednatele: **Jan Olexa,** vedoucí oddělení IT provoz
e-mail: olexa.jan@stc.cz, tel.: +420 732 176 752

za dodavatele: **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**

Článek I.

Úvodní ustanovení

1. Tato smlouva je uzavírána na základě výsledku otevřeného řízení dle ZZVZ na nadlimitní veřejnou zakázku s názvem *„Služby poskytování implementace a podpory IDM a PAM"* (dále jen **„Zadávací řízení"**), a to s dodavatelem, který splnil všechny zadávací podmínky, a jehož nabídka byla vybrána jako ekonomicky nejvýhodnější.
2. Dodavatel prohlašuje, že se seznámil se všemi podklady, které byly součástí zadávací dokumentace Zadávacího řízení, a které stanovují předmět této smlouvy, a že je odborně způsobilý ke splnění jeho závazků podle této smlouvy a v souladu se svou nabídkou na plnění veřejné zakázky ze dne **[zadavatel doplní datum podání nabídky účastníka]**, jejíž obsah je oběma smluvním stranám znám (dále jen jako „**Nabídka**").
3. Při výkladu obsahu této smlouvy jsou smluvní strany povinny přihlížet k zadávacím podmínkám a účelu veřejné zakázky. Ustanovení právních předpisů o výkladu právních jednání tím nejsou nijak dotčena.
4. Ve smyslu čl. VIII odst. 1 Statutu Státní tiskárny cenin, s. p. ze dne 19.12.2023, č.j.: MF-38643/2023/02-4, vyslovila dozorčí rada objednatele dne **[zadavatel doplní před podpisem smlouvy]** souhlas s uzavřením této smlouvy.

   [Před uzavřením smlouvy může zadavatel vypustit ustanovení v čl. I odst. 4 této smlouvy, pokud dle interních předpisů zadavatele k uzavření smlouvy nebude nutné získat souhlas dozorčí rady.]
5. Objednatel prohlašuje, že je povinnou osobou – poskytovatelem regulované služby v režimu vyšších povinností ve smyslu zákona č. 264/2025 Sb., o kybernetické bezpečnosti (ZoKB), zákona č. 266/2025 Sb., o kritické infrastruktuře a vyhlášky č. 409/2025 Sb., o bezpečnostních patřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „**Vyhláška**"). Dodavatel bere na vědomí, že jej objednatel ve smyslu § 9 Vyhlášky

bude identifikovat a evidovat jako významného dodavatele.

6. Definice odborných pojmů a zkratek obecně zaužívaných nebo stanovených pro plnění předmětu této smlouvy, které jsou používané v této smlouvě a jejích přílohách, jsou uvedeny v příloze č. 8, která je nedílnou součástí této smlouvy.

Článek II.

Účel a předmět smlouvy

1. Účelem této smlouvy je

   1.1. úprava vzájemných práv a povinností smluvních stran při zajištění dodání a provozování systému Identity Management – správy uživatelských účtů (dále jen „**IdM**“) a systému Privileged Access Management – systému pro řízení privilegovaných účtů (dále jen „**PAM**“) v prostředí objednatele zajišťující dlouhodobou koncepci řízení privilegovaných účtů, řízení identit a přístupových oprávnění;

   (IdM a PAM také společně jako „**systémy**“)

   1.2. implementace systémů umožňující centralizovanou, bezpečnou a efektivní správu identit (uživatelských účtů a přístupových práv), automatizace procesů spojených s přidělováním a odnímáním přístupů a monitorování aktivit privilegovaných uživatelů a

   1.3. dodání řešení, které bude možné provozovat jak prostřednictvím dodavatele, tak jiným externím subjektem nebo samotným objednatelem.

   Podrobnější popis konkrétních cílů je uveden v kapitole 1 bodě 1.2.1 přílohy č. 1a této smlouvy (Technická specifikace), která je nedílnou součástí této smlouvy.

2. Veškeré v této smlouvě a jejích přílohách uvedené požadavky na IdM a PAM a s nimi spojené služby musí být primárně vykládány tak, aby objednatel realizací předmětu této smlouvy dodavatelem dosáhl zde uvedeného účelu.

3. Předmětem této smlouvy je povinnost dodavatele dodat na svůj náklad a nebezpečí pro objednatele řádně a včas systémy IdM a PAM a tyto systémy implementovat do prostředí objednatele, zajistit jejich vzájemnou integraci a integraci s vybranými systémy objednatele a dodat příslušné licence k IdM a PAM, a tato dodávka a implementace bude v souladu s:

   3.1. požadavky objednatele uvedenými v příloze č. 1a této smlouvy (Technická specifikace) a v příloze č. 1b (Koncové systémy a počet uživatelů), které jsou nedílnou součástí této smlouvy;

   3.2. specifikací navrženého řešení dodavatele uvedenou v příloze č. 2a této smlouvy *(Návrh technického řešení dodavatele pro systém IdM*) a v příloze č. 2b této smlouvy *(Návrh technického řešení dodavatele pro systém PAM*) včetně položkových seznamů komponent, které dodavatel předložil v rámci své Nabídky a které jsou nedílnou součástí této smlouvy;

   3.3. licenčními podmínkami stanovenými v čl. VI odst. 10 a čl. VII této smlouvy;

   a pro tyto systémy pro objednatele zajišťovat technickou podporu a další služby v rozsahu stanoveném touto smlouvou.

4. Dodávka a implementace systémů IdM a PAM je rozdělena na

4.1. Etapu 1: Implementace IdM a jeho napojení na aktiva definovaná v Tabulce A bodu 1.1 přílohy č. 1b této smlouvy,

4.2. Etapu 2: Implementace PAM a jeho napojení na aktiva definovaná v Tabulce D bodu 1.4 přílohy č. 1b této smlouvy,

4.3. Etapu 3: Napojení dalších aktiv definovaných v Tabulce B bodu 1.2 přílohy č. 1b této smlouvy na IdM.

5. Součástí plnění dle této smlouvy jsou:

5.1. Činnosti (Fáze) pro jednotlivé Etapy:

Pro Etapu 1:

5.1.1. Provedení předimplementační analýzy v rozsahu dle podkapitoly 5.1 přílohy č. 1a této smlouvy; Výstupy z této části plnění podléhají akceptační proceduře obdobně dle čl. VI odst. 4 až 7 této smlouvy (dále také jako „**předimplementační analýza**“);

5.1.2. Implementace a integrace IdM v rozsahu dle podkapitoly 5.2 přílohy č. 1a této smlouvy v souladu s objednatelem akceptovanou předimplementační analýzou;

5.1.3. Předání dokumentace vztahující se k systému IdM v rozsahu dle podkapitoly 5.3 přílohy č. 1a této smlouvy;

5.1.4. Zajištění školení v rozsahu dle podkapitoly 5.4 přílohy č. 1a této smlouvy;

5.1.5. Poskytnutí nezbytných licencí k IdM v rozsahu dle čl. VI odst. 10 a čl. VII této smlouvy;

5.1.6. Testovací provoz v rozsahu dle podkapitoly 5.5 přílohy č. 1a této smlouvy a akceptační řízení dle čl. VI odst. 4 až 7 této smlouvy včetně akceptačních testů.

Jednotlivými testy v rámci akceptační procedury bude ověřeno, že dodávané plnění naplňuje v jednotlivých oblastech rozsah plnění stanovený touto smlouvou.
Provedení akceptační procedury je nezbytné k předání a převzetí celého systému IdM a souvisejícího plnění a uvedení IdM do produkčního provozu (Go-live).

Pro Etapu 2:

5.1.7. Aktualizace a doplnění předimplementační analýzy pro Etapu 2 v rozsahu dle podkapitoly 6.1 přílohy č. 1a této smlouvy;

5.1.8. Implementace a integrace PAM v rozsahu dle podkapitoly 6.2 přílohy č. 1a této smlouvy a s objednatelem akceptovanou předimplementační analýzou;

5.1.9. Předání dokumentace vztahující se k systému PAM v rozsahu dle podkapitoly 6.3 přílohy č. 1a této smlouvy;

5.1.10. Zajištění školení v rozsahu dle podkapitoly 6.4 přílohy č. 1a této smlouvy;

5.1.11. Dodání HW včetně poskytnutí záruky v rozsahu dle čl. IX této smlouvy; pokud bude součástí dodávaného řešení dodavatele dle přílohy č. 2b této

smlouvy;

5.1.12. Poskytnutí nezbytných licencí k PAM v rozsahu dle čl. VI odst. 10 a čl. VII této smlouvy;

5.1.13. Testovací provoz v rozsahu dle podkapitoly 6.5 přílohy č. 1a této smlouvy a akceptační řízení dle čl. VI odst. 4 až 7 této smlouvy včetně akceptačních testů.

Jednotlivými testy v rámci akceptační procedury bude ověřeno, že dodávané plnění naplňuje v jednotlivých oblastech rozsah plnění stanovený touto smlouvou.
Provedení akceptační procedury je nezbytné k předání a převzetí celého systému PAM a souvisejícího plnění a uvedení PAM do produkčního provozu (Go-live).

Pro Etapu 3:

5.1.14. Aktualizace a doplnění předimplementační analýzy pro Etapu 3 v rozsahu dle podkapitoly 7.1 přílohy č. 1a této smlouvy;

5.1.15. Integrace IdM na koncové systémy v rozsahu dle podkapitoly 7.2 přílohy č. 1a této smlouvy v souladu s objednatelem akceptovanou předimplementační analýzou;

5.1.16. Předání dokumentace v rozsahu dle podkapitoly 7.3 přílohy č. 1a této smlouvy;

5.1.17. Zajištění školení v rozsahu dle podkapitoly 7.4 přílohy č. 1a této smlouvy;

5.1.18. Testovací provoz v rozsahu dle podkapitoly 7.5 přílohy č. 1a této smlouvy a akceptační řízení dle čl. VI odst. 4 až 7 této smlouvy včetně akceptačních testů.

Jednotlivými testy v rámci akceptační procedury bude ověřeno, že dodávané plnění naplňuje v jednotlivých oblastech rozsah plnění stanovený touto smlouvou.
Provedení akceptační procedury je nezbytné k předání a převzetí předmětného plnění a uvedení do produkčního provozu (Go-live).

5.2. Poskytování technické podpory pro systém IdM a PAM spočívající v zajišťování Monitoringu (servisní podpora v režimu 24/7 u systému PAM a 8x5 u systému IdM, včetně garance SLA), možnosti neomezeného řešení incidentů (Incident Management), provádění servisních zásahů, služby podpory produktů (maintenance) a konzultací, a to v rozsahu dle podkapitoly 7.6 přílohy č. 1a této smlouvy pro systém IdM a podkapitoly 7.7 přílohy č. 1a této smlouvy pro systém PAM a v souladu s požadavky na provoz řešení a SLA stanovenými v příloze č. 5 této smlouvy, která tvoří nedílnou součást této smlouvy.

(dále také jako „**Služby podpory**“)

5.2.1. Dodavatel je povinen ke konci každého kalendářního měsíce předložit zmocněnci objednatele pro jednání věcná a technická ke schválení protokol vymezující, zda byly Služby podpory poskytnuty v daném kalendářním měsíci v plném rozsahu dle této smlouvy nebo v jaké poměrné části, tj. po dobu kolika dnů v daném kalendářním měsíci (dále jen „**Protokol o poskytnutí Služeb podpory**"). Nedílnou součástí Protokolu o poskytnutí Služeb podpory bude rovněž reporting plnění SLA ve smyslu a rozsahu dle přílohy č. 5 této smlouvy. Protokol o poskytnutí Služeb podpory bude dodavatelem zasílán elektronicky k odsouhlasení na e-mailovou adresu **[zadavatel doplní před podpisem smlouvy]**.

5.2.2. Zmocněnec objednatele pro jednání věcná a technická odsouhlasí, popř. odsouhlasí s výhradami, kvalitu a rozsah poskytnutých Služeb podpory do 5 pracovních dnů od doručení Protokolu o poskytnutí Služeb podpory, a to elektronicky na e-mailovou adresu dodavatele **[zadavatel doplní údaje dle Nabídky]**. V případě, že má objednatel výhrady ke kvalitě či rozsahu poskytnutých Služeb podpory a uvede je v Protokolu o poskytnutí Služeb podpory a dohodne se s dodavatelem na nápravě vad, je dodavatel povinen zjednat nápravu cestou odstranění vad ve lhůtě 3 pracovních dnů od oznámení takových výhrad objednatelem, pokud se smluvní strany nedohodnou jinak. Protokol o poskytnutí Služeb podpory bude podepsán zmocněnci obou smluvních stran pro jednání věcná a technická a vyhotoven ve dvou stejnopisech, z nichž každá ze smluvních stran obdrží po jednom, nebo v elektronické podobě při jeho elektronickém podepsání.

5.3. Služby na vyžádání na provedení úprav dodaných systémů IdM a PAM a jejich rozvoj, provedení dalších rozvojových integrací systémů IdM a další nezbytné činnosti (dále jen **„ad hoc služby“**) v rozsahu dle podkapitoly 7.8 přílohy č. 1a této smlouvy.

5.3.1. Objednatel je oprávněn požadovat ad hoc služby v maximálním celkovém rozsahu 1000 člověkodnů (dále jen „**MD**“) za dobu trvání této smlouvy, a to na základě objednávky objednatele za podmínek stanovených touto smlouvou. Poskytování ad hoc služeb závisí pouze na uvážení a potřebách objednatele a bez uzavření příslušné dílčí smlouvy nevzniká na poskytování tohoto plnění právní nárok ani nárok na úhradu ceny za ně. U každé z ad hoc služeb bude před jejich realizací proveden dodavatelem odhad pracnosti těchto služeb v MD, který objednatel odsouhlasí.

5.3.2. Veškeré ad hoc služby budou realizovány na základě písemných objednávek, které jsou návrhem na uzavření dílčí smlouvy (dále jen „**objednávka**“), a potvrzení těchto objednávek, jež jsou přijetím návrhu na uzavření jednotlivé dílčí smlouvy (výše a dále jen „**dílčí smlouva**“). Dílčí smlouva je uzavřena okamžikem, kdy objednatel obdrží potvrzení objednávky od dodavatele, které potvrzuje objednávku bez výhrad.

5.3.3. Objednávka bude obsahovat minimálně tyto náležitosti:

a) identifikační údaje objednatele a dodavatele;

b) vymezení plnění a jeho podrobnou specifikaci včetně formy výstupu, požadovaný dílčí termín plnění těchto ad hoc služeb a maximální rozsah těchto služeb v člověkohodinách a MD; a

c) označení osoby vystavující objednávku, jež je oprávněna jednat jménem objednatele.

5.3.4. V případě pochybností je dodavatel povinen vyžádat si od objednatele doplňující informace. Neučiní-li tak, má se za to, že pokyny jsou pro něho dostačující a nemůže se z tohoto důvodu zprostit odpovědnosti za nesplnění či vadné splnění.

5.3.5. Objednávka bude objednatelem zasílána dodavateli na e-mailovou adresu dodavatele **[zadavatel doplní údaje dle Nabídky]**.

5.3.6. Dodavatel je povinen objednateli obratem písemně potvrdit přijetí této objednávky na e-mailovou adresu objednatele, ze která byla objednávka odeslána, nejpozději však ve lhůtě 5 pracovních dnů od jejího obdržení, jinak odpovídá objednateli za veškerou škodu vzniklou nepotvrzením této objednávky. Potvrzení objednávky musí obsahovat minimálně identifikaci objednatele, dodavatele a identifikaci objednávky, která je potvrzována.

5.3.7. Jednotlivé dílčí smlouvy podléhající povinnosti uveřejnění v registru smluv nabývají účinnosti dnem jejich uveřejnění v registru smluv; zveřejnění v registru smluv zajistí objednatel. Ostatní dílčí smlouvy nepodléhající povinnosti uveřejnění v registru smluv nabývají účinnosti dnem jejich potvrzení dodavatelem.

5.3.8. Dodavatel je povinen ke konci kalendářního čtvrtletí, ve kterém byly poskytovány ad hoc služby, předložit zmocněnci objednatele pro jednání věcná a technická ke schválení čtvrtletní výkaz vyúčtovaných hodin, který bude dodavatelem zasílán elektronicky k odsouhlasení na e-mailovou adresu **[zadavatel doplní před podpisem smlouvy]** a ve kterém bude uveden počet hodin poskytnutých ad hoc služeb v daném kalendářním čtvrtletí s tím, že lze vykázat počet hodin s přesností na 2 desetinná čísla. Objednatel je povinen odsouhlasit dodavateli výkaz vyúčtovaných hodin nebo uplatnit výhrady k poskytnutým ad hoc službám nebo k obsahu výkazu vyúčtovaných hodin do 5 pracovních dní od jeho obdržení na e-mailovou adresu dodavatele **[zadavatel doplní údaje dle Nabídky]**. V případě, že má objednatel výhrady ke kvalitě či rozsahu poskytnutých ad hoc služeb a uplatní je u dodavatele dle předchozí věty, je dodavatel povinen zjednat nápravu cestou odstranění vad ve lhůtě 3 pracovních dnů od oznámení takových výhrad objednatelem, pokud se smluvní strany nedohodnou jinak. Čtvrtletní výkaz vyúčtovaných hodin je odsouhlasen a podepsán zmocněnci pro jednání věcná a technická obou smluvních stran a vyhotoven ve dvou stejnopisech, z nichž každá ze smluvních stran obdrží po jednom, nebo v elektronické podobě při jeho elektronickém podepsání. Výkaz vyúčtovaných hodin za každé kalendářní čtvrtletí bude přílohou faktury za ad hoc služby za každé uplynulé kalendářní čtvrtletí.

5.3.9. Provedení ad hoc služeb, resp. vytvořené výstupy podléhají akceptační proceduře obdobně dle čl. VI odst. 4 až 7 této smlouvy.

5.4. Vypracování Exit plánu a poskytnutí služeb Exitu v rozsahu a za podmínek dle podkapitoly 4.2 přílohy č. 1a této smlouvy; Výstupy z fáze vypracování Exit plánu podléhají akceptační proceduře obdobně dle čl. VI odst. 4 až 7 této smlouvy.

(dále také jako „**služby Exitu**“).

6. Dodavatel se zavazuje provést plnění dle této smlouvy v souladu se všemi platnými právními předpisy, jakož i se všemi relevantními normami obsahujícími technické specifikace a technická řešení, technologické postupy nebo jiná určující kritéria k zajištění souladu plnění s požadavky objednatele a podmínkami a požadavky uvedenými v zadávací dokumentaci Zadávacího řízení.
7. Část plnění dle této smlouvy, konkrétně plnění Etapy 1 až 3 má povahu díla ve smyslu ustanovení § 2586 a násl. OZ, která se na plnění dle této smlouvy uplatní, ledaže je v této smlouvě sjednáno jinak. Smluvní strany se dohodly, že dodavateli nevzniká právo na odstoupení dle ustanovení § 2591 a § 2595 OZ. Dále se nepoužije ustanovení § 2611 a § 2610 OZ z důvodu vlastní úpravy smluvními stranami v této smlouvě.
8. Předmětem této smlouvy je dále závazek objednatele převzít řádně a včas dodané plnění a zaplatit celkovou cenu za podmínek stanovených dále v této smlouvě a závazek objednatele hradit za dodávku systémů, poskytnuté licence, Služby podpory, služby Exitu a za ad hoc služby dodavateli cenu specifikovanou v čl. IV této smlouvy.
9. Objednatel si ve smyslu § 100 odst. 1 ZZVZ vyhrazuje právo na uplatnění vyhrazené změny závazku zajišťující splnění požadavků ZoKB a Vyhlášky na řízení dodavatelů souvisejících s předmětem plnění veřejné zakázky a touto smlouvou. Podrobnosti o této vyhrazené změně závazku jsou uvedeny v odst. 10 tohoto článku. Pro vyloučení jakýchkoliv pochybností smluvní strany uvádějí, že objednatel je oprávněn, nikoli však povinen, uplatnit vyhrazenou změnu závazku dle tohoto odstavce. Dodavatel je povinen vyhovět této změně, pokud je v souladu s podmínkami této smlouvy.
10. Smluvní strany vědomy si postavení objednatele jako povinné osoby – poskytovatele regulované služby v režimu vyšších povinností ve smyslu ZoKB a Vyhlášky, se zavazují upravit rozsah plnění dodavatele, resp. práva a povinnosti smluvních stran tak, aby odpovídal požadavkům ZoKB a Vyhlášky, zejména doplnění pravidel zohledňujících požadavky systému řízení bezpečnosti informací dle ZoKB a doplnění relevantních ustanovení uvedených v příloze č. 5 Vyhlášky. Objednatel oznámí dodavateli své rozhodnutí uplatnit vyhrazenou změnu závazku podle předchozího odstavce tohoto článku písemným oznámením doručeným dodavateli kdykoliv v době trvání této smlouvy dle čl. XIV odst. 2 této smlouvy. Doplnění požadavků, resp. úprava práv a povinností smluvních stran bude realizována formou dodatku k této smlouvě dle čl. XV odst. 1 této smlouvy.

Článek III.
Doba a místo plnění

1. Dodavatel se zavazuje kompletní plnění dle této smlouvy (s výjimkou poskytování Služeb podpory, Maintenance a zadaných ad hoc služeb), tj. Dodávku systémů IdM a PAM a napojení dalších aktiv na systém IdM, resp. Etapy 1, 2 a 3, provést ve lhůtách dle **Harmonogramu uvedeného v příloze č. 3** (výše a dále jen „**Harmonogram**“), která je nedílnou součástí této smlouvy.
2. Smluvní strany se dohodly, že Harmonogram bude s ohledem na dílčí charakter plnění doplněn a upřesněn v předimplementační analýze, přičemž ze strany dodavatele není možné měnit termíny určené ze strany objednatele.

3. Neurčí-li tato smlouva, Harmonogram nebo předimplementační analýza konkrétní lhůtu plnění, má se za to, že je dodavatel povinen plnit bez zbytečného odkladu nejpozději ve lhůtě do 10 pracovních dnů.
4. Poskytování Služeb podpory dle čl. II odst. 5 bod 5.2 této smlouvy bude dodavatelem zahájeno v okamžiku přechodu do produkčního provozu jednotlivých systémů (go-live), tj. dnem podpisu Akceptačního protokolu Etapy 1 u Služeb podpory pro systém IdM, dnem podpisu Akceptačního protokolu Etapy 2 u Služeb podpory pro systém PAM a dnem podpisu Akceptačního protokolu Etapy 3 u Služeb podpory pro systém IdM po provedení Etapy 3. Služby podpory dle čl. II odst. 5 bod 5.2 této smlouvy budou poskytovány po dobu 48 měsíců od podpisu Akceptačního protokolu Etapy 2 nebo Etapy 3 podle toho, která akceptace, přechod do produkčního provozu, nastane později.
5. Ad hoc služby budou poskytovány v termínech dle konkrétní dílčí smlouvy.
6. Místem plnění je sídlo objednatele a výrobní závody objednatele:
   - **Výrobní závod I – na adrese: Růžová 943/6, Nové Město, 110 00 Praha 1;**
   - **Výrobní závod II – na adrese: Za Viaduktem 8, 170 00 Praha 7;**

   pokud z povahy konkrétní činnosti nutné k plnění této smlouvy nevyplývá něco jiného (např. vzdálený přístup k systému prostřednictvím VPN),

   a to vždy v souladu s Technickou specifikací uvedenou v příloze č. 1 této smlouvy a Návrhem technického řešení uvedeným v příloze č. 2 této smlouvy.

   (případně dále jako **„místo plnění“**)

Článek IV.

Cena

1. Cena dodávky systému IdM, tj. činností Etapy 1 (dále jen „**celková cena IdM**“) je stanovena podle Nabídky dodavatele, a činí:

   [zadavatel doplní cenu dle Nabídky] Kč

   (slovy: [zadavatel doplní cenu dle Nabídky slovy]) bez DPH.
2. Cena dodávky systému PAM, tj. činností Etapy 2 (dále jen „**celková cena PAM**“) je stanovena podle Nabídky dodavatele, a činí:

   [zadavatel doplní cenu dle Nabídky] Kč

   (slovy: [zadavatel doplní cenu dle Nabídky slovy]) bez DPH.
3. Cena napojení IdM, tj. činností Etapy 3 (dále jen „**celková cena Napojení**“) je stanovena podle Nabídky dodavatele, a činí:

   [zadavatel doplní cenu dle Nabídky] Kč

   (slovy: [zadavatel doplní cenu dle Nabídky slovy]) bez DPH.
4. Cena za subskripci licencí pro systém IdM činí pololetní paušální částku **[zadavatel doplní pololetní paušální cenu dle Nabídky] Kč** (slovy: **[zadavatel doplní pololetní paušální cenu slovy]** korun českých)**.** Pokud bude subskripce licencí poskytována pouze po určitou část kalendářního roku, např. z důvodu konce platnosti této smlouvy, bude tato částka přiměřeně krácena tak, že za každý započatý kalendářní měsíc náleží dodavateli odměna (cena) ve výši **[zadavatel doplní cenu ve výši 1/6 ceny dle Nabídky]** Kč bez DPH.

5. Cena za subskripci licencí pro systém PAM činí pololetní paušální částku **[zadavatel doplní pololetní paušální cenu dle Nabídky] Kč** (slovy: **[zadavatel doplní pololetní paušální cenu slovy]** korun českých)**.** Pokud bude subskripce licencí poskytována pouze po určitou část kalendářního roku, např. z důvodu konce platnosti této smlouvy, bude tato částka přiměřeně krácena tak, že za každý započatý kalendářní měsíc náleží dodavateli odměna (cena) ve výši **[zadavatel doplní cenu ve výši 1/6 ceny dle Nabídky]** Kč bez DPH.

6. Podrobný rozpad celkové ceny IdM, celkové ceny PAM, celkové ceny Napojení a licenční metriky pro systémy IdM a PAM je uveden v příloze č. 4 této smlouvy, která je nedílnou součástí této smlouvy.

   [Před uzavřením smlouvy může zadavatel vypustit ustanovení čl. IV odst. 4 a/nebo odst. 5, upravit čl. IV odst. 6 této smlouvy a upravit číslování tohoto článku a odkazy na tento článek, pokud dodavatelův licenční plán nebude obsahovat subskripční licence.]

7. Cena Služeb podpory IdM dle čl. II odst. 5 bod 5.2 této smlouvy po dobu od zahájení produkčního provozu (Go-live) Etapy 1 až po zahájení produkčního provozu (Go-live) Etapy 3 činí měsíční paušální částku **[zadavatel doplní měsíční paušální cenu dle Nabídky] Kč** (slovy: **[zadavatel doplní měsíční paušální cenu slovy]** korun českých)**.** V případě, že Služby podpory IdM nebyly poskytovány v plném rozsahu, bude výše ceny za daný měsíc snížena poměrně dle počtu dnů, po které nebyly Služby podpory IdM poskytovány. To nevylučuje aplikaci čl. XI odst. 5 této smlouvy.

8. Cena Služeb podpory IdM dle čl. II odst. 5 bod 5.2 této smlouvy od zahájení produkčního provozu Etapy 3 činí měsíční paušální částku **[zadavatel doplní měsíční paušální cenu dle Nabídky] Kč** (slovy: **[zadavatel doplní měsíční paušální cenu slovy]** korun českých)**.** V případě, že Služby podpory IdM nebyly poskytovány v plném rozsahu, bude výše ceny za daný měsíc snížena poměrně dle počtu dnů, po které nebyly Služby podpory IdM poskytovány. To nevylučuje aplikaci čl. XI odst. 5 této smlouvy.

9. Cena Služeb podpory PAM dle čl. II odst. 5 bod 5.2 této smlouvy činí měsíční paušální částku **[zadavatel doplní měsíční paušální cenu dle Nabídky] Kč** (slovy: **[zadavatel doplní měsíční paušální cenu slovy]** korun českých)**.** V případě, že Služby podpory PAM nebyly poskytovány v plném rozsahu, bude výše ceny za daný měsíc snížena poměrně dle počtu dnů, po které nebyly Služby podpory PAM poskytovány. To nevylučuje aplikaci čl. XI odst. 5 této smlouvy.

10. **Sazba za jeden MD poskytování ad hoc služeb** dle čl. II odst. 5 bod 5.3 této smlouvy je stanovena v souladu s Nabídkou a činí částku bez DPH ve výši:

    [zadavatel doplní cenu dle Nabídky] Kč
    (slovy: [zadavatel doplní cenu dle Nabídky slovy]).

11. Celkové ceny i paušální ceny dle tohoto článku a sazba za člověkohodinu dle odst. 10 tohoto článku jsou cenami maximálními, nejvýše přípustnými, které není přípustné změnit a které obsahují veškeré náklady na plnění předmětu této smlouvy dodavatelem dle čl. II této smlouvy, s tím že:

    11.1. součástí ceny jsou i náklady na dodávky a služby, které v zadávací dokumentaci veřejné zakázky, Nabídce ani v této smlouvě a jejích přílohách nejsou

výslovně uvedeny, ale dodavatel jakožto odborník ví nebo má vědět, že jsou nezbytné pro řádné a včasné provedení plnění;

11.2. ceny obsahují i případné správní a místní poplatky, vedlejší náklady, náklady spojené s dopravou do místa plnění včetně nákladů souvisejících s celními poplatky a s provedením všech zkoušek a testů;

11.3. cena za případnou dodávku HW v rámci Etapy 2 je součástí celkové ceny PAM, tj. ceny Etapy 2, a to včetně nákladů na poskytnutí záruky v rozsahu dle čl. IX této smlouvy;

11.4. cena za licence Softwaru a/nebo Standardního Softwaru (testovací, vývojářské aj.), které jsou nezbytné pro provádění implementace systémů IdM nebo PAM je zahrnuta v celkové ceně IdM a PAM, resp. Etapy 1 nebo 2;

11.5. cena za perpetuální licence Softwaru a/nebo Standardního Softwaru dodavatele nebo výrobců třetích stran je zahrnuta v celkové ceně IdM nebo PAM, resp. Etapy 1 nebo 2 s výjimkou ceny licencí externí notifikační služby (např. SMTP, SMS brána) a software/platformy objednatele uvedené v podkapitole 4.1 Přílohy č. 1a této smlouvy, které nejsou součástí dodávky;

11.6. náklady na využití FOSS licence v rámci plnění dle této smlouvy jsou zahrnuty v celkové ceně IdM nebo PAM, resp. Etapy 1 nebo 2.

11.7. součástí ceny za předmět plnění jsou i případné náklady dodavatele na implementaci opatření vyplývajících z uplatnění vyhrazené změny závazku dle čl. II odst. 9 této smlouvy.

[Před uzavřením smlouvy může zadavatel upravit čl. IV odst. 11 této smlouvy, tj. vypustit bod 11.5 a/nebo 11.6 tohoto odstavce a upravit číslování tohoto odstavce, pokud dodavatelova licenční metrika nebude obsahovat perpetuální licence nebo FOSS licence.]

12. DPH bude účtována podle právních předpisů platných a účinných v době uskutečnění zdanitelného plnění.

Článek V.
Platební podmínky

1. **Celkovou cenu IdM podle čl. IV odst. 1 této smlouvy** objednatel uhradí dodavateli bankovním převodem následovně:

1.1. zálohovou platbu ve výši 30 % z celkové ceny podle čl. IV odst. 1 této smlouvy, tj. ve výši **[zadavatel doplní 30 % z celkové ceny podle čl. IV odst. 1 této smlouvy]** Kč navýšenou o DPH po podpisu Akceptačního protokolu dle čl. VI odst. 4 výstupu z předimplementační analýzy dle čl. II odst. 5 bod 5.1.1 této smlouvy bez vad a nedodělků.

Právo vystavit zálohovou fakturu na platbu dle bodu 1.1 tohoto odstavce vzniká dodavateli následující pracovní den po podpisu Akceptačního protokolu dle čl. VI odst. 4 výstupu z předimplementační analýzy dle čl. II odst. 5 bod 5.1.1 této smlouvy bez vad a nedodělků. Přílohou zálohové faktury bude kopie podepsaného příslušného Akceptačního protokolu. Splatnost uvedené části ceny je 30 dní ode dne vystavení

zálohové faktury. Dodavatel je po obdržení zálohové platby povinen zaslat objednateli nejpozději do 5 dnů od připsání platby na účet dodavatele daňový doklad na přijatou úhradu.

1.2. platbu ve výši 70 % z celkové ceny podle čl. IV odst. 1 této smlouvy, tj. ve výši **[zadavatel doplní 70 % z celkové ceny podle čl. IV odst. 1 této smlouvy]** Kč navýšenou o DPH po podpisu Akceptačního protokolu dle čl. VI odst. 4 dokládající akceptaci/přechod do produkčního provozu (Go-live) Etapy 1.

Právo vystavit konečnou fakturu (daňový doklad) vzniká dodavateli následující pracovní den po podpisu Akceptačního protokolu dle čl. VI odst. 4 dokládající akceptaci/přechod do produkčního provozu (Go-live) Etapy 1. Dodavatel vystaví a zašle objednateli konečnou fakturu (daňový doklad) do 5 pracovních dnů od vzniku práva na její vystavení. Přílohou této faktury (daňového dokladu) bude kopie podepsaného příslušného Akceptačního protokolu. Prostřednictvím této konečné faktury (daňového dokladu) bude započtena zálohová platba ve výši 30 % ceny uhrazená dle bodu 1.1 tohoto odstavce; splatnost uvedené části ceny dle tohoto písmene tohoto odstavce je 30 dní od vystavení konečné faktury (daňového dokladu).

2. **Celkovou cenu PAM podle čl. IV odst. 2 této smlouvy** objednatel uhradí dodavateli bankovním převodem následovně:

2.1. platbu ve výši 90 % z celkové ceny podle čl. IV odst. 2 této smlouvy, tj. ve výši **[zadavatel doplní 90 % z celkové ceny podle čl. IV odst. 2 této smlouvy]** Kč navýšenou o DPH po podpisu Akceptačního protokolu dle čl. VI odst. 4 dokládající akceptaci/přechod do produkčního provozu (Go-live) Etapy 2.

Právo vystavit konečnou fakturu (daňový doklad) na celkovou cenu podle čl. IV odst. 2 této smlouvy vzniká dodavateli následující pracovní den po podpisu Akceptačního protokolu dle čl. VI odst. 4 dokládající akceptaci/přechod do produkčního provozu (Go-live) Etapy 2. Dodavatel vystaví a zašle objednateli konečnou fakturu (daňový doklad) do 5 pracovních dnů od vzniku práva na její vystavení. Přílohou této faktury (daňového dokladu) bude kopie podepsaného příslušného Akceptačního protokolu. Splatnost uvedené části ceny dle tohoto písmene tohoto odstavce je 30 dní od vystavení konečné faktury (daňového dokladu).

2.2. platbu ve výši 10 % z celkové ceny podle čl. IV odst. 2 této smlouvy, tj. ve výši **[zadavatel doplní 10 % z celkové ceny podle čl. IV odst. 2 této smlouvy]** Kč navýšenou o DPH po podpisu Akceptačního protokolu dle čl. VI odst. 4 dokládající předání EXIT Plánu dle č. II odst. 5 bodu 5.5 této smlouvy. Přílohou konečné faktury (daňového dokladu) dle bodu 2.1 tohoto odstavce bude kopie příslušného Akceptačního protokolu. Splatnost uvedené části celkové ceny dle tohoto písmene tohoto odstavce je 30 dní od podpisu příslušného Akceptačního protokolu.

3. **Celkovou cenu Napojení podle čl. IV odst. 3 této smlouvy** objednatel uhradí dodavateli bankovním převodem po podpisu Akceptačního protokolu dle čl. VI odst. 4 dokládající akceptaci/přechod do produkčního provozu (Go-live) Etapy 3.

Právo vystavit konečnou fakturu (daňový doklad) vzniká dodavateli následující pracovní den po podpisu Akceptačního protokolu dle čl. VI odst. 4 dokládající akceptaci/přechod do produkčního provozu (Go-live) Etapy 3. Dodavatel vystaví a zašle objednateli konečnou fakturu (daňový doklad) do 5 pracovních dnů od vzniku práva na její vystavení. Přílohou této faktury (daňového dokladu) bude kopie podepsaného příslušného Akceptačního

protokolu. Splatnost ceny dle tohoto písmene tohoto odstavce je 30 dní od vystavení konečné faktury (daňového dokladu).

4. Cena za subskripci licencí pro systémy dle čl. IV odst. 4 a/nebo 5 této smlouvy, resp. dle rozpadu cen za subskripce licencí uvedené v příloze č. 4 této smlouvy bude hrazena **pololetně ode dne dodání licencí, tedy od podpisu příslušného Akceptačního protokolu ve smyslu čl. VI odst. 4 této smlouvy dokládající akceptaci/přechod do produkčního provozu (Go-live) Etapy 1/Etapy 2.** Právo vystavit daňový doklad (fakturu) na pololetní paušální částku podle čl. IV odst.4 a/nebo 5 této smlouvy, resp. dle rozpadu cen za subskripce licencí uvedené v Příloze č. 4 této smlouvy, vzniká dodavateli poprvé dnem podpisu příslušného Akceptačního protokolu ve smyslu čl. VI odst. 4 této smlouvy na období následujících 6 měsíců a dále pak ve dny výročí. Za den výročí platby se považuje den v kalendáři odpovídající dni podpisu Akceptačního protokolu ve smyslu čl. VI odst. 4 této smlouvy; tento den se opakuje v šestiměsíčních intervalech a je rozhodný pro splatnost každé platby ceny za subskripci licencí. Pokud takový den v příslušném měsíci neexistuje, připadá výročí na poslední kalendářní den daného měsíce. Splatnost pololetní paušální částky je 30 dní ode dne vystavení daňového dokladu (faktury). Datem uskutečnění zdanitelného plnění je den podpisu příslušného Akceptačního protokolu, resp. den výročí pro následující pololetní poskytování předmětu plnění.

   [Před uzavřením smlouvy může zadavatel vypustit ustanovení čl. V odst. 4 a upravit číslování tohoto článku a odkazy na tento článek, pokud dodavatelův licenční plán nebude obsahovat subskripční licence.]

5. Cena za Služby podpory **dle čl. IV odst. 7, 8 a/nebo 9 této smlouvy** bude hrazena **měsíčně zpětně** za předpokladu, že byly Služby podpory poskytovány v tomto období v plném rozsahu dle této smlouvy, o čemž bude smluvními stranami za každý kalendářní měsíc vyhotoven Protokol o poskytnutí Služeb podpory. Tento Protokol o poskytnutí Služeb podpory bude přílohou daňového dokladu (faktury) za Služby podpory poskytnuté za uplynulý kalendářní měsíc. V případě, že Služby podpory nebyly poskytovány v plném rozsahu, bude výše ceny za daný měsíc snížena poměrně dle počtu dnů, po které byly Služby podpory poskytovány. Datum uskutečnění zdanitelného plnění za Služby podpory je poslední den daného kalendářního měsíce, ve kterém byly Služby podpory poskytovány. Dodavateli vzniká právo vystavit daňový doklad (fakturu) do 15. kalendářního dne ode dne konce daného kalendářního měsíce, ve kterém byly Služby podpory poskytovány.

6. **Cena za ad hoc služby je stanovena jako součin skutečně poskytnutých ad hoc služeb a hodinové sazby dle čl. IV odst. 10 této smlouvy a bude hrazena kvartálně zpětně po poskytnutí ad hoc služeb.** Datum uskutečnění zdanitelného plnění za ad hoc služby je poslední den kalendářního čtvrtletí, ve kterém byly ad hoc služby poskytnuty. Dodavateli vzniká právo vystavit daňový doklad (fakturu) do 15. kalendářního dne od posledního dne daného kalendářního čtvrtletí, ve kterém byly ad hoc služby poskytnuty. Přílohou faktury za ad hoc služby za uplynulé kalendářní čtvrtletí bude Výkaz vyúčtovaných hodin odsouhlasený objednatelem.

7. Daňový doklad (faktura) bude obsahovat náležitosti daňového dokladu podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, OZ a podle této smlouvy. Současně bude daňový doklad (faktura) obsahovat číslo evidenční objednávky objednatele, které objednatel dodavateli sdělí po podpisu této smlouvy.

8. Dodavatel je povinen doručit daňový doklad (fakturu) objednateli na e-mailovou adresu

podatelna@stc.cz. Zaplacením se pro účely této smlouvy rozumí den připsání příslušné částky na účet dodavatele uvedený na titulní straně této smlouvy.

9. V případě, že daňový doklad (faktura) vystavený dodavatelem nebude obsahovat potřebné náležitosti nebo bude obsahovat nesprávné či neúplné údaje, je objednatel oprávněn daňový doklad (fakturu) vrátit dodavateli s uvedením důvodu vrácení, aniž se dostane do prodlení s placením. Nová lhůta splatnosti počíná běžet ode dne doručení řádně opraveného či doplněného daňového dokladu (faktury) objednateli.
10. Dodavatel není oprávněn bez písemného souhlasu objednatele provádět jakékoli zápočty svých pohledávek vůči objednateli proti jakýmkoli pohledávkám objednatele vůči dodavateli.
11. Dodavatel není oprávněn postoupit pohledávky za objednatelem z této smlouvy nebo v souvislosti s ní.
12. Dodavatel se zavazuje, že žádným způsobem nezatíží své pohledávky za objednatelem z této smlouvy nebo v souvislosti s ní zástavním právem ve prospěch třetí osoby.
13. V případě, že je dodavatel plátcem DPH registrovaným v České republice, uplatní se a jsou pro něj závazná ujednání následujících odstavců tohoto článku (odst. 14 až 17 tohoto článku).
14. Dodavatel prohlašuje, že ke dni uzavření této smlouvy není v likvidaci a není vůči němu vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů. Dodavatel prohlašuje, že ke dni uzavření této smlouvy správce daně nerozhodl, že dodavatel je nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty (dále jen „ZDPH“). Dodavatel je povinen neprodleně, nejpozději do 2 pracovních dnů od zjištění skutečnosti dle první věty tohoto odstavce nebo od vydání rozhodnutí správce daně, že je dodavatel nespolehlivým plátcem dle § 106a ZDPH, oznámit takovou skutečnost prokazatelně objednateli, příjemci zdanitelného plnění. V případě, že se po dobu platnosti a účinnosti této smlouvy prohlášení dodavatele uvedená v tomto odstavci ukážou jako nepravdivá, nebo dodavatel poruší povinnost oznámit objednateli skutečnost uvedenou v předchozí větě ve stanovené lhůtě, bude to smluvními stranami považováno za podstatné porušení této smlouvy.
15. Dodavatel se zavazuje, že bankovní účet jím určený pro zaplacení jakéhokoliv závazku objednatele na základě této smlouvy bude od data podpisu této smlouvy do ukončení její platnosti zveřejněn způsobem umožňujícím dálkový přístup ve smyslu § 98 ZDPH, v opačném případě je dodavatel povinen sdělit objednateli jiný bankovní účet řádně zveřejněný ve smyslu § 98 ZDPH. Pokud bude dodavatel označen správcem daně za nespolehlivého plátce ve smyslu § 106a ZDPH, zavazuje se zároveň o této skutečnosti neprodleně, nejpozději do 2 pracovních dnů od zjištění skutečnosti dle první věty tohoto odstavce nebo od vydání rozhodnutí správce daně, informovat objednatele spolu s uvedením data, kdy tato skutečnost nastala.
16. Pokud objednateli vznikne podle § 109 ZDPH ručení za nezaplacenou DPH z přijatého zdanitelného plnění od dodavatele, nebo se objednatel důvodně domnívá, že tyto skutečnosti nastaly nebo mohly nastat, má objednatel právo bez souhlasu dodavatele uplatnit postup zvláštního zajištění daně, tzn., že je objednatel oprávněn odvést částku DPH podle faktury – daňového dokladu vystavené dodavatelem přímo příslušnému finančnímu úřadu, a to v návaznosti na § 109 a § 109a ZDPH.

17. Úhradou DPH na účet finančního úřadu se pohledávka dodavatele vůči objednateli v částce uhrazené DPH považuje bez ohledu na další ustanovení této smlouvy za uhrazenou. Zároveň je objednatel povinen dodavatele o takové úhradě bezprostředně po jejím uskutečnění písemně informovat.

Článek VI.

Akceptace plnění

1. Dodavatel umožní objednateli kontrolovat průběh provádění plnění a za tím účelem poskytne objednateli potřebnou součinnost.
2. Provedení dílčích činností (Fází) Etapy 1, 2 a 3 předmětu plnění ve smyslu čl. II odst. 5 této smlouvy bude ze strany objednatele akceptováno dle akceptačních milníků stanovených v Harmonogramu, tj. budou akceptovány fáze předimplementační analýza Etapy 1, akceptace/přechod do produkčního provozu (Go-live) Etapy 1, 2 a 3 a předání Exit plánu. Provedení ad hoc služeb, resp. vytvořené výstupy dle dílčí smlouvy budou ze strany objednatele akceptovány způsobem a v termínech daných objednávkou. Postup akceptační procedury je stanoven v odst. 4 až 7 tohoto článku.
3. Dílčí činnosti (Fáze), resp. výstupy z takové činnosti (Fáze) musí být dodavatelem předloženy a objednatelem akceptovány nejpozději v termínu uvedeném v Harmonogramu. Pro úspěšnou akceptaci dílčích činností (Fází) je nezbytné, aby je dodavatel provedl v šíři a kvalitě požadované v příloze č. 1 (1a, 1b) této smlouvy, stanovené v příloze č. 2 (2a, 2b) této smlouvy a příslušné objednatelem schválené předimplementační analýze.
4. Dodavatel vyzve objednatele k akceptaci dílčího plnění, a to nejméně **2 (slovy: dva) pracovní dny** před plánovaným termínem ukončení dílčí činnosti (Fáze). O průběhu akceptačního řízení bude v případě akceptace bez výhrad nebo s výhradami vyhotoven příslušný akceptační protokol označený vždy pro konkrétní akceptovanou dílčí činnost (Fázi), který bude vyhotoven ve dvou stejnopisech nebo v elektronické podobě a podepsán zmocněnci obou smluvních stran pro jednání věcná a technická, a každá ze smluvních stran obdrží po jednom stejnopisu nebo v elektronické podobě (výše a dále jen „**Akceptační protokol**").V případě neakceptace bude vyhotoven příslušný zápis o neakceptaci označený pro konkrétní dílčí neakceptovanou činnost (Fázi), který bude vyhotoven ve dvou stejnopisech nebo v elektronické podobě a podepsán zmocněnci obou smluvních stran pro jednání věcná a technická, a každá ze smluvních stran obdrží po jednom stejnopisu nebo v elektronické podobě (výše a dále jen „**zápis o neakceptaci**"). Vzor Akceptačního protokolu a zápisu o neakceptaci tvoří jako příloha č. 6 nedílnou součást této smlouvy.
5. Objednatel je oprávněn plnění v rámci akceptačního řízení, a to ve **lhůtě 10 (slovy: deseti) pracovních dní** od výzvy dodavatele:

   5.1. **akceptovat bez výhrad:** Objednatel plnění akceptuje bez výhrad za předpokladu, že plnění je připraveno k zahájení produkčního provozu (Go-live), že odpovídá této smlouvě, a je prosté jakýchkoliv vad a nedodělků.

   5.2. **akceptovat s výhradami:** Objednatel je oprávněn akceptovat plnění s výhradami v případě výskytu vad a nedodělků, které však nebrání zahájení produkčního provozu plnění a rovněž nebrání užívání plnění obvyklým způsobem. Plnění může být

akceptováno s výhradami pouze, pokud obsahuje objednatelem identifikovaných maximálně 5 nízkých výhrad a/nebo 2 střední výhrady ve smyslu odst. 6 bodu 6.2 a/nebo 6.3 tohoto článku). Takto zjištěné vady nebo nedodělky budou v příslušném akceptačním protokolu popsány a uvedeny lhůty jejich odstranění dodavatelem. Nedojde-li mezi oběma smluvními stranami k dohodě o termínu odstranění vad nebo nedodělků, pak platí, že vady a nedodělky musí být odstraněny nejpozději do 15 dnů ode dne vyhotovení příslušného akceptačního protokolu. Dodavatel bere na vědomí, že posouzení a rozhodnutí, zda se v konkrétním případě jedná o vadu spadající pod bod 5.2 nebo pod bod 5.3 tohoto článku smlouvy závisí zcela na vůli objednatele a dodavatel nemá na akceptaci s výhradou právní nárok. Pro vyloučení pochybností smluvní strany uvádějí, že v případě akceptace s výhradou nebo akceptace bez výhrad není dodavatel v prodlení s akceptací plnění.

5.3. **neakceptovat:** Vady nebo nedodělky bránící nebo ztěžující zahájení produkčního provozu plnění nebo užívání plnění obvyklým způsobem jsou důvodem k neakceptování plnění. Plnění nebude akceptováno v případě, že obsahuje více výhrad, než je stanovený maximální limit počtu výhrad pro případ akceptování s výhradami (bod 5.2 tohoto odstavce). Dílo nebude dále akceptováno, jakmile je identifikována alespoň 1 vážná výhrada ve smyslu odst. 6 bodu 6.1 tohoto článku nezávisle na počtu nízkých a středních výhrad. V **Zápise o neakceptaci** plnění bude uveden soupis vad a nedodělků, včetně lhůt jejich odstranění. Nedojde-li mezi oběma smluvními stranami k dohodě o termínu odstranění vad a nedodělků, pak platí, že vady a nedodělky musí být odstraněny nejpozději do 15 dnů ode dne vyhotovení zápisu o neakceptaci plnění. Dodavatel je povinen ve stanovené lhůtě odstranit vady nebo nedodělky i v případě, kdy podle jeho názoru za vady a nedodělky neodpovídá. Náklady na odstranění vad a nedodělků v těchto sporných případech nese až do rozhodnutí soudu dodavatel.

6. Pro účely akceptačního řízení se smluvní strany pro předejití pochybností dohodly na kategorizaci výhrad předávaného plnění a důsledky těchto výhrad:

6.1. Definici vážné výhrady naplní plnění, které obsahuje vady zásadním způsobem bránící řádnému používání předávaného dílčího plnění v souladu s touto smlouvou. Vady například způsobují nefunkčnost celého systému, případně jeho klíčových komponent, anebo umožňují zneužití oprávnění k systémům a aplikacím objednatele či způsobují jiná významná bezpečnostní rizika.

6.2. Definici střední výhrady naplní plnění obsahující vady, které omezují funkčnost systému či jeho klíčových komponent, přestože lze základní funkcionality předávaného dílčího plnění provozovat.

6.3. Definici nízké výhrady naplní plnění obsahující vady, které nenarušují funkčnost systému ani jeho klíčových komponent. Předávané dílčí plnění zčásti neodpovídá požadavkům na uživatelské rozhraní a reporting danými touto smlouvou.

6.4. Při uplatnění vážné, střední nebo nízké výhrady je objednatel oprávněn uplatnit smluvní sankci dle čl. XI odst. 2 této smlouvy.

7. Je-li předmětem dodaného řešení PAM i dodání HW, řádně dodaný HW se předává a přebírá na základě předávacího protokolu podepsaného alespoň jedním zmocněncem pro jednání věcná a technická každé smluvní strany. Nestanoví-li tato smlouva či její přílohy jinak, objednatel ověřuje v rámci akceptace HW:

7.1. parametry, vlastnosti a funkcionality uvedené v přílohách 1 a 2 této smlouvy;

7.2. příslušenství a dokumentaci, jež mělo být dodáno spolu s HW.

8. Za den předání a převzetí dílčích částí plnění je považováno:

8.1. u dodávky systému IdM datum podpisu Akceptačního protokolu pro Fázi F1.7 dle Harmonogramu.

8.2. u dodávky systému PAM datum podpisu Akceptačního protokolu pro Fázi F2.7 dle Harmonogramu.

8.3. u napojení dalších aktiv na IdM datum podpisu Akceptačního protokolu pro Fázi F3.7 dle Harmonogramu.

9. V případě dodání HW nebezpečí škody na věci a vlastnické právo k HW přechází na objednatele podpisem předávacího protokolu ve smyslu odstavce 7 tohoto článku, který bude součástí Akceptačního protokolu Etapy 2. Vzor Předávacího protokolu je uveden v příloze č. 6 této smlouvy.

10. Dodavatel garantuje a podpisem Akceptačního protokolu potvrdí, že:

10.1. dodané, instalované a zavedené plnění nebude obsahovat škodlivý software nebo známé zranitelnosti (dle seznamu OWASP TOP10 a CWE/SANS TOP 25) a bude vyvíjeno v souladu se standardy SSDLC (Secure Software Development LifeCycle);

10.2. dodané, instalované a zavedené plnění bude funkční dle předané dokumentace;

10.3. dodané, instalované a zavedené systémy IdM a PAM jsou schopné rutinního provozu ve standardním systémovém prostředí objednatele s daty objednatele, a to i za pravidelného nasazování aktualizací (update/upgrade/patch/hotfix) komponent systémového prostředí objednatele. Pokud bude nezbytné k užívání systémů využít SW produkty a služby nad rámec rozsahu Maintenance, dodavatel musí zajistit na své náklady potřebné licence nebo podlicence a jejich provozní podporu tak, aby je bylo možné provozovat bez nutnosti zásahů a speciálních znalostí technické správy objednatele. Tyto licence se zavazuje dodavatel poskytnout objednateli v rámci plnění dle této smlouvy a zajistit plnou podporu těchto SW produktů v rámci provozní podpory systému, přičemž celková cena dle čl. IV zahrnuje i tyto náklady;

10.4. v případě negativního dopadu do stávajících provozovaných systémů objednatele upraví řešení takovým způsobem, aby tyto dopady vyloučil;

10.5. plnění bude vytvořeno v souladu se všemi příslušnými právními předpisy;

10.6. že dodané, instalované a zavedené systémy IdM a PAM nejsou plněním, které může poskytnout výhradně dodavatel; uzavřením této smlouvy nedochází k proprietárnímu uzamčení IdM a PAM;

10.7. že v případě, že budou součástí implementace nebo provozu systému řešení třetích stran, existují na trhu alespoň dva certifikovaní partneři, kteří jsou schopni zajistit jejich implementaci i jejich následnou podporu;

10.8. systémy jsou navrženy tak, aby byl plně interoperabilní s běžně používanými systémy na trhu a umožní snadný přenos dat a funkcionalit do jiných systémů;

10.9. dodané licence musí umožňovat používání systémů jak zaměstnanci objednatele, tak i zaměstnanci externích partnerů;

10.10. dodané licence pokrývají veškerá dodaná prostředí (minimálně produkční, testovací, vývojové) dle požadavků v příloze č. 1a této smlouvy po celou dobu trvání této smlouvy dle potřeb pro implementaci, nasazení, provoz a rozvoj systémů.

10.11. dodané licence pokrývají minimálně 1000 řízených identit v systému IdM a licence musí umožnit napojení veškerých systémů uvedených v příloze č. 1b, Tabulkách A, B a C bez dalšího navýšení cen dle čl. V této smlouvy.

10.12. dodané licence pokrývají minimálně 100 uživatelů v systému PAM a licence musí umožnit napojení veškerých systémů uvedených v příloze č. 1b, Tabulkách D a E bez dalšího navýšení cen dle čl. IV této smlouvy.

11. Porušení jakéhokoliv z požadavků uvedených v odst. 10 tohoto článku představuje podstatné porušení této smlouvy, na jehož základě má objednatel právo od této smlouvy odstoupit za podmínek uvedených v čl. XIV této smlouvy.

Článek VII.

Licenční ujednání

1. Ve vztahu k Software (dle definice v příloze č. 8 této smlouvy), který je součástí plnění této smlouvy včetně Software, který naplňuje definici a podléhá ochraně Autorského zákona (dále jen „**Autorské dílo**“), tj. Autorské dílo vznikající v průběhu plnění, dodavatel tímto uděluje objednateli okamžikem podpisu Akceptačního protokolu k příslušnému dílčímu plnění, nevýhradní oprávnění k výkonu práva užít Software v souladu s níže uvedenými stanovenými podmínkami (dále „**Licence**“). Ustanovení tohoto odstavce se nevztahují na oprávnění objednatele k Standardnímu Software (dle definice v příloze č. 8 této smlouvy); tato oprávnění jsou upravena samostatně v odst. 7 až 15 tohoto článku.
2. Licence se uděluje jako nevýhradní a opravňuje objednatele k výkonu práva užít veškerá Autorská díla, jež jsou součástí plnění této smlouvy, a to k jakémukoliv účelu, na dobu trvání majetkových práv autorských pro případ perpetuální licence a minimálně na dobu trvání této smlouvy pro případ subskripční licence (dle definice v příloze č. 8 této smlouvy), na jakémkoliv území; jakýmkoliv způsobem; a v minimálním množstevním rozsahu vyplývajícím z čl. VI odst. 10 bod 10.11 a/nebo 10.12 této smlouvy.
3. Dodavatel v rámci Licence uděluje rovněž oprávnění takový Software upravovat a měnit (včetně Zdrojového a strojového kódu), dokončovat, včetně práva takto upravený, změněný či dokončený Software užívat v rozsahu Licence, a dále tyto původní, upravené, změněné či dokončené části spojovat s jiným dílem či zařazovat do díla souborného, zpracovávat, překládat či jinak do nich zasahovat, a to vše i prostřednictvím třetí osoby.
4. Objednatel má v rámci Licence právo udělit k Softwaru podlicenci třetím osobám a právo postoupit Licenci zcela či z části na třetí osoby, s čímž dodavatel výslovně souhlasí.
5. Licence zahrnuje povinnost dodavatele předat objednateli Zdrojový kód a dokumentaci k Software dle přílohy č. 1a této smlouvy.
6. Licence se vztahuje ve stejné míře a rozsahu jako k Software taktéž na dokumentaci specifikovanou v této smlouvě nebo jejích přílohách a jakoukoliv jinou dokumentaci

předávanou k Software nad rámec dokumentace specifikované v této smlouvě.

7. V případech, kdy je součástí plnění této smlouvy Standardní Software, dodavatel uděluje objednateli okamžikem podpisu Akceptačního protokolu k příslušnému dílčímu plnění, jehož součástí je Standardní Software, k veškerému takovému Standardnímu Software nevýhradní oprávnění k výkonu práva užít příslušný Standardní Software v souladu níže uvedenými stanovenými podmínkami (dále „**Licence k Standardnímu Software**“). Na FOSS licence se uplatní odstavce 16 a 17 tohoto článku.
8. Licence k Standardnímu Software se uděluje jako nevýhradní a opravňuje objednatele k výkonu práva užít veškerý Standardní Software, a to:
   8.1. všemi způsoby odpovídajícími účelu, pro který je takový Standardní Software určen;
   8.2. na dobu trvání majetkových práv autorských, nebo alespoň na dobu trvání této smlouvy;
   8.3. na jakémkoliv území a v minimálním množstevním rozsahu vyplývající z čl. VI odst. 10 bodu 10.11 a/nebo 10.12 této smlouvy.
9. Dodavatel je v rámci Licence k Standardnímu Software povinen zajistit poskytnutí podpory (subscription/license maintenance) k veškerému Standardnímu Software, tj. zajistit poskytování nejnovějších verzí Standardního Software Objednateli a dalších služeb v souladu se standardními licenčními podmínkami Standardního Software, a to alespoň na dobu trvání této smlouvy.
10. Licence k Standardnímu Software se vztahuje ve stejné míře jako k Standardnímu Software taktéž na
    10.1. aktualizaci Standardního Software, který je součástí plnění dle této smlouvy,
    10.2. dokumentaci k Standardnímu Software a
    10.3. loga či jiné předměty duševního vlastnictví, které se Standardním Software, jež je součástí plnění dle této smlouvy, souvisí a jsou vhodné či nezbytné k užití spolu s takovým Standardním Software.
11. V parametrech, které nejsou upraveny touto smlouvou, jejími přílohami anebo jinou částí zadávací dokumentace a jsou nezbytné pro řádné a včasné plnění této smlouvy, se Licence k Standardnímu Software řídí příslušnými licenčními podmínkami výrobce Standardního Software. Odkaz na konkrétní licenční podmínky k Standardnímu Software (dále jen jako „**podmínky EULA**“) jsou uvedeny v příloze č. 4 této smlouvy. Dodavatel poskytne objednateli informace o změně podmínek EULA včetně informace o dni účinnosti změn, nejméně 30 dní přede dnem účinnosti změn, a to zpřístupněním této informace na příslušném odkazu uvedeném v příloze č. 4 této smlouvy a zasláním oznámení na podatelna@stc.cz nebo do datové schránky objednatele. Objednatel je povinen se s novým zněním podmínek EULA seznámit.
12. Smluvní strany se dohodly, že podmínky EULA musí být v souladu s požadavky zadávací dokumentace Zadávacího řízení a této smlouvy. Taková úprava práv a povinností smluvních stran ze strany dodavatele, resp. výrobce Standardního Softwaru nesmí snížit standard plnění této smlouvy a/nebo stanovit jakékoliv poplatky, doplatky nebo jiné finanční závazky nad rámec této smlouvy a za splnění stejných podmínek může být předmětný dokument dodavatele jednostranně dodavatelem měněn. Dodavatel je povinen v případě změny podmínek EULA nebo dalších licenčních podmínek třetích stran v rozporu

s předchozí větou zajistit nápravu nebo ekvivalentní řešení tak, aby nedošlo k dopadu na práva objednatele ani k navýšení cen dle čl. V této smlouvy. V případě rozporu ustanovení této smlouvy a podmínek EULA nebo dalších licenčních podmínek třetích stran do doby zajištění nápravy ze strany dodavatele platí, že má přednost úprava obsažená v této smlouvě před úpravou obsaženou v dokumentu dodavatele nebo třetích stran. V případě rozporu mezi jednotlivými dokumenty dodavatele nebo třetích stran, budou platné v rozsahu, v jakém si neodporují.

13. V případě, že dodavatel využije při plnění předmětu této smlouvy Standardní Software, je dodavatel za účelem vyloučení vzniku proprietárního uzamčení objednatele (tzv. vendor lock-in) povinen použít výlučně takový Standardní Software, u kterého jsou splněny po dobu využívání Standardního Software následující podmínky:

    13.1. jedná se o software renomovaných výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň dvěma na sobě nezávislými a vzájemně se neovládajícími subjekty, a který je v době uzavření této smlouvy prokazatelně užíván v produkčním prostředí nejméně u pěti na sobě nezávislých a vzájemně nepropojených subjektů nebo

    13.2. u kterého je s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v IT prostředí bez nutnosti vynakládání větších prostředků (více než 50.000 Kč/rok) zajištěno, že další rozvoj softwaru jinou osobou než tvůrcem/distributorem takového softwaru je možné provádět bez toho, aby tím byla dotčena práva autorů takovéhoto softwaru, neboť nebude nutné zasahovat do zdrojových kódů takovéhoto softwaru anebo proto, že případné nahrazení takovéhoto softwaru nebude představovat výraznější komplikaci a náklad na straně objednatele nebo

    13.3. API („Application Programming Interface“) software, které pokrývá všechny moduly a funkcionality softwaru, je dobře dokumentované, umožňuje zapouzdření softwaru a jeho adaptaci v rámci měnících se podmínek IT prostředí objednatele a softwaru bez nutnosti zásahu do zdrojových kódů softwaru, a dodavatel poskytne objednateli právo užít toto rozhraní pro programování aplikací ve stejném rozsahu jako software,

    a u kterého lze zároveň důvodně předpokládat, že tento stav zůstane zachován minimálně po dobu trvání této smlouvy.

14. V případě, že dodavatel v rámci plnění této smlouvy použije Standardní Software, který v průběhu trvání této smlouvy nebude anebo přestane splňovat podmínky stanovené v odst. 13 tohoto článku, je dodavatel povinen, po dohodě s objednatelem, a v případě, že tato dohoda nebude možná, pak dle volby dodavatele:

    14.1. na vlastní náklady dodat objednateli zdrojový kód předmětného Standardního Software a poskytnout objednateli oprávnění užívat tento Standardní Software včetně zdrojového kódu (včetně dalších způsobů nakládání) v rozsahu Licence; nebo

    14.2. nahradit na vlastní náklady předmětný Standardní Software jiným Standardním Software, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software a zároveň splňovat podmínky stanovené v odst. 13 tohoto článku, a poskytnout k tomuto

Standardnímu Software objednateli Licenci k Standardnímu Software dle odst. 13 tohoto článku; nebo

14.3. nahradit na vlastní náklady předmětný Standardní Software vlastním Softwarem, tj. přeprogramovat část plnění představovanou předmětným Standardním Softwarem za využití vlastního software vytvořeného na míru objednateli, který bude mít alespoň srovnatelné funkcionality, kvalitu a technickou způsobilost jako nahrazovaný Standardní Software, a poskytnout k tomuto vlastnímu Softwaru Objednateli Licenci dle odst. 1 a 2 tohoto článku, a to včetně Zdrojového kódu.

15. Postupy dle odst. 14 bodů 14.1 až 14.3 tohoto článku podléhají samostatnému akceptačnímu řízení, na které se přiměřeně použije článek VI této smlouvy. Vznikla-li dodavateli povinnost dle odst. 14 tohoto článku, je dodavatel povinen splnit povinnosti dle uvedeného odstavce i po ukončení této smlouvy. Ustanovení této smlouvy relevantní pro splnění povinností dle předchozí věty se použijí i po ukončení této smlouvy.

16. Dodavatel je při plnění této smlouvy oprávněn využít programy s otevřeným kódem či jejich části distribuovanými pod FOSS licencemi. Dodavatel však není oprávněn využít programy s otevřeným kódem či jejich části, které jsou distribuovány pod FOSS licencemi, jejichž podmínky by objednateli ukládaly povinnost sdělovat nebo jinak šířit Software či jeho části, včetně Zdrojových kódů, třetím osobám, nebo umožnit jim změny, úpravy či jiné zásahy do Softwaru nebo jeho části.

17. Dodavatel je povinen zajistit objednateli udělení oprávnění k veškerým programům s otevřeným kódem poskytnutým objednateli v rozsahu takových FOSS licencí, které se na konkrétní program s otevřeným kódem, který je součástí plnění, vztahují. Konkrétní rozsah FOSS licence musí analogicky splňovat podmínky dle odst. 11 a 12 tohoto článku odkaz na aktuální znění licenčních podmínek FOSS licencí bude uveden v příloze č. 4 této smlouvy.

18. V souvislosti s poskytnutou Licencí a oprávněními objednatele je dodavatel povinen každou změnu Zdrojových kódů Software poskytnout objednateli na vyžádání (nejvýše však jednou za jeden kalendářní měsíc) do 10 pracovních dnů ode dne obdržení žádosti objednatele. Povinnost dodavatele uvedená v tomto odstavci se použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update zdrojového kódu každé jednotlivé části Software, která je počítačovým programem, k nimž dojde při poskytování plnění dodavatele nebo v rámci záručních oprav (dále jen „**změny Zdrojového kódu**“).

19. Předané Zdrojové kódy dle předchozího odstavce musí být spustitelné v prostředí objednatele a zaručující možnost ověření, že je kompletní a ve správné poslední verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality. Změny Zdrojového kódu předá dodavatel objednateli vždy na technickém nosiči dat (hardwarově šifrovaná USB flash paměť) s viditelně označeným názvem „Zdrojový kód IS + datum“ a označením počítačového programu či jeho části a jeho verze a dne předání zdrojového kódu, a to včetně instalačních souborů, struktury a základního programátorského textového popisu databáze. Současně s předáním nosiče dat předá dodavatel objednateli dešifrovací klíče.

20. S každou novou vydanou verzí Software musí dodavatel dodat objednateli i tzv. „Release notes“, tedy soupis veškerých změn, včetně zapracování změn do veškeré dokumentace a předání aktualizované verze veškeré dokumentace.

21. Současně se dodavatel zavazuje ve stejném rozsahu jako v předchozích odstavcích tohoto článku předat objednateli nejpozději poslední den před ukončením platnosti a účinnosti této smlouvy poslední aktuální verzi Zdrojových kódů Software, resp. poslední verzi změny Zdrojového kódu, včetně příslušných dešifrovacích klíčů.

22. Dodavatel výslovně prohlašuje, že odměna za předávání změn Zdrojových kódů a oprávnění k nim v rozsahu Licence poskytnutá objednateli dle tohoto článku je již zahrnuta v ceně Služeb podpory dle této smlouvy a považuje tuto cenu za dostatečnou a odpovídající a zahrnující plné vypořádání jeho nároků ve vztahu k využití práv z licencí a podlicencí. Dodavatel bere na vědomí, že i s ohledem na explicitně vyjádřený účel této smlouvy nemá dodavatel ani případné třetí osoby právo na dodatečnou odměnu ani na vypořádání a objednateli nemohou vzniknout dodatečné peněžité ani jiné povinnosti vůči třetím osobám ani dodavateli.

23. Všechna data, ať už v jakékoliv podobě, a jejich hmotné nosiče, která vznikla či vzniknou při plnění předmětu této smlouvy, jsou výlučným vlastnictvím objednatele a objednatel nabývá vlastnické právo okamžikem jejich převzetí. Veškeré podklady, které byly objednatelem dodavateli předány, zůstávají v jeho vlastnictví a dodavatel za ně odpovídá od okamžiku jejich převzetí.

24. Dodavatel není oprávněn použít podklady, data a hmotné nosiče předané mu objednatelem dle této smlouvy pro jiné účely, než je poskytování plnění předmětu této smlouvy. Nejpozději do 15 pracovních dnů od doručení žádosti objednatele nebo od ukončení této smlouvy je dodavatel povinen tato data a jejich nosiče objednateli předat.

25. Objednatel si vyhrazuje právo zapůjčit dodanou dokumentaci třetí straně za účelem zajištění provozu nebo rozvoje systému po ukončení poskytování Služeb podpory dodavatelem.

26. Dodavatel prohlašuje, že

    26.1. je oprávněn udělit objednateli veškerá oprávnění v souladu s tímto článkem smlouvy a odpovídá objednateli za zajištěni všech nezbytných oprávnění a souhlasů autora či autorů Software či Standardního Software k oprávněním udělovaným Objednateli dle tohoto článku této smlouvy; Dodavatel výlučně odpovídá za neoprávněný zásah do autorských i jiných práv třetích osob;

    26.2. veškeré plnění dodané podle této smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění. V případě, že by nárok třetí osoby vzniklý v souvislosti s plněním dodavatele podle této smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání některého z plnění či jeho části, zavazuje se dodavatel zajistit ve spolupráci s objednatelem na vlastní náklady náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu plnění sjednanou podle této smlouvy, přičemž současně nebudou dotčeny ani nároky objednatele na náhradu škody.

27. Dodavatel se zavazuje kdykoliv v průběhu trvání této smlouvy umožnit objednateli provedení auditu licenčního souladu (tedy kontrolu, zda je Software a Standardní Software používán v rámci platných licenčních metrik) a je povinen poskytnout veškeré související dokumenty zejména podmínky EULA. Pokud se objednatel rozhodne provést audit

licenčního souladu dle tohoto odstavce, tento záměr oznámí dodavateli minimálně s 30denním předstihem a zároveň poskytne dodavateli předpokládaný harmonogram auditu, jeho rozsah a očekávané potřebné součinnosti ze strany dodavatele. Provedení auditu včetně zajištění příslušného auditora je odpovědností objednatele, a to na náklady objednatele. Dodavatel je povinen poskytnout potřebné součinnosti a předat potřebné podklady pro provedení auditu a vyhotovení auditní zprávy s tím, že náklady na tyto součinnosti jsou zahrnuty v ceně plnění této smlouvy.

Článek VIII.
Práva a povinnosti smluvních stran

1. Dodavatel je povinen mít po dobu účinnosti této smlouvy uzavřeno pojištění odpovědnosti za škodu způsobenou dodavatelem třetí osobě, a to ve výši nejméně **25 000 000 Kč**. Dodavatel se zavazuje, že pojištění v uvedené výši a rozsahu zůstane účinné po celou dobu účinnosti této smlouvy, do 5 pracovních dnů od výzvy objednatele je dodavatel povinen toto objednateli prokázat, a to ve formě prosté kopie pojistné smlouvy. Rovnocenným dokladem pro prokázání tohoto požadavku je také prostá kopie pojistného certifikátu nebo prostá kopie potvrzení o uzavření pojistné smlouvy vystaveného pojistitelem.
2. Dodavatel se zavazuje, že práva a závazky vyplývající z této smlouvy nepřevede na třetí osoby bez souhlasu objednatele.
3. Smluvní strany se zavazují úzce spolupracovat, zejména si poskytovat úplné, pravdivé a včasné informace potřebné k řádnému plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění smlouvy. Dodavatel se zavazuje objednateli na základě jeho výzvy jej bez zbytečného odkladu informovat o aktuálním stavu provádění plnění.
4. Smluvní strany se dále zavazují poskytnout druhé smluvní straně dohodnutou součinnost umožňující řádné plnění závazků ze smlouvy.
5. Smluvní strany se zavazují plnit své závazky v souladu se všemi příslušnými obecně závaznými právními předpisy. Smluvní strany jsou zároveň povinny plnit své závazky tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžitých závazků.
6. Dodavatel se zavazuje plnění dle této smlouvy poskytovat řádně a tak, aby byl v co nejmenší míře omezen provoz objednatele.
7. K řádnému splnění předmětu této smlouvy objednatel zajistí pro dodavatele zejména:
   7.1. technickou pomoc a
   7.2. vzdálený přístup k systémům prostřednictvím VPN pro případnou možnost konfigurace systému mimo interní síť objednatele či další činnosti předpokládané touto smlouvou;
   7.3. poskytnutí interní dokumentace objednatele, kterou je dodavatel povinen se při implementaci, podpoře a rozvoji IdM či PAM řídit, resp. se kterou musí být dodaný systém v souladu,

7.4. vstup zaměstnancům dodavatele do objektu objednatele k plnění předmětu této smlouvy včetně poučení zaměstnanců dodavatele o dodržování ochranných a bezpečnostních opatření v objektu objednatele,

7.5. hygienické a bezpečné pracovní podmínky, odpovídající normám EU.

8. Zaměstnanci dodavatele jsou zejména:

8.1. oprávněni vstupovat pouze do těch prostorů v objektu objednatele, které budou písemně dohodnuty mezi zmocněnci pro jednání věcná a technická obou smluvních stran,

8.2. oprávněni využívat vzdálený přístup k systému prostřednictvím VPN za účelem řádného splnění předmětu této smlouvy,

8.3. povinni nosit viditelně průkazy pro vstup do objektu objednatele a mít u sebe platný průkaz totožnosti,

8.4. povinni zdržet se vynášení jakýchkoli dat souvisejících s výrobou, jak na datových nosičích, tak v písemné podobě,

8.5. povinni dodržovat veškeré platné právní předpisy (zejména zákoník práce a bezpečnostní předpisy) a interní směrnice a předpisy objednatele, se kterými byli objednatelem seznámeni.

9. Dodavatel bere na vědomí, že přístup k IT prostředí objednatele:

9.1. je udělován fyzickým osobám dodavatele, jakož i pro konkrétní zařízení, na základě výslovného požadavku dodavatele a objednatel je oprávněn dle svého uvážení přístup neudělit či kdykoli odebrat, zejména v případě Kybernetické bezpečnostní události či porušení povinností stanovených ve vnitropodnikových předpisech objednatele;

9.2. je poskytován na základě principů “need to know” a “deny by default”; a

9.3. je poskytován za podmínky dodržování veškerých bezpečnostních opatření a požadavků objednatele

9.4. může být objednatelem monitorován a objednatel je oprávněn logovat přístupy dodavatele do IT prostředí objednatele, jakož i veškerou další aktivitu dodavatele významnou z hlediska bezpečnosti;

10. Dodavatel se zavazuje, že:

10.1. veškerá data budou ukládána v otevřených formátech, aby měl objednatel vždy přístup k datům ve standardizovaném formátu, který umožní jejich snadný přenos do jiného systému bez nutnosti konverze dat dodavatelem;

10.2. počínat si při provádění plnění dle této smlouvy tak, aby nedošlo k infikaci Softwaru, Standardního Softwaru nebo IT prostředí objednatele virem či jiným škodlivým kódem (malware apod.) způsobujícím narušení zabezpečení Softwaru a Standardního Softwaru za účelem jeho poškození či jiného narušení běhu;

10.3. upozorňovat objednatele včas na všechny hrozící vady systémů či potenciální výpadky systémů, jakož i poskytovat objednateli veškeré informace, které jsou pro plnění dle této smlouvy potřebné;

10.4. bez zbytečného odkladu oznamovat objednateli všechny Kybernetické bezpečnostní události a Kybernetické bezpečnostní incidenty s potenciálním negativním dopadem na objednatele;

11. Dodavatel je povinen mít po dobu účinnosti této smlouvy, resp. po dobu poskytování plnění

dle této smlouvy zaveden systém řízení bezpečnosti informací dle ČSN EN ISO/IEC 27001:2023 pro předmět činnosti, který je vztažen k předmětu této smlouvy. Dodavatel se zavazuje, že systémem řízení bezpečnosti informací dle ČSN EN ISO/IEC 27001:2023 bude disponovat po celou dobu účinnosti této smlouvy, a do 5 pracovních dnů od výzvy objednatele je dodavatel povinen toto objednateli prokázat, a to ve formě prosté kopie certifikátu systému řízení bezpečnosti informací dle ČSN EN ISO/IEC 27001:2023 vydaný podle českých technických norem akreditovanou osobou, nebo ve formě certifikátu vydaného podle českých technických norem akreditovanou osobou v členském státě Evropské unie. V případě pochybnosti o pravosti certifikátu si objednatel vyhrazuje právo vyžádat si originál nebo ověřenou kopii certifikátu. Porušení povinnosti dodavatele udržovat v platnosti předmětný certifikát po celou dobu platnosti a účinnosti této smlouvy, nebo skutečnost, že dodavatel neprokázal držení tohoto certifikátu na výzvu objednatele dle tohoto odstavce, představuje podstatné porušení této smlouvy, na jehož základě má objednatel právo od této smlouvy odstoupit za podmínek uvedených v čl. XIV této smlouvy. Dodavatel je povinen zajistit splnění povinnosti dle předchozí věty také ze strany poddodavatelů v případě, že je využije k plnění této smlouvy.

12. Veškeré podklady, které byly objednatelem dodavateli předány, zůstávají v jeho vlastnictví a dodavatel za ně zodpovídá od okamžiku jejich převzetí a je povinen je vrátit objednali po splnění svého závazku.

13. Dodavatel se zavazuje alokovat na realizaci této smlouvy pracovní kapacitu osob realizačního týmu uvedeného v Nabídce a k plnění této smlouvy využít osob, kterými byla prokazována kvalifikace v Zadávacím řízení. Seznam těchto hlavních členů realizačního týmu tvoří přílohu č. 7 – Realizační tým, která je nedílnou součástí této smlouvy. Porušení této povinnosti přetrvávající déle než 20 pracovních dnů je považováno za porušení této smlouvy podstatným způsobem. Dodavatel je oprávněn realizovat předmět plnění i jinými osobami než hlavními členy realizačního týmu. K jejich zapojení je třeba postupovat dle odst. 16 tohoto článku.

14. V případě, že některý hlavní člen realizačního týmu, přestane v průběhu trvání této smlouvy splňovat jakýkoliv z požadavků stanovených objednatelem v zadávacích podmínkách veřejné zakázky, je dodavatel povinen takovouto osobu v realizačním týmu bezodkladně nahradit jinou, splňující veškeré požadavky objednatele.

15. Dodavatel je oprávněn nahradit hlavní členy realizačního týmu pouze osobami splňujícími minimální požadavky v zadávacích podmínkách Zadávacího řízení.

16. Jakékoliv změny realizačního týmu dodavatele (doplnění nebo nahrazení dalšího nebo nahrazení hlavního člena realizačního týmu) budou možné vždy pouze s předchozím písemným souhlasem objednatele. Objednatel není oprávněn odmítnout souhlas se změnou osoby tvořící realizační tým navrženou dodavatelem, pokud tato osoba splňuje veškeré shora uvedené požadavky. Dodavatel je povinen společně se svojí žádostí o souhlas s takovou změnou hlavního člena realizačního týmu, předložit dokumenty prokazující splnění zadávacích podmínek Zadávacího řízení, a to v prosté kopii. Za dostatečný souhlas objednatele s touto změnou je považováno vyjádření souhlasu prostřednictvím e-mailu mezi zmocněnci pro jednání věcná a technická obou smluvních stran. Takováto změna bude při nejbližší vhodné příležitosti ošetřena dodatkem k této smlouvě s deklaratorním účinkem uvedené změny.

17. Dodavatel je oprávněn plnit tuto smlouvu nebo její část prostřednictvím svého (svých)

poddodavatele(ů). V případě, že dodavatel použije poddodavatele ve smyslu předchozí věty,

17.1. není jakkoli dotčena odpovědnost dodavatele za případné nesplnění či vadné plnění příslušných závazků, a dodavatel má i nadále odpovědnost za plnění předmětu této smlouvy jako by ho plnil sám;

17.2. byl povinen objednateli předložit seznam poddodavatelů dle zadávací dokumentace Zadávacího řízení za podmínek tam uvedených;

17.3. v případě změny v seznamu uvedených poddodavatelů (např. jiný rozsah plnění, změna poddodavatele, nový poddodavatel) je dodavatel povinen oznámit takovou změnu bez zbytečného odkladu objednateli, nejpozději však 3 pracovní dny před takovou změnou. Dodavatel je oprávněn změnit poddodavatele jímž prokazoval kvalifikaci pouze v případě, že dodavatel doloží veškeré doklady, které prokážou, že nový poddodavatel splňuje kvalifikaci alespoň ve stejném rozsahu jako původní poddodavatel, jímž byla kvalifikace prokazována;

17.4. dodavatel je povinen zajistit řádné a včasné plnění svých finančních závazků vůči svým poddodavatelům po celou dobu trvání této smlouvy, přičemž za řádné a včasné plnění se považuje úplná úhrada faktur vystavených poddodavatelem za plnění poskytovaná pro účely plnění závazků dodavatele dle této smlouvy, a to nejpozději do 30 dnů od přijetí platby objednatele dle této smlouvy. V případě, že se objednatel hodnověrným a prokazatelným způsobem dozví, že ze strany dodavatele došlo nebo dochází k nesplnění povinností dodavatele dle věty první tohoto bodu 17.4, a dodavatel i přes předchozí písemné upozornění objednatele pokračuje v neplnění těchto svých povinností nebo nezjedná nápravu, má objednatel právo odstoupit od této smlouvy za podmínek uvedených v čl. XIV této smlouvy.

Tato smlouva nebude měněna z důvodu použití poddodavatelů nebo jejich změny dle tohoto odstavce.

18. Dodavatel prohlašuje v souladu s čl. 5 k Nařízení Rady (EU) č. 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014, o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, že není:

18.1. ruským státním příslušníkem, fyzickou či právnickou osobou nebo subjektem či orgánem se sídlem v Rusku;

18.2. právnickou osobou, subjektem nebo orgánem, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písmenu a) tohoto odstavce;

18.3. fyzickou nebo právnickou osobou, subjektem nebo orgánem, které jednají jménem nebo na pokyn některého ze subjektů uvedených v písmenech a) nebo b) tohoto odstavce.

19. Dodavatel současně prohlašuje, že žádný z jeho poddodavatelů, který bude dodavatelem využit pro plnění této smlouvy, a jehož rozsah činnosti a/nebo odměny překročí 10 % hodnoty plnění této smlouvy, není subjektem uvedeným v bodu 18.1 nebo 18.2 nebo 18.3 odstavce 18 tohoto článku.

20. Dodavatel dále prohlašuje, že ve smyslu:

20.1. čl. 2 odst. 2 Nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, v platném znění (dále jen „Nařízení č. 269/2014), a

20.2. čl. 2 odst. 2 Nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014, o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, v platném znění (dále jen „Nařízení č. 208/2014“), a

20.3. čl. 2 odst. 2 Nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska, v platném znění (dále jen „Nařízení č. 765/2006“),

není fyzickou nebo právnickou osobou, subjektem či orgánem nebo fyzickou nebo právnickou osobou, subjektem či orgánem s nimi spojeným uvedeným v příloze I Nařízení č. 269/2014, Nařízení č. 208/2014 nebo Nařízení č. 765/2006.

21. Dodavatel prohlašuje a zavazuje se, že žádné finanční prostředky ani hospodářské zdroje nebudou pro účely plnění této smlouvy, přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům uvedeným v příloze I Nařízení č. 269/2014, Nařízení č. 208/2014 nebo Nařízení č. 765/2006 nebo v jejich prospěch.

22. Pokud by v průběhu platnosti a účinnosti této smlouvy mělo dojít k nedodržení podmínek uvedených v odst. 18, 19, 20 nebo 21 tohoto článku, zavazuje se dodavatel bezodkladně, od momentu, kdy se o dané změně okolností dozví, o této skutečnosti písemně objednatele informovat.

23. Porušení povinnosti dodavatele v odst. 18 nebo 19 nebo 20 nebo 21 nebo 22 tohoto článku je považováno za podstatné porušení této smlouvy, na jehož základě má objednatel právo od této smlouvy odstoupit za podmínek uvedených v čl. XIV této smlouvy.

Článek IX.

Odpovědnost za vady, záruka, záruční servis

1. Dodavatel přebírá závazek a odpovědnost za vady systému, jež bude mít systém v době jeho předání objednateli, tj. v den podpisu Akceptačního protokolu ve smyslu čl. VI odst. 4 této smlouvy. Analogicky se bude postupovat v případě ad hoc služeb, kdy dodavatel přebírá závazek a odpovědnost za to, že výstupy ad hoc služeb budou způsobilé k použití ke smluvnímu účelu a v době předání objednateli nebudou vykazovat žádné vady. V případě výskytu vady je objednatel oprávněn požadovat po dodavateli bezplatné odstranění vady.

2. Dodavatel se zavazuje, že plnění z odpovědnosti za vady bude řešit v rámci Služeb podpory v dostupnosti a reakčních lhůtách dle přílohy č. 5 této smlouvy. Při nedodržení reakčních lhůt se uplatní sankce dle čl. XI odst. 3 této smlouvy.

3. Pokud bude součástí plnění dodávka HW, dodavatel poskytuje objednateli ve smyslu § 2619 OZ záruku za jakost na to, že HW bude mít vlastnosti stanovené touto smlouvou, bude plně funkční a způsobilý pro použití ke smluvenému účelu, bude odpovídat

sjednaným funkčním požadavkům a parametrům uvedeným v této smlouvě a bude bez jakýchkoliv vad a nedodělků, a to ode dne následujícího po podpisu předávacího protokolu po celou dobu trvání této smlouvy, resp. po celou dobu poskytování Služeb podpory (dále jen „**záruční doba**“).

4. Dodavatel se zavazuje po dobu záruční doby poskytovat podporu na tento HW (dále jen „**podpora na HW**“), a to v následujícím rozsahu. Servisní technik dodavatele zahájí řešení vady týkající se HW, nejpozději do 1 pracovního dne („**NBD**“) po oznámení vady v pracovní době, která je pro účely této smlouvy určena jako doba v pracovních dnech (v zemi objednatele) od 8 hodin do 16 hodin (dále jen „**Pracovní doba**“) na e-mailovou adresu dodavatele **[zadavatel doplní údaje vybraného dodavatele dle Nabídky]**. Objednatel je povinen reklamované vady popsat, uvést, jak se projevují a též doložit potřebnými doklady (např. printscreeny obrazovky aj.), pokud to bude vhodné a možné. Objednatel je oprávněn oznámit vadu dodavateli také telefonicky na telefonním čísle **[zadavatel doplní údaje vybraného dodavatele dle nabídky]**, nicméně rozhodným okamžikem pro běh reakčních lhůt je písemné oznámení na e-mailové adrese uvedené v tomto odstavci.
5. Servisní technik vadný HW nebo jeho část opraví či vymění za bezvadný nejpozději do 5 pracovních dní od okamžiku oznámení vady, pokud se v jednotlivém případě nedohodne s objednatelem jinak na základě oboustranného písemného odsouhlasení přiměřené dodatečné lhůty, která bude stanovena v pracovních dnech. Vada nahlášená po Pracovní době se považuje za nahlášenou následující pracovní den v 8 hodin ráno.
6. Pokud dodavatel neodstraní záruční vady ve sjednané době od jejich oznámení objednatelem dodavateli, je objednatel oprávněn podle vlastního uvážení vadu buď sám odstranit, nebo pověřit jejím odstraněním třetí osobu, v obou případech na náklady dodavatele. Všechny případy svépomoci uvedené v tomto odstavci nenarušují žádná práva plynoucí objednateli ze záruky.
7. Dodavatel zaručuje objednateli, že veškeré náhradní díly, které použije při odstranění vady, budou původní a nové. V případě, že o to objednatel požádá, může dodavatel nabídnout i díly repasované nebo použité.
8. Záruční doba neběží po dobu, po kterou objednatel nemůže užívat HW k účelu, ke kterému ho objednatel objednal.
9. Jakékoli vady dle odst. 1 nebo odst. 3 je dodavatel povinen odstranit na své náklady.

Článek X.

Ochrana bezpečnosti informací

1. Smluvní strany nejsou oprávněny zpřístupnit třetí osobě neveřejné informace, které získaly či získají při vzájemné spolupráci, jakož i informace spojené s vytvořením a obsahem této smlouvy. To neplatí, mají-li být za účelem plnění této smlouvy potřebné informace zpřístupněny zaměstnancům smluvních stran nebo dalším osobám (zpracovatelům informací), kteří se podílejí na plnění dle této smlouvy, a to za stejných podmínek, jaké jsou stanoveny smluvním stranám v tomto článku, a vždy jen v rozsahu zcela nezbytně nutném pro řádné plnění této smlouvy.
2. Smluvní strany jsou povinny zabezpečit, že povinnosti vyplývající z tohoto článku budou

dodržovány všemi osobami, které se s neveřejnými informacemi seznámily dle předchozího odstavce. Porušení závazku mlčenlivosti ze strany těchto osob je považováno za porušení způsobené smluvní stranou, která jim neveřejné informace poskytla.

3. Za neveřejné informace jsou považovány veškeré informace vzájemně poskytnuté v písemné, ústní, vizuální, elektronické nebo jiné formě, jakož i know-how, které mají skutečnou nebo alespoň potenciální hodnotu a které nejsou v příslušných obchodních kruzích běžně dostupné, a dále informace, které jsou písemně označeny jako diskrétní (zkratka "DIS") nebo u kterých se z povahy věci dá předpokládat, že se jedná o informace neveřejné.

4. Smluvní strany se zavazují, že pokud v rámci vzájemné spolupráce přijdou do styku s osobními údaji či zvláštní kategorií osobních údajů ve smyslu Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „GDRP“) a zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění, učiní veškerá opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k těmto údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jinému neoprávněnému zpracování, jakož i k jejich jinému zneužití.

5. V této souvislosti se smluvní strany zejména zavazují:

   a) nesdělit neveřejné informace třetím osobám;
   b) zajistit, aby neveřejné informace nebyly zpřístupněny třetím osobám;
   c) zabezpečit data či údaje v jakékoli formě, včetně jejich kopií, obsahující neveřejné informace, před zneužitím třetími osobami a zajistit proti ztrátě.

6. Ochrana neveřejných informací se nevztahuje zejména na případy, kdy:

   a) smluvní strana prokáže, že je daná informace veřejně dostupná, aniž by tuto dostupnost sama způsobila;
   b) smluvní strana prokáže, že měla danou informaci k dispozici ještě před datem zpřístupnění druhou stranou a že ji nenabyla v rozporu se zákonem;
   c) smluvní strana obdrží od druhé strany písemný souhlas zpřístupňovat dále danou informaci;
   d) je zpřístupnění dané informace vyžadováno zákonem nebo závazným rozhodnutím příslušného orgánu státní správy či samosprávy;
   e) auditor provádí u některé ze smluvních stran audit na základě oprávnění vyplývajícího z příslušných právních předpisů.

7. Smluvní strany se zavazují na žádost druhé smluvní strany:

   a) vrátit všechny neveřejné informace, které byly předány „hmotnou formou“ (zejména písemně či elektronicky), a jakékoliv další materiály obsahující nebo odvozující neveřejné informace;
   b) vrátit či zničit kopie, výpisy nebo jiné celkové nebo částečné reprodukce či záznamy neveřejných informací;
   c) zničit bez zbytečného odkladu všechny dokumenty, memoranda, poznámky a ostatní písemnosti vyhotovené na základě neveřejných informací;
   d) zničit materiály, uložené v počítačích, textových editorech nebo jiných zařízeních, obsahující neveřejné informace ve smyslu této smlouvy.

Smluvní strany se rovněž zavazují zajistit, že totéž učiní všechny další osoby, které se s neveřejnými informacemi seznámily prostřednictvím jedné ze smluvních stran.

8. Zaměstnanec povinné smluvní strany, který byl zničením dokumentů ve smyslu předchozího odstavce pověřen, na výzvu druhé smluvní strany písemně potvrdí zničení příslušných dokumentů.

9. V případě, že se některá ze smluvních stran, resp. její zaměstnanci nebo další osoby (zpracovatelé informací) hodnověrným způsobem dozví, popřípadě budou mít odůvodněné podezření, že došlo ke zpřístupnění neveřejných informací neoprávněnému subjektu, jsou povinni o tom bez zbytečného odkladu informovat druhou smluvní stranu.

10. Závazek mlčenlivosti není časově omezen. Povinnost zachovávat mlčenlivost o neveřejných informacích získaných v rámci spolupráce s druhou smluvní stranou trvá i po ukončení platnosti a účinnosti této smlouvy. Závazek mlčenlivosti přechází i na případné právní nástupce smluvních stran.

11. Smluvní strany jsou povinny zajistit ochranu informací, které jedna ze smluvních stran označí jako obchodní tajemství ve smyslu § 504 OZ. Smluvní strany jsou povinny zabezpečit informace označené jako obchodní tajemství minimálně ve stejném rozsahu jako neveřejné informace definované v této smlouvě. Informace označené smluvními stranami jako obchodní tajemství nebudou zveřejněny v registru smluv ve smyslu čl. XV odst. 12 této smlouvy. Pokud dodavatel považuje některé informace uvedené v této smlouvě za své obchodní tajemství ve smyslu § 504 občanského zákoníku, informuje o tom objednatele nejpozději před uzavřením této smlouvy.

Článek XI.

Smluvní pokuty, úrok z prodlení

1. V případě prodlení dodavatele s předáním plnění, resp. jednotlivých akceptačních milníků dle čl. VI odst. 2 této smlouvy ve lhůtách stanovených v Harmonogramu spočívajících na jeho straně, vzniká objednateli právo na smluvní pokutu ve výši 4.000, - Kč za každý i započatý den prodlení.

2. V případě prodlení dodavatele s odstraněním vad ve lhůtě dle čl. VI odst. 5 bod 5.2. nebo 5.3. této smlouvy je dodavatel povinen uhradit objednateli smluvní pokutu

    a) v případě vážné výhrady ve výši 2.000,- Kč, a to za každý i započatý den prodlení a každou uplatněnou vadu;

    b) v případě nízké nebo střední výhrady ve výši 1.000,- Kč, a to za každý i započatý den prodlení a každou uplatněnou vadu.

3. V případě prodlení dodavatele s vyřízením reklamace a odstraněním vad ve lhůtě dle čl. IX odst. 5 této smlouvy je dodavatel povinen uhradit objednateli smluvní pokutu ve výši 5.000,- Kč, a to za každý i započatý pracovní den prodlení. Znění první věty tohoto odstavce platí pouze v případě, že součástí plnění dle této smlouvy bude dodávka HW, resp. dodavatel bude zajišťovat podporu na HW dle čl. IX odst. 5 této smlouvy.

4. V případě nedodržení parametrů SLA dle přílohy č. 5 této smlouvy, je dodavatel povinen uhradit objednateli smluvní pokutu dle následujícího rozpisu:

Parametr	IdM	PAM
	Výše smluvní pokuty za prodlení s dodržením sjednané doby řešení parametru	**Výše smluvní pokuty za prodlení s dodržením sjednané doby řešení parametru**
RTO (Recovery time objective – obnova)	**2000,- Kč** za každou započatou hodinu prodlení nad rámec sjednané doby dle přílohy č. 5	**2000,- Kč** za každou započatou hodinu prodlení nad rámec sjednané doby dle přílohy č. 5
RPO (Recovery point objective – ztráta dat)	**500,- Kč** za každých započatých 5 minut prodlení nad rámec sjednané doby dle přílohy č. 5	**500,- Kč** za každých započatých 5 minut prodlení nad rámec sjednané doby přílohy č. 5
Reakce na kritickou závadu	**500,-Kč** za každých započatých 5 minut prodlení nad rámec 30 minutové reakční doby dle přílohy č. 5	**500,- Kč** za každých započatých 5 minut prodlení nad rámec 30 minutové reakční doby dle přílohy č. 5
Odstranění kritické závady	**2000,- Kč** za každou započatou hodinu prodlení nad rámec sjednané doby dle přílohy č. 5	**2000,- Kč** za každou započatou hodinu prodlení nad rámec sjednané doby dle přílohy č. 5
Odstranění vážné závady	**2000,- Kč** za každou započatou hodinu prodlení nad rámec sjednané doby dle přílohy č. 5	**2000,- Kč** za každou započatou hodinu prodlení nad rámec sjednané doby dle přílohy č. 5
Odstranění ostatních závad	**1000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5	**1000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5
Permanentní fix (všech) závad	**1000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5	**1000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5.
Bezpečnostní update (CVSS 0.1–3.9)	**500,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5	**500,-Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5
Bezpečnostní update (CVSS 4.0–6.9)	**1000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5	**1000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5
Bezpečnostní update (CVSS 7.0–8.9)	**2000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle	**2000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle

	přílohy č. 5	přílohy č. 5
Bezpečnostní update (CVSS ≥ 9)	**5000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5	**5000,- Kč** za každý započatý den prodlení nad rámec sjednané doby dle přílohy č. 5

Výše poklesu dostupnosti oproti stanovené dostupnosti v SLA, v rámci kalendářního měsíce	Výše smluvní pokuty za pokles dostupnosti sytému IdM v rámci kalendářního měsíce	Výše smluvní pokuty za pokles dostupnosti systému PAM v rámci kalendářního měsíce
Do 1 %	**10 000,- Kč**	**10 000,- Kč**
Od 1 (včetně) do 5 %	**20 000,- Kč**	**20 000,- Kč**
Od 5 (včetně) do 10 %	**35 000,- Kč**	**35 000,- Kč**
Od 10 % (včetně) a více	**50 000,- Kč**	**50 000,- Kč**

5. Smluvní strany pro vyloučení všech pochybností uvádí, že smluvní pokuty se za jednotlivá prodlení se splněním příslušných reakčních lhůt i v rámci stejné oznámené vady sčítají.
6. V případě porušení jakéhokoliv požadavku vyplývajícího z čl. VI odst. 10 této smlouvy má objednatel právo na smluvní pokutu ve výši 100.000, - Kč, a to za každý jednotlivý případ porušení.
7. V případech porušení povinností vyplývajících z čl. X této smlouvy má objednatel právo na smluvní pokutu ve výši 200.000, - Kč za každý zjištěný případ porušení těchto povinností.
8. V případě porušení některé z povinností nebo prohlášení uvedených v čl. VIII odst. 18, 19, 20, 21 nebo 22 této smlouvy ze strany dodavatele nebo ukáže-li se prohlášení dle čl. VIII odst. 20 až 21 této smlouvy nepravdivým, má objednatel právo uplatnit vůči dodavateli smluvní pokutu ve výši 100.000, - Kč, a to za každý jednotlivý případ porušení.
9. V případě porušení některé z povinností nebo prohlášení uvedených v čl. VII odst. 26 této smlouvy ze strany dodavatele nebo ukáže-li se prohlášení dle čl. VII odst. 26 této smlouvy nepravdivým, má objednatel právo uplatnit vůči dodavateli smluvní pokutu ve výši 2 000 000 Kč, a to za každý jednotlivý případ porušení.
10. Povinnost zaplatit smluvní pokutu vzniká dodavateli do 30 kalendářních dnů ode dne vystavení faktury objednatelem dodavateli k zaplacení smluvní pokuty.
11. Zaplacení smluvní pokuty nezbavuje dodavatele povinnosti splnit závazky přijaté Smlouvou.
12. Ujednáním smluvní pokuty není nijak dotčeno právo na náhradu vzniklé škody v celém jejím rozsahu.
13. Při prodlení s úhradou jakékoliv ceny dle této smlouvy je dodavatel oprávněn požadovat úrok z prodlení ve výši stanovené nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob, ve znění pozdějších předpisů.

14. V případě, že k porušení povinnosti nebo prodlení se splněním povinnosti ze strany dodavatele, na kterou se váže smluvní pokuta, dojde z důvodu neposkytnutí součinnosti ze strany objednatele nebo třetích stran není objednatel oprávněn smluvní pokutu uplatnit. V případě, že se liberační důvody vztahují pouze na část prodlení dodavatele, může být smluvní pokuta uplatněna na část prodlení, které bylo způsobeno dodavatelem.

Článek XII.
Odpovědnost za škodu

1. Každá ze smluvních stran je povinna nahradit újmu způsobenou v souvislosti s porušením obecně závazných právních předpisů a porušením této smlouvy, a to v souladu s příslušnými ustanoveními OZ. Obě smluvní strany se zavazují vyvíjet maximální úsilí k předcházení vzniku újmy a k minimalizaci její případné výše.
2. Celková odpovědnost dodavatele za nároky jakéhokoli druhu uplatněné vůči němu objednatelem podle této smlouvy, bez ohledu na jejich právní důvod, tj. včetně uplatněných smluvních pokut dle čl. XI této smlouvy jako paušalizovaných náhrad škody, nesmí přesáhnout částku odpovídající 1,5násobku hodnoty plnění dle této smlouvy. Hodnotou plnění dle této smlouvy se rozumí součet celkových cen Etapy 1 až 3, ceny licencí, Služeb podpory dle čl. V této smlouvy po celou dobu trvání smlouvy, bez DPH. V případě, že součet všech uplatněných smluvních pokut dosáhne této maximální částky, další nároky z odpovědnosti za škodu již nemohou být ze strany objednatele vůči dodavateli uplatněny, s výjimkou případů, kdy bude prokázáno, že porušení příslušné smluvní povinnosti, na kterou se váže náhrada škody, bylo ze strany dodavatele
    a) způsobeno podvodem, úmyslným jednáním a/nebo hrubou nedbalostí dodavatele nebo
    b) bude porušení povinnosti a související náhrada škody souviset s autorskoprávním nebo jiným nárokem plynoucím z právní vady poskytnutého plnění dle této smlouvy nebo
    c) se bude jednat o majetkové škody, které jsou kryty pojistným plněním ve smyslu čl. VIII odst. 1 této smlouvy.*PTK
3. Žádná ze smluvních stran není povinna hradit újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany, pokud druhou stranu na nesprávnost takového zadání předem upozornila.
4. Smluvní strana (dále v tomto článku též jako „**škůdce**“) je zproštěna povinnosti poskytnout náhradu škody vzniklé v důsledku liberačních důvodů ve smyslu § 2913 odst. 2 OZ.
5. Pro účely této smlouvy se "liberačními důvody" rozumí mimořádná, nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na vůli škůdce, která dočasně nebo trvale zabránila ve splnění smluvní povinnosti škůdce. Překážka vzniklá z osobních poměrů škůdce nebo vzniklá v době, kdy byl škůdce v prodlení s plněním své smluvní povinnosti, nebo překážka, kterou byl škůdce povinen podle této smlouvy překonat, jej nezbavuje povinnosti k náhradě škody.
6. Pokud je zřejmé, že v důsledku skutečností uvedených v odstavci 5 tohoto článku nebude škůdce schopen splnit své závazky v dohodnuté lhůtě, oznámí to bez

zbytečného odkladu druhé smluvní straně. Smluvní strany mezi sebou případ projednají a rozhodnou o případném postupu. Nedojde-li k takové dohodě, má kterákoli ze smluvních stran právo od této smlouvy odstoupit, pokud od vzniku liberačních důvodů bránících plnění uplynuly více než tři měsíce a vadný stav trvá.

7. Pokud se vyskytne případ liberačních důvodů, strana, která se liberačních důvodů dovolává, poskytne druhé straně dokumenty týkající se tohoto případu.

Článek XIII.

Rozhodné právo, řešení sporů

1. Tato smlouva se řídí právním řádem České republiky, zejména OZ, ZZVZ a rovněž příslušnými ustanoveními Autorského zákona.
2. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této smlouvy. Nedohodnou-li se smluvní strany na řešení vzájemného sporu, má každá ze smluvních stran právo uplatnit svůj nárok u příslušného soudu v České republice; pravomoc soudu jiného státu je vyloučena. Smluvní strany se dohodly, že příslušným soudem pro řešení sporů vzniklých mezi smluvními stranami z této smlouvy je obecný soud dle sídla objednatele.

Článek XIV.

Trvání smlouvy

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv.
2. **Tato smlouva se uzavírá na dobu určitou, a to do splnění závazků smluvních stran podle této smlouvy.**
3. Před uvedenou dobou je možné tuto smlouvu ukončit:
    a. písemnou dohodou na základě shodné vůle obou smluvních stran;
    b. odstoupením od smlouvy ve smyslu § 2001 a násl. OZ za podmínek níže uvedených v případě porušení této smlouvy druhou smluvní stranou podstatným způsobem anebo v dalších případech uvedených v této smlouvě;
    c. odstoupením od smlouvy ze strany objednatele v případě, že v průběhu předimplementační analýzy v rámci Etapy 1 ve smyslu čl. II odst. 5 bodu 5.1 této smlouvy, bude zjištěno, že dodavatel není schopen zajistit požadované parametry systému IdM a/nebo PAM v prostředí objednatele dle přílohy č. 1a této smlouvy.
    d. vypovědí bez výpovědní doby, nelze-li v plnění dle této smlouvy pokračovat, aniž by bylo porušeno opatření obecné povahy vydané ze strany NÚKIB, zejména protiopatření ve smyslu § 20 ZoKB.
4. Strany sjednávají, že vznikne-li objednateli nárok na odstoupení od této smlouvy, může podle své volby odstoupit od této smlouvy v celém rozsahu či jen od některé části plnění určené objednatelem.

5. Strany se dohodly na vyloučení použití § 1978 odst. 2 a § 2595 OZ.
6. Smluvní strany se dohodly, že kromě důvodů vymezených OZ považují za podstatné porušení smlouvy zejména tyto případy:
    a. dodavatel je v prodlení ve kterékoliv lhůtě dané Harmonogramem dle čl. III odst. 1 této smlouvy nebo dílčí smlouvou delším než 30 dnů;
    b. plnění nebo jednotlivé části bylo/y dodáno/y s vadami, které jsou neopravitelné/neodstranitelné nebo s jejichž opravou by byly spojeny nepřiměřené náklady nebo jejichž oprava by trvala nepřiměřeně dlouho;
    c. dodavatel přes písemné upozornění provádí svoje práce neodborně nebo v rozporu s touto smlouvou;
    d. ohledně dodavatele byl podán insolvenční návrh, bylo rozhodnuto o úpadku dodavatele nebo bude ve vztahu k dodavateli vydáno jiné rozhodnutí s obdobnými účinky;
    e. bylo-li rozhodnuto o likvidaci dodavatele, popř. bylo-li rozhodnuto o zrušení dodavatele bez likvidace;
    f. dodavatel neoznámil objednateli skutečnosti dle poslední věty čl. V odst. 14 této smlouvy;
    g. dodavatel poruší povinnosti vyplývající z čl. X této smlouvy;
    h. porušení povinnosti dodavatele dle čl. VIII odst. 1 této smlouvy;
    i. pokud dodavatel opakovaně nedodrží reakční doby dle čl. IX odst. 5 této smlouvy, a to ani v dodatečné přiměřené lhůtě, která byla dodavateli objednatelem v písemném upozornění poskytnuta. Opakovaným nedodržením se rozumí nejméně druhé nedodržení reakční doby nebo doby vyřešení o více než 24 hodin oproti parametrům stanoveným v čl. IX odst. 5 této smlouvy. Možnost odstoupení z důvodů nedodržení reakčních dob dle první věty tohoto odstavce platí pouze v případě, že součástí plnění dle této smlouvy bude dodávka HW, resp. dodavatel bude zajišťovat podporu na HW dle čl. IX odst. 4 této smlouvy.
    j. pokud dodavatel opakovaně nedodrží parametry SLA dle přílohy č. 5 této smlouvy, a to ani v dodatečné přiměřené lhůtě, která byla dodavateli objednatelem v písemném upozornění poskytnuta. Opakovaným nedodržením parametrů SLA se rozumí nejméně druhé nedodržení Reakční doby nebo Doby vyřešení o více než 24 hodin oproti stanoveným parametrům SLA.
    k. ocitne-li se objednatel v prodlení s úhradou řádně vystavené faktury (daňového dokladu) o více než 30 dní oproti termínu její splatnosti.
7. Právo na náhradu škody, případně nárok na smluvní pokutu či úrok z prodlení odstupující smluvní strany není dotčeno.
8. Oznámení o odstoupení od této smlouvy musí být učiněno písemně, musí v něm být uveden důvod odstoupení a musí být doručeno druhé smluvní straně. Oznámení o odstoupení od této smlouvy musí být odesláno doporučeně prostřednictvím dodavatel poštovních služeb nebo prostřednictvím datové zprávy. V případě pochybností o dni doručení se v případě doporučování prostřednictvím dodavatele poštovních služeb za den doručení považuje 3.

pracovní den po podání oznámení o odstoupení k odeslání provozovateli poštovních služeb. Účinky odstoupení od této smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

9. V případě odstoupení jsou si smluvní strany povinny vypořádat vzájemné závazky, a to nejpozději ve lhůtě 30 dní od ukončení této smlouvy.

10. V případě jakéhokoliv ukončení smlouvy je dodavatel povinen poskytnout objednateli nebo objednatelem určené osobě maximální nezbytnou součinnost za účelem plynulého a řádného ukončení činností dle této smlouvy či jejich příslušné části tak, aby objednateli nevznikla škoda. Dodavatel se současně zavazuje předat objednateli relevantní dokumentaci. Povinnosti dodavatele jsou podrobněji uvedeny v kapitole 4.2 přílohy č.1a, která blíže popisuje pravidla a služby exitu.

Článek XV.

Společná a závěrečná ustanovení

1. Smluvní strany se dohodly, že jakékoliv změny a doplňky této smlouvy jsou možné pouze písemnými dodatky takto označovanými, číslovanými vzestupnou řadou a po dohodě obou smluvních stran, to neplatí v případě změny zmocněnců pro jednání smluvní a ekonomická, či zmocněnců pro jednání věcná a technická, uvedených v záhlaví této smlouvy, pro jejichž změnu se smluvní strany shodly, že postačí jednostranně písemně oznámit druhé smluvní straně a dále v případě změny poddodavatelů dle čl. VIII odst. 17 této smlouvy, v případě změny členů realizačního týmu dle čl. VIII odst. 16 této smlouvy a případů dle odstavce 2 tohoto článku.

2. Komunikace mezi smluvními stranami může kromě příslušných zmocněnců uvedených v záhlaví této smlouvy rovněž probíhat prostřednictvím dalších osob, které k tomu strany v jednotlivém případě nebo pro určitý okruh případů pověří. Osobou dle první věty tohoto odstavce může být i osoba odlišná od smluvních stran nebo zaměstnanců smluvních stran. Smluvní strana je v případě pověření osoby dle první věty tohoto odstavce, včetně informace, pro jaké případy je taková osoba oprávněna za stranu komunikovat, povinna toto písemně včetně e-mailové komunikace oznámit druhé straně; přičemž oznámení je účinné dnem jeho doručení druhé straně. Smluvní strany výslovně uvádějí, že o oznámeních nebo změnách dle tohoto odstavce není nutné uzavírat dodatek k této smlouvě. Oznámení dle tohoto odstavce se v případě pochybností považují za doručená pět dnů po jejich prokazatelném odeslání.

3. Jakákoli oznámení, která mají být dle této smlouvy doručena smluvní straně, budou považována za řádně doručená, pokud budou adresována smluvní straně na adresu uvedenou v záhlaví této smlouvy a mohou být zaslána poštovní zásilkou nebo elektronickou poštou, resp. datovou zprávou do datové schránky, není-li ve smlouvě stanoveno jinak. Nebude-li však dohodnuto jinak, písemnosti, s jejichž doručením je spojen vznik určité právní skutečnosti, která má podle této smlouvy vliv na vznik, trvání nebo zánik práv a povinností smluvních stran, budou doručovány pouze doporučenou poštovní zásilkou na adresu sídla smluvní strany nebo datovou zprávou do datové schránky. V případě změny adresy je smluvní strana, u které ke změně adresy došlo, povinna tuto změnu písemně sdělit druhé smluvní straně doporučeným dopisem zaslaným na adresu uvedenou na titulní straně této smlouvy nebo datovou zprávou zaslanou do datové schránky.

4. Smluvní strany výslovně prohlašují, že si nepřejí, aby nad rámec výslovných ustanovení této smlouvy jakákoliv práva a povinnosti dovozovány z budoucí praxe zavedené mezi smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této smlouvy, ledaže je v této smlouvě výslovně stanoveno jinak. Zároveň smluvní strany prohlašují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.
5. Dodavatel zaručuje, že předmět plnění není zatížen právy třetích osob.
6. Práva a povinnosti vyplývající z této smlouvy nelze bez předchozího písemného souhlasu druhé smluvní strany převést na třetí stranu.
7. Tato smlouva je za podmínek v této smlouvě uvedených závazná i pro případné právní nástupce smluvních stran.
8. Je-li nebo stane-li se některé ustanovení této smlouvy neplatné či neúčinné, nedotýká se to ostatních ustanovení této smlouvy, která zůstávají platná a účinná. Smluvní strany se v tomto případě zavazují nahradit neplatné/neúčinné ustanovení ustanovením platným/účinným, které nejlépe odpovídá původně zamýšlenému účelu ustanovení neplatného/neúčinného. Ukáže-li se některé ustanovení této smlouvy zdánlivým (nicotným), posoudí se vliv této vady na ostatní ustanovení této smlouvy obdobně podle § 576 OZ.
9. Dodavatel tímto prohlašuje, že dodržuje základní lidská práva a všeobecně uznávané etické a morální standardy v souladu s Všeobecnou deklarací lidských práv (dále jen „Práva“). V případě, že se objednatel hodnověrným a prokazatelným způsobem dozví, že ze strany dodavatele došlo nebo dochází k porušení Práv, a dodavatel i přes předchozí písemné upozornění objednatele pokračuje v porušování Práv nebo nezjedná nápravu, má objednatel právo odstoupit od této smlouvy za podmínek uvedených v čl. XIV této smlouvy.
10. Dodavatel dále prohlašuje, že při plnění této smlouvy bude dodržovat spravedlivé pracovní podmínky a uznávat a zajišťovat práva zaměstnanců v souladu s pracovněprávními předpisy a předpisy o bezpečnosti práce platnými v zemi, ve které je předmět této smlouvy plněn. Dodavatel podpisem této smlouvy prohlašuje, že dodržuje povinnosti uvedené v tomto odstavci a zavazuje se je dodržovat po celou dobu trvání této smlouvy. V případě, že se objednatel hodnověrným a prokazatelným způsobem dozví, že ze strany dodavatele došlo nebo dochází k nesplnění povinností dle věty první tohoto odstavce, a dodavatel i přes předchozí písemné upozornění objednatele pokračuje v neplnění těchto svých povinností nebo nezjedná nápravu, má objednatel právo odstoupit od této smlouvy za podmínek uvedených v čl. XIV této smlouvy
11. Smlouva je vyhotovena v elektronické podobě, přičemž obě smluvní strany obdrží její elektronický originál opatřený kvalifikovanými elektronickými podpisy odpovědné osoby a opatřený kvalifikovaným elektronickým časovým razítkem podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů. V případě, že tato smlouva z jakéhokoli důvodu nebude vyhotovena v elektronické podobě, bude sepsána a podepsána ve dvou vyhotoveních, přičemž každá ze smluvních stran obdrží jedno vyhotovení.
12. Smluvní strany berou na vědomí, že tato smlouva bude v souladu § 219 odst. 1 písm. d) ZZVZ uveřejněna v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru

smluv), ve znění pozdějších předpisů. Uveřejnění zajistí objednatel.

13. Smluvní strany prohlašují, že si tuto smlouvu přečetly, souhlasí s jejím obsahem, že tato smlouva byla sepsána určitě, srozumitelně, na základě jejich pravé, svobodné a vážné vůle, bez nátlaku na některou ze stran. Na důkaz toho připojují své podpisy.

14. Nedílnou součástí této smlouvy jsou přílohy:

- Příloha č. 1: Technická specifikace, jež se skládá z následujících částí:
  - část 1a: Technické požadavky (zadavatel doplní podobu přílohy dle nabídky vybraného dodavatele v souladu s čl. 15.5.1 této ZD)
  - část 1b: Koncové systémy a počet uživatelů
- Příloha č. 2: Návrh technického řešení dodavatele včetně položkových seznamů komponent (účastník předloží v rámci Nabídky v souladu s čl.15.5.2, 15.5.3 a 15.5.4 této ZD), který se skládá z následujících částí:
  - část 2a: Návrh technického řešení pro systém IdM
  - část 2b: Návrh technického řešení pro systém PAM
- Příloha č. 3: Harmonogram
- Příloha č. 4: Podrobný rozpad ceny a licencí
- Příloha č. 5: Požadavky na provoz řešení a SLA
- Příloha č. 6: Akceptační protokol (vzor) *(k budoucí úpravě dle faktického stavu)*, jež se skládá z následujících částí:
  - část 6a: Akceptační protokol bez výhrad (vzor) *(k budoucí úpravě dle faktického stavu)*
  - část 6b: Akceptační protokol s výhradami (vzor) *(k budoucí úpravě dle faktického stavu)*
  - část 6c: Zápis o neakceptaci (vzor) *(k budoucí úpravě dle faktického stavu)*
  - *část 6d: Předávací protokol* (vzor) *(k budoucí úpravě dle faktického stavu)*
  - Příloha č. 7: Realizační tým (zadavatel doplní podobu přílohy dle nabídky vybraného dodavatele v souladu s čl. 10.5.2 této ZD)
- Příloha č. 8: Definice pojmů a zkratek

Za objednatele:	Za dodavatele:
V Praze dne _____	V _____ dne _____
_____	_____
Mgr. Marek Šimandl, MPA	**[zadavatel doplní údaje vybraného dodavatele dle nabídky**
generální ředitel	
Státní tiskárna cenin, s. p.	

Technická specifikace

1 Úvod

1.1 Účel dokumentu

Účelem tohoto dokumentu je definovat požadavky na dodávku a implementaci systémů IdM a PAM do prostředí objednatele, včetně integrace s vybranými systémy objednatele a dodání příslušných licencí k IdM a PAM, a to včetně technické podpory na dobu uvedenou v této Technické specifikaci a ve Smlouvě. Jedním z klíčových bodů implementace IdM a PAM je jejich vzájemná integrace, která vyplývá z požadavků uvedených dále.

Tento dokument, dále rovněž „Technická specifikace“, byl součástí zadávací dokumentace zadávacího řízení s názvem *Služby poskytování implementace a podpory IDM a PAM (dále jen „Zadávací řízení“)* a je přílohou č. 1a Smlouvy na dodávku, implementaci a podporu systému pro správu identit (IdM) a systému pro řízení privilegovaných účtů (PAM) (výše a dále také jen „Smlouva“), která byla uzavřena na základě výsledku zadávacího řízení.

1.2 Záměr STC v oblasti řízení identit a privilegovaných účtů

Implementace systémů PAM a IdM a jejich napojení na aktiva objednatele je v souladu s dlouhodobou koncepcí řízení privilegovaných účtů, řízení identit a přístupových oprávnění, jejich kontroly a zvýšení zabezpečení přístupů ke správě aktiv Státní tiskárny cenin, s.p. (dále jen „STC“).

1.2.1 Konkrétní cíle

- Centralizace správy identit a datové oddělení procesní správy životního cyklu identit od cílových systémů
- Zajištění jednoho referenčního zdroje pro všechny identity IdM.
- Eliminace roztříštěných a nejednotných evidencí identit v různých systémech
  - **Automatizace životního cyklu identit**
    - Automatizace procesů při nástupu, změně a výstupu zaměstnance.
    - Minimalizace manuálních zásahů IT útvaru.
    - Zajištění rychlé reakce na změny v HR systému.
    - Automatizace schvalovacích procesů.
    - Jednoznačná odpovědnost za konkrétní přístupová oprávnění.
  - **Zvýšení bezpečnosti a souladu s legislativou**
    - Zajištění, že přístupy mají pouze oprávněné osoby v nezbytném rozsahu.
    - Okamžitá deaktivace přístupů při ukončení pracovního poměru.
    - Podpora auditní dohledatelnosti a souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDRP“), ISO 27001 a dalšími předpisy.
    - Splnění legislativních požadavků vyplývajících ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“), zákona č. 266/2025 Sb., o kritické infrastruktuře, vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností a dalších relevantních právních předpisů.
    - Řízení, monitorování, zabezpečení a audit všech lidských i automatizovaných privilegovaných identit a činností při správě systémů STC.
    - Ochrana před hrozbami krádeže privilegovaných účtů a zneužití privilegovaných oprávnění.
  - **Efektivní řízení přístupových oprávnění**
    - Nastavení pravidel pro přiřazování přístupů dle rolí, útvarů a pozic.

    - Zajištění pravidelné recertifikace oprávnění (pravidelný audit přístupů).
    - Zajištění systematické a strukturované správy privilegovaných identit a účtů a na ně navázaných privilegovaných přístupů ke správě ICT systémů.
  - **Zlepšení uživatelského komfortu**
    - Podpora jednotného přihlašování (SSO) do IdM.
    - Samoobslužné portály pro správu hesel a žádosti o přístupy.
    - Zjednodušení administrativních procesů pro uživatele i IT útvar.
  - **Podpora správy externistů a nestandardních případů**
    - Zavedení řízeného procesu pro správu externích identit.
    - Řízení přístupů externistů v souladu s bezpečnostní politikou objednatele.
  - **Integrace klíčových systémů**

- Zajištění propojení mezi HR systémem, AD, Microsoft Entra ID (Azure AD), DMS, ERP Cicero a dalšími systémy.

2 Předmět plnění VZ

Předmětem plnění veřejné zakázky, resp. Smlouvy je pořízení a implementace systémů pro správu identit (IdM) a privilegovaného přístupu (PAM) do STC.

2.1 Požadavky na rozsah plnění

Celková aktivita implementace systémů IdM a PAM v prostředí objednatele musí být provedena ve třech etapách:

- **Etapa 1:** implementace systému IdM a jeho napojení na aktiva definovaná v Příloze č. 1b Smlouvy bod 1.1.
- **Etapa 2:** implementace systému PAM a jeho napojení na aktiva definovaná v Příloze č. 1b Smlouvy bod 1.4.
- **Etapa 3:** napojení dalších aktiv definovaných v Příloze č. 1b Smlouvy bod 1.2.

Pro naplnění předmětu plnění veřejné zakázky objednatel požaduje dodávku a nasazení řešení v následujícím rozsahu (níže uvedené požadavky jsou dále rozpracovány v kapitolách níže):

- Příprava předimplementační analýzy pro všechny jednotlivé Etapy 1 až 3;
- Implementace systémů IdM a PAM a jejich napojení na požadované zdrojové a koncové systémy;
- Poskytnutí potřebných licencí IdM a PAM a dalších licencí potřebných k provozu implementovaných řešení, vyjma licencí k externím notifikačním službám (např. SMTP, SMS brána) a software/platforem objednatele, které jsou uvedené v bodě 4.1 Technické specifikace a které nejsou součástí dodávky;
- Výrobcem vyžadované speciální HW komponenty pro PAM (např. fyzické/virtuální vault/PSM appliance, HSM, KVM/serial console, MFA/PKI prvky, WORM/immutable úložiště pro nahrávky) jsou součástí dodávky systémů, pokud jsou uvedeny v technické specifikaci výrobce. Dodavatel dále v rámci dodávky dodá veškeré výrobcem doporučené komponenty, kterou jsou potřebné pro provoz řešení dle jeho Nabídky a v souladu se Zadávací dokumentací Zadávacího řízení. *PTK Veškerý dodávaný HW se stává majetkem STC a musí být dodán včetně podpory a záruky celého řešení po celou dobu trvání smlouvy v rámci dostupnosti systému viz příloha č. 5 (Požadavky na provoz řešení);
- Dokumentace implementovaných systémů (dokumentace skutečného provedení, administrátorská dokumentace a uživatelská dokumentace);
- Školení, školící materiály a dodání podkladů pro HR adopční kampaň;
- Testovací provoz;
- Nasazení do ostrého provozu (go-live);
- Podpora implementovaných systémů a jejich licenční zajištění po celou dobu trvání smlouvy – viz kap. 7.6 a 7.7;
- Ad hoc služby (rozvoj) – viz kap. 7.8;
- Poskytnutí služeb exitu – viz. kap. 4.2.

2.2 Oblasti, které nejsou předmětem plnění VZ

Pro vyloučení pochybností objednatel uvádí, že následující oblasti nejsou předmětem plnění veřejné zakázky, resp. Smlouvy:

- Úprava systémů třetích stran, u nichž bude probíhat napojení na IdM a PAM (vyjma součinnosti pro analýzu a technické podpory při integraci a testech integračních/koncepčních vazeb; tyto činnosti budou čerpány z fondu Služby na vyžádání).
- Dodávka uživatelských licencí pro AD.
- HW vybavení a obecné OS pro provoz IdM a PAM; výjimkou je dodání a základní konfigurace předpřipravených virtuálních appliance (OVA/OVF) pro IdM a/nebo PAM včetně jejich embedded/base OS. Objednatel poskytne virtualizační platformu (např. VMware vSphere/ESXi), síť, IP adresy, úložiště a zálohovací politiku.

- HW/SW pro ukládání a archivaci relací (session recording), pokud není výslovně uvedeno jinak v technické specifikaci.

3 Současný stav (ke dni uzavření Smlouvy)

Současný stav (ke dni uzavření Smlouvy) správy identit a přístupů ve společnosti STC je založen na stabilní a moderní IT infrastruktuře, která zahrnuje klíčové systémy jako HR systém OKbase, Microsoft Active Directory, DMS a ERP systém CICERO. Všechny uvedené systémy jsou provozovány pouze on-premise a jedinou výjimku tvoří hybridní cloudové řešení Microsoft 365 včetně synchronizace s Microsoft Entra ID. Objednatel využívá automatizované procesy pro správu uživatelských účtů, přidělování základních oprávnění a správu organizační struktury, přičemž HR systém OKbase slouží jako primární zdroj identit zaměstnanců. V rámci současného prostředí je kladen důraz na efektivní spolupráci mezi IT, HR a bezpečnostním útvarem, a to včetně digitalizovaných workflow v DMS pro procesy nástupu a výstupu zaměstnanců.

Přestože je prostředí dobře nastaveno a využívá moderní technologie, objevují se oblasti, kde je prostor pro další optimalizaci a zvýšení efektivity. Patří sem například automatizace a centralizace správy externistů, zjednodušení procesů přidělování a odebrání přístupových práv, zlepšení evidence oprávnění a auditovatelnosti procesů, nebo integrace ERP systému CICERO s centrální autoritou identit. Tyto výzvy představují přirozenou příležitost pro další rozvoj a zvyšování kybernetické bezpečnosti prostřednictvím implementace systému Identity Management a Privileged Access Management.

Cílem je zachovat stávající výhody, jako jsou robustní infrastruktura, automatizované procesy a transparentní workflow, a zároveň využít potenciál IdM a PAM k ještě větší efektivitě, bezpečnosti a přehlednosti správy identit a přístupů ve společnosti.

3.1 Personální základna

- **Počet zaměstnanců:** cca 300–400
- **Počet členů IT týmu:** vlastní interní IT útvar (10 lidí)
- **Externí Dodavatelé služeb:** v rozsahu cca 50 identit

3.2 IT infrastruktura

Hardwarová infrastruktura

- Fyzické servery ve vlastních serverovnách s dostatečnou redundancí
- Redundantní LAN infrastruktura
- Redundantní SAN infrastruktura
- Redundantní víceúrovňová NEXT-GEN FW infrastruktura

Virtualizace

- VMware vSphere 8
- Redundance přes HA cluster, failover řešení

Softwarová infrastruktura

- **Adresářová služba:** Windows Server 2016/2022 synchronizace s Microsoft Entra ID (Azure AD)
- **Active Directory pro správu identity a přístupu** (uživatelské účty, GPO)
- **Entra ID pro správu M365 účtů**
- **SharePoint On-Prem pro interní dokumenty a workflow**
- **ERP systém CICERO pro řízení provozu**
- **Tiskové servery a řízení tisku přes SafeQ**

3.3 Active Directory

Objednatel využívá lokální AD s napojením na cloud řešení MS Azure do systému MS Entra ID. MS Entra ID je využívána primárně z důvodu řízení M365 uživatelů. Lokální AD slouží jako centrální autorita pro

autentizaci uživatelů, ale neplatí to pro všechny systémy. Například ERP systém CICERO má zavedeny lokální uživatele a ti se autentizují proti lokální databázi.

3.3.1 Technická architektura

- V prostředí STC existuje jedna doména
- Doména běží na Windows Server 2016/2022
- Virtualizace pomocí VMware 8
- AD je on-premise a je replikováno do systému Entra ID pomocí Microsoft Entra connect
- Standardní schéma atributů v AD
- Skupiny v AD reflektují organizační strukturu
- Organizace pracuje s dvěma podstromy OU
- Strukturou účtů a skupin
- Strukturou DMS skupin

3.3.2 Synchronizace a propojení

- Synchronizace do cloudu pomocí Entra ID Connect
- Synchronizovány jen vybrané OU

3.3.3 Připojené služby

- **Microsoft 365 (M365):** správa licencí M365, Teams, OneDrive
- **Exchange:**
- V hybridním režimu (Exchange online a on-premise)
- mailové schránky, sdílené mailboxy a aliasy
- **DMS:** žádosti o přístup/M365, schvalování

3.3.4 Vytváření a správa účtů

Účty se zakládají automatizovaně skriptem při nástupu. Účet je vytvořen, script automaticky pošle heslo do fronty nového uživatele na tiskárnu. Uživatel si heslo vyzvedne po přihlášení osobní přístupovou kartou.

Je nastavena vynucená změna hesla při prvním přihlášení a resetu hesla. Neaktivní uživatelé jsou přesouváni do separátního OU, po retenční lhůty jsou automaticky mazáni. Stejný proces je reflektován v Entra ID. Výjimku tvoří uživatelé na mateřské/rodičovské dovolené (MD/RD) a dlouhodobé nepřítomnosti, ti se nemažou.

3.3.5 Struktura OU (Organizačních jednotek)

OU struktura reflektuje organizační schéma z HR systému OKbase.

Použitý model: víceúrovňová hierarchie, např.:

```
/Useky/
    /Usek1/
        /User/
            /Utvar1/
        /Computer/
        /Groups/
        /Contacts/
```

Používá se cca 250 OU s vnořenými OU, cca 1-6 úrovní.

3.3.6 Atributy a jejich správa

Atributy se dělí do 3 kategorií (podle úrovně automatizace a zdroje), typicky:

- **Předávané z HR systému (OKbase):** např. jméno, příjmení, nástup, pozice, nadřízený apod.
- **Custom atributy**: např. typ MS licence, tyto jsou upravovány dalším skriptem na základě HR dat.
- Ručně spravované atributy.

3.4 Exchange

Objednatel provozuje lokální Microsoft Exchange v hybridním režimu s napojením na Microsoft 365. Aktuálně ve verzi 2016, kdy se přepokládá nejpozději do konce roku 2025 přechod na verzi Microsoft Exchange SE.

3.4.1 Technická architektura

- V prostředí STC existuje jeden Microsoft Exchange server.
- OS Windows Server 2016, kdy do konce roku 2025 se bude jednat o Windows Server 2022.
- Běží ve virtuálním prostředí jako VM.

3.4.2 Synchronizace a propojení

- Synchronizace do cloudu pomocí Entra ID Connect.

3.4.3 Připojené služby

- Microsoft Exchange Online.

3.4.4 Instance a prostředí

Systém je provozován v jedné instanci:

- Produkční prostředí

3.5 HR systém

3.5.1 Obecná charakteristika systému

Objednatel provozuje HR systém OKbase, který představuje lokálně provozovaný HR informační systém pro komplexní správu zaměstnaneckých údajů a agend. Primárním zdrojem identit pro interní zaměstnance je HR systém, identity externistů budou zakládány a **spravovány v IdM** a následně přenášeny do AD. Veškeré klíčové změny v životním cyklu zaměstnance (nástup, změna, ukončení, změna úvazku, MD/RD) jsou v OKbase zaznamenány a automatizovaně přenášeny do IdM, které následně provádí potřebné úkony v navazujících systémech.

HR Systém eviduje organizační strukturu společnosti. Organizační struktura obsahuje organigram a lze z ní určit podřízenost zaměstnanců. Organizační struktura je načítána pomocí scriptu, který zajistí automatické přiřazování organizačních rolí na základě zařazení uživatele ve struktuře.

3.5.2 Technická architektura

- Lokální provoz HR systému
- Data uložena v SQL databázi vhodné pro integraci
- V současnosti neexistuje nativní API

3.5.3 Evidované typy osob a úvazků

Systém eviduje následující kategorie pracovníků:

- Zaměstnanci v HPP (hlavní pracovní poměr)
- DPP (dohoda o provedení práce)

- DPČ (dohoda o pracovní činnosti)
- Externisté nejsou evidováni – zakládají se přímo v AD manuálně. Nově požadujeme, aby byli externisté zakládáni a spravováni v IdM.

3.5.4 Klíčové funkce a vlastnosti systému

Jedinečná identifikace

Každému zaměstnanci je přiřazeno osobní číslo, které je neměnné a zůstává zachováno i při opakovaném nástupu do organizace.

Správa zaměstnaneckých stavů

Systém rozlišuje mezi:

- Aktivními zaměstnanci
- Zaměstnanci vyňatými z evidenčního stavu (MD/RD, neplacené volno)
- Neaktivními zaměstnanci (nastoupí, odešel…)

3.5.5 Vícenásobné úvazky

Systém umožňuje evidenci více pracovních úvazků současně (např. kombinace HPP a DPP/DPČ). Objednatel umožňuje souběh více úvazků např. při mateřské dovolené a vedlejšího úvazku.

3.5.6 Identifikační atributy zaměstnanců

Systém uchovává nejméně následující klíčové atributy:

- **Osobní číslo**: Unikátní, neměnný identifikátor
- **Jméno a příjmení**
- **Číslo PPV (více pracovních vztahů u jednoho zaměstnance)**
- **Typ pracovního poměru**: HPP/DPP/DPČ/statutáři
- **Evidenční stav**: /MD/RD/neplacené volno/aktivní/…
- **Útvar:** Podle organizační struktury
- **Manažer**: Vedoucí podle organizační struktury
- **Pracovní pozice**: Zařazení na pracovní pozici
- **Organigram**: Umístění v organigramu
- **Datum nástupu**: Datum začátku kontraktu podle smlouvy
- **Datum ukončení**: Pro plánované a proběhlé deaktivace
- **Čísla ID karty**: Pro fyzický přístup, dávkový přenos

3.5.7 Procesy nástupu a výstupu

Proces nástupu je částečně automatizován, výstupy jsou řízeny ručně a vyžadují manuální potvrzení několika nadřízených. Správa speciálních stavů (např. MD/RD) není automatizovaná.

Poznámka: Login a e-mail se negeneruje přímo v HR systému, ale vytváří je script na straně IT útvaru na základě dat z HR systému.

3.5.8 Správa externistů a výjimky

Externisté nejsou evidováni v HR systému a dříve se zakládali ručně v AD. Vznik účtů mimo OKbase probíhá cca 1× měsíčně přes workflow v DMS.

3.5.9 ID karty

Bezpečnostní útvar vede v **offline systému** kompletní evidenci přístupových karet včetně **auditní stopy** (kdo, kdy vydal/vrátil – nástup/výstup). Tento stav je **automatizovaně přenášen do OKbase**.

3.6 DMS

3.6.1 Současný stav autentizace a integrace s AD

DMS je plně integrován s AD a využívá AD pro autentizaci uživatelů. V rámci AD existuje samostatný organizační strom specificky pro DMS, který odráží strukturu organizace a jsou v ní umístěny skupiny pro DMS.

3.6.2 Technická architektura

- Systém běží na on-premise SharePoint platformě s nadstavbou spisové služby od společnosti Allium, s.r.o.
- Jednou denně probíhá synchronizace SharePoint listu z AD.
- Uživatelé s vyššími oprávněními jsou spravováni prostřednictvím SharePoint skupin.

3.6.3 Technické možnosti integrace

Systém využívá SharePoint platformu, která poskytuje standardní možnosti integrace s AD.

3.6.4 Instance a prostředí

Systém je provozován ve třech instancích:

- Produkční prostředí
- Testovací prostředí
- Vývojové prostředí

3.6.5 Správa přístupových práv

Řízení přístupu v DMS je kompletně založeno na skupinách z AD. Systém reflektuje firemní strukturu a využívá následující mechanismy:

- **Základní oprávnění:** řízena prostřednictvím AD skupin
- **Vyšší oprávnění:** spravována skrze SharePoint skupiny, které mohou být naplňovány AD skupinami
- **Automatická synchronizace:** SharePoint list si denně stahuje data z AD kvůli spisové službě, která nemá přímý přístup k AD

3.6.6 Uživatelská základna a životní cyklus účtů

Počet uživatelů: Maximální počet odpovídá všem zaměstnancům organizace

3.6.7 Správa uživatelských účtů

- Proces založení, zrušení a správy oprávnění uživatelů v aplikaci neexistuje ve formalizované podobě.
- Řízení probíhá prostřednictvím AD skupin a SharePoint skupin. Ale přístup k dokumentu je také možné získat napřímo ručním předáním ve spisové službě, nebo automaticky systémem díky účasti ve schvalovacím/ připomínkovacím workflow.
- Systém je role-based s řízením na úrovni skupin.

3.7 ERP CICERO

CICERO je ERP systém vyvíjený společností CICERO Stapro Group s.r.o. Jedná se o jeden z hlavních systémů pro řízení ve společnosti STC a plánuje se jeho další rozvoj (doplnění dalších modulů).

3.7.1 Současný stav přihlašování a autentizace

CICERO v současnosti není žádným způsobem napojeno na Active Directory. Z tohoto pohledu se jedná o autonomně řízený systém na základě manuální správy.

Systém má dvě uživatelská rozhraní:

1. **Tlustý klient (aplikace na PC)** – například pro modul fakturací. Přihlašování jménem a heslem (lokální autentizace).
2. **Tenký klient (web)** – například pro moduly výroby, ale i moduly využívané pracovníky mimo výrobu. Přihlašování jménem a heslem nebo čipovou kartou (lokální autentizace).

Přihlašování probíhá dvěma způsoby podle typu uživatele:

1. **Výrobní zaměstnanci**: Přihlašování prostřednictvím karet do JSU (PC ve výrobě) prostřednictvím tenkého klienta. Autentizace pomocí karty je implementována přímo v systému CICERO.
2. **Kancelářští zaměstnanci**: Přihlašování pomocí uživatelského jména a hesla. Používají jak tlustého, tak tenkého klienta dle toho, které funkce/moduly systému CICERO využívají.

3.7.2 Organizační struktura a správa uživatelů

Entity, role a pravá v systému:

- Entita
- Zaměstnanec: všichni pracovníci STC – manuální zaevidování
- Uživatel: manuálně aktivovaní zaměstnanci s přístupovými právy spadající pod entitu zaměstnanec
- Role
- Pracovní zařazení: manuální přiřazení role uživateli na základě pracovní pozice
- Vykonávané činnosti: manuální přiřazení role uživateli na základě vykonávané činnosti
- Práva: jsou přidělena na roli a prostřednictvím role propůjčena uživateli.

V systému CICERO jsou evidováni všichni zaměstnanci STC, avšak organizační struktura neodpovídá skutečnosti, tedy stavu, jak je evidován v HR systému OKBase. CICERO pracuje s nákladovými středisky. Každá entita „uživatel“ je napojena právě na jednu entitu typu „zaměstnanec“. ID karty je evidováno u entity „uživatel“.

3.7.3 Správa uživatelů a osobních čísel

Uživatelské účty i přístupové karty jsou do systému CICERO zadávány manuálně a ověřují se proti lokálnímu záznamu.

Osobní číslo v CICERO obsahuje předponu z prvních dvou písmen příjmení, z čehož vyplývá, že není shodné s ID zaměstnance v HR systému OKbase. Po konzultaci s výrobcem bylo potvrzeno, že Osobní číslo v CICERO není nikde v systému použito jako hlavní nositel unikátní položky, a tak je možné ho změnit, tedy sjednotit, aby bylo shodné s ID v OKbase.

Ve stávajícím stavu nelze měnit jména existujících uživatelů.

3.8 Aktuální stav řízení privilegovaných účtů

Účty se zakládají a ruší ručně, na základě schválené žádosti. Žádost o založení / zrušení privilegovaného účtu schvaluje vedoucí IT útvaru, případně i další zaměstnanci dle typu aplikace nebo systému a nastaveného workflow (v rámci systému DMS).

Následující tabulka obsahuje přehled hlavních skupin IS s uvedením informace, jakým způsobem jsou privilegované účty těchto skupin IS v současnosti spravovány.

Typ IS	Způsob správy privilegovaných účtů
Microsoft Windows servery	Privilegované účty v rámci Windows serverů (které jsou zařazeny v doméně) jsou spravovány ručně prostřednictvím administračních nástrojů / RSAT na základě schválené žádosti v DMS.

Linux servery	Účty se zakládají a ruší ručně na základě schválené žádosti v DMS prostřednictvím SSH na základě schválené žádosti v DMS.
Síťové prvky	Účty se zakládají a ruší ručně na základě schválené žádosti v DMS. Natavení probíhá přes SSH nebo přes management konzoli, nebo přes webovou management konzoli.
Virtualizační platformy	Účty se zakládají a ruší ručně prostřednictvím administrační konzole na základě schválené žádosti v DMS
Active Directory, Exchange servery	Účty se zakládají a ruší ručně prostřednictvím administračních nástrojů na základě schválené žádosti v DMS.
Další	Ostatní prvky využívají privilegované účty v AD a zařazení do specifických kontejnerů
IS	DMS SharePoint on-premis, ERP Cicero, RIS NET, Helpdeskový systém, Spisová služba, ISDS, OKBase, BNS, Správa certifikátů a časových razítek, MetaServer (vytěžování faktur), Správa www a e-shopu
Infrastruktura	Firewally, VMware, Antivir, LogManager, FlowMon, Veeam, ADDNET, Zabbix, správa serverů, správa diskových polí, telefonní ústředna, Bitwarden, ADDNET, síťová infrastruktura, správa firewallů

Typy privilegovaných účtů, které se aktuálně používají:

- Účty interních a externích uživatelů (tj. administrátorů),
- Sdílené účty,
- Účty aplikací,
- Servisní účty,
- SSH klíče.

3.9 Životní cyklus identit

3.9.1 Zaměstnanci

Identita zaměstnance vzniká automaticky při jeho nástupu, a to na základě informace z HR systému. Ručně je vytvořena žádost v DMS o nastavení přístupových práv dané identitě. Po schválení jsou ručně nastaveny přístupy do požadovaných aplikací a systémů. Obdobný postup se uplatní i v případě odchodu zaměstnance, kdy jsou před ukončením pracovního poměru vygenerovány žádosti o odebrání přístupů a po ukončení pracovního poměru v HR systému dojde k automatickému zablokování účtu v AD.

3.9.2 Externí Dodavatelé

Každý systém má svého garanta. Požádat o přístup externisty může kdokoli, schvaluje Garant aktiva, Manažer kybernetické bezpečnosti a Správce IS.

3.10 Procesy související s privilegovanými účty

V současné době u objednatele chybí jednotné a formalizované procesy související s řízením a používáním privilegovaných účtů napříč jednotlivými ICT a technologiemi. Rovněž neexistuje centrální evidence všech privilegovaných účtů a osob, které k nim mají přístup. Procesy se mohou lišit dle jednotlivých ICT systémů. Cílem objednatele je sjednotit a formalizovat procesy a začít řídit přístup k privilegovaným účtům pomocí technického řešení (PAM).

Účty jsou používány v rámci skriptů a integračních komponent IS, kde mohou být uloženy buď v otevřené formě, nebo v zabezpečeném úložišti.

3.11 Architektura

ICT infrastruktura objednatele je rozmístěna v geograficky oddělených datových centrech, jejichž propojení a rozmístění ukazuje obrázek. Předpokládá se, že infrastruktura PAM řešení bude provozována v obou datových centrech.

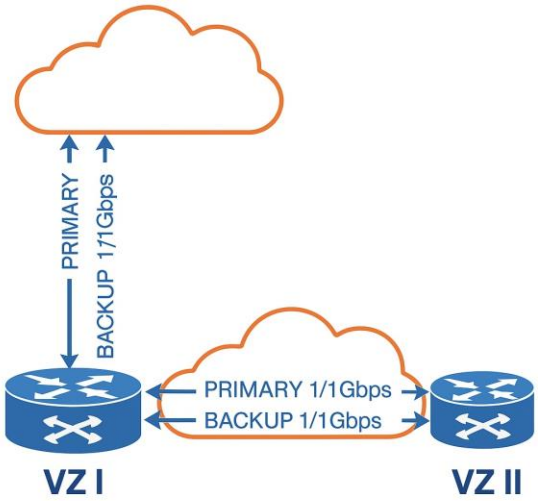

Diagram č. 1: Topologie datových center

Jednotlivé lokality jsou připojeny do společné MPLS sítě. Primární a záložní datové centrum jsou vlastními linkami připojeny do internetu rychlostí 1/1Gbps. Pro zajištění přístupu interních administrátorů a externích Dodavatelů ke spravovaným prvkům je využíván vzdálený přístup pomocí technologie VPN s 2FA/MFA, popř. pomocí externího prostředí bez využití VPN (např. administrace Microsoft 2FA/MFA umístění v MS Azure). VPN typu site-to-site není možná.

3.11.1 Provozní dohled

V rámci ICT prostředí objednatele je vybudován systém provozního monitoringu na technologii Zabbix. Objednatel požaduje využití tohoto dohledového systému pro sledování dostupnosti a vytížení PAM a jeho komponent.

4 Požadavky na celkové plnění dodávky

Kapitola 4 popisuje obecné požadavky na plnění předmětu Smlouvy. Další požadavky na plnění předmětu Smlouvy jsou podrobněji definovány v kapitolách 5 až 10 této Technické specifikace. Pro odstranění pochybností jsou v kapitolách 4 až 10 uvedeny požadavky na dodavatele nezávisle na tom, zda jsou psány v přítomném či budoucím čase.

4.1 Kompatibilita s infrastrukturou objednatele

- **Virtualizace:** VMware vSphere **8.0.3** (vCenter, HA/DRS; podporovány **OVA/OVF** appliance pro IdM/PAM).
- **OS Windows:** Windows Server **Datacenter 2022** a **2025**.
- **OS Linux**:
  - Debian **11.x / 12.x**
  - Red Hat/CentOS **6.x / 7.x.**
- **Adresářové služby:** Microsoft Active Directory (DFL **2012 R2**), LDAPS/Kerberos.
- **Databáze:** Microsoft SQL Server **2022 (16.0.4205.1) – Standard Edition**.
- **Síťová segmentace:** oddělené **DMZ / APP / DB** VLAN
- **Monitoring: Zabbix**
- **Logy / audit: LogManager**
- **Úložiště:** k dispozici **NAS** (NFS/SMB) pro sdílená data a zálohy *(exporty/importy, archivy logů, nahrávky relací)*.
- **Zálohy/DR:** centrální zálohování VM a DB; obnova dle SLA (RTO/RPO).

Maximální dostupná kapacita pro implementaci a nasazení dodávaných systémů:

- **Pro systém IdM**: 2× VM: **12 vCPU, 24 GB RAM, 200 GB SSD**.
- **Pro systém PAM**: 6× VM: **8 vCPU, 16 GB RAM, 150 GB SSD**.
- **Úložiště**: 2× **NAS 2 TB** *(NFS/SMB; pro nahrávky).*PTK*

Souhrnná maximální kapacita:

- 72 vCPU
- 144 GB RAM
- 1,3 TB SSD (diskový prostor virtuálních serverů)
- 4 TB diskového prostoru NAS

Uvedené parametry představují maximální kapacitu virtualizačního a úložného prostředí, kterou objednatel pro provoz systémů IdM a PAM poskytne. Dodavatel je povinen navrhnout architekturu řešení tak, aby nevyžadovala vyšší počet virtuálních serverů ani vyšší výkon (vCPU, RAM, disk) a kapacitu úložiště, než je uvedeno.**PTK*

Objednatel garantuje zajištění vysoce dostupné infrastruktury jako předpokladu implementace a provozu IdM/PAM (redundantní výpočetní uzly, napájení, síťová konektivita a úložiště v režimu HA).

4.2 Pravidla a služby exitu

4.2.1 Bezprostředně po Go-live systému PAM

Nejpozději 1 měsíc po go-live (viz harmonogram Etapa 2: Go-live (F2.7)) je dodavatel povinen vypracovat Exit plán obsahující souhrn podmínek a pravidel nezbytných k dalšímu řádnému užívání systémů

IdM/PAM v případě výměny dodavatele pro podporu implementovaných systémů. Tento Exit plán musí být akceptován minimálně obsahovat:

- aktualizovanou dokumentaci skutečného provedení,
- export všech přiřazených atributů každé identity, včetně jejich hodnot,
- auditní záznamy všech provedených operací související s přidělováním oprávnění u jednotlivých identit,
- popis všech aktuálně využívaných napojení na okolní systémy (API, Rest-API, Web Services, apod.),
- předání Master klíče / built-in administrátora systému PAM.

4.2.2 Při ukončení smluvního vztahu

V případě ukončení smluvního vztahu (ať už řádného či předčasného) se Dodavatel zavazuje bez nároku na dodatečnou odměnu:

- Aktualizovat (případně vytvořit, pokud v momentě ukončení Smlouvy neexistuje) Exit plán do 1 měsíce od doby, co se o ukončení dozvěděl, včetně aktualizace všech částí, exportů, záznamů, klíčů atd. obsažených v Exit plánu (viz. Kapitola 4.24.2.1).
- Provést činnosti uvedené v Exit plánu (služby exitu).
- Poskytnout konzultační služby minimálně v rozsahu 5 MD objednateli a/nebo třetí osobě pro účely možného pokračování jiným dodavatelem.

Přičemž rozsah a podoba Exit plánu bude v případě předčasného ukončení Smlouvy odpovídat tomu v jaké fázi realizace předmětu plnění, byla Smlouva ukončena a z jaké části byl objednateli předmět plnění předán.

5 Požadavky na plnění Etapy 1

5.1 Předimplementační analýza

Z důvodu provázanosti architektury řešení implementovaných v Etapách 1–3 je požadováno, aby předimplementační analýza prováděná v rámci Etapy 1 již obsahovala v potřebném (high-level) detailu analýzu PAM (Etapa 2) a analýzu napojení dalších systémů na IdM (Etapa 3) (dále jen jako „předimplementační analýza“).

Cílem předimplementační analýzy bude zpracovat analýzu obsahující minimálně tyto body:

- Základní popis řešení, technologií a technických konceptů.
- Analýza zdrojových systémů a dat a cílových systémů a způsobů integrace.
- Analýza a návrh provozního modelu v rámci infrastruktury, potřebných zdrojů, sizingu.
- Obecné technické předpoklady a požadavky na realizaci řešení.
- Cílová architektura řešení.
- Požadavky na součinnost objednatele.

Pro implementaci IdM a integrace systémů v Příloze č. 1b, Tabulce A:

- Analýza identit, rolí, procesů a metodik
- Definování business rolí, aplikačních a technických rolí a forem jejich tvorby (příprava migračního plánu do nástroje IdM)
- Návrh procesů správy životního cyklu identit
- Návrh schvalovacích workflow pro napojované systémy a pro jednotlivé businessové a aplikační role
- Návrh postupu pro napojování systémů (bude sloužit jako podklad pro dodavatele těchto systémů k integraci na IdM) pro systémy uvedené v **Příloze č. 1b v Tabulce A**
- Pro zdrojové systémy (OKbase)
- Pro systémy napojené prostřednictvím AD včetně způsobu napojení na MS AD samotné

- Pro koncové systémy napojené přímo na IdM (v rámci rozvojových aktivit)
- Podrobný harmonogram implementace IdM (v rozsahu týkajícím se Etapy 1)
- Osnova, rozsah a harmonogram školení pro administrátory a garanty (klíčové uživatele) zapojených systémů
- Návrh testovacích scénářů a use-caseů, minimálně: UAT, funkční testy, integrační testy, systémové testy, výkonnostní testy, bezpečnostní testy, regresní testy, test výpadku jednoho z datových center
- Návrh metodiky/postupu testování
- Návrh use-caseů (upřesnění use-case proběhne v rámci implementace)

Pro implementaci PAM:

- Architektura řešení s jejím vysvětlením.
- Procesy a služby systému s jejich rozpisem a vysvětlením jejich účelu v rámci řešení.
- Integrační architektura s infrastrukturními a monitorovacími systémy objednatele (Logmanger, SNMP, AD, SMTP, NTP, IdM).
- Popis nakládání s daty, jejich uložení, zabezpečení, ochrana.
- Detailní síťový a komunikační model řešení včetně interní komunikace mezi vnitřními prvky řešení.
- Základní bezpečnostní analýza výchozího stavu, pokrývající minimálně privilegované účty, dlouhodobě neměněná hesla, Pass-the-Hash zranitelnosti a přístupové údaje, s ohledem na jejich dopad na návrh a implementaci PAM řešení.**PTK*
- Návrh řešení, které zamezí administrátorům PAM mít přístup k citlivým informacím, ke kterým mají přístup uživatelé aplikací spravovaných pomocí nástroje PAM (např. informace o mzdách). **PTK*

Pro napojení dalších systémů na IdM uvedených v Příloze č. 1b v Tabulce E:

- Analýza identit, rolí, procesů a metodik.
- Definování business rolí, aplikačních a technických rolí.
- Návrh postupu pro napojování systémů (bude sloužit jako podklad pro dodavatele těchto systémů k integraci na IdM) pro systémy uvedené v **Příloze č. 1b v Tabulce E**.

Obecné požadavky na předimplementační analýzu:

Předimplementační analýza bude objednateli předána ve zdrojových formátech i kompletní PDF formě a bude v českém jazyce. Mohou v ní být použité části v anglickém jazyce, např. ilustrace přímo od výrobce technologie apod., ale s doplňujícím vysvětlením, případně výkladem odborných pojmů v českém jazyce.

Dodavatel je zodpovědný za obsah předimplementačních analýz pro všechny Etapy (1, 2 a 3), jelikož je držitelem know-how nabízených technologií IdM a PAM, a doplní potřebná témata předimplementačních analýz, která dle jeho zkušení a názoru v této Technické specifikaci chybí.

5.2 Implementace a integrace Etapy 1

Cílem této fáze Etapy 1 bude dodávka a implementace systému IdM v prostředí STC a realizace implementací a integrací se zdrojovými systémy a s koncovými systémy vymezenými pro tuto etapu, jejichž uživatelská základna bude spravována pomocí nástroje IdM. Součástí milníku je i migrace dat do nástroje IdM.

5.2.1 Instalace systému IdM

Dodavatel provede instalaci IdM do třech nezávislých prostředí (1× Vývoj, 1× Test,1× Produkce). Počet nodů a hardwarové požadavky budou upřesněny v rámci předimplementační analýzy.

5.2.2 Migrace dat

V rámci implementace systému IdM budou do nástroje převedena data ze zdrojových systémů, jako jsou organizační struktura, činnostní a organizační role, identity a další relevantní informace, které budou upřesněny v rámci předimplementační analýzy. Současně budou migrována data z napojovaných systémů, zejména aplikační role a další specifické údaje identifikované během analýzy. Přesný rozsah a obsah migrovaných dat bude detailně specifikován v dokumentaci předimplementační analýzy.

5.2.3 Integrace na systémy Etapy 1

Bude provedena integrace systémů uvedených v Příloze č. 1b, Tabulce A na IdM.

5.2.3.1 OKbase - HR systém

Je požadována pouze jednosměrná komunikace z HR systému OKbase do IdM, zpětná synchronizace z IdM do OKbase neprobíhá.

OKbase ve vztahu k IdM bude vystupovat jako zdrojový systém pro informace o interních zaměstnancích, tak i jako napojovaný systém (skrze AD), k němuž jsou přístupy řízeny pomocí IdM.

Napojení z OKbase do IdM

STC požaduje napojení (čtení) autoritativního zdroje dat z HR systému.

Integrace bude realizována jako napojení na databasové Views.

Konsolidace dat bude upřesněna v rámci předimplementační analýzy a je požadována v rámci plnění této veřejné zakázky.

Z autoritativního zdroje budou do IdM načítány minimálně tyto typy objektů:

- Zaměstnanci (PP, DPČ, DPP)
- Organizační struktura a její parametry
- Ostatní parametry nutné pro správný chod a funkčnost IdM

5.2.3.2 Active Directory

Objednatel požaduje obousměrnou integraci na on-premise MS Active Directory, které je synchronizováno s Entra ID pomocí nástroje Microsoft Entra Connect Sync.

Scénáře přihlašování a ověřování

Zajištění integrace IdM na SMS gateway STC, která umožní předání hesla interním i externím uživatelům prostřednictvím SMS.

Správa a provoz

Automatizace správy účtů – IdM zajišťuje automatizované zakládání, změny a deaktivace účtů v AD i Entra ID na základě událostí z OKbase a schválených workflow.

Organizační struktura – účty jsou v AD zařazovány do OU dle struktury z HR systému, což zajišťuje správné přiřazení skupin a politik.

Správa skupin – IdM naplňuje skupiny v AD, které jsou dále synchronizovány do Entra ID a využívány pro řízení přístupů v cloudových aplikacích a DMS.

Deaktivace a mazání účtů: při ukončení pracovního poměru interních zaměstnanců dle OKbase a při ukončení smlouvy externistů nově dle IdM (resp. nyní dle schvalovacího workflow v DMS) je účet v AD deaktivován a přesunut do dedikované OU, po uplynutí retenční lhůty je smazán. Stejný stav je zrcadlen v Entra ID.

5.2.3.3 DMS (SharePoint SE)

DMS bude i nadále řízeno přes AD. IdM bude tedy řídit DMS prostřednictvím AD. Stávající workflow bude převedeno do IdM.

5.2.3.4 Integrace s IdM a Active Directory

Autentizace a autorizace: DMS využívá pro ověřování uživatelů a řízení přístupů Microsoft Active Directory (AD), přičemž struktura AD (OU, skupiny) odráží organizační strukturu definovanou v HR systému, nově bude řízeno v IdM.

Správa skupin: Přístupová práva v DMS jsou řízena prostřednictvím AD skupin. Vyšší oprávnění a speciální role jsou spravovány v SharePoint skupinách, které jsou naplňovány na základě členství v AD skupinách synchronizovaných z IdM.

Napojení na testovací prostředí: IdM bude řídit jak produkční, tak testovací instanci DMS, což umožní snadné testování nových procesů a změn bez dopadu na ostrý provoz.

Workflow a žádosti o přístupy

Migrace workflow do IdM: Stávající workflow žádostí o přístupy (včetně VPN, DMS, ERP a dalších aplikací), která byla dosud realizována v DMS, bude převedena do IdM. DMS bude nahrazeno systémem IdM.

Schvalovací procesy: Schvalování žádostí o přístupy bude řízeno v IdM na základě definovaných rolí a vlastnictví systémů. Vlastníci systémů budou automaticky notifikováni a workflow bude transparentně evidováno pro auditní účely.

Automatizace provisioning: Po schválení žádosti v IdM dojde k automatizovanému přiřazení uživatele do příslušných skupin v AD, což se okamžitě promítne do přístupových práv v DMS.

5.2.3.5 Exchange

STC požaduje obousměrnou integraci na on-premise MS Exchange a Microsoft Exchange Online, které je synchronizováno s Entra ID pomocí nástroje Microsoft Entra Connect Sync.

Správa a provoz

Automatizace správy účtů – IdM zajišťuje automatizované zakládání, změny a deaktivace mailboxů uživatelů na základě událostí z HR systému a schválených workflow.

Na základě přidělené role v IdM se změní extension atribut v AD, který zajistí automatické nastavení Microsoft 365 licence, viz. kapitola 3.3.6 Atributy a jejich správa.

- Automatická migrace lokálního mailboxu do Microsoft Exchange Online.

Automatická konverze mailboxu na typ Shared Mailbox při ukončení pracovního poměru, nastavení automatické odpovědi, s kontaktem na nadřízeného.

Na základě odebrání role v IdM proběhne změna extension atributu v AD, což následně zajistí automatické uvolnění Microsoft 365 licence, při ukončení pracovního poměru.

5.2.3.6 Integrace s řešením PAM

Pokud to řešení vyžaduje, tak přípravy pro budoucí integraci systému PAM musí být provedeny již během Etapy 1 nasazení řešení IdM. Tímto přístupem je zajištěna plynulá a bezpečná následná integrace PAM, která umožní efektivní správu privilegovaných přístupů a minimalizuje rizika spojená s přechodem mezi oběma systémy a zajistí efektivní správu privilegovaných přístupů v souladu s bezpečnostními požadavky organizace.

Budoucí integrace systému PAM do centrálního systému řízení identit (IdM) bude zajišťovat automatizované a řízené předávání informací o uživatelích, jejich rolích a oprávněních, včetně životního cyklu přístupů k privilegovaným účtům. IdM bude sloužit jako jednotný zdroj informací o identitách uživatele a na základě definovaných pravidel bude řídit poskytování, změny a odebrání přístupů v systému PAM.

5.2.3.7 Off-line systémy

IdM bude provádět v případě off-line systémů pouze formální evidenci, správu a schvalování požadavků na identity, uživatele a role a ty jsou pak manuálně zadávány do koncových systémů prostřednictvím řešitelské skupiny.

Tyto systémy budou identifikovány v rámci předimplementační analýzy pro Etapu 1 a 3.

5.3 Dokumentace Etapy 1

Veškerá dokumentace k realizaci předmětu Smlouvy musí být vypracována v českém jazyce. Mohou v ní být použité části v anglickém jazyce, např. ilustrace přímo od výrobce technologie apod., ale s doplňujícím vysvětlením, případně výkladem odborných pojmů v českém jazyce. Dodávka musí zahrnovat minimálně následující dokumenty:

- **Dokumentace skutečného provedení**: Obsahuje detailní návrh dodaného řešení a popis všech úprav provedených v prostředí objednatele oproti výchozí či standardní konfiguraci jednotlivých komponent.
- **Dokumentace instalace softwaru**: Musí obsahovat kompletní postupy pro instalaci a konfiguraci řešení (např. nastavení sítě, pojmenování služeb apod.). Na základě této dokumentace bude možné instalaci kdykoliv opakovat bez nutnosti dalších znalostí.
- **Plán obnovy (DR plan)**: Definuje postupy obnovy systému v různých krizových situacích, jako je nechtěné smazání či změna dat, ztráta přístupu k administrátorským účtům apod. Pro každý scénář je uveden přesný postup obnovy s ohledem na dostupné zálohovací mechanismy.

- **Testovací scénáře**: Budou připraveny akceptační testy využívané jak objednatelem při ověřování funkčnosti aplikace, tak i později jako regresní testy pro kontrolu základních funkcí při nasazování nových verzí a upgradů řešení.
- **Plán přechodu do produkčního provozu:** Před spuštěním IdM v produkčním prostředí bude vytvořen detailní plán nasazení. Ten bude obsahovat checklist se všemi nezbytnými kroky: instalace a konfigurace produkční instance IdM, import konfigurace z testovacího prostředí, rozplánování úloh, tvorba reportu rozdílů dat mezi IdM a řízenými systémy, čištění dat ve spolupráci s objednatelem, zálohování systémů a koordinace s objednatelem a případnými dodavateli, až po postupné nebo dávkové spuštění propisu dat do řízených systémů.
- **Plán zálohování**: Dokumentace bude obsahovat návrh a popis zálohovacích postupů, které provádí jak objednatel (zálohy virtualizační platformy, zálohy dat ze serveru apod.), tak dodavatel (zálohy aplikačních dat IdM, konfigurace a logů). Veškerá uživatelská data musí být zálohována v šifrované podobě.

Dokumentace musí být kompletní a průběžně aktualizována po celou dobu trvání smluvního vztahu tak, aby vždy odpovídala aktuální verzi SW. Dokumentace může být poskytnuta i formou přístupu k online dokumentaci.

5.4 Školení Etapy 1

Dodavatel zajistí přípravu podkladů pro HR adopční kampaň v rámci Etapy 1, přičemž tato adopční kampaň bude pokrývat všechny Etapy této veřejné zakázky. Součástí dodávky budou minimálně šablony e-mailů, texty pro intranet/FAX, one-pager a slide deck.

Dodavatel zajistí školení pracovníků STC v oblasti administrace, provozu a uživatelském používání implementovaného nástroje IdM dle požadavků uvedených níže.

Dodávaný produkt musí být doplněn o školící materiály a návody pro správu systému, a to alespoň v následujícím rozsahu:

Příručka administrátora

Tato příručka bude obsahovat detailní popis všech funkcí potřebných pro správu IdM. Slouží jako základní materiál pro školení nových administrátorů. Součástí příručky budou také návody krok za krokem s doprovodnými obrázky a výřezy obrazovek pro lepší orientaci.

Příručka vývojáře

Zahrnuje kompletní dokumentaci implementace IdM včetně:

- Postupů pro vytváření vlastních funkcí a modulů pro rozšiřování řešení,
- Návodů na vývoj nových konektorů pro integraci s dalšími systémy,
- Pokynů pro psaní skriptů na transformaci dat mezi systémy.

Požadavky na školení

Řešení musí zahrnovat školení v rozsahu minimálně **3 MD** v součtu pro tyto skupiny uživatelů:

- **Klíčoví uživatelé a garanti systémů** (vč. online nahrávky)
- **Bezpečnostní správce** (vč. online nahrávky)
- **Systémoví administrátoři** (vč. online nahrávky)
- **Běžní uživatelé** – online školení a nahrávky tohoto školení on-demand
- minimálně 1× standardní on-line školení se záznamem

Obsah školení musí pokrýt i procesní změny:

- jak HR zadává údaje v OKbase, aby fungovala automatická deaktivace,
- jak probíhá onboarding/offboarding přes IdM.

5.5 Testovací provoz a akceptace pro Etapu 1

5.5.1 Testovací provoz

Testovací provoz představuje fázi, během níž jsou na produkční prostředí nasazeny scénáře ověřené v testovacím prostředí, avšak pod zvýšeným dohledem všech zúčastněných stran. Před uvedením IdM řešení do plného produkčního režimu provozuje dodavatel v úzké spolupráci se objednatelem IdM nástroj v režimu testovací provozu. Cílem této fáze je identifikace a následné odstranění případných provozních či konfiguračních nedostatků před zahájením produkčního provozu. Dodavatel v průběhu testovacího provozu poskytuje zvýšenou podporu při řešení zjištěných nedostatků.

Data a role během testovacího provozu

- Výstupy analýzy AR/BR (Application Roles/Business Roles) mohou být v době napojování systémů založeny na **starších datech** (typicky 3–4 měsíce, pravděpodobně 6+).
- **Po napojení systémů musí dodavatel provést aktualizaci exportů uživatelů a re-konfiguraci/rekalibraci rolí** (tj. znovu přiřadit role dle aktuální reality) tak, aby **testovací provoz již pracoval s aktuálními daty**.
- **Smluvní požadavek:** Tyto aktivity (aktualizace exportů a opětovné přiřazení rolí vyvolané stářím dat) musí být **výslovně zahrnuty v ceně a harmonogramu** testovacího provozu.

Testovací provoz je ukončen schválením přechodu do produkčního provozu ze strany objednatele. Tímto aktem se IdM řešení jako celek předává do plného provozu. Testovací provoz tvoří závěr Etapy 1 a jeho délka bude činit **min. 1 měsíc** po dokončení fáze F1.2 dle harmonogramu. Testovací provoz bude probíhat po dobu nezbytně nutnou k ověření funkčnosti systému IdM.

5.5.2 Akceptace a přechod do produkčního provozu – Go-live

Během testovacího provozu využívá objednatel IdM řešení v plném rozsahu a přistupuje k němu z provozního hlediska jako k plnohodnotnému produkčnímu prostředí. Zároveň průběžně sleduje a vyhodnocuje, zda prostředí splňuje stanovené požadavky.

Na konci testovacího provozu dodavatel provede akceptační testy (dle odsouhlasených testovacích scénářů definovaných v rámci předimplementační analýzy), které ověří, že systém IdM splňuje všechny požadavky stanovené v této Technické specifikaci a že příslušná část předmětu plnění je provedena v souladu s předimplementační analýzou (dále jen „testy“).

V okamžiku, kdy objednatel dospěje k závěru, že prostředí je plně funkční a odpovídá požadavkům zadání, podepíše s dodavatelem akceptační protokol o převzetí systému IdM a jeho předání do produkčního provozu.

Akceptace a přechod do produkčního provozu **nemůže být provedeno dříve** než po uplynutí prvního měsíce testovacího provozu a současně nemůže být dříve než vypracování dokumentace a průběh školení dle kapitol 5.3 a 5.4.

Součástí akceptace je kontrola existence a aktuálnosti dokumentace v rozsahu odpovídajícím dodávané verzi SW, resp. implementaci a konfiguraci v prostředí STC.

Dodavatel je povinen při přechodu do produkčního provozu předat veškeré zdrojové kódy a build/CI skripty s výjimkou případů, kdy se jedná o Standardní Software nebo jiné komponenty, ke kterým dodavatel nemá licenční oprávnění ke zdrojovým kódům.

5.6 Technické požadavky na řešení IdM

Tato kapitola specifikuje funkční požadavky objednatele na budoucí řešení pro správu identit (IdM), které navrhované řešení dodavatele musí bezezbytku splňovat.

5.6.1 Použitá technologie a architektura

Požadavky v této kapitole se týkají použité technologie a celkové architektury IdM řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A1	Využití cloud řešení	Je požadováno „on-premise“ řešení IdM, cloudové řešení IdM se nepřipouští.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A2	Zabezpečení IdM	Všechny komponenty dodaného IdM řešení musí být dostatečným způsobem zabezpečeny prostřednictvím následujících minimálně nutných opaření: • Musí být proveden hardening jednotlivých komponent IdM. • Veškeré přenosy dat a informací musí být náležitě zabezpečeny z pohledu požadavků na jejich důvěrnost, integritu a dostupnost. • Musí být dostatečně zabezpečen přístup k citlivým údajům a funkcím systému (jako jsou například hesla, nebo funkcionalita změny hesel) pomocí kryptografických opatření.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A3	Dodání a implementace	Implementace systému IdM musí být navržena tak, aby umožňovala rychlé, efektivní a co nejméně komplikované nasazení pro zjednodušení zahájení projektu; řešení musí být dodáno jako kompletní balíček (preferenčně OVA/OVF) včetně všech potřebných licencí a SW komponent pro jeho provoz (aplikační/middleware vrstva, runtime, konektory a případné DB komponenty), přičemž z rozsahu licencí jsou výslovně vyloučeny zdroje a platformy dle bodu 4.1, které zajišťuje objednatel.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A4	Konektory	Součástí dodávky musí být také předem připravená sada základních konektorů (tzv. out-of-the-box), jejichž seznam je specifikován níže v požadavku A17 a A18.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A5	Provozní prostředí	Řešení bude nasazeno minimálně ve třech oddělených prostředích: • **Testovací prostředí** bude sloužit pro účely integrace a ověřování funkčnosti systému. V tomto prostředí budou probíhat testy jak ze strany dodavatele, tak ze strany objednatele. Testovací prostředí IdM bude minimálně napojeno na test prostředí OKbase, Dev prostředí DMS, a testovací prostředí AD (resp. strukturu OU), přičemž napojení ostatních systémů na testovací prostředí IdM bude definováno v rámci předimplementační analýzy. • **Produkční prostředí** bude určeno pro ostrý provoz systému identity managementu v reálném prostředí organizace.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		• **Vývojové prostředí.**		
A6	Modulární architektura	Architektura řešení bude modulární. Jednotlivé funkční celky budou odděleny do vlastních modulů s jasně definovaným rozhraním pro komunikaci s ostatními moduly. Každý z modulů půjde samostatně zapnout a vypnout a tím se zpřístupní nebo zablokuje jeho funkce i příslušné agendy v grafickém rozhraní. Po vypnutí a opětovném zapnutí modulu nedojde ke ztrátě dat, se kterými modul (například seznam uživatelských licencí) pracuje. Modularita řešení zajistí jednoduchou rozšiřitelnost o další nové funkce a moduly. Nově vydané moduly bude možné do IdM jednoduše začlenit jejich stažením a přidáním k již existujícím modulům. Veškeré implementace objednateli na míru v rámci plnění předmětu Smlouvy budou implementovány do odděleného modulu pro usnadnění nasazování nových verzí produktu a zajištění dlouhodobé udržitelnosti.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A7	Škálovatelnost aplikace	Dodané řešení musí podporovat škálovatelnost v počtu spravovaných identit i napojených systémů; je požadována kapacita na **150–200 nových interních identit ročně** a **1–3 nová systémová napojení ročně** (s možností dalšího navýšení) a architektura umožňující **paralelní, asynchronní a prioritizované** zpracování požadavků (produkční/uživatelské nejvyšší priorita, reporty/dávky nižší).	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.2 HW a SW nároky

Požadavky v této kapitole se týkají základních požadavků na hardwarové a softwarové nároky IdM řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A8	Využití virtualizace	IdM řešení musí být implementovatelné na platformě **x86** a určeno ke spuštění na virtualizační platformě typu **VMware** (viz 4.1). Dodavatel musí v nabídce specifikovat: - **počet požadovaných virtuálních serverů a jejich parametry** s ohledem na dostatečnou výkonnost řešení a současnou adekvátnost parametrů, - **požadavky na parametry komunikačních tras a síťových prostupů** mezi jednotlivými komponentami řešení (pokud jsou takové kritické pro funkčnost).	(Doplní dodavatel)	(Splňuje/Nesplňuje)

Maximální sizing IdM :

- **2× virtuální server:** 12 vCPU, 24 GB RAM, 200 GB SSD

5.6.3 Základní požadavky na uživatelské rozhraní

Požadavky v této kapitole se týkají základních požadavků na uživatelské rozhraní IdM řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A10	Lokalizace	Uživatelské prostředí musí být lokalizováno minimálně do českého a anglického jazyka.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A11	Webové rozhraní	Všichni uživatelé budou pracovat v jednotném webovém grafickém rozhraní. Webové rozhraní je přístupné pouze prostřednictvím protokolu https.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A12	Přizpůsobení	Rozhraní musí umožňovat základní grafické přizpůsobení, a to alespoň v tomto rozsahu: • Zobrazení loga organizace, Možnost vložení odkazu na technickou podporu.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A13	Intuitivní používání	Uživatelské rozhraní systému musí být přehledné a snadno ovladatelné jak pro běžné uživatele, tak pro administrátory. V rámci různých oblastí systému (např. správa rolí, identit, organizací, systémů) musí být umožněn intuitivní přechod mezi souvisejícími obrazovkami. Například z detailu uživatele bude možné jedním klikem zobrazit podrobnosti o jeho přiřazených rolích, včetně informací o schvalovateli – pokud k těmto datům má uživatel oprávněný přístup.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A14	Nástěnka uživatele	Jedno místo se všemi základními informacemi (identita, role, úvazky) a souborem úkolů pro právě přihlášeného uživatele v IdM.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A15	Uživatelské role	Webové rozhraní systému IdM zpřístupňuje jednotlivé funkce na základě oprávnění konkrétního uživatele. V prostředí objednatele lze počítat minimálně s těmito kategoriemi uživatelů: • **IdM administrátor** – Zajišťuje kompletní správu systému IdM, včetně monitoringu provozu, správy rolí a přístupových oprávnění. Řeší nestandardní situace, kontroluje výstupy a sleduje životní cyklus identit. Má možnost delegovat svá oprávnění a nastavovat přístup na úrovni	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		jednotlivých agend a datových objektů (např. identity, role, OU). • **Administrátor vybraných částí systému** – Tento typ administrátora má oprávnění spravovat jen určité části organizační struktury (např. konkrétní úřady nebo skupiny uživatelů). Jeho úkolem je zajišťovat správu uživatelů v rámci svěřeného segmentu. • **Helpdesk pracovník** – Má přístup k údajům o identitách a jejich přiřazených rolích. Mezi jeho hlavní činnosti patří resetování hesel. • **Role garant** – Osoba zodpovědná za schvalování přidělení konkrétní role. Obvykle jde o vlastníka systému nebo dat. Může definovat obsah role, nastavovat atributy a seskupovat jím spravované role. • **Nadřízený** – Má přístup k informacím o svých podřízených. Může jim podávat žádosti o přidělení rolí a zároveň schvalovat žádosti vycházející od nich. Dále může resetovat hesla svým podřízeným nebo upravovat vybrané atributy jejich účtů. • **Správce externistů** – Zodpovídá za správu identit a přístupových práv externích pracovníků, kteří mu byli svěřeni. • **Běžný uživatel** – Využívá samoobslužné funkce, jako je změna hesla, přehled o vlastních účtech a rolích, podávání žádostí o nové role a přístup k přehledu stavu svých požadavků. • **Správce offline systému** – Provádí operace, jako je vytvoření, úprava nebo zrušení účtu, na základě notifikací zaslaných systémem IdM. Po provedení zásahu pak potvrzuje jeho dokončení zpět v systému IdM.		
A16	Hromadné změny	IdM umožní hromadně v grafickém rozhraní provádět změny na objektech identit, rolí a organizačních prvků. Minimálně budou dostupné hromadné operace pro: • vkládání objektů, úprava objektů, mazání objektů. V případě identit bude možné vyfiltrovat hledané identity a přidělit jim hromadně role/oprávnění, změnit jim vedoucího, zablokovat, změnit organizační zařazení, změnit platnost kontraktu atd. Bude možné spustit proces předschválení přidělených přístupů pro vybrané role nebo vybrané uživatele. Každá změna provedená pomocí hromadné akce je auditovaná.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

Cílem je vybudovat stabilní a dlouhodobě udržitelné řešení, které bude možné provozovat jak prostřednictvím dodavatele, tak jiným externím subjektem nebo samotným objednatelem.

5.6.4 Konektory

Požadavky v této kapitole se týkají základních požadavků na konektorovou vybavenost IdM řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A17	Konektory	Součástí dodávky bude minimálně následující sada konektorů. Tyto konektory musí být použitelné pro připojení standardních systémů bez nutnosti úprav, s výjimkou REST/WS konektoru a PowerShell, kde je potřeba doplnit konkrétní volání dle technické specifikace cílového systému. Obecné skriptovatelné konektory (např. DB, SSH) budou obsahovat ukázkové skripty pro operace CRUD nad napojenými systémy.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A18	Minimální sada konektorů	Součástí dodávky bude minimálně následující sada konektorů. Tyto konektory musí být použitelné pro připojení standardních systémů bez nutnosti úprav, s výjimkou REST/WS konektoru a PowerShell, kde je potřeba doplnit konkrétní volání dle technické specifikace cílového systému. • Microsoft Active Directory • Exchange (Powershell) • Azure (GraphAPI) • CSV konektor • REST a Web Service konektor • PowerShell konektor • LDAP konektor • Databázový konektor (obecný skriptovaný konektor) • Konektor pro offline/virtuální napojení systémů (např. pro systémy bez přímého rozhraní)	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A19	Vzorové skripty	Obecné skriptovatelné konektory (např. DB, SSH, PowerShell) budou obsahovat ukázkové skripty pro operace CRUD nad napojenými systémy.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A20	Konektorová rozšiřitelnost	Systém IdM musí umožňovat snadné rozšíření o další konektory a podporovat jejich běh nejen v rámci samotného řešení, ale i na externích konektorových serverech.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A21	Univerzální API	Řešení umožní kromě správy přes grafické webové rozhraní také kompletní správu přes univerzální API (např. REST): • například pro napojení provozních systémů – monitoring, datawarehouse, SIEM atd.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		• nebo pro aktivní (push) správu dat v IdM – například dávkové založení uživatelů, stažení reportu, stažení certifikátů atd. Veškeré operace umožněné v grafickém rozhraní musí být dostupné i pro automatizovanou správu přes univerzální API. Univerzální rozhraní komunikuje vždy šifrovaně.		
A22	API volání	Univerzální API bude podporovat interaktivní volání přímo z grafického rozhraní pro testování a konfiguraci.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.5 Základní požadavky na synchronizaci dat

Požadavky v této kapitole se týkají základních požadavků na funkcionality v oblasti synchronizace a správy dat.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A23	Provisioning	IdM musí podporovat synchronizaci změn (provisioning) směrem do řízených systémů v reálném čase. V případě dočasného výpadku cílového systému musí být k dispozici mechanismus pro automatické opakování neúspěšných operací, aby bylo zajištěno spolehlivé doručení změn.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A24	Synchronizace	V případě obousměrného napojení musí řešení umožňovat jak přenos dat z IdM do koncového systému (např. vytvoření nebo úprava uživatele a jeho atributů), tak i zpětnou synchronizaci dat z cílového systému do IdM (např. získání informací o přidělených rolích).	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A25	Synchronizace dat	IdM umožní synchronizovat data o identitách, organizačních strukturách, kontraktech, rolích ze zdroje dat (HR, AD, csv, import) v režimech: • plné synchronizace – tzn. veškerá data budou autoritativně načtena do IdM. • rozdílové synchronizace – s využitím příznaku časové značky záznamu. Tzn. IdM zpracovává pouze ty záznamy, které mají časovou značku změny ve zdroji dat novější než běh poslední synchronizace IdM. • Synchronizace všech objektů nebo definice filtru omezení synchronizovaných dat. Např. při zavádění IdM bude možné nejdříve vyzkoušet synchronizaci pro jednoho uživatele (vyfiltrovaného například podle příjmení) nebo skupinu uživatelů. Synchronizace dat lze spouštět manuálně z grafického rozhraní nebo plánovaně pomocí grafického plánovače úloh.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

A26	Testovací synchronizace	Synchronizace dat umožní běh v režimu, který nemění data v IdM. Výstupem takového běhu je seznam objektů, které by se při běžném běhu synchronizace změnily. Tento režim lze použít jak při iniciální synchronizaci pro kontrolu procesu, tak i opakovaně v provozu při očekávání velkých dávek změn.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A27	Synchronizace pro párování dat	V rámci synchronizace dat bude možné nejen importovat data do IdM, ale také spárovat identity k jejich existujícím účtům (např. pro AD). Párování IdM umožní na základě konfigurace: • vybraný atribut – např. osobní číslo • korelace více atributů – např. jméno + příjmení	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A28	Iniciální synchronizace rolí uživatelů	IdM automatickou synchronizací zajistí iniciální načtení stavu přiřazených rolí účtu z napojeného systému do IdM (např. stav přiřazených skupin u účtu v AD). IdM umožní iniciální nalití stavu systému i pro nepřímo (off-line) řízené systémy – např. pomocí importu ze souboru (účty, role, přiřazení rolí k účtům, organizační struktura, katalogizace rolí).	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A29	Zobrazení stavu synchronizace	V grafickém rozhraní je zobrazen stav probíhající synchronizace – zpracované objekty, log chyb, rychlost synchronizace nebo odhad zbývající doby trvání. Výsledek synchronizace je uchováván v auditu a lze zpětně dohledat v grafickém rozhraní veškeré běhy, výsledky a obsah předcházejících synchronizací.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A30	Plánování běhu synchronizace	Synchronizace dat lze plánovat v grafickém rozhraní IdM. Synchronizace lze naplánovat na konkrétní čas. Synchronizace i jiné úlohy lze v plánovači v grafickém rozhraní zřetězit. Např. lze definovat, že synchronizace identit zaměstnanců začne v návaznosti na úspěšné dokončení synchronizace organizační struktury.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A31	Transformace a mapování atributů	IdM musí umožňovat definici pravidel pro mapování atributů mezi systémy pomocí transformačních výrazů nebo pravidel. Systém bude obsahovat předdefinovanou knihovnu běžných transformačních pravidel (např. pro display Name v prostředí MS Active Directory). Dále musí být k dispozici integrované vývojové prostředí (IDE) v rámci webového rozhraní IdM pro tvorbu a úpravu transformačních skriptů.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A32	Podpora pokročilých atributů	IdM musí být schopno pracovat i s komplexními a binárními atributy – jako jsou například certifikáty, fotografie uživatelů nebo autentizační tokeny – a zajistit jejich správnou synchronizaci.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

A33	Párování účtů a identit	Systém musí umožňovat nastavení pravidel pro spárování identity s účtem napříč napojenými systémy (např. propojení pomocí e-mailové adresy jako loginu).	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A34	White-list účtů	IdM musí podporovat možnost definice výjimek – tzv. white-list účtů, které nebudou nikdy automaticky upravovány (např. technické nebo servisní účty).	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A35	Auditní záznamy	Veškeré operace spojené se synchronizací a provisioningem musí být detailně zaznamenávány do auditního logu pro účely zpětné kontroly a bezpečnosti.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.6 Přihlašování a přístupová oprávnění

Požadavky v této kapitole se týkají základních požadavků na přihlašování a přidělování přístupových oprávnění do systému IdM.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A36	Jednotné přihlášení (SSO) do IdM	• Systém IdM musí podporovat jednotné přihlášení (SSO) prostřednictvím integrace s Microsoft Active Directory. Uživatel, který je již ověřen v doméně MS AD, bude do IdM automaticky přihlášen bez nutnosti opětovného zadávání přihlašovacích údajů.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A37	Centrální reset hesla	• IdM umožní centrální správu hesla (změna, reset) pro MS AD i další napojované systémy. Změnu může provést uživatel, nadřízený, helpdesk nebo správce IdM. Oprávnění provést reset nebo změnu hesla lze konfigurovat v IdM dle potřeby. • Při propisu hesla do řízených systémů umožní IdM propagovat i metadata o hesle, jako je platnost hesla, příznak povinné změny hesla (must change password) atd.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A38	Jednotné heslo	• IdM musí podporovat centrální správu jednotného hesla: • pro všechny napojené systémy i • pro několik skupin systémů – musí umožnit definici skupin systémů s vlastním jednotným heslem a specifickou politikou hesla.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A39	Komplexní politika pro hesla	• IdM musí umožnit definovat politiky hesel pro generování nových hesel a validování změn hesla. Politika musí splňovat komplexnost politik domény MS AD, zákonu o kybernetické bezpečnosti a příslušných vyhlášek a nařízení. • IdM z bezpečnostních důvodů neumožní zobrazit heslo identit v ní spravované, a to	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		ani administrátorovi s nejvyššími právy (ani při využití funkce generátoru hesel). • Navíc musí umožnit definovat skupiny povolených a zakázaných znaků (whitelist, blacklist) kvůli možné distribuci hesel pomocí kanálů jako SMS, aby se znaky vzájemně nepletly. Např. malé el „l“ vs. velké i „I“. Produkt musí podporovat historii hesel uživatelů, v případě změny hesla přes IdM. Nová hesla zadaná v IdM jsou kontrolována proti historii. Hesla v historii jsou uložena tak, že není možné získat jejich čitelnou podobu. • Hesla nesmí být ukládána v čitelné podobě a musí být použity bezpečné hashovací algoritmy odolné vůči útokům.		
A40	Bezpečnost práce s hesly	• Hesla, která je nutné ukládat do IdM v podobě umožňující jejich použití (např. hesla technických účtů napojovaných systémů nutná pro navazování spojení) musí být uložena v šifrovaném úložišti odděleně od zbytku dat.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A41	Generátor a validátor hesel dle komplexních politik	• IdM umožní definování rozdílných politik pro generování nového hesla a pro validaci změny hesla. Pro generování hesla může být například využita politika, dle které se nepoužívají zaměnitelné znaky `I` a `l` - velké i a malé el, protože se můžou automaticky posílat v psané podobě a vyvolaly by zmatení uživatelů. Naopak ve validačních politikách se toto pravidlo neuplatní, protože uživatel/administrátor sám heslo zadává dle svého uvážení.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A42	Auditní záznamy	• Ve všech případech jsou informace o přihlášení zaznamenávány do auditního logu pro účely zpětné kontroly a bezpečnosti.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A43	Řízení přístupu	• Systém musí využívat pro řízení přístupu ke svým funkcím a datům stejný princip jako řízené cílové systémy – RBAC (). Přístupová práva jsou přiřazována prostřednictvím rolí, které definují oprávnění k jednotlivým oblastem systému a konkrétním datovým objektům.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A44	Oprávnění k agendám	• IdM umožňuje přesně nastavit oprávnění k jednotlivým agendám, jako je např. správa uživatelů, konfigurace systému, správa napojených systémů apod. Pro každou agendu lze zároveň určit, nad jakými daty může konkrétní role operovat. • Např.: • Garant externistů má přístup pouze ke správě „svých“ externistů. • Běžný uživatel může upravovat jen vybrané atributy své vlastní identity, ale zároveň má právo zobrazit seznam identit v rámci organizace. • Administrátor může mít oprávnění k realizaci konkrétních operací – spouštění workflow, vyplňování a schvalování	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		formulářů, prohlížení reportů, přidělování/odebírání rolí apod.		
A45	Aplikační (business) role	• Autorizace je nastavována prostřednictvím aplikačních (business) rolí a její princip je konzistentní s ostatními systémy zapojenými do IdM.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A46	Multitenantní přístup	• Systém musí rovněž umožňovat multitenantní řízení přístupu, což znamená možnost vymezit administrátorská oprávnění pouze na konkrétní části organizační struktury, vybrané skupiny uživatelů či specifické objekty. Tím je umožněno delegování správy na nižší organizační úrovně – každý delegovaný administrátor má práva pouze na "svůj" vymezený okruh uživatelů a dat.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

A47	Oprávnění pro běžného uživatele	IdM dále musí umožnit:
		• Nastavit oprávnění i pro běžného uživatele, včetně možnosti:
		  ○ zobrazit vlastní oprávnění a zařazení v organizační struktuře,
		  ○ schvalovat žádosti,
		  ○ spouštět přidělené reporty.
		• Omezit práva na úroveň konkrétních atributů, např. uživatel může upravit své telefonní číslo, ale nemůže měnit přihlašovací jméno.
			(Doplní dodavatel)	(Splňuje/Nesplňuje)

A48	Zobrazení přidělených rolí	Veškerá oprávnění jsou spravována prostřednictvím rolí v rámci RBAC modelu. IdM musí poskytovat přehledný náhled na aktuálně platná oprávnění uživatele přímo v grafickém rozhraní – včetně informace, na jaké objekty, s jakým rozsahem oprávnění a na základě jakého pravidla byla práva přidělena.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A49	Recertifikace přístupů	IdM musí umožnit pravidelnou recertifikaci přístupů odpovědnými osobami nebo garanty rolí.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.7 Identity

Požadavky v této kapitole se týkají základních požadavků na práci s identitami.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A50	Práce s identitami	Řešení poskytne v grafickém rozhraní přehlednou práci s identitami: • Vyhledávání a filtrování uživatelů/identit podle atributu (jméno, příjmení, email, …), organizačního zařazení, přiřazených rolí, stavu identity (na mateřské, aktivní, odešlí, …)	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A51	Stav identity	IdM v grafickém rozhraní přehledně zobrazí stav identity – odlišeny budou nejméně:	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		• Aktivní/neaktivní identity • Identity vyňaté z evidenčního stavu • Identity s budoucím nástupem • Identity s ukončenými úvazky Přes stav identit půjde jednoduše filtrovat, například pro rychlou kontrolu blížících se nástupů.		
A52	Příprava identity před nástupem	IdM musí umožnit identitě uživatelů, kteří mají nastoupit do organizace, přidělovat role pro aplikace dopředně. U jednotlivých rolí půjde definovat, zda se role má na identitu aplikovat a propsat do koncového systému. U systémů, jako např. AD, je požadována možnost vytvořit účet dopředu. Bude-li se účet propisovat před nástupem, bude účet vytvořen neaktivní a heslo k němu nebude předáno, dokud držitel identity nenastoupí. Některé jiné systémy tento režim využívat nemusí. Řešení musí zajistit distribuci jednotného iniciálního hesla do všech systémů v den nástupu zaměstnance.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A53	Karanténa účtů	IdM musí umožnit karanténu účtů na definovanou dobu po ukončení identity s možností obnovení původních atributů. Zejména bude zachován login a e-mail v řízených systémech. Účty identit v karanténě nemají žádné přístupy (role) a jsou blokovány – tzn. uživatelé je nemohou používat. Po uplynutí doby karantény je účet ze systémů smazán. Na systémech, kde není karanténa nastavena, je účet smazán ihned při ukončení identity. Karanténu bude možné nakonfigurovat pro každý řízený systém zvlášť.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A54	Ukončení identity	Při ukončení identity v identity manageru je pro účely auditů přístupů zachována kompletní auditní stopa. Lze zpětně dohledat, kam měla identita přístup v kterémkoli časovém úseku existence identity. V případě potřeby umožní identity manager periodické nebo ad-hoc odmazání (archivaci) auditních dat od konkrétního data (např. auditní informace starší 2 let).	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.8 Role

Požadavky v této kapitole se týkají základních požadavků na role a práci s nimi.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A55	RBAC model	Řešení musí podporovat správu rolí podle principů RBAC modelu.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

A56	Fulltextové vyhledávání	IdM podporuje fulltextové vyhledávání skrze celou aplikaci. Běžný uživatel si tak například najde roli, o kterou chce žádat. Správce uživatelů dle loginu vyhledá požadovanou identitu atd.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A57	Automatické přidělení rolí	IdM musí podporovat automatické přidělování rolí: • na základě zařazení uživatele v organizační struktuře, • na základě atributů identity, úvazku nebo jejich kombinace.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A58	Schvalování pravidel	IdM musí umožnit schvalování pravidel pro automatické přidělování rolí.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A59	Synchronizace skupin z AD	IdM musí umožnit načítání pouze vybraných skupin z AD na základě filtrů (vybraná OU, skupiny s vyplněnými konkrétními atributy) a označení skupin, o které nelze žádat v uživatelském rozhraní.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A60	Seskupování rolí	IdM musí umožnit seskupování rolí do skupin, o které lze žádat a schvalovat jako celek, včetně možnosti vnořování a katalogizace skupin rolí. Skupinám rolí lze také nastavit automatická pravidla pro přidělování uživatelům jako běžné role. Skupiny rolí musí být v uživatelském rozhraní jasně graficky odlišeny od běžných rolí. Role lze seskupovat v grafickém rozhraní IdM nebo hromadně importovat seskupení rolí z jiných systémů či souboru.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A61	Katalog rolí	Role nebo skupiny rolí musí být možné třídit do katalogu pro přehlednost. Role lze do katalogu vložit vícekrát. Jednou např. do složek tříděných podle systémů (AD, IS…) a podruhé např. do složky pro konkrétní útvar/projekt.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A62	Kopírování rolí od uživatele	IdM musí podporovat kopírování role od jiného uživatele – v grafickém rozhraní umožní zkopírovat všechny nebo vybrané role. Při kopírování rolí od uživatele je graficky odlišeno, které role jsou speciálního typu – skupina rolí, automaticky přidělená role, manuálně přidělená role, role je součástí skupiny jiných rolí. Pokud je zapnuto schvalování, pak je žádost o změnu schvalována jako při běžném výběru z katalogu rolí.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A63	Role management	Řešení musí obsahovat přehlednou agendu v grafickém webovém rozhraní pro správu rolí. Správa rolí umožní definovat jak administrátory IdM, tak delegovaným uživatelům – správcům rolí. IdM umožní v grafickém webovém prostředí zobrazovat oprávněným uživatelům kompletní informace o rolích včetně: • seznamu držitelů role;	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		• seznamu systémů, pro které je role definována; • seznamu systémů, odkud byla role synchronizována nebo kam byla zpropagována (provisioning dat); • schvalovacího workflow a garantů role; • skupin rolí, jejíž je role členem a zároveň seznamu rolí, kterým je role nadřazena; • SoD – seznamu rolí, které jsou s danou rolí neslučitelné; • parametrů role; • složek katalogu, kam je role zařazena. IdM přehledně zobrazí u každé identity, jaké role má přidělena a jakým způsobem (žádostí vs automaticky dle pravidla). Zároveň bude zobrazeno, zda má uživatel roli přidělenu napřímo nebo skrze seskupení rolí. V případě skupiny rolí umožní zobrazit (rozkliknout či jinak zobrazit) všechny role dané přidělené skupiny. Zároveň bude u uživatele zřejmé, z jakého kontraktu/úvazku role pochází. IdM umožní automaticky načítat seznam skupin/rolí z řízených systémů – zejména MS AD. Role je možné zadávat i manuálně skrze grafické webové rozhraní nebo dávkově přes univerzální API nebo importem ze souboru. IdM umožní definovat vlastníky rolí, kteří mohou role upravit, smazat či přiřadit uživatelům. Vlastníci rolí a privilegovaní uživatelé mohou v grafickém rozhraní získat seznam držitelů role či si mohou role vyexportovat do reportu. Uživatelé s patřičnými oprávněními mohou nad vybranými uživateli spustit deduplikaci přiřazení rolí. Tento proces vyčistí duplicitně přiřazené role u uživatele – například pokud má uživatel roli automaticky a zároveň ji dříve získal manuální žádostí, je mu manuální role odebrána (nekončí-li platnost přidělení automatické role dříve než manuální).		
A64	Parametrizace přidělení rolí	IdM umožní parametrizovat přidělení rolí. Role může mít libovolný počet parametrů, které vyplňuje žadatel v rámci žádosti o roli. Parametry mohou být povinné nebo nepovinné. Parametry role jsou u role uloženy a je možné je změnit jinou žádostí o roli. Parametry role jsou součástí schvalování a jsou zřetelně viditelné pro schvalovatele žádosti. Hodnotu parametru může žadatel vepsat do textového pole. IdM bude podporovat i výběr hodnoty z číselníku udržovaného v IdM.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A65	SoD (segregation of duties)	Role musí být možné definovat jako vzájemně výlučné s kontrolou při žádosti a možností dodatečného schvalování neslučitelných kombinací rolí. Přidělení neslučitelných rolí musí být možno evidovat v reportu.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.9 Atributy

Požadavky v této kapitole se týkají základních požadavků na atributy.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A66	Konfigurovatelné číselníky	IdM musí umožnit definovat různé číselníky v grafickém rozhraní. Příklady některých očekávaných číselníků: • číselník stavu úvazku – pro výpočet vynětí z evidenčního stavu • typ úvazku – DPP, HPP, DPČ, … • typ uživatele – interní, externí, dohodář, stážista, …	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A67	Rozšířené atributy identit, rolí a organizačních prvků	Základní objekty v IdM musí mít možnost definovat v grafickém rozhraní, jaké atributy budou u objektu evidovány a jakých datových typů jsou. Počet uživatelsky definovaných atributů nesmí být omezen.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A68	Oprávnění nakládat s rozšířenými atributy	Uživatelsky definované rozšířené atributy bude moci editovat pouze uživatel s oprávněním správy tohoto atributu. Například IdM umožní nastavit, aby každý uživatel sám sobě mohl vyplnit soukromou e-mailovou adresu, ale nedovolí editovat tyto údaje ostatním uživatelům. Naopak některé atributy budou pouze popisné (např. ty, které jsou automaticky generovány systémem nebo synchronizovány z jiných systémů) a uživatel je uvidí v režimu pouze pro čtení, aby je nemohl nedopatřením změnit.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A69	Validace hodnot rozšířených atributů	U každého uživatelsky definovaného atributu bude moci administrátor v grafickém rozhraní definovat, jak budou hodnoty při zadávání validovány. Například bude určeno, že korespondenční adresa je textový řetězec s nejméně třemi znaky. Validátor soukromého tel. čísla bude moci vyhodnotit, že objednatel zadává správný formát čísla. Validátory budou umět používat základní regulární výrazy pro práci s textem. Validátory umí vyhodnocovat zadaná data online, tzn. uživatel píše do formuláře a IdM vyhodnotí, zda zadaná hodnota odpovídá validátorům, případě graficky vyznačí chybu v zadání.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A70	Standardní generátory hodnot	IdM umožní použít pokročilé generátory v GUI pro běžně generované atributy jako je login a e-mail. Taktéž umožní vybrat si tvar loginu a e-mailu uživatelů, například určitý počet písmen ze jména a určitý počet písmen z příjmení (nebo celé) a spojovací znak (nebo bez spojovacího znaku).	(Doplní dodavatel)	(Splňuje/Nesplňuje)

A71	Validace unikátnosti hodnot	Generátory a validátory umožní zjištění unikátnosti hodnoty generovaného atributu v rámci IdM, ale i v rámci napojeného systému. Například IdM umožní validovat unikátnost vygenerovaného e-mailu v rámci IdM a domény MS AD, a to včetně e-mailových aliasů uživatelů.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.10 Schvalování a zástupnost

Požadavky v této kapitole se týkají základních požadavků na schvalování a zástupnost.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A72	Zástupnost pro schvalování – delegace	IdM umožní uživatelům, aby si v grafickém rozhraní nastavili zástupnost schvalování úkolů na: • dobu určitou – např. z důvodu dovolené nebo dlouhodobé nemoci, • dobu neurčitou – např. delegace schvalování úkolů na svého zástupce." Všechny úkoly, které byly delegovány jsou následně ve všech agendách grafického rozhraní jednoznačně označeny od koho -> na koho byl úkol delegován. Stejně tak je vyřešený úkol v rámci auditu uchován se stejnou informací o delegaci.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A73	Zástupnost práv (stejná židle)	IdM umožní dočasně (dle data od-do) posadit uživatele na pozici jiného uživatele, jehož zastupuje, aby tak získal veškerá automatická práva v IdM i řízených systémech jako zastupovaný uživatel. Pokud je třeba, aby zastupující získal i role přidělené zastupovanému, IdM nabídne nástroj, jak tyto role jednoduše zkopírovat včetně možnosti nastavení platnost od-do, aby odpovídala posazení na pozici.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A74	Zástupnost komunikace	IdM umožní delegovat posílání notifikací na jiného uživatele. Např. půjde veškerá notifikace z vedoucího přesměrovat na jeho asistentku.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A75	Možnost přesunout schvalovací úkol na jiného řešitele.	Uživatelé s vyšším oprávněním, např. administrátor IdM, mohou úkol přesunout na jiného řešitele nebo úkol zrušit – typicky v situaci, kdy je současný řešitel nedostupný (nemoc, nenadálá nepřítomnost). Systém zároveň podporuje automatickou eskalaci: pokud úkol překročí definovanou SLA lhůtu, IdM jej automaticky předá náhradnímu řešiteli nebo nadřízenému dle eskalační matice (s možností více úrovní) a odešle notifikace. Eskalace může být kalendářně citlivá (pracovní dny/čas). Přesun, zrušení i eskalační události jsou řádně evidovány v auditu IdM.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

A76	Náhled za jiného uživatele	IdM umožní náhled do IdM pohledem jiného uživatele v režimu pro čtení. Tato funkce je zpřístupněna vybraným uživatelům dle nastavených práv v IdM.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A77	Schvalovatel na základě role	IdM musí nabídnout možnost definovat skupinu (roli), jejíž členové budou vystupovat jako garanti/schvalovatelé nějaké jiné role. Tím bude zajištěna zastupitelnost v případě nepřítomnosti konkrétního garanta nebo při odchodu garanta. Členství ve skupině/roli lze automatizovat pomocí definovaných pravidel.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.11 Žádosti a schvalování

Požadavky v této kapitole se týkají základních požadavků na žádosti a schvalovacího workflow.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A78	Žádost o změnu oprávnění	Řešení musí disponovat samoobslužným portálem, kde uživatelé mohou žádat o změnu oprávnění. Podléhá-li žádost schvalování, je automaticky spuštěno schvalovací workflow. V žádosti o roli je zřetelně vyznačeno, kdo žádá, komu je žádáno, o jaké role, jaké jsou současné role identity a jaké jsou změny rolí (přidané, odebrané, nezměněné). IdM eviduje všechny žádosti o role v přehledu včetně jejich stavu a schvalovatelů, aby bylo dohledatelné, kdo aktuálně žádost řeší, nebo kdo ji finálně schválil. Obsahuje-li žádost o roli také role, které zajišťují provisioning (propis dat do řízeného systému), je ihned po schválení žádosti vyvolán propis dat do systémů. Každá žádost obsahuje evidenci, v jakém stavu se nachází, a to jak z pohledu schválení žádosti, tak z pohledu následné aplikace rolí do řízených systémů – tzn. zda již proběhl propis dat na základě aktuálně změněných rolí v dané žádosti. Schvalovací workflow je konfigurovatelné v aplikaci schvalovací kola lze zapínat/vypínat a workflow může být vícekrokové (více úrovní schvalování dle role či typu požadavku) U každé role je možné definovat, jakým workflow bude schvalována nebo zda nepodléhá schvalování. Konfigurace schvalování je dostupná v GUI pro administrátora IdM a změna nesmí vyžadovat restart aplikace.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A79	Žádost o vybrané role	Administrátor IdM bude mít možnost definovat, o které role v IdM lze žádat a které se nebudou v žádostech uživatelů nabízet. Takto bude možné některé role načítat například z AD a definovat jejich automatické	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		přidělování, avšak uživatelům se nebudou nabízet (a mást je) v žádostech. Jiným příkladem může být seskupování rolí, kdy uživatelé budou moci žádat o definované skupiny, avšak z důvodu složitosti se nebudou nabízet dílčí role.		
A80	Vizualizace průběhu workflow	Průběh konkrétního běžícího schvalovacího workflow je vizualizován ve webovém rozhraní. Vizualizovaný průběh je uložen v auditu pro možnost pozdější revize např. helpdeskem.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A81	Přehled workflow	IdM zpřístupní přehled všech workflow včetně stavu (běží, ukončeno, …). Z přehledu workflow bude možné prohlédnout detail workflow včetně grafické vizualizace průběhu.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.12 Plánovač úloh

Požadavky v této kapitole se týkají základních požadavků na plánovač úloh.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A82	Plánovač úloh	IdM umožní procesy, hromadné operace a reporty spouštět pomocí plánovače. V plánovači bude moci administrátor v grafickém webovém rozhraní naklikat, kdy se má daná úloha spouštět a s jakou periodou. IdM umožní spouštět úlohy v návaznosti. Například v plánovaný čas je spuštěna synchronizace organizační struktury a po úspěšném dokončení synchronizace je spuštěna synchronizace identit, poté kontraktů, poté přidělování rolí, následně třeba report atd. IdM umožní pokročilejší plánování pomocí regulárních výrazů, CRONu nebo podobných výrazových prvků. IdM bude zobrazovat a uchovávat veškeré informace o plánovaných úlohách, zejména: • Všechny rozplánované úlohy s vyznačením termínu příštího spuštění. • V případě, že se úlohy spouštějí v návaznosti (synchronizace identit po synchronizaci organizační struktury), tak je tato závislost v plánovači vyznačená. • IdM musí uchovávat pro auditní účely záznam o proběhlých úlohách včetně zpracovaných objektů a výsledku zpracování, chybových hlášení či varování. V rámci plánovače bude možné spustit vlastní připravené úlohy, jako třeba script pro hromadné operace. Spuštění vlastních úloh nevyžaduje rebuild či restart aplikace.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		IdM bude při dodání obsahovat sadu rozplánovaných úloh pro běžný provoz IdM, jako jsou úlohy životního cyklu identity, systémové úlohy, úlohy pro čištění zastaralých logů atd. IdM umožní plánované úlohy spouštět nanečisto, aby bylo možné kritické úlohy (např. mazací operace) vyzkoušet bez dopadu na data před plným spuštěním.		

5.6.13 Řízené systémy a jejich napojení

Požadavky v této kapitole se týkají základních požadavků na napojení řízených systémů.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A83	Grafický průvodce napojením systémů	IdM nabídne možnost napojit běžné systémy, minimálně: databáze, LDAP, MS AD, CSV a další pomocí grafického průvodce v GUI. Grafický průvodce zajistí jak vytvoření napojení systému, tak ověření funkčnosti napojení pro CRUD operace a přidělení role. Dále zajistí veškeré potřebné konfigurace jako vytvoření potřebných rolí pro napojený systém, vytvoření synchronizační úlohy pro iniciální spárování účtů k identitám.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A84	Režimy online napojených systémů	IdM nabízí při komunikaci s koncovým systémem minimálně tyto režimy: • Plný propis, • Propis s kontrolou, • Pouze pro čtení, • Neaktivní.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A85	Zobrazení operací	IdM umožní přehledně v grafickém webovém rozhraní zobrazit všechny operace, které čekají na propis do napojeného systému i všech již propsaných operací. IdM taktéž umožní: • vyprázdnit vybrané čekající požadavky na propis do sytému • opakovat požadavky (např. při nedostupnosti systému) automaticky v určených intervalech nebo manuálně v GUI. Při manuálním opakování operací zajistí IdM, že bude zachována posloupnost operací pro jednotlivé identity. (např. Create, update, delete), i když uživatel vybere pouze poslední operaci. Každou čekající či provedenou operaci přehledně zobrazí včetně kompletního výčtu všech hodnot, které IdM pro daný účet posílá. Zobrazí, jak stav v IdM, tak stav na systému a	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		přehledně zvýrazní rozdíl hodnot, který je zpropagován do řízeného systému.		
A86	Aktivní hlídání operací	IdM umožní monitorovat všechny prováděné operace (Create, Update, Delete) pro každý systém. V IdM bude možné konfiguračně definovat bezpečné limity (varování, blokace) pro každou operaci na každém systému. Při překročení limitu varování bude IdM notifikovat administrátora. Při překročení limitu blokace bude IdM blokovat veškeré následné operace. Např. IdM umožní nastavit limit operací DELETE pro systém MS AD na úroveň 5 účtů za 30 minut pro varování a 10 účtů za 60 minut na zablokování. Takto bude možné ochránit účty v napojených systémech proti různým incidentům jako velká změna dat z HR systému.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A87	Online zobrazení aktuálních atributů účtu na napojeném systému	IdM umožní v grafickém uživatelském rozhraní online náhled na účet a jeho atributy v napojeném systému. Administrátoři tak budou moci kontrolovat propis dat bez nutnosti použít jinou aplikaci pro správu řízených systémů, například pokud k ní nemají přístup.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A88	Rozdílový seznam stavu účtů	IdM umožní pravidelně validovat stav účtů na koncovém systému oproti stavu v identity manageru a na základě toho vystaví report rozdílů. Rozdíly jsou evidovány až na úroveň konkrétních hodnot atributů účtů a stavu přidělených rolí/skupin.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A89	Knihovna transformačních pravidel pro napojování systémů.	V rámci průvodce lze nastavit standardní pravidla pro změnu dat směrem do systému IdM i z IdM do řízeného systému. Knihovna obsahuje běžné transformace jako: • změna datových typů. String <-> Int <-> Date apod. • slučování více atributů do jednoho výstupního atributu. Např. jméno + příjmení -> display Name.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.14 Evidence

Požadavky v této kapitole se týkají základních požadavků na evidenci certifikátů, licencí nebo drobného majetku.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A90	Podpora managementu uživatelských certifikátů a licencí	IdM umožní napojení na certifikační autoritu pro: • žádosti o certifikáty, • hlídání platnosti a notifikace o blížícím se vypršení platnosti s odkazem na obnovu,	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		• obnova a stažení certifikátu. Validace manuálně nahraného certifikátu IdM přehledně v grafickém rozhraní zobrazí seznam certifikátů uživatele včetně sériového čísla a aktuálního data platnosti. IdM také umožní: • manuálně vložit certifikát k identitě skrz grafické webové rozhraní a stáhnout certifikát, • distribuovat certifikáty a sériová čísla do napojených systémů. IdM umožní v samoobsluze uživatelů požádat o licenci a její vydání je schvalováno podobně jako přidělení rolí.		
A91	Podpora evidence a managementu vydaného drobného majetku identitám	IdM v rámci správy životního cyklu identit zajistí možnost k identitám evidovat drobný vydaný majetek jako např. mobilní telefon, notebook, přístupové karty atd. Evidenci a přidělení drobného majetku bude přehledně řešeno v grafickém webovém rozhraní.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.15 Notifikace

Požadavky v této kapitole se týkají základních požadavků na napojení řízených systémů.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A92	Správa notifikací	IdM musí poskytovat možnost odesílat mailové a SMS notifikace. Rozhraní správy notifikací a náhledu na odeslané notifikace bude v grafickém rozhraní systému. IdM umožní konfiguračně v grafickém rozhraní deaktivovat odesílání e-mailů i SMS se zachováním logování pokusů o odeslání pro kontrolu notifikací. IdM musí podporovat odesílání testovacích zpráv.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A93	Napojení na SMS bránu	Řešení musí obsahovat mechanismus na odesílání SMS notifikací. Mechanismus je možné napojit na SMS bránu. SMS brána není součástí poptávaného řešení. objednatel již provozuje vlastní SMS bránu.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A94	E-mailové a SMS notifikační šablony	IdM nabídne možnost v grafickém rozhraní upravovat šablony notifikací odcházejících z IdM. Nejméně je možné upravovat: • příjemce • předmět a obsah dané notifikace	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		E-mailové notifikace je možné definovat ve formátu čistého textu (plaintext) i stylovaného formátu (HTML). Do HTML šablony musí být možné vkládat hodnoty objektů z IdM, jako např. login identity, a také odkazy na objekty v IdM (např. odkaz na schvalovací úkol nebo odkaz na roli v IdM).		

5.6.16 Reporting

Požadavky v této kapitole se týkají základních požadavků na napojení řízených systémů.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A95	Požadavky na reporting	IdM musí podporovat generování reportů minimálně do formátu kompatibilního s MS Excel a do strojově zpracovatelných formátů jako např. JSON. IdM řešení umožní reporty generovat na vyžádání z grafického webového rozhraní i plánovat jejich pravidelné spouštění (např. každý den ráno přehledový report). V případě plánovaného spuštění IdM odešle po vytvoření reportu notifikaci s reportem či odkazem na získání reportu. Data obsažená v reportech budou podléhat stejnému systému řízení práv jako při prohlížení dat v grafickém webovém rozhraní nebo univerzálním API. Tzn. uživatel si do reportu může dát pouze taková data, na která má v IdM právo – např. vedoucí si může do reportu vyexportovat pouze sebe a své podřízené. Administrátor může exportovat všechny uživatele. Garant rolí může exportovat pouze role, jimž je garantem apod.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A96	Základní set reportů	Dodané řešení bude obsahovat nejméně následující reporty: • Denní přehled změn v životním cyklu identit – nástupy, odchody, nové mateřské apod… • Denní přehled monitoringu aplikace – všechna varování či chyby procesů IAM (chyba v propisu, synchronizaci apod.) • Přehled identit, kontraktů a přidělených rolí • Přehled rolí a příslušných držitelů • Změny v přiřazení rolí uživatelů v definovaném období • Přehled změn hesla uživatelů pro vybraný systém • Všechny změny účtů na vybraném koncovém systému	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.17 Migrační nástroje

Požadavky v této kapitole se týkají základních požadavků na migrační nástroje nezbytné pro implementaci, rozvoj IdM, ale i pro případný přechod na jiné řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A97	Export/Import	IdM bude obsahovat migrační nástroje pro export konfigurací a naplnění IdM daty. Import dat: • import externistů mimo HR – identit, platností kontraktů, garantů externistů, … • naplnění off-line systémů – účty a atributy, role a jejich přiřazení k účtům, vazby na identity v IdM, • import katalogů rolí, • import organizačních struktur mimo HR – například z AD, csv, DB (struktury projektů), • import pravidel pro automatické přidělování rolí Export/Import konfigurací (migrace IdM) je nutný zejména pro dávkový či automatizovaný přenos konfigurací z testovacího prostředí do předprodukčního/referenčního či produkčního systému. IdM umožní importovat/exportovat: • konfiguraci aplikace IdM • konfiguraci napojených systémů • role pro napojené systémy i rolí pro přidělování práv v IdM	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A98	Export dat z grafického rozhraní	Objekty identit, systémů a rolí lze v grafickém webovém rozhraní přehledně vyfiltrovat a hromadně exportovat do formátu kompatibilního s MS Excel. Dále lze z IdM jednoduše zálohovat do souboru konfigurace všech napojených systémů a všech rolí.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.18 Bezpečnost

Požadavky v této kapitole se týkají základních požadavků na bezpečnost dodávaného řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
A99	Okamžitá blokace účtů identity	IdM musí být schopno řešit mimořádné události při zcizení identity – okamžité zakázání identity ve všech řízených systémech.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

A100	Požadavky na auditní nástroje	IdM musí uchovávat kompletní auditní záznamy všech objektů s možností porovnání jejich stavů v různých časových okamžicích. Audit dále bude obsahovat nejméně: • audit změn hesla, • audit přidělení rolí včetně odkazu na proces a schvalovatele procesu, • audit všech synchronizací – průběh, log chyb, log zpracovaných objektů, • audit všech odchozích operací do řízených systémů včetně obsahu přenášených dat, • provozní aplikační audit – zaznamenává události systému, • notifikační log – zaznamenává log odeslaných emailových a sms notifikací, • audit plánovaných úloh – všechny běhy úloh spuštěných v rámci plánovače, • audit hromadných změn. IdM musí poskytovat kompletní auditní stopu od konkrétní změny až k její inicializaci včetně všech mezikroků.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
A101	Podpora prohlížeče	Uživatelské rozhraní IdM musí být přístupné přes webové rozhraní s podporou prohlížeče MS Edge v nejnovějších verzích	(Doplní dodavatel)	(Splňuje/Nesplňuje)

5.6.19 Požadavky na zálohování

Řešení bude zahrnovat pravidelné a aktivní zálohování dat a konfigurací, aby byla v případě neočekávaných událostí zajištěna jejich spolehlivá obnova dle definovaných recovery plánů. Součástí dodávky bude také doporučení pro zálohování infrastrukturních komponent spravovaných objednatelem, například zálohování virtualizačního prostředí nebo přenos záloh IdM na jiný server, což zajistí ochranu proti ztrátě dat v případě nenávratného poškození primárního serveru.

5.6.20 Požadavky na monitoring IdM zajistí monitoring na několika úrovních

Komplexní monitoring provozu IdM s přehledem dostupným v grafickém webovém rozhraní. Administrátor bude mít možnost z jednoho místa snadno vyhodnotit aktuální stav systému a zjistit, zda je třeba zasáhnout. K dispozici budou zejména tyto přehledy:

- Kompletní záznamy událostí systému s označením nevyřešených chyb.
- Přehled chyb v komunikaci se systémy, zahrnující jak synchronizaci, tak propis dat.
- Přehled čekajících a neprovedených úloh, reportů a operací směřujících do koncových systémů.
- Denní souhrn obchodních změn týkajících se identit, jako jsou nástupy, odchody nebo nové výjimky z evidenčního počtu.

API pro externí monitoring a správu logů, které umožní integraci s nástroji Zabbix, Logmanager.

6 Požadavky na plnění Etapy 2

6.1 Doplnění předimplementační analýzy pro Etapu 2

Dodavatel doplní a aktualizuje předimplementační analýzu zpracovanou v rámci Etapy 1 o minimálně tyto body:

- Případná aktualizace provozního modelu v rámci infrastruktury, potřebných zdrojů, sizingu.
- Návrh politik PAM řešení detailně specifikovaných během analýzy a vycházející z „best practice“ doporučení výrobce technologie.
- Technologické požadavky na zajištění provozu.
- Popis konfigurace komponent PAM řešení.
- Detailní popis instalačních postupů, a to včetně testovacího prostředí.
- Detailní popis zálohování a obnovy PAM systému, řešení DR scénářů včetně návrhů testovacích scénářů zahrnujících totální výpadek a obnovy do provozního stavu (bude součástí akceptačních testů).
- Návrh metodiky nakládání s break-glass účty a scénáře na jejich otestování (bude součástí akceptačních testů).
- Popis způsobů aktualizace PAM řešení (všechny části PAM).
- Monitoring PAM řešení.
- Návrh detailního harmonogramu Etapy 2 a procesních kroků pro implementaci řešení včetně návrhu konfigurace řešení v jednotlivých fázích implementace a definice finální podoby dodávaného řešení.
- Popis náběhu systému (popis testovacího provozu až do doby akceptace).
- Návrh testovacích scénářů a use-caseů, minimálně: uživatelské akceptační testy (UAT), funkční testy, integrační testy, systémové testy, výkonnostní testy, bezpečnostní testy, regresní testy, test výpadku jednoho z datových center.
- Návrh maximálně automatizovaného discovery procesu privilegovaných účtů po zavedení PAM.

6.2 Implementace a integrace Etapy 2

Cílem této fáze bude dodávka a implementace systému PAM, v prostředí STC a realizace všech souvisejících implementací a integrací se zdrojovými systémy a s koncovými systémy, jejichž uživatelská základna bude spravována pomocí systému PAM.

6.2.1 Instalace systému PAM

Objednatel provede instalaci systému do prostředí STC minimálně v tomto rozsahu:

- nastavení politik pro PAM,
- nastavení nahrávání privilegovaných relací,
- integrace s dalšími systémy prostředí STC (zejména AD/LDAP a SSO, nástroje pro bezpečnostní a provozní monitoring)
- nastavení zálohování atd.

V rámci této fáze dodavatel vybuduje také testovací prostředí systému PAM s plnou funkčností produkčního prostředí. HW zdroje formou virtuálních strojů a síťové prostředí pro testovací prostředí zajistí STC podle specifikace, kterou dodá dodavatel nejpozději po předimplementační analýze.

6.2.2 Integrace na systémy Etapy 2

Dodavatel provede úvodní implementaci systému PAM pro vybrané koncové systémy

v prostředí STC a konfiguraci všech komponent systému pro tyto systémy:

VMware

Integrace VMware prostředí do PAM řešení tak, aby byla zajištěna vzdálená správa plně přes PAM technologii.

AD

Kompletní správa Microsoft AD přes technologii PAM.

Microsoft 365

Správa cloudového prostředí M365 výhradně přes technologii PAM.

IdM

Správa IdM technologie pomocí PAM.

Windows Servery

Zajištění správy Windows serverů přes RDP protokol výhradně přes technologii PAM, včetně zajištění nahrávání session (zajišťuje PAM).

6.3 Dokumentace Etapy 2

Veškerá dokumentace k předmětu Smlouvy musí být vypracována v českém jazyce. Mohou v ní být použité části v anglickém jazyce, např. ilustrace přímo od výrobce technologie apod., ale s doplňujícím vysvětlením, případně výkladem odborných pojmů v českém jazyce.

Dodávka musí zahrnovat minimálně následující dokumenty:

- **Dokumentace dodaného systému**: Produktovou dokumentaci výrobce ke všem dodávaným modulům PAM.
- **Dokumentace skutečného provedení**: Obsahuje detailní návrh dodaného řešení formou diagramů a popis všech úprav provedených v prostředí objednatele oproti výchozí či standardní konfiguraci jednotlivých komponent.
- **Dokumentace instalace softwaru**: Instalační dokumentaci (předpis pro prvotní instalaci a instalační postupy pro údržbu a rozvoj systému PAM) a dokumentaci k integrovaným systémům.
- **Plán obnovy (DR plan)**: Popis havarijních plánů pro obnovu služeb Systému PAM.
- **Testovací scénáře**: Budou připraveny akceptační testy využívané jak objednatelem při ověřování funkčnosti aplikace, tak i později jako regresní testy pro kontrolu základních funkcí při nasazování nových verzí a upgradů řešení.
- **Plán přechodu do produkčního provozu**: Před spuštěním PAMu v produkčním prostředí bude vytvořen detailní plán nasazení. Ten bude obsahovat checklist se všemi nezbytnými kroky: instalace a konfigurace produkční.
- **Plán zálohování**: Dokumentace bude obsahovat návrh a popis zálohovacích postupů, které provádí jak objednatel, tak dodavatel.

Dokumentace musí být kompletní a průběžně aktualizována po celou dobu trvání smluvního vztahu tak, aby vždy odpovídala aktuální verzi softwaru. Dokumentace může být poskytnuta i formou přístupu k online dokumentaci.

6.4 Školení Etapy 2

Dodavatel zajistí školení pracovníků objednatele v oblasti administrace, provozu a uživatelském používání implementovaného nástroje PAM dle níže uvedených požadavků objednatele.

Dodávaný produkt musí být doplněn o školící materiály a návody pro správu systému, a to alespoň v následujícím rozsahu:

- **Příručka administrátora**: Popisující Systém PAM z pohledu administrátorů, která obsahuje popis všech administrátorských úkonů vyplývajících z požadavků této TS.

Požadavky na školení

Řešení musí zahrnovat školení v rozsahu minimálně **3 MD** v součtu pro tyto skupiny uživatelů:

- Klíčové uživatele a garanty systémů,
- Bezpečnostní správce,

- Systémové administrátory.

6.5 Testovací provoz a akceptace pro Etapu 2

6.5.1 Testovací provoz

Před uvedením systému PAM do produkčního prostředí bude dodavatel ve spolupráci se objednatelem provozovat PAM v testovacím prostředí. Cílem tohoto období bude identifikace případných provozních/konfiguračních nedostatků a jejich oprava před uvedením nástroje do produkčního provozu. V rámci tohoto období bude Dodavatel poskytovat zvýšenou podporu při řešení identifikovaných nedostatků.

Testovací provoz je ukončen schválením přechodu do produkčního provozu ze strany objednatele. Tímto aktem se PAM řešení jako celek předává do plného provozu. Testovací provoz tvoří závěr Etapy 2 a jeho délka bude činit **min. 1 měsíc** po dokončení fáze F2.2 Harmonogramu. Testovací provoz bude probíhat po dobu nezbytně nutnou k ověření funkčnosti systému PAM.

6.5.2 Akceptace a přechod do produkčního provozu

Během testovacího provozu využívá objednatel PAM řešení v plném rozsahu a přistupuje k němu z provozního hlediska jako k plnohodnotnému produkčnímu prostředí. Zároveň průběžně sleduje a vyhodnocuje, zda prostředí splňuje stanovené požadavky.

Na konci testovacího provozu dodavatel provede akceptační testy (dle odsouhlasených testovacích scénářů definovaných v rámci Předimplementační analýzy), které ověří, že systém PAM splňuje všechny požadavky stanovené v této Technické specifikaci a že příslušná část předmětu plnění Smlouvy je provedena v souladu s předimplementační analýzou (dále jen „testy“). Testy proběhnou dle testovacích plánů, které jsou obsaženy v akceptované předimplementační analýze. objednatel je oprávněn vyžádat si doplnění plánu testů o další konkrétní testy, pokud to bude považovat za účelné pro ověření kompletní funkčnosti systému PAM. V okamžiku, kdy objednatel dospěje k závěru, že prostředí je plně funkční a odpovídá požadavkům zadání, podepíše s dodavatelem akceptační protokol o převzetí prostředí PAM a jeho předání do produkčního provozu.

Akceptace a přechod do produkčního provozu do produkčního provozu **nemůže být provedeno dříve** než po uplynutí prvního měsíce testovacího provozu a současně nemůže být dříve než vypracování dokumentace a průběh školení dle kapitol 6.3 a 6.4.

Součástí akceptace je kontrola existence a aktuálnosti dokumentace v rozsahu odpovídajícím dodávané verzi softwaru, resp. implementaci a konfiguraci v prostředí objednatele.

Dodavatel je povinen při přechodu do produkčního provozu předat veškeré zdrojové kódy a build/CI skripty s výjimkou případů, kdy se jedná o Standardní Software třetích stran nebo jiné komponenty, ke kterým dodavatel nemá licenční oprávnění ke zdrojovým kódům.

6.6 Technické požadavky na řešení PAM

Tato kapitola specifikuje funkční požadavky objednatele na budoucí řešení pro správu privilegovaných účtů (PAM), které navrhované řešení dodavatele musí bezezbytku splňovat.

Tato kapitola je členěna dle jednotlivých požadavků následovně:

- V kapitole 6.6 jsou uvedeny **Obecné požadavky** na PAM řešení,
- V kapitole 6.7 jsou uvedeny požadavky na **Řízení privilegovaných účtů a hesel,**
- V kapitole 6.8 jsou uvedeny požadavky na **Řízení a nahrávání relací.**

6.6.1 Použitá technologie a architektura

Požadavky v této kapitole se týkají použité technologie a celkové architektury PAM řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
B1	On premise řešení	Je požadováno „on-premise“ řešení PAM, cloudové řešení PAM se nepřipouští. Aplikační brány PAM řešení mohou být umístěné v cloudu za podmínky, že neobsahují uživatelská data.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B2	Použití bezagentního řešení	PAM řešení musí být „bezagentní“, nesmí tedy vyžadovat instalaci agentů na koncové systémy.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B3	Zabezpečení PAM	Všechny komponenty dodaného PAM řešení musí být dostatečným způsobem zabezpečeny prostřednictvím následujících minimálně nutných opaření: • Musí být proveden hardening jednotlivých komponent PAM. • Musí být zabezpečena citlivá komunikace mezi komponentami, s externími systémy, nebo s uživateli s využitím dostatečně robustních kryptografických opatření. • Musí být dostatečně zabezpečen přístup k citlivým údajům a funkcím systému (jako jsou například hesla, nebo funkcionalita změny hesel) pomocí kryptografických opatření.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

6.6.2 HW a SW nároky

Požadavky v této kapitole se týkají základních požadavků na hardwarové a softwarové nároky PAM řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
B5	Využití virtualizace	PAM řešení musí být implementovatelné na platformě x86 a musí být instalováno do virtuální VMware infrastruktury objednatele. Výjimku může tvořit úložiště hesel produkčního prostředí, které (pokud tak dodavatel navrhne ve svém řešení) může být instalováno na fyzický server. Dodavatel dále doplní: Počet požadovaných virtuálních serverů (příp. fyzických serverů) a jejich parametrů s ohledem na dostatečnou výkonnost řešení a současnou adekvátnost parametrů, Požadavky na parametry komunikačních tras a síťových prostupů mezi jednotlivými komponentami řešení (pokud jsou takové kritické pro funkčnost).	(Doplní dodavatel)	(Splňuje/Nesplňuje)

B6	Podpora	PAM řešení musí podporovat koncové systémy, které jsou u objednatele provozovány, viz Příloha 1b, Tabulka D, E. Součástí dodávky PAM musí být návrh úložiště pro archivaci nahrávek. Dodavatel uvede specifikaci potřebné kapacity, typu úložiště a připojení v popisu nabízeného plnění/řešení dodavatele.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B7	Velikost úložiště pro archivaci	Pro výpočet potřebné kapacity úložiště může dodavatel vycházet z následujících předpokladů: • Budou nahrávány všechny administrátorské relace, přičemž počet administrátorů je uveden v Příloze č. 1b bod 1.6. - Je požadováno uchování nahrávek pro okamžitý přístup (tj. bez nutnosti jejich vyvolání z archivu) po dobu alespoň 18 měsíců. Tato doba může být upřesněna v průběhu Etapy 2.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B8	Podpora prohlížeče	Uživatelské rozhraní PAM musí být přístupné přes webové rozhraní s podporou prohlížeče MS Edge v nejnovějších verzích.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B9	Využití nativních klientských aplikací	PAM musí umožnit připojení ke koncovému systému pomocí SSH/RDP z klientské stanice s využitím nativních klientských aplikací (např. PuTTY, Připojení ke vzdálené ploše) tak, že se uživatel nejprve ověří vůči systému PAM a následně PAM automatizovaně přihlásí privilegovaný účet na koncovém systému, po celou dobu musí být zajištěna izolace session, nahrávání a přihlašovací údaje privilegovaného účtu nesmí být uživatelem zadávány ani mu být zobrazeny.*PTK	(Doplní dodavatel)	(Splňuje/Nesplňuje)

6.6.3 Zajištění vysoké dostupnosti

Požadavky v této kapitole se týkají zajištění vysoké dostupnosti (*HA*) PAM řešení.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
B11	Vysoká dostupnost PAM	Produkční prostředí PAM bude provozováno v režimu vysoké dostupnosti tak, aby výpadek jednotlivé komponenty neomezil funkčnost řešení ani přístup privilegovaných uživatelů ke koncovým systémům. U komponent, jejichž výpadek nemá za následek nedostupnost PAM služby ani omezení přístupu uživatelů, není režim vysoké dostupnosti požadován, pokud to odpovídá doporučení výrobce a je to řádně odůvodněno v předimplementační analýze včetně posouzení dopadů na bezpečnost a provoz.*PTK	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		Každá z komponent PAM tedy musí obsahovat minimálně dvě samostatné instance provozované v HA módu active/active, nebo active/passive. Řešení vysoké dostupnosti musí být plně automatické. Řešení, která vyžadují jakoukoliv manuální intervenci pro přepnutí mezi instancemi v případě vzniku chybového stavu, nejsou přípustná. Vysoká dostupnost musí být plně zajištěna na úrovni dodávaného řešení, tedy buď na úrovni samotné aplikace a/nebo OS.		
B12	Dostupnost	Minimální požadovaná dostupnost PAM řešení v úrovni 99,75 % / měsíc. Do nedostupnosti služby PAM se nezapočítává čas, kdy je nedostupnost způsobena nedostupností infrastruktury zajišťované objednatelem.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

Integrace

Požadavky v této kapitole se týkají požadavků na integraci PAM řešení s okolními systémy.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
B13	Lokálně vytvořené účty	PAM řešení musí umožnovat spravovat i lokálně vytvořené privilegované účty, tj. účty, které nejsou spravovány pomocí AD, ale byly založeny „manuálně“ na koncových systémech.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B14	Integrace se Service Desk nástrojem	**PAM řešení musí podporovat integraci se Service Desk nástrojem HelpDesk Requestor tak, aby z PAM bylo možné automatizovaně zakládat tikety (žádosti) v Requestoru pro požadavky související s privilegovanými účty (zejména zřízení, změna a zrušení privilegovaného účtu nebo přístupu).** Minimálním požadavkem je možnost založit v Requestoru ticket s předáním relevantních údajů (typ požadavku, žadatel, cílový systém, požadovaný privilegovaný účet/přístup, odůvodnění, případně priorita). Integrace může být realizována prostřednictvím REST API, webových služeb nebo jiného standardního rozhraní podporovaného nástrojem HelpDesk Requestor. **Není požadována plná obousměrná integrace**, minimem je výše uvedené zakládání ticketů z PAM do Requestoru.**PTK*	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B15	Workflow pro řízení privilegovaných účtů	Součástí dodávky PAM řešení musí být návrh workflow pro řízení životního cyklu privilegovaných účtů (zřízení, změny, zrušení), které využívá Service Desk nástroj HelpDesk Requestor. Workflow musí při vzniku požadavku využívat integraci dle bodu B14, tj. **automaticky založit odpovídající ticket v Requestoru**.**PTK*	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B16	Integrace logů	Součástí dodávky musí být integrace PAM se stávajícím nástrojem pro sběr logů LogManager.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

B17	Integrace s IdM systémem	Integrací se rozumí napojení PAM na nástroj tak, aby se přenášely bezpečnostní záznamy (logy) z PAM do systému LogManager. Dodávané řešení musí podporovat integraci s dodávaným IdM systémem, který je součástí tohoto výběrového řízení. Integrací se rozumí možnost automatizované správy uživatelů a privilegovaných účtů	(Doplní dodavatel)	(Splňuje/Nesplňuje)

6.6.4 Auditing, reporting a notifikace

Požadavky v této kapitole se týkají funkcionalit auditingu, reportingu a upozornění (notifikace).

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
B18	Zaznamenávání událostí	PAM řešení musí zaznamenávat události ve formě strukturovaných logů, které jsou v reálném čase přenášeny a vyhodnocovány v nástroji objednatele a ukládány pro případnou zpětnou analýzu. Musí být zaznamenány aktivity provedené: • Uživateli PAM (tj. administrátoři, kteří používají PAM řešení pro přístup k spravovaným koncovým systémům), • Správci PAM, kteří provádí konfiguraci PAM řešení a správu politik.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B19	Typy zaznamenávaných událostí	Minimálně musí být zajištěno logování následujících typů událostí vykonaných v rámci PAM: • Úspěšné a neúspěšné přihlášení a odhlášení PAM, • Změny v konfiguraci PAM, • Přístup k heslu privilegovaného účtu nebo jeho použití, • Přístup k nahrané session.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B20	Zabezpečení logů	Logy PAM musí být řádně zabezpečeny proti možným úpravám/smazání. PAM musí poskytovat funkce automatické archivace logů s možností nastavení frekvence a retence.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B21	Reporting	PAM řešení musí podporovat vytváření reportů ve formátech PDF, CSV nebo MS Excel (XLS/XLSX). Měli by být k dispozici minimálně následující předdefinované typy reportů: • Seznam uživatelů a jejich oprávnění, včetně výpisu účtů, které mají k dispozici, • Seznam všech spravovaných účtů, včetně přiřazených politik hesel a výčtu	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		uživatelů, kteří mají k danému účtu přístup, • Seznam aktivit nad účty (check out/in, přidělení účtu atp.).		
B22	Upozorňování na události	PAM řešení musí umožnit nastavit upozornění na základě vybraných událostí (např. přístup na systém, použití určitého účtu atd.). Upozornění musí být zasíláno e-mailem určené osobě.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B23	Monitoring pomocí RestAPI	Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI - integrace s monitoring systémy objednatele.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

6.7 Řízení privilegovaných účtů a hesel

Požadavky v této kapitole se týkají požadavků na správu privilegovaných účtů a hesel.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splnění konkrétního požadavku)	Splňuje/Nesplňuje
B24	Typy privilegovaných účtů	PAM řešení musí zajistit řízení následujících typů privilegovaných účtů: • Účty interních a externích uživatelů (tj. administrátorů), • Sdílené účty, • Účty aplikací, • Servisní účty, • SSH klíče.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B25	Funkcionalita objevování účtů	PAM řešení musí v pravidelných intervalech provádět automatické objevování (tzv. „*account discovery*“) koncových systémů a privilegovaných účtů. Nově objevené účty musí být před přidáním do PAM posouzeny odpovědnou osobou (Správcem PAM), zda se jedná o uživatelský účet patřící konkrétní identitě, nebo zda se jedná o sdílený účet. Odpovědná osoba rozhodne o zařazení účtu do PAM, přiřadí privilegovaný účet příslušným uživatelům a nastaví odpovídající politiku hesel.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B26	Zabezpečení úložiště hesel	Součástí PAM řešení musí být zabezpečené úložiště privilegovaných účtů a hesel. Toto úložiště musí být pravidelně zálohováno tak, aby byla zaručena jeho dostupnost. Zálohy musí být dostatečně zabezpečeny proti neoprávněnému přístupu šifrováním.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B27	Řízení přístupu k heslům	Musí být implementován proces zajišťující bezpečný přístup k heslům uložených v PAM, a to i v případě jeho částečné nebo úplné nedostupnosti.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

B28	Správa rolí v rámci PAM	PAM řešení musí umožňovat členit uživatele do následujících rolí: • Uživatel PAM – je mu umožněn přístup k PAM a jeho běžné používání. Uživatelé PAM jsou administrátoři (interní zaměstnanci) nebo externí dodavatelé odpovědní za správu koncových systémů. • Auditor – má přístup k auditním informacím a nahrávkám. • Správce PAM – konfiguruje PAM nebo jeho část, může vytvářet/upravovat/odstraňovat objekty PAM. • Správce PAM nesmí mít možnost odstraňovat auditní informace a nahrávky. • Schvalovatel – schvaluje přístupy k vybraným skupinám účtů.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B29	Politiky hesel	V PAM řešení musí být definovány politiky hesel, které budou aplikovány na uživatele nebo skupiny uživatelů. Politika hesel musí zajistit alespoň následující parametry: • Minimální délka hesla, • Složitost hesla (požadavky na povinné znaky), • Maximální stáří hesla, • Historie hesel (opakovatelnost hesla). Politiky hesel musí být vynucovány během generování nových hesel, nebo při manuálních změnách hesel prostřednictvím PAM. PAM musí automaticky provést změnu hesla na koncovém systému, pokud vypršelo jeho maximální stáří, které je definované v přiřazené politice hesel.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B30	Vzdálená změna hesla	PAM řešení musí podporovat funkci vzdálené změny hesla na řízených koncových systémech (Příloha 1b, Tabulky D, E). Změna hesla musí být poskytnuta v rámci následujících akcí na řízeném účtu: • Reset hesla, • „Check-out“ nebo „Check-in“ hesla (poskytnutí hesla uživateli spolu s označením účtu jako používaného daným uživatelem, resp. jeho odznačení)	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B31	Upozornění na neautorizovanou změnu hesla	PAM řešení musí v pravidelném intervalu kontrolovat, zda heslo na koncovém systému odpovídá evidovanému heslu v PAM. V případě rozdílu musí být odeslána notifikace.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B32	Identifikace a autentizace k PAM	Uživatelé musí přistupovat k PAM řešení prostřednictvím webového rozhraní a musí se autentizovat s využitím dvou faktorů následovně: • První faktor autentizace: oproti lokálnímu, nebo externímu adresáři (např. AD/LDAP),	(Doplní dodavatel)	(Splňuje/Nesplňuje)

		• Druhý faktor autentizace bude vůči existujícímu 2FA řešení Microsoft MFA nebo SMS. Přihlašování k vybranému spravovanému privilegovanému účtu musí probíhat pomocí automatizovaného přihlášení (SSO) tak, aby nebyly zveřejněny přihlašovací údaje. Uživatelé si tedy nebudou muset pamatovat mnoho hesel k různým koncovým systémům, ale budou využívat jen heslo svého účtu. Během SSO musí být heslo automaticky zadáno na pozadí bez možnosti jeho odhalení, tedy heslo nesmí být aplikaci předáno v prostředí uživatele (např. nesmí být v paměti uživatelské stanice).		
B33	Požadavky na dvoufaktorovou autentizaci	V prostředí objednatele je implementován Microsoft MFA / SMS. Jako autentizační prostředek jsou využívány jednorázová hesla (OTP). Je požadováno, aby pro přístup k PAM řešení bylo využito tohoto existujícího 2FA řešení.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B34	Autorizace k použití privilegovaného účtu	Po úspěšném přihlášení k PAM získává uživatel množinu privilegovaných účtů, které může používat. Kromě účtů, které má uživatel volně k dispozici, může mít také přiřazeny účty, ke kterým smí získat přístup na základě vyplnění žádosti a jejím schválením. PAM musí zajistit podporu schvalovacího workflow tak, že pro konkrétní privilegové účty nebo skupiny privilegovaných účtů musí být definováni oprávnění schvalovatelé nebo skupiny schvalovatelů.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B35	Schvalovací workflow	Součástí dodávky PAM musí být návrh schvalovacího workflow pro přidělení privilegovaného účtu uživateli (na základě podané žádosti). Navržené schvalovací workflow musí podporovat: • víceúrovňové kaskádovité schvalování, • schvalování skupinou v režimu 1 z N (alespoň jedno schválení z N schvalovatelů).	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B36	Žádost o použití privilegovaného účtu	Žádost o použití privilegovaného účtu musí být zaslána schvalovatelům na e-mail s uvedením důvod přístupu a požadovaného času přístupu. Na základě schválení ze strany schvalovatele získává uživatel přístup, a to buď na omezenou dobu, nebo na stálo. Součástí žádosti o použití účtu musí být zdůvodnění žádajícího uživatele a tato žádost musí být v PAM prokazatelně zaznamenána bez možnosti ji vymazat či jakkoliv změnit. Uživatel musí mít dále možnost zadat čas, na jak dlouho požaduje přístup a systém mu umožní přístup pouze ve stanoveném čase (vícenásobně).	(Doplní dodavatel)	(Splňuje/Nesplňuje)

B37	Nouzové (emergency) přístupy	Musí být navržen a implementován proces pro nouzové (tzv. „emergency“) přístupy, kdy je potřeba získat okamžitě přístup k privilegovanému účtu a není dostupná příslušná odpovědná osoba. Při spuštění takového procesu musí být vytvořen záznam o této události a odeslána notifikace na určenou kontaktní osobu/osoby. Je požadováno, aby bylo součástí dodávky PAM návrh základních DR procesů.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B38	Řízení aplikačních účtů	PAM musí zajistit správu účtů aplikací a poskytnout mechanismy pro omezení použití otevřeného hesla přímo ve zdrojovém kódu aplikace nebo skriptu.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B39	Řízení SSH klíčů	PAM musí umožňovat ukládat a automaticky měnit SSH klíče na koncových systémech.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B40	Sdílení privilegovaných účtů	PAM řešení musí umožňovat zamezit paralelnímu využívání sdíleného privilegovaného účtu různými uživateli, tj. musí umožnit označit řízené účty jako exkluzivní. Takové účty může v jednu chvíli používat (prostřednictvím funkce check-out/in a SSO) maximálně jeden uživatel.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B41	Správa řešení pomocí Rest API	Řešení je možné spravovat pomocí Rest API a to minimálně na úrovni - vytváření uživatelů a účtů, nastavení oprávnění, změny politik, system health monitoring, schvalování požadavků, autentizace atp.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B42	Integrace uživatelů z IdM nástroje do PAM řešení	Řešení PAM musí umožňovat automatizovaný onboarding uživatelů z IdM nástroje. Nový uživatel, který bude spravovat interní systémy, bude automatizovaně přidán do PAM řešení. Odebrání uživatele v IdM nástroji bude automatizovaně odebírat uživatele z PAM řešení.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B43	Integrace privilegovaného účtu z IdM nástroje do PAM řešení	Řešení PAM musí umožňovat automatizovaný onboarding privilegovaných účtů pro správu systémů z IdM nástroje. Pro nově vytvořeného správce v IdM nástroji dojde k automatizovanému vytvoření privilegovaného účtu v PAM řešení. Odebráním správce z IdM nástroje dojde k odebrání privilegovaného účtu z PAM řešení.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

6.8 Řízení a nahrávání relací

Požadavky v této kapitole se týkají požadavků na řízení a nahrávání relací.

ID	Název požadavku	Popis požadavku	Hodnota (popis nabízeného plnění, splněníkonkr	Splňuje/Nesplňuje

			étního požadavku)	
B44	Způsob nahrávání relací	Musí být zajištěno nahrávání relací, uskutečněných prostřednictvím PAM řešení. V případě, že je nahrávání pro daný privilegovaný účet zapnuto, musí být snímána obrazovka a logovány vstupy, které Uživatel zadá na klávesnici (key-logging). Lze tedy jednoznačně dohledat, kdo daný privilegovaný účet použil a jaké operace byly pod tímto účtem provedeny.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B45	Formáty nahrávaných relací	PAM musí umožňovat nahrávat následující formáty relací: • SSH, • RDP, • HTTPS.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B46	Maximální velikost nahrávky	Nahrávky musí být efektivním způsobem zaznamenávány a přenášeny (např. formou komprimace, zaznamenávání pouze aktivní relace), aby nedocházelo ke výraznému zatěžování prostředků (úložiště, sítě).	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B47	Rozsah nahrávaných relací	Přesné politiky pro nahrávání relací Uživatelů PAM budou stanoveny v průběhu Implementace PAM. Nicméně, PAM musí být kapacitně schopen nahrávat současně relace všech Administrátorů připojených PAM.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B48	Upozornění uživatelů	Uživatelé musí být PAM řešením upozorněni na skutečnost, že je jejich aktivita nahrávána.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B49	Zabezpečení nahrávek	PAM řešení musí zajistit důvěrnost, integritu a dostupnost nahrávaných záznamů po celou dobu, kdy jsou pod správou PAM. PAM musí zaručit, že není možné nahrávky jednoduše odstranit ani upravit, aby nemohla být zpochybněna jejich průkaznost.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B50	Řízení přístupu k nahrávkám	Nahrávky musí být bezpečně přenášeny a ukládány v centrálním úložišti nahrávek. Po celou dobu jejich existence v PAM musí být zaručen pouze autorizovaný přístup k nim. Pouze autorizované osoby mohou mít k nahrávkám přístup, mohou je exportovat a prohlížet.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B51	Princip čtyř očí	V případě potřeby musí PAM zajistit, že přístup k nahrávkám je umožněn pouze na základě metody čtyř očí (tj. je požadována autorizace přístupu k nahrávce další osobou).	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B52	Pozastavení/terminace relací	PAM řešení musí nabídnout možnost automatického pozastavení, nebo terminace potenciálně nebezpečných relací. Pravidla pro detekci potenciálně nebezpečných relací je možné plně editovat - typ události, uživatelé (možnost nastavení výjimek na úrovni skupin v AD) a typ reakce.	(Doplní dodavatel)	(Splňuje/Nesplňuje)

B53	Možnost sledování relací v reálném čase	PAM řešení musí umožňovat sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci. Sledování "živých" relací je také možné pomocí prohlížeče a protokolu HTTPS.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B54	Detekce a blokování podezřelých aktivit	PAM řešení musí umožňovat detekci podezřelých aktivit chování uživatelů v reálném čase a musí umožňovat automatické vynucení nápravných opatření - alerting, změna přihlašovacích údajů, terminace/pozastavení relací.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B55	Export nahrávek	PAM musí umožňovat export nahrávek do samostatného souboru, který lze přenést na externí úložiště a přehrát „offline“, tj. bez nutnosti připojení k PAM.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B56	Analýza nahrávek a vyhledávání	PAM musí umožňovat vyhledávání v rámci nahrávek relací dle klíčových slov a dalších parametrů, například: vyhledání určitého příkazu a získání výsledku všech relací, kde byl daný příkaz použit. PAM musí umožňovat v živém režimu připojení třetí osoby (např. Auditora, Správce PAM) k probíhající relaci. Třetí osoba může probíhající relaci předčasně ukončit.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B57	Zálohování nahrávek	Úložiště s nahrávkami musí být pravidelně zálohováno, musí být zajištěna dostupnost těchto záloh a ochrana proti neoprávněnému smazání. Zálohy nahrávek musí být dostatečně zabezpečeny proti neoprávněnému přístupu šifrováním.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B58	Dostupnost záloh	Je požadováno uchování nahrávek pro okamžitý přístup (tj. bez nutnosti jejich vyvolání z archivu) po dobu 18 měsíců. Tato doba může být upřesněna v průběhu Etapy 2.	(Doplní dodavatel)	(Splňuje/Nesplňuje)
B59	Požadavky na archivaci nahrávek	Je požadováno zajistit archivaci nahrávek na bezpečném úložišti. Z tohoto úložiště nemusí být nahrávky nutně okamžitě dostupné, je možné využít tzv. cold archive, tedy archivu, ze kterého je nutné před jejich prohlížením nejprve nahrávky přenést na určené místo (vyvolat).	(Doplní dodavatel)	(Splňuje/Nesplňuje)

7 Požadavky na plnění Etapy 3, Podporu systémů (Služby podpory) a Rozvoj (ad hoc služby)

7.1 Doplnění předimplementační analýzy pro Etapu 3

Doplnění a aktualizace předimplementační analýzy provedené v rámci Etapy 1 pro integraci systémů do systémů IdM uvedených v Tabulce B Přílohy č. 1b Smlouvy a aktualizace předimplementační analýzy dle potřeb pro integraci systémů v Etapě 3, minimálně v rozsahu:

- Cílová architektura řešení
- Aktualizace analýzy identit, rolí, procesů a metodik
- Aktualizace business rolí, aplikačních a technických rolí a forem jejich tvorby

7.2 Integrace na systémy Etapy 3

V rámci této Etapy bude provedena integrace (přes AD) koncových systémů na IdM uvedených v Příloze 1b, Tabulce B.

7.3 Dokumentace Etapy 3

Veškerá dokumentace k realizaci předmětu Smlouvy musí být vypracována v českém jazyce. Mohou v ní být použité části v anglickém jazyce, např. ilustrace přímo od výrobce technologie apod., ale s doplňujícím vysvětlením, případně výkladem odborných pojmů v českém jazyce.

V rámci této Etapy bude provedena aktualizace a rozšíření dokumentace vzniklé v předchozích Etapách 1 a 2 tak, aby odpovídala nově integrovaným systémům a provedeným úpravám řešení.

- **Dokumentace skutečného provedení**: Bude doplněna o detailní popis integrace nových systémů, včetně všech úprav provedených v prostředí objednatele oproti předchozí konfiguraci jednotlivých komponent.
- **Dokumentace instalace softwaru**: Bude aktualizována o případné změny v instalačních a konfiguračních postupech související s přidáním nových systémů. Dokumentace musí i nadále umožnit úplnou opakovatelnost instalace bez nutnosti dalších znalostí.
- **Plán obnovy (DR plan)**: Bude rozšířen o postupy obnovy pro nové integrační body a scénáře specifické pro připojené systémy.
- **Testovací scénáře**: Budou doplněny o nové akceptační testy pokrývající integraci nových systémů. Původní scénáře budou v případě potřeby aktualizovány s ohledem na změny v konfiguraci či funkcionalitě.
- **Plán přechodu do produkčního provozu**: Bude aktualizován s ohledem na kroky nezbytné pro nasazení nových integrací do produkčního prostředí. Aktualizovaný plán bude obsahovat doplněný checklist a harmonogram aktivit.
- **Plán zálohování**: Bude rozšířen o popis zálohovacích postupů pro nově integrované systémy, včetně případných změn v zálohování aplikačních dat, konfigurací nebo logů.

Dokumentace musí být kompletní a průběžně aktualizována po celou dobu trvání smluvního vztahu tak, aby vždy odpovídala aktuální verzi SW. Dokumentace může být poskytnuta i formou přístupu k online dokumentaci.

7.4 Školení Etapy 3

Dodavatel zajistí školení pracovníků STC v oblasti používání systému IdM rozšířeného o nově integrované systémy dle níže uvedených požadavků objednatele.

Dodávaný produkt musí být doplněn o školící materiály a návody pro správu systému, rozšířené o informace vztahující se k nově integrovaným systémům a rozšířené funkcionalitě IdM, a to alespoň v následujícím rozsahu:

- **Příručka administrátora**: Aktualizovaná příručka bude rozšířena o popis správy a nastavení nově integrovaných systémů. Musí obsahovat detailní popis všech funkcí potřebných pro správu IdM v jeho rozšířené podobě. Příručka bude i nadále sloužit jako základní materiál pro školení nových administrátorů a bude doplněna o návody krok za krokem, doprovázené obrázky a výřezy obrazovek pro snadnější orientaci.
- **Příručka vývojáře**: Příručka vývojáře bude aktualizována o popis nových integrací. Musí obsahovat dokumentaci všech změn a rozšíření provedených oproti Etapě 1 a popis způsobu integrace nově napojených systémů do IdM.

Požadavky na školení

Řešení musí zahrnovat školení v rozsahu minimálně **3 MD** v součtu pro tyto skupiny uživatelů:

- **Klíčoví uživatelé a garanti systémů**
- **Bezpečnostní správce**
- **Systémoví administrátoři**

- **Běžní uživatelé – online školení a nahrávky tohoto školení on-demand**
- minimálně 1× standardní on-line školení se záznamem

7.5 Testovací provoz a akceptace pro Etapu 3

7.5.1 Testovací provoz

Cílem této fáze je identifikace a následné odstranění případných provozních či konfiguračních nedostatků před zahájením produkčního provozu. Dodavatel v průběhu testovacího provozu poskytuje zvýšenou podporu při řešení zjištěných nedostatků. Postupy realizace testovacího provozu budou vycházet z postupů ověřených a uplatněných během testovacího provozu Etapy 1 projektu, přičemž budou přiměřeně upraveny s ohledem na charakter nově integrovaných systémů a rozsah jejich napojení.

Data a role během testovacího provozu

- Výstupy analýzy AR/BR (Application Roles/Business Roles) mohou být v době napojování systémů založeny na **starších datech**.
- **Po napojení systémů musí Dodavatel provést aktualizaci exportů uživatelů a re-konfiguraci/rekalibraci rolí** (tj. znovu přiřadit role dle aktuální reality) tak, aby **testovací provoz již pracoval s aktuálními daty**.
- **Smluvní požadavek:** Tyto aktivity (aktualizace exportů a opětovné přiřazení rolí vyvolané stářím dat) musí být **výslovně zahrnuty v ceně a harmonogramu** testovacího provozu.

Testovací provoz je ukončen po schválení přechodu do produkčního provozu ze strany objednatele. Tímto aktem se IdM řešení jako celek (řídící tedy i koncové systémy integrované v rámci Etapy 3) předává do plného provozu. Testovací provoz tvoří závěr Etapy 3 a jeho délka bude činit **max. 1 měsíc** po dokončení fáze F3.2. Testovací provoz bude probíhat po dobu nezbytně nutnou k ověření funkčnosti integrace na příslušné systémy.

7.5.2 Akceptace a přechod do produkčního provozu

Během testovacího provozu využívá objednatel IdM řešení v plném rozsahu a přistupuje k němu z provozního hlediska jako k plnohodnotnému produkčnímu prostředí. Zároveň průběžně sleduje a vyhodnocuje, zda prostředí splňuje stanovené požadavky.

Na konci testovacího provozu proběhnou akceptační testy, které ověří, že systém IdM splňuje všechny požadavky stanovené v této Technické specifikaci a že příslušná část předmětu plnění je provedena v souladu s předimplementační analýzou (dále jen „testy“). Testy proběhnou dle testovacích plánů, které jsou obsaženy v akceptované předimplementační analýze. Objednatel je oprávněn vyžádat si doplnění plánu testů o další konkrétní testy, pokud to bude považovat za účelné pro ověření kompletní funkčnosti systému IdM.

Akceptace a přechod do produkčního provozu do produkčního provozu **nemůže být provedeno dříve** než po uplynutí dvou týdnů testovacího provozu a současně nemůže být dříve než vypracování dokumentace a průběh školení dle kapitol 7.3 a 7.4.

V okamžiku, kdy Objednatel dospěje k závěru, že prostředí je plně funkční a odpovídá požadavkům zadání, podepíše s dodavatelem akceptační protokol o převzetí prostředí IdM a jeho předání do produkčního provozu.

Součástí akceptace je kontrola existence a aktuálnosti dokumentace v rozsahu odpovídajícím dodávané verzi SW, resp. implementaci a konfiguraci v prostředí STC.

Dodavatel je povinen při přechodu do produkčního provozu předat veškeré zdrojové kódy a build/CI skripty s výjimkou případů, kdy se jedná o standardní software třetích stran nebo jiné komponenty, ke kterým dodavatel nemá licenční oprávnění ke zdrojovým kódům.

7.6 Podpora systému IdM

Dodavatel zajistí odbornou technickou podporu k implementovanému řešení IdM od jeho nasazení do produkčního provozu (vč. podpory integrace dalších koncových systémů v rámci Etapy 3) po dobu dle čl. III odst. 4 Smlouvy.

Detailní požadavky obsahuje následující tabulka:

Oblast	Požadavky
Servis produktů (maintenance) využitých implementovaném IdM	Dodavatel zajistí oficiální podporu výrobce, která zahrnuje minimálně: • registrace a odstraňování nalezených chyb v produktech včetně komunikace na výrobce produktů, • poskytování nových verzí produktů včetně certifikovaných i tak vyvinutých konektorů (upgrade), • zajištění oprav případných chyb produktů (patches),
Servisní služby (podpora) k implementovanému IdM	Dodavatel zajistí podporu, která zahrnuje minimálně: - režim podpory dle definice v příloze č. 5 Smlouvy, včetně zajištění alokace kvalifikovaných kapacit a garance jejich dostupnosti; - Zajištění a provoz jednotného kontaktního místa pro příjem a evidenci (dále též „**kontaktní místo**“) servisních požadavků, incidentů, vad a požadavků na konzultaci (dále též „**požadavek**“) uplatněných objednatelem, včetně reportingu o čerpaných službách; • konzultační služby spojené s provozem a správou dodaného řešení IdM (vč. školení dle potřeby), použitých produktů a všech konektorů v rozsahu maximálně 20 člověkohodin měsíčně • diagnostika a odstranění vad funkcionality dodaného řešení IdM, • řešení problémů a havarijních situací v souvislosti s provozem dodaného řešení IdM, jednotlivých produktů a konektorů, • servis při upgrade, patch řešení IdM nebo úpravě IdM konektorů napojených na koncové systémy.

7.7 Podpora systému PAM

Dodavatel zajistí odbornou technickou podporu k implementovanému řešení PAM od jeho nasazení do produkce po dobu dle čl. III odst. 4 Smlouvy.

Detailní požadavky obsahuje následující tabulka:

Oblast	Požadavky
Servis produktů (maintenance) využitých implementovaném PAM	Dodavatel zajistí oficiální podporu výrobce, která zahrnuje minimálně:

	• registrace a odstraňování nalezených chyb v produktech včetně komunikace na výrobce produktů, • poskytování nových verzí produktů včetně certifikovaných i tak vyvinutých konektorů (upgrade), • zajištění oprav případných chyb produktů (patches),
Servisní služby (podpora) k implementovanému PAM	Dodavatel zajistí podporu, která zahrnuje minimálně: - režim podpory dle definice v příloze č. 5 Smlouvy, včetně zajištění alokace kvalifikovaných kapacit a garance jejich dostupnosti; - Zajištění a provoz jednotného kontaktního místa (je požadováno, aby se jednalo o totožné kontaktní místo, jako v případě produktu IdM) pro příjem a evidenci (dále též „**kontaktní místo**“) servisních požadavků, incidentů, vad a požadavků na konzultaci (dále též „**požadavek**“) uplatněných objednatelem, včetně reportingu o čerpaných službách; • konzultační služby spojené s provozem a správou dodaného řešení PAM (vč. školení dle potřeby), použitých produktů a všech konektorů v rozsahu maximálně 20 člověkohodin měsíčně • diagnostika a odstranění vad funkcionality dodaného řešení PAM, • řešení problémů a havarijních situací v souvislosti s provozem dodaného řešení PAM, jednotlivých produktů a konektorů, • servis při upgrade, patch řešení PAM nebo úpravě PAM konektorů napojených na koncové systémy.

7.8 Rozvoj

Dodavatel poskytne objednateli ad hoc služby, přičemž:

- Ad hoc služby mohou být čerpány pro rozšiřování implementace systémů PAM a IdM na další koncové systémy dle přílohy č. 1b Smlouvy, Tabulek C a E.
- Ad hoc služby mohou být dále čerpány na úpravu poskytnutého plnění, tj. systémů, jejich rozvoj a pro další potřebné činnosti, které objednatel bude od dodavatele vyžadovat.
- Čerpání bude probíhat dle konkrétních potřeb objednatele, a to postupem dle čl. II odst. 5 bod 5.3 Smlouvy.
- V případě rozvoje je dodavatel povinen aktualizovat dokumentaci skutečného provedení o provedené změny či rozšíření dotčených systémů

Koncové systémy a počet uživatelů

1 Prostředí objednatele

1.1 Tabulka A – Implementace IdM dle kapitoly 5.2.3 Technické specifikace (Etapa 1)

Níže uvedená tabulka uvádí přehled koncových systémů.

Koncový systém	Verze	Počet fyzických instancí	Napojeno na AD
MS Active Directory	2016	5	
Microsoft 365			ANO
OKbase	6.xx	2	ANO
DMS / Spisová služba	Sharepoint SE	3	ANO
Exchange (správa uživ. Schránek)	Exchange online/ On-pem SE	3	ANO

1.2 Tabulka B – Implementace IdM dle kapitoly 7.2 Technické specifikace (Etapa 3)

Níže uvedená tabulka uvádí přehled koncových systémů.

Koncový systém	Verze	Počet fyzických instancí	Napojeno na AD
RIS.NET (účetnictví a správa majetku)	2.3.xxx	2	ANO
SafeQ (tiskový server)	D.0.110.xxx	1	ANO
BNS – Manažerský systém pro finanční plánování	4.9.xxx	2	ANO

1.3 Tabulka C – Ostatní systémy pro uvažovanou implementaci IdM (Rozvoj)

(v rámci ad hoc služeb)

Níže uvedená tabulka uvádí přehled koncových systémů.

Koncový systém	Verze	Počet fyzických instancí	Napojeno na AD
Fileshare	2022	2	ANO
Bitwarden	2023.4.xx	1	NE
Intune			ANO
Checkpoint: (endpoint, fw, atd.)	R81.xx	1	ANO
Logmanager	3.11.xx	1	ANO
Flowmon	12	3	ANO
ESET endpoint security	11.xx	1	ANO
LibreNMS (monitoring aktivních síťových prvku)			ANO
Linux servery		20	NE
HP OneView			ANO
Arista AP management			ANO
A5 Client (Správa kávomatů)		1	ANO
HelpDesk – Requestor	5.x	1	ANO
SCCM	2503	5	ANO
Zabbix	7	2	ANO
VmWare Vsphere	8.0.x	2	ANO
SQL servery / Instance	16.x	2	ANO
Sharepoint Sites administrator	SE	3	ANO
Dotykačka		1	ANO
NextCloud (úložiště pro externisty)		1	ANO
Cicero (ERP od společnosti Stapro Group)	9.x	2	NE
Windows servery	2025 Datacenter	2	NE

1.4 Tabulka D – Implementace PAM dle článku 6.2.2 Technické specifikace (Etapa 2)

Níže uvedená tabulka uvádí přehled koncových systémů.

Koncový systém	Verze	Počet fyzických instancí	Počet spojení přes různé protokoly
MS Windows (fyzické a virtuální servery)	2016 +	76	76 - RDP
VMware vSphere + vCenter	8.x	7	7 – HTTPS 7 - SSH
MS Active Directory	Domain functional level – Windows Server 2012 R2	5	5 - veškeré nástroje sady RSAT
Microsoft 365		1	1 - HTTPS
IdM			

1.5 Tabulka E – Ostatní systémy pro uvažovanou integraci PAMu (Rozvoj)

(v rámci ad hoc služeb)

Níže uvedená tabulka uvádí přehled koncových systémů.

Koncový systém	Verze	Počet fyzických instancí	Počet spojení přes různé protokoly
Debian (Linux servery)	11.x / 12.x	14	14 - SSH
RedHat / Centos (Linux servery)	6.x / 7.x	11	11 - SSH
MS SQL (AD SQL servery)	16.x	2	2 – RDP, nativní aplikační klient
MySQL (MariaDB)	10.x	2	2 – HTTPS 2 - SSH
Firewall CheckPoint	R81.xx	10	10 – SSH 10 - HTTPS
Checkpoint endpoint protection	R81.xx	1	1 - HTTPS / 1 SSH
Exchange online / onprem	SE		
Bitwarden	2023.x	1	1 - HTTPS
Sharepoint Sites administrator	SE		2 – RDP

1.6 Počet uživatelů

Níže uvedená tabulka uvádí přehled počtu Uživatelů, kteří budou využívat PAM řešení.

Předpokládaný počet uživatelů přistupujících k PAM (mají vždy účet v AD)	Infrastrukturní administrátoři (interní): 5 Infrastrukturní administrátoři (externí): cca 70 Aplikační administrátoři (interní/externí): 5
Počet současně připojených uživatelů v běžném provozu	20
Počet současně připojených uživatelů ve špičce	80
Průměrná délka uživatelské relace za den	4 h
Počet jmenných uživatelů	80
Počet privilegovaných účtů v koncových systémech	200

Příloha č. 3 Smlouvy č. 074/OS/2025

Harmonogram

ID fáze	Etapa	Název	Termín dodání (měsíce)	Podmínka / Popis	
F1.0	1	Účinnost smlouvy	T+ 0		
F1.1	1	**Etapa 1: Předimplementační analýza**	T+ 6	Dle TS - kapitola	5.1
F1.2	1	Etapa 1: Implementace a integrace	T+ 12	Dle TS - kapitola	5.2
F1.3	1	Etapa 1: Dokumentace	T+ 13	Dle TS - kapitola	5.3
F1.4	1	Etapa 1: Školení a adopce	T+ 14	Dle TS - kapitola	5.4
F1.5	1	Etapa 1: Testovací provoz	T+ 15	Dle TS - kapitola	5.5.1
F1.6	1	Etapa 1: Akceptace	T+ 15	Dle TS - kapitola	5.5.2
F1.7	1	**Etapa 1: Go-live**	T+ 15		
F2.1	2	Etapa 2: Predimplementační analýza	T+ 17	Dle TS - kapitola	6.1
F2.2	2	Etapa 2: Implementace a integrace	T+ 23	Dle TS - kapitola	6.2
F2.3	2	Etapa 2: Dokumentace	T+ 24	Dle TS - kapitola	6.3
F2.4	2	Etapa 2: Školení a adopce	T+ 25	Dle TS - kapitola	6.4
F2.5	2	Etapa 2: Testovací provoz	T+ 26	Dle TS - kapitola	6.5.1
F2.6	2	Etapa 2: Akceptace	T+ 26	Dle TS - kapitola	6.5.2
F2.7	2	**Etapa 2: Go-live**	T+ 26		
F2.8	2	Příprava exit plánu	T+ 27	Dle TS - kapitola	4.2
F2.9	2	**Akceptace exit plánu**	T+ 28	Dle TS - kapitola	4.2
F3.1	3	Etapa 3: Predimplementační analýza	T+ 24	Dle TS - kapitola	7.1
F3.2	3	Etapa 3: Integrace na systémy	T+ 27	Dle TS - kapitola	7.2
F3.3	3	Etapa 3: Dokumentace	T+ 27	Dle TS - kapitola	7.3
F3.4	3	Etapa 3: Školení a adopce	T+ 28	Dle TS - kapitola	7.4
F3.5	3	Etapa 3: Testovací provoz	T+ 28	Dle TS - kapitola	7.5.1
F3.6	3	Etapa 3: Akceptace	T+ 28	Dle TS - kapitola	7.5.2
F3.7	3	**Etapa 3: Go-live**	T+ 28		

Tučně zvýrazněné řádky označují platební milníky.
Termín dodání je uváděn v měsících.

Požadavky na provoz řešení

Níže uvedené hodnoty uvádějí minimální provozní parametry (SLA) implementovaných a provozovaných systémů IdM a PAM.

Metrika	Systém IdM	Systém PAM	Měření / zdroj dat	Vysvětlivka
Dostupnost služby	≥ **99 %** / měsíc	≥ **99,75 %** / měsíc	nástroj monitoringu zadavatele	Max. výpadek: IDM ≈ 7,2 h, PAM ≈ 1,5 h / měsíc
RTO (Recovery time objective - obnova)	≤ 4 h	≤ 4 h	DR test, ticket log	Čas do plné obnovy služby
RPO (Recovery point objective - ztráta dat)	≤ 15 min	≤ 15 min	log replikace	Max. přípustná ztráta dat
Reakce na kritickou závadu	≤ 30 min	≤ 30 min	ticket systém	Zahájení řešení, ne oprava
Odstranění kritické závady	≤ 4 hodiny	≤ 2 hodiny	ticket systém	Doba do odstranění kritické závady
Odstranění vážné závady	≤ 8 hodin	≤ 4 hodiny	ticket systém	Doba do odstranění vážné závady
Odstranění ostatních závad	3 pracovní dny*	2 pracovní dny*	ticket systém	Doba do odstranění ostatních závad
Permanentní fix (všech) závad	≤ 10 prac. dní*	≤ 10 prac. dní*	ticket systém	Definitivní odstranění chyby
Bezpečnostní update (CVSS 0.1–3.9)	≤ 60 dní*	≤ 30 dní*	Evidence dodavatele	Low; stejné pravidlo mitigace a počítání času; není-li patch, mitigace
Bezpečnostní update (CVSS 4.0–6.9)	≤ 20 dní*	≤ 10 dní*	Evidence dodavatele	Medium; stejné pravidlo mitigace a počítání času; není-li patch, mitigace
Bezpečnostní update (CVSS 7.0–8.9)	≤ 5 dní*	≤ 48 h	Evidence dodavatele	High; čas od dostupnosti patchu nebo potvrzené detekce; není-li patch, nasadit mitigaci
Bezpečnostní update (CVSS ≥ 9)	≤ 24 h	≤ 24 h	Evidence dodavatele	Kritické zranitelnosti

* Limit počtu dní se začíná započítávat dnem následujícím po nahlášení závady či objevení zranitelnosti. Pokud je například „ostatní závada“ nahlášena v pondělí, termín její odstranění je následující čtvrtek 24:00 (termín 3 pracovní dny).

Reporting plnění SLA

Dodavatel je povinen pro každý kalendářní měsíc provozu zvlášť pro systém IdM a zvlášť pro systém PAM vytvořit a objednateli zpřístupnit Report plnění SLA. Tento report musí minimálně obsahovat:

- měsíční počet incidentů (celkem a dle priorit),
- způsob vyřešení (plné / workaround),
- přehled otevřených změn velkého rozsahu a jejich termínů.
- Měsíční report dostupnosti služby a všech výše uvedených SLA parametrů

Vysvětlivky k parametrům SLA

- **Dostupnost služby (Availability)**
  Podíl času, kdy je služba funkční a přístupná pro uživatele.
- **RTO – Recovery Time Objective (Obnova)**
  Maximální čas od výpadku do plného obnovení služby (včetně všech komponent).
  RPO – Recovery Point Objective (Ztráta dat)
  Maximální přípustná ztráta dat (např. při obnově ze zálohy nebo replikace).
  ≤ 15 minut znamená, že data starší než 15 minut by neměla být ztracena.
- **Kritická závada**: závada, která způsobuje nefunkčnost celého systému, případně jeho klíčových komponent, anebo umožňuje zneužití oprávnění k systémům a aplikacím STC.
- **Vážná závada**: závada, která způsobuje nemožnost využít nějaké funkčnosti systému (např. nemožnost přiřadit novému zaměstnanci dle jeho role přístupy nebo nefunkčnost samoobslužného portálu).
- **Reakce na kritickou závadu:** Doba od nahlášení závady (např. výpadek, bezpečnostní incident) do zahájení řešení. Neznamená opravu, ale **zahájení aktivní reakce**.
- **Permanentní fix:** Doba, do kdy musí být **definitivně odstraněna chyba**. Nejedná se o dočasné řešení (tzv. workaroundy). Počítá se v **pracovních dnech**.
- **Bezpečnostní update (CVSS)**
  Vysvětleno níže.

CVSS – Common Vulnerability Scoring systém

CVSS (Common Vulnerability Scoring System) je standardizovaný systém hodnocení závažnosti zranitelností v softwaru. Používá se celosvětově pro posouzení rizik a určení priorit pro bezpečnostní opravy (tzv. patche).

Rozsah a interpretace skóre:

Skóre CVSS	Kategorie	Doporučená reakce
0.0	Nulové riziko	Není potřeba zásah
0.1 – 3.9	Nízké (Low)	Monitorovat, oprava není urgentní
4.0 – 6.9	Střední (Medium)	Opravit dle standardního cyklu
7.0 – 8.9	Vysoké (High)	Zvýšená priorita opravy
9.0 – 10.0	**Kritické (Critical)**	**Okamžité řešení, oprava do 24 h**

VZOR
AKCEPTAČNÍ PROTOKOL
bez výhrad

Objednatel: **Státní tiskárna cenin, s. p.**
se sídlem Růžová 943/6, Nové Město, 110 00, Praha 1
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, oddíl ALX, vložka 296
zastoupený: **Mgr. Markem Šimandlem**, MPA, generálním ředitelem
IČO: 00001279
DIČ: CZ00001279

Dodavatel: **[•]**
se sídlem **[•]**
zapsaný v obchodním rejstříku vedeném **[•]**
zastoupený: **[•]**
IČO: **[•]**
DIČ: **[•]**

Objednatel:

a) tímto v souladu s čl. VI odst. 5 bod 5.1 Smlouvy na dodávku, implementaci a podporu systému pro správu identit (IdM) a systému pro řízení privilegovaných účtů (PAM) č. …/OS/2025 (dále jen „smlouva“) potvrzuje **akceptaci bez výhrad** a prohlašuje, že systém je připraven k zahájení produkčního provozu, že systém odpovídá této smlouvě, a je prostý jakýchkoliv vad a nedodělků;

b) prohlašuje, že systém splňuje požadavky objednatele a veškeré technické parametry uvedené ve smlouvě;

c) prohlašuje, že převzal následující položky *(pokud relevantní zejména v případě multilicence, dokumentace, zdrojových kódů aj.)*:

Název položky	**Výrobní/sériové/licenční číslo/jiný popis**

Dodavatel:

a) zaručuje, že systém je funkční a je proveden tak, aby vyhovoval technickým a bezpečnostním normám platným v ČR, jakož i účelu, k němuž byl objednán.

Tento protokol je vyhotoven ve dvou stejnopisech nebo v elektronické podobě a podepsán zmocněnci pro jednání věcná a technická obou smluvních stran.

V Praze dne .....

Za objednatele:

_____

jméno [•]

funkce [•]

V [•] dne .....

Za dodavatele:

_____

jméno [•]

funkce [•]

[za obě strany doplnit jméno a funkci zmocněnce pro jednání věcná a technická]

VZOR
AKCEPTAČNÍ PROTOKOL
s výhradami

Objednatel: **Státní tiskárna cenin, s. p.**
se sídlem Růžová 943/6, Nové Město, 110 00, Praha 1
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, oddíl ALX, vložka 296
zastoupený: **Mgr. Markem Šimandlem**, MPA, generálním ředitelem

IČO: 00001279
DIČ: CZ00001279

Dodavatel: [•]
se sídlem [•]
zapsaný v obchodním rejstříku vedeném [•]
zastoupený: [•]
IČO: [•]
DIČ: [•]

Objednatel:

a) tímto v souladu s čl. VI odst. 5 bod 5.2 Smlouvy na dodávku, implementaci a podporu systému pro správu identit (IdM) a systému pro řízení privilegovaných účtů (PAM) č. …/OS/2025 (dále jen „smlouva“) potvrzuje **akceptaci s výhradami** a prohlašuje, že v systému se vyskytly vady a nedodělky, které však nebrání zahájení produkčního provozu systému a rovněž nebrání užívání systému obvyklým způsobem.

Jedná se o následující vady a nedodělky, přičemž smluvní strany zároveň uvádějí termíny pro odstranění konkrétní vady:

vada nebo nedodělek	popis	termín k odstranění
[•]	[•]	[•]
[•]	[•]	[•]
[•]	[•]	[•]

Nedojde-li mezi oběma smluvními stranami k dohodě o termínu odstranění vad nebo nedodělků, pak platí, že vady a nedodělky musí být odstraněny nejpozději do 15 dnů ode dne vyhotovení Akceptačního protokolu.

b) prohlašuje, že systém splňuje požadavky objednatele a veškeré technické parametry uvedené ve smlouvě, mimo výše vytknutých vad a nedodělků;

c) prohlašuje, že převzal následující položky *(pokud relevantní zejména v případě multilicence, dokumentace, zdrojových kódů aj.)*:

Název položky	**Výrobní/sériové/licenční číslo/jiný popis**

Dodavatel:

a) zaručuje, že systém je funkční a proveden tak, aby vyhovoval účelu, k němuž byl objednán, a technickým a bezpečnostním normám platným v ČR, mimo výše vytknuté vady a nedodělky.

Tento protokol je vyhotoven ve dvou stejnopisech nebo v elektronické podobě a podepsán zmocněnci pro jednání věcná a technická obou smluvních stran.

V Praze dne .....

Za objednatele:

_____

jméno **[•]**

funkce **[•]**

V **[•]** dne .....

Za dodavatele:

_____

jméno **[•]**

funkce **[•]**

[za obě strany doplnit jméno a funkci zmocněnce pro jednání věcná a technická]

VZOR
ZÁPIS O NEAKCEPTACI

Objednatel: **Státní tiskárna cenin, s. p.**
se sídlem Růžová 943/, Nové Město, 110 00, Praha 1
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, oddíl ALX, vložka 296
zastoupený: **Mgr. Markem Šimandlem**, MPA, generálním ředitelem

IČO: 00001279
DIČ: CZ00001279

Dodavatel: [•]
se sídlem [•]
zapsaný v obchodním rejstříku vedeném [•]
zastoupený: [•]
IČO: [•]
DIČ: [•]

Objednatel:

a) tímto v souladu s čl. VI odst. 5 bod 5. 3 Smlouvy na dodávku, implementaci a podporu systému pro správu identit (IdM) a systému pro řízení privilegovaných účtů (PAM) č. …/OS/2025 (dále jen „smlouva“) **neakceptuje** plnění**,** neboť v plnění se vyskytují vady nebo nedodělky bránící nebo ztěžující zahájení produkčního provozu obvyklým způsobem a jsou důvodem k neakceptování předmětu plnění.

Jedná se o následující vady a nedodělky, přičemž smluvní strany zároveň uvádějí termíny pro odstranění konkrétní vady:

vada nebo nedodělek	popis	termín k odstranění
[•]	[•]	[•]
[•]	[•]	[•]
[•]	[•]	[•]

Nedojde-li mezi oběma smluvními stranami k dohodě o termínu odstranění vad a nedodělků, pak platí, že vady a nedodělky musí být odstraněny nejpozději do 15 dnů ode dne vyhotovení zápisu o neakceptaci předmětu plnění.

b) prohlašuje, že převzal následující položky *(pokud relevantní zejména v případě multilicence, dokumentace, zdrojových kódů aj.)*:

Název položky	**Výrobní/sériové/licenční číslo/jiný popis**

Dodavatel:

a) bere na vědomí, že je povinen ve stanovené lhůtě odstranit vady nebo nedodělky i v případě, kdy podle jeho názoru za vady a nedodělky neodpovídá. Náklady na odstranění vad a nedodělků v těchto sporných případech nese až do rozhodnutí soudu dodavatel.

Tento protokol je vyhotoven ve dvou stejnopisech nebo v elektronické podobě a podepsán zmocněnci pro jednání věcná a technická obou smluvních stran.

V Praze dne .....

Za objednatele:

_____

jméno **[•]**

funkce **[•]**

V **[•]** dne .....

Za dodavatele:

_____

jméno **[•]**

funkce **[•]**

[za obě strany doplnit jméno a funkci zmocněnce pro jednání věcná a technická]

VZOR
PŘEDÁVACÍ PROTOKOL

Objednatel: **Státní tiskárna cenin, s. p.**
se sídlem Růžová 943/6, Nové Město, 110 00 Praha 1
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze,
oddíl ALX, vložka 296
zastoupený: **Mgr. Markem Šimandlem**, MPA, generálním ředitelem

IČO: 00001279
DIČ: CZ00001279

Dodavatel: [•]
se sídlem [•]
zapsaný v obchodním rejstříku vedeném [•]
zastoupený:
IČO: [•]
DIČ: [•]

Objednatel potvrzuje tímto dodávku HW pro systém PAM.

Dodavatel zaručuje, že HW je funkční a nainstalován tak, aby vyhovoval technickým a bezpečnostním normám platným v ČR, jakož i účelu, k němuž byl objednán.

V Praze dne .....

Za objednatele:

_____
jméno
funkce

Za dodavatele:

_____
jméno [•]
funkce [•]

Příloha Předávacího protokolu ke smlouvě č. _____: SOUPIS POLOŽEK PŘEVZATÉHO PLNĚNÍ

Název položky	Výrobní/sériové číslo	Poznámka/výhrada

(…)

Definice odborných pojmů a zkratek

Níže uvedená tabulka obsahuje seznam ve Smlouvě a jejích přílohách použitých odborných pojmů a zkratek.

Pojem	**Definice / Význam**
2FA	Dvoufaktorová autentizace
AD	Microsoft Active Directory
BNS	Business Navigation System (manažerský informační systém pro celofiremní finanční plánování)
Break-glass	Nouzový přístup v krizové situaci.
Call-home	Funkce, kdy systém automaticky posílá výrobci hlášení o poruchách nebo stavu, aby mohl zajistit podporu.
CVSS (Common Vulnerability Scoring System)	Mezinárodní škála 0–10, která určuje, jak závažná je bezpečnostní chyba.
DMS	Document management system MS Sharepoint, používaný pro schvalování/workflow
DR (Disaster Recovery)	Plán a řešení, jak rychle obnovit systémy a data po velkém výpadku nebo havárii.
DRP test (Disaster Recovery Plan test)	Ověření, že záložní plány a postupy obnovy systémů po výpadku fungují v praxi.
EoL/EoS (End of Life / End of Support)	Výrobce ukončil vývoj (EoL) nebo podporu a záplaty (EoS) produktu; po tomto datu je používání rizikové.
EULA – licenční smlouvy	EULA stanovuje podmínky pro koncové uživatele
FOSS licence	Free Open Source Software licence
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679, Obecné nařízení o ochraně osobních údajů
GUI	Graphical User Interface (Grafické uživatelské rozhraní)
HA	Režim vysoké dostupnosti (*High Availability*), např. prostřednictvím redundance.
HR (Human Resources)	Útvar, který je odpovědné za správu lidských zdrojů (nábor, smlouvy, mzdy, školení).
HTTPS	HyperText Transfer Protocol Secure
HW/ Hardware	Veškeré hmotné součásti počítačových systémů a veškeré související vybaveni hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.

ICT	Informační a komunikační technologie (Information and Communication Technologies)
IdM	Správa uživatelských účtů (Identity Management).
IS	Informační systém
JMeter	Nástroj pro testování výkonu, který simuluje více uživatelů a ukáže, jak systém zvládá zátěž.
Jump server	Server zprostředkující veškerou komunikaci do vnitřní sítě izolující přístup uživatele (např. Windows terminál).
Koncový systém	Koncový systém, jehož privilegované účty a relace jsou řízeny pomocí PAM řešení (např. databáze, aplikace, komunikační a bezpečnostní prvky atd.).
Kybernetický bezpečnostní incident	Narušení bezpečnosti informací v kybernetickém prostoru ve smyslu § 2 odst. 2 písm. f) ZoKB
Kybernetická bezpečností událost	Událost, která může vyústit v kybernetický bezpečnostní incident
LDAP	Lightweight Directory Access Protocol
Licenční metrika	Smluvně stanovené kritérium, které vymezuje oprávnění k užívání softwaru a určuje, kolik licencí je nutné pořídit v závislosti na způsobu nasazení a využití softwaru.
On/Off-boarding	Procesy při nástupu a odchodu zaměstnance: vytvoření nebo zrušení přístupů, vybavení a školení.
OS	Operační Systém
OTP	Jednorázové heslo (*One time password*)
OU	Organizační jednotka v Active Directory — kontejner pro uživatele, skupiny a počítače; slouží k delegaci správy a cílení GPO.
PAM	Správa privilegovaných přístupů (*Privileged Access Management*)
Perpetuální (trvalá) licence	Licence k užití softwaru poskytovaná na dobu neurčitou, která opravňuje nabyvatele k trvalému užívání softwaru v souladu s licenčními podmínkami, bez časového omezení platnosti licence, ledaže je výslovně sjednáno jinak.
PIR (Post-Implementation Review)	Kontrola po zavedení změny, jestli vše funguje podle plánu a co je možné příště udělat lépe.
Playbooky	Návody pro řešení útoků
Privilegovaný účet	Uživatelský účet informačního systému se širokou nebo neomezenou množinou administrátorských oprávnění, který je zpravidla nepersonalizovaný a může být sdílen mezi vícero uživateli.
QA inženýr (Quality Assurance Engineer)	Tester, který hlídá kvalitu softwaru a pomáhá odhalit chyby ještě před nasazením.
QA Lead (Quality Assurance Lead)	Osoba zodpovědná za testování a dohled nad kvalitou výsledného řešení.
RBAC (Role-Based Access Control)	Způsob přidělování oprávnění podle rolí (např. účetní, admin), ne každému uživateli zvlášť.

RCA (Root Cause Analysis)	Vyšetření hlavní příčiny incidentu a návrh opatření, aby se problém už neopakoval.
RDP	Protokol na přenos vzdálené plochy (*Remote Desktop Protocol*)
Regresní testy	Testování, že po úpravě systému dál fungují i všechny původní funkce.
RFC (Request for Change)	Oficiální žádost o změnu v systému nebo ve službě, kterou zakládá žadatel změny (Business/IT owner).
RPO (Recovery Point Objective)	Maximální stáří dat, o která se může při havárii přijít (např. 2 hodiny).
RSAT	Remote Server Administration Tools (Nástroje pro vzdálenou správu serveru)
RTO (Recovery Time Objective)	Doba, do které musí být služba po výpadku obnovena.
Runbooky	Návody krok za krokem, jak spravovat systémy nebo řešit incidenty, aby to mohl provést i jiný než původní specialista.
SLA (Service Level Agreement)	Smluvní dohoda o tom, jak rychle a spolehlivě má dodavatel službu poskytovat.
Sandbox	Oddělené testovací prostředí, kde lze bezpečně zkoušet změny bez rizika pro ostrý provoz.
SOC	Security Operations Center je centrální bezpečnostní operační centrum, které nepřetržitě monitoruje, detekuje a reaguje na bezpečnostní hrozby v organizaci.
Správce PAM	Správce PAM, který má na starosti správu a konfiguraci PAM (např. nastavování politik).
SSH	Zabezpečený protokol pro připojení k serverům
SSO	Systém jednotného přihlášení (*Single Sign-On*)
Standardní Software	Software, který je ke dni uzavření Smlouvy na trhu nabízen jako produkt, je dostupný po uzavření příslušné licenční smlouvy, ať za úplatu nebo bezúplatně, a nebyl vytvořen cíleně pro plnění Smlouvy, a to včetně počítačových programů distribuovaných pod veřejnou licencí (tzv. open source), jejichž licenční podmínky umožňují komukoli získat licenci a zasahovat do zdrojového kódu a dále jej upravovat, modifikovat, překládat, využívat nebo rozvíjet bez omezení, včetně tzv. proprietárního SW, u něhož držitel majetkových autorských práv běžně neposkytuje třetím osobám zdrojový kód, a včetně SW splňujícího uvedené podmínky a vytvořeného Dodavatelem před uzavřením Smlouvy; Standardním Software nejsou úpravy Standardního Softwaru (customizace) vytvořené pro účely plnění této Smlouvy, které vyžadují zásahy do zdrojového kódu Standardního Softwaru nebo vytvoření nového zdrojového kódu.
Subskripční (předplatitelská) licence	Pprávnění nabyvatele užívat Software nebo Standardní Software po dobu trvání sjednaného předplatného, podmíněného pravidelnou úhradou licenční odměny. Po dobu platnosti má nabyvatel právo na průběžné aktualizace, nové verze a technickou podporu v rozsahu dle této smlouvy; uplynutím doby předplatného právo užívat Software nebo Standardní Software zaniká.
SW/Software	Část elektronického informačního systému, která sestává z počítačového kódu, zejména počítačové programy, a to včetně přípravných a koncepčních materiálů.

Triage	Rychlé vyhodnocení a určení priority požadavku nebo problému, aby se nejdřív řešily ty nejdůležitější věci.
UAT (User Acceptance Testing)	Testování uživateli, kteří ověřují, že změna nebo systém funguje podle jejich potřeb a je připravený k nasazení.
VM (Virtual Machine)	Virtuální stroj — samostatný „počítač“ spuštěný jako program uvnitř fyzického počítače; chová se jako oddělené prostředí.
Uživatel PAM	Uživatel PAM je administrátor (interní či externí), který používá PAM řešení pro přístup k spravovaným koncovým systémům.
Workaround	Dočasné náhradní řešení, které obejde problém, dokud nebude k dispozici trvalá oprava.
zdrojový kód	Zápis kódu počítačového programu (Softwaru) v programovacím jazyce, který je uložen v jednom nebo více editovatelných souborech, čitelný, opatřeny komentáři vysvětlujícími jeho jednotlivé časti alespoň ve standardu obvyklém pro open source projekty a procesy, ve spustitelném formátu odpovídajícím programovacímu jazyku a produkčnímu prostředí, včetně ověřeného a podrobného postupu nezbytného pro sestaveni plně funkčního strojového kódu, a v podobě, aby jej bylo možné zkompilovat do strojového kódu bez nutnosti provedeni jiných uprav než kompilace v souladu s postupem k sestavení.
ZoKB	Zákon č. 264/2025 Sb., Zákon o kybernetické bezpečnosti

KRYCÍ LIST NABÍDKY

Veřejná zakázka zadávána v otevřeném nadlimitním řízení dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů

Název:	**„Služby poskytování implementace a podpory IDM a PAM“**

Základní identifikační údaje

Zadavatel	
Název:	Státní tiskárna cenin, s. p.
Sídlo:	Růžová 943/6, Nové Město,110 00 Praha 1
IČO:	00001279
Osoba oprávněná jednat jménem zadavatele:	Mgr. Marek Šimandl, MPA, generální ředitel
Účastník řízení	
Název:	**[VYPLNÍ ÚČASTNÍK]**
Sídlo:	**[VYPLNÍ ÚČASTNÍK]**
Identifikátor datové schránky:	**[VYPLNÍ ÚČASTNÍK]**
Korespondenční adresa:	**[VYPLNÍ ÚČASTNÍK]**
IČO, DIČ:	**[VYPLNÍ ÚČASTNÍK]**
Osoba oprávněná za účastníka jednat:	**[VYPLNÍ ÚČASTNÍK]**
Kontaktní osoba:	**[VYPLNÍ ÚČASTNÍK]**
Tel.:	**[VYPLNÍ ÚČASTNÍK]**
E-mail:	**[VYPLNÍ ÚČASTNÍK]**
Malý nebo střední podnik:	ANO / NE
(dále jen “**účastník**”)	

(1) ČESTNÉ PROHLÁŠENÍ K ZÁKLADNÍ ZPŮSOBILOSTI

Jako osoba oprávněná jednat jménem či za výše uvedeného účastníka podáním nabídky prostřednictvím elektronického nástroje prohlašuji místopřísežně, že výše uvedený účastník je účastníkem:

a) který nebyl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 k zákonu č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, nebo obdobný trestný čin podle právního řádu země sídla účastníka; k zahlazeným odsouzením se nepřihlíží; jde-li o právnickou osobu, musí tento předpoklad splňovat jak tato právnická osoba, tak zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu účastníka právnická osoba, musí výše uvedené podmínky splňovat jak tato právnická osoba, tak každý člen statutárního orgánu této právnické osoby a také osoba zastupující tuto právnickou osobu v statutárním orgánu účastníka.

   Podává-li nabídku či žádost o účast pobočka závodu zahraniční právnické osoby, musí výše uvedené podmínky splňovat tato právnická osoba a vedoucí pobočky závodu.

   Podává-li nabídku či žádost o účast pobočka závodu české právnické osoby, musí výše uvedené podmínky splňovat vedle výše uvedených osob rovněž vedoucí pobočky.

b) který nemá v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek, včetně spotřební daně,

c) který nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,

d) který nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,

e) který není v likvidaci, nebylo proti němu vydáno rozhodnutí o úpadku, nebyla vůči němu nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla účastníka.

(2) ČESTNÉ PROHLÁŠENÍ O STŘETU ZÁJMŮ

Jako osoba oprávněná jednat jménem či za výše uvedeného účastníka tímto prohlašuji místopřísežně, že výše uvedený účastník předmětné veřejné zakázky **není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů, nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti**, stejně tak prohlašuji, že výše uvedený účastník neprokazuje kvalifikaci v rámci dané veřejné zakázky prostřednictvím poddodavatele, který by byl takovou obchodní společností, a to v souladu s požadavkem zadavatele uvedeném ve výzvě k podání nabídek.

(3) ČESTNÉ PROHLÁŠENÍ K APLIKOVANÝM SANKCÍM

Tzv. ekonomické sankce

1. Jako osoba oprávněná jednat jménem či za účastníka tímto čestně prohlašuji, že účastník, v souladu s čl. 5 k Nařízení Rady (EU) č. 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014, o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, není:

   a. ruským státním příslušníkem, fyzickou či právnickou osobou nebo subjektem či orgánem se sídlem v Rusku;

b. právnickou osobou, subjektem nebo orgánem, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písmenu a) tohoto odstavce;

c. fyzickou nebo právnickou osobou, subjektem nebo orgánem, které jednají jménem nebo na pokyn některého ze subjektů uvedených v písmenech a) nebo b) tohoto odstavce.

2. Jako osoba oprávněná jednat jménem či za účastníka tímto čestně prohlašuji, že žádný z poddodavatelů účastníka, který bude účastníkem využit pro plnění smlouvy z této veřejné zakázky, a jehož rozsah činnosti a/nebo odměny překročí 10 % hodnoty plnění smlouvy, není subjektem uvedeným v písmenu a) nebo b) nebo c) odstavce 1 tohoto prohlášení.

Tzv. Individuální sankce

1. Jako osoba oprávněná jednat jménem či za účastníka tímto čestně prohlašuji, že účastník ve smyslu:

   a. čl. 2 odst. 2 Nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, v platném znění, (dále jen „Nařízení č. 269/2014), a

   b. čl. 2 odst. 2 Nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014, o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, v platném znění, (dále jen „Nařízení č. 208/2014“), a

   c. čl. 2 odst. 2 Nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska, v platném znění, (dále jen „Nařízení č. 765/2006“),

   není fyzickou nebo právnickou osobou, subjektem či orgánem nebo fyzickou nebo právnickou osobou, subjektem či orgánem s nimi spojeným uvedeným v příloze I Nařízení č. 269/2014, Nařízení č. 208/2014 nebo Nařízení č. 765/2006.

2. Jako osoba oprávněná jednat jménem či za účastníka tímto čestně prohlašuji, že žádné finanční prostředky ani hospodářské zdroje nebudou pro účely plnění dané veřejné zakázky, přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům uvedeným v příloze I Nařízení č. 269/2014, Nařízení č. 208/2014 nebo Nařízení č. 765/2006 nebo v jejich prospěch.

(4) ČESTNÉ PROHLÁŠENÍ K AKCEPTACI NÁVRHU SMLOUVY

Jako osoba oprávněná jednat jménem či za účastníka tímto čestně prohlašuji, že účastník plně a bezvýhradně akceptuje Návrh smlouvy.

Účastník bere na vědomí, že pokud bude vybrán v rámci této veřejné zakázky, uzavře se zadavatelem dané znění Návrhu smlouvy.

Údaje ke kompletaci Návrhu smlouvy:

Číslo smlouvy dodavatele	**[VYPLNÍ ÚČASTNÍK*]** *** vyplňte pouze pokud chcete ve smlouvě uvádět**
Bankovní spojení:	**[VYPLNÍ ÚČASTNÍK]**

Číslo účtu:	**[VYPLNÍ ÚČASTNÍK]**
Zmocněnec pro jednání smluvní a ekonomická za dodavatele včetně uvedení jeho funkce:	**[VYPLNÍ ÚČASTNÍK]**
Zmocněnec pro jednání věcná a technická za dodavatele včetně uvedení jeho funkce:	**[VYPLNÍ ÚČASTNÍK]**
E-mailový kontakt zmocněnce:	**[VYPLNÍ ÚČASTNÍK]**
Telefonický kontakt zmocněnce:	**[VYPLNÍ ÚČASTNÍK]**
E- mailový kontakt dle čl. II odst. 5 bod 5.2.2. Návrhu smlouvy:	**[VYPLNÍ ÚČASTNÍK]**
E- mailový kontakt dle čl. II odst. 5 bod 5.3.5 Návrhu smlouvy:	**[VYPLNÍ ÚČASTNÍK]**
E- mailový kontakt dle čl. II odst. 5 bod 5.3.8 Návrhu smlouvy:	**[VYPLNÍ ÚČASTNÍK]**
E-mailový kontakt dle čl. IX odst. 4 Návrhu smlouvy:	**[VYPLNÍ ÚČASTNÍK]**
Telefonický kontakt dle čl. IX odst. 4 Návrhu smlouvy:	**[VYPLNÍ ÚČASTNÍK]**
Osoba/y, která/é bude/ou podepisovat Návrh smlouvy, pokud se liší od osoby uvedené na první straně tohoto krycího listu, včetně uvedení funkce, z jaké pozice daná osoba Návrh smlouvy podepisuje:	**[VYPLNÍ ÚČASTNÍK]**

Cena celkem - Dodávka IdM a PAM

Etapa	Název	Cena	
1	**Etapa 1: Dodávka IdM** (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.1 až 5.1.3 a 5.1.6 Smlouvy)	10,00 Kč	
	Etapa 1: Školení (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.4 Smlouvy)	10,00 Kč	
	Etapa 1: Perpetuální licence IdM (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.5 Smlouvy)	0,00 Kč	List licence IdM
Celkem		**20,00 Kč**	
2	**Etapa 2: Dodávka PAM** (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.7 až 5.1.9 a 5.1.13 Smlouvy)	10,00 Kč	
	Etapa 2: Dodávka HW (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.11 Smlouvy)	0,00 Kč	HW
	Etapa 2: Školení (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.10 Smlouvy)	10,00 Kč	
	Etapa 2: Perpetuální licence PAM (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.12 Smlouvy)	0,00 Kč	List licence PAM
Celkem		**20,00 Kč**	
3	**Etapa 3: Dodávka** (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.14 až 5.1.16 a 5.1.18 Smlouvy)	10,00 Kč	
	Etapa 3: Školení (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.17 Smlouvy)	1,00 Kč	
Celkem		**11,00 Kč**	
	Subskripční Licence IdM (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.5 Smlouvy)	0,00 Kč	List licence IdM
	Subskripční Licence PAM (plnění dle čl. II odst. 5, bod 5.1., odrážka 5.1.12 Smlouvy)	0,00 Kč	List licence PAM
	Cena Služeb podpory IdM od Go-live Etapy 1 do Go-live Etapy 3	130,00 Kč	List podpora
	Cena Služeb podpory IdM od Go-live Etapy 3	480,00 Kč	List podpora
	Cena Služeb podpory PAM od Go-live Etapy 2	480,00 Kč	List podpora
	Ad hoc služby - Rozvoj celkem	5 000 000,00 Kč	
Celkem		**5 001 141,00 Kč**	

Vyplňte žlutá pole

Obecné pokyny

- Dodavatel **vyplňuje výhradně buňky označené žlutou barvou**.
- Ostatní buňky obsahují vzorce a **nesmí být upravovány**.
- Všechny částky se uvádějí **bez DPH**, pokud není uvedeno jinak.
- Součty a celkové ceny se **počítají automaticky**.

List Celkem

- Na tomto listu vyplňte **žlutá pole za každou Etapu a školení**.
- Do listu se **automaticky přenášejí výsledné částky** z jednotlivých listů:
  - Podpora
  - Licence IdM
  - Licence PAM
  - HW
- Výsledkem je **celková nabídková cena**.

Cena Služeb podpory

Cena Služeb podpory dle dle čl. II odst. 5 bod 5.2 Smlouvy	Počet měsíců poskytování Služeb podpory	paušální částka/měsíc	
Cena Služeb podpory IdM od Go-live Etapy 1 do Go-live Etapy 3	13	10,00 Kč	130,00 Kč
Cena Služeb podpory IdM od Go-live Etapy 3	48	10,00 Kč	480,00 Kč
Cena Služeb podpory PAM od Go-live Etapy 2	48	10,00 Kč	480,00 Kč

	Počet MD	Sazba za poskytování 1 MD ad hoc služeb	
Ad hoc služby - Rozvoj celkem	1 000	5 000,00 Kč	5 000 000,00 Kč

Celkem	5 001 090,00 Kč

Zpět

List Podpora

- Vyplňte **žlutá pole s cenami služeb podpory** poskytovaných v jednotlivých etapách.
- Cena je zadávána:
  - jako **měsíční paušál**,
  - po stanovený počet měsíců dle etapy.
- Celková cena podpory se **automaticky dopočítá**.

Licence IdM

Ke každé licenci zaškrtněte pouze jednu možnost (FOSS, Perpetuální nebo Subskripční)

Poradové číslo	Název licence	SW vyberte z ROLOVACÍHO SEZNAMU klikněte zde pro nápovědu	klikněte zde pro nápovědu FOSS	Klikněte zde pro nápovědu Perpetuální	Cena / jednorazová platba/perpetuální	Klikněte zde pro nápovědu Subskripční	Cena / platba za pololetí/subskripční	Celkem v Kč bez DPH perpetuální	Celkem v Kč bez DPH za 4 roky subskripční (celkem 8 plateb)	Celkem za všechny licence/4 roky	*Vložte odkaz na obecná licenční pravidla
1		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
2		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
Celkem			**0 ks**	**0 ks**	**0,00 Kč**	**0 ks**	**0,00 Kč**	**0,00 Kč**	**0,00 Kč**	**0,00 Kč**	

Dodavatel vyplní všechna pole označená žlutou barvou, včetně polí, která se zvýrazní žlutě až po výběru jedné z možností nebo po zaškrtnutí příslušného políčka.

Zpět

Licence

Ke každé licenci vyplňte následující údaje:

1. **Sloupec A** – pořadové číslo.
2. **Sloupec B** – název licence.
3. **Sloupec C** – výběr typu software z rolovacího seznamu *(standardní SW / SW)*.
4. **Standardní software** – pokud dodavatel ve sloupci C zvolí možnost **„Standardní SW“**, automaticky se zvýrazní (zežlutí) pole **„Vložte odkaz na obecná licenční pravidla“**. Do tohoto pole dodavatel **vloží aktivní odkaz (URL)** na obecná licenční pravidla výrobce nebo poskytovatele daného software.
5. **Typ licence** – zaškrtněte **pouze jednu** z následujících možností:
   - FOSS (bezplatná licence),
   - Perpetuální (jednorázová platba),
   - Subskripční (cena za 6 měsíců).

U subskripční licence je cena za 6 měsíců **automaticky vynásobena koeficientem 8**, což odpovídá době trvání kontraktu **4 roky**.

6. **Cena licence**
   - u FOSS licence se cena nevyplňuje,
   - u Perpetuální a Subskripční licence se cena vyplňuje do příslušného sloupce, který se **automaticky zvýrazní (zežlutí)** po potvrzení odpovídající volby v zaškrtávacím políčku.

Pod tabulkou se **automaticky zobrazují součty**:

- **finanční** (v Kč) za dobu trvání kontraktu,
- **množstevní** (počet licencí).

Licence PAM

Ke každé licenci zaškrtněte pouze jednu možnost (FOSS, Perpetuální nebo Subskripční)

Poradové číslo	Název licence	SW vyberte z ROLOVACÍHO SEZNAMU klikněte zde pro nápovědu	klikněte zde pro nápovědu FOSS	Klikněte zde pro nápovědu Perpetuální	Cena / jednorazová platba/perpetuální	Klikněte zde pro nápovědu Subskripční	Cena / platba za pololetí/subskripční	Celkem v Kč bez DPH perpetuální	Celkem v Kč bez DPH za 4 roky subskripční (celkem 8 plateb)	Celkem za všechny licence/4 roky	*Vložte odkaz na obecná licenční pravidla
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
		Vyberte z možností	☐	☐		☐		0,00 Kč	0,00 Kč	0,00 Kč	
Celkem			**0 ks**	**0 ks**	**0,00 Kč**	**0 ks**	**0,00 Kč**	**0,00 Kč**	**0,00 Kč**	**0,00 Kč**	

Dodavatel vyplní všechna pole označená žlutou barvou, včetně polí, která se zvýrazní žlutě až po výběru jedné z možností nebo po zaškrtnutí příslušného políčka.

Zpět

Licence

Ke každé licenci vyplňte následující údaje:

1. **Sloupec A** – pořadové číslo.
2. **Sloupec B** – název licence.
3. **Sloupec C** – výběr typu software z rolovacího seznamu *(standardní SW / SW)*.
4. **Standardní software** – pokud dodavatel ve sloupci C zvolí možnost **„Standardní SW“**, automaticky se zvýrazní (zežlutí) pole **„Vložte odkaz na obecná licenční pravidla“**. Do tohoto pole dodavatel **vloží aktivní odkaz (URL)** na obecná licenční pravidla výrobce nebo poskytovatele daného software.
5. **Typ licence** – zaškrtněte **pouze jednu** z následujících možností:
   - FOSS (bezplatná licence),
   - Perpetuální (jednorázová platba),
   - Subskripční (cena za 6 měsíců).

U subskripční licence je cena za 6 měsíců **automaticky vynásobena koeficientem 8**, což odpovídá době trvání kontraktu **4 roky**.

6. **Cena licence**
   - u FOSS licence se cena nevyplňuje,
   - u Perpetuální a Subskripční licence se cena vyplňuje do příslušného sloupce, který se **automaticky zvýrazní (zežlutí)** po potvrzení odpovídající volby v zaškrtávacím políčku.

Pod tabulkou se **automaticky zobrazují součty**:

- **finanční** (v Kč) za dobu trvání kontraktu,
- **množstevní** (počet licencí).

Cena HW

Poradové číslo	Označte, jestli bude HW součástí dodávky	HW (klikněte pro nápovědu)	Počet ks	Cena za KS	Cena celkem
1	☐				- Kč
2	☐				- Kč
3	☐				- Kč
4	☐				- Kč
5	☐				- Kč
6	☐				- Kč
7	☐				- Kč
8	☐				- Kč
9	☐				- Kč
10	☐				- Kč
11	☐				- Kč
12	☐				- Kč
13	☐				- Kč
14	☐				- Kč
15	☐				- Kč
16	☐				
Celkem					- Kč

Zpět

7. HW

- V případě, že je hardware součástí dodávky, označte příslušné zaškrtávací políčko.
- Po jeho označení se automaticky zvýrazní (zežlutí) pole určená k vyplnění, do kterých dodavatel doplní požadované údaje o hardware.
- Pokud hardware není součástí dodávky, ponechte zaškrtávací políčko neoznačené a příslušná pole nevyplňujte.

Standardní Software	Software, který je ke dni uzavření Smlouvy na trhu nabízen jako produkt, je dostupný po uzavření příslušné licenční smlouvy, ať za úplatu nebo bezúplatně, a nebyl vytvořen cíleně pro plnění Smlouvy, a to včetně počítačových programů distribuovaných pod veřejnou licencí (tzv. open source), jejichž licenční podmínky umožňují komukoli získat licenci a zasahovat do zdrojového kódu a dále jej upravovat, modifikovat, překládat, využívat nebo rozvíjet bez omezení, včetně tzv. proprietárního SW, u něhož držitel majetkových autorských práv běžně neposkytuje třetím osobám zdrojový kód, a včetně SW splňujícího uvedené podmínky a vytvořeného Dodavatelem před uzavřením Smlouvy; Standardním Software nejsou úpravy Standardního Softwaru (customizace) vytvořené pro účely plnění této Smlouvy, které vyžadují zásahy do zdrojového kódu Standardního Softwaru nebo vytvoření nového zdrojového kódu.
Subskripční (předplatitelská) licence	Oprávnění nabyvatele užívat Software nebo Standardní Software po dobu trvání sjednaného předplatného, podmíněného pravidelnou úhradou licenční odměny. Po dobu platnosti má nabyvatel právo na průběžné aktualizace, nové verze a technickou podporu v rozsahu dle této smlouvy; uplynutím doby předplatného právo užívat Software nebo Standardní Software zaniká.
Perpetuální (trvalá) licence	Licence k užití softwaru poskytovaná na dobu neurčitou, která opravňuje nabyvatele k trvalému užívání softwaru v souladu s licenčními podmínkami, bez časového omezení platnosti licence, ledaže je výslovně sjednáno jinak.
FOSS licence	Free Open Source Software licence, náklady na využití FOSS licence v rámci plnění dle této smlouvy jsou zahrnuty v celkové ceně IdM a PAM, resp. Etapy 1 nebo 2.
SW/Software	Část elektronického informačního systému, která sestává z počítačového kódu, zejména počítačové programy, a to včetně přípravných a koncepčních materiálů.
HW/ Hardware	Veškeré hmotné součásti počítačových systémů a veškeré související vybaveni hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.

List licence IdM
List licence PAM
List podpora
HW
Zpět

ČESTNÉ PROHLÁŠENÍ K TECHNICKÉ KVALIFIKACI

Název veřejné zakázky:

„Služby poskytování implementace a podpory IDM a PAM“

Název účastníka (vč. právní formy):	**[VYPLNÍ ÚČASTNÍK]**
Sídlo:	**[VYPLNÍ ÚČASTNÍK]**
IČO:	**[VYPLNÍ ÚČASTNÍK]**

V souladu s požadavkem zadavatele v bodě 10.5.1. zadávací dokumentace uvádím seznam významných dodávek:

Významná dodávka	
Identifikace dodavatele, který dané plnění poskytl a jeho role (dodavatel/poddodavatel):	**[VYPLNÍ ÚČASTNÍK]**
Identifikace objednatele, kterému bylo dané plnění poskytnuto:	**[VYPLNÍ ÚČASTNÍK]**
Doba plnění s přesností na kalendářní měsíce:	**[VYPLNÍ ÚČASTNÍK]**
Stručný popis předmětu plnění:	**[VYPLNÍ ÚČASTNÍK]**
Finanční objem (celková cena v Kč bez DPH):	**[VYPLNÍ ÚČASTNÍK]**
Kontaktní osoba objednatele pro účely ověření uvedených informací (jméno, telefon a e-mail):	**[VYPLNÍ ÚČASTNÍK]**

Pozn.: Účastník vždy použije tabulku tolikrát, kolikrát je třeba. Zadavatel požaduje po dodavateli minimálně 3 referenční dodávky, kdy alespoň jedna byla na dodávku systému IdM v minimálním finančním objemu 5.000.000 Kč bez DPH za dodávku a alespoň jedna byla na dodávku systému PAM v minimálním finančním objemu 5.000.000 Kč bez DPH za dodávku, vždy včetně poskytnuté podpory pro oba systémy v délce minimálně 6 měsíců.

A zároveň

v souladu s požadavkem zadavatele v bodě 10.5.2 zadávací dokumentace uvádím seznam členů řešitelského týmu:

Expert IdM:	
Jméno a příjmení fyzické osoby:	**[VYPLNÍ ÚČASTNÍK]**
Informaci, v jakém pracovněprávním či jiném vztahu je daná fyzická osoba vůči účastníkovi, tj. zejména zda je poddodavatelem účastníka.	**[VYPLNÍ ÚČASTNÍK]**
Stručný popis referenčního projektu, a rozsah zapojení dané fyzické osoby včetně označení jeho role *(účastník doplní tolik řádků, kolik významných zakázek předkládá)*	**[VYPLNÍ ÚČASTNÍK]**
Název a IČO společnosti, kde byl referenční projekt realizován. Kontaktní osoba společnosti pro účely ověření uvedených informací (jméno, telefon a e-mail).	**[VYPLNÍ ÚČASTNÍK]**
Délka dosavadní praxe z oblasti implementace systémů IdM v obdobné roli:	**[VYPLNÍ ÚČASTNÍK]**

Expert PAM:	
Jméno a příjmení fyzické osoby:	**[VYPLNÍ ÚČASTNÍK]**
Informaci, v jakém pracovněprávním či jiném vztahu je daná fyzická osoba vůči účastníkovi, tj. zejména zda je poddodavatelem účastníka.	**[VYPLNÍ ÚČASTNÍK]**
Stručný popis referenčního projektu, a rozsah zapojení dané fyzické osoby včetně označení její role: *(účastník doplní tolik řádků, kolik významných zakázek předkládá)*	**[VYPLNÍ ÚČASTNÍK]**
Název a IČO společnosti, kde byl referenční projekt realizován. Kontaktní osoba společnosti pro účely ověření uvedených informací (jméno, telefon a e-mail).	**[VYPLNÍ ÚČASTNÍK]**
Délka dosavadní praxe z oblasti implementace systémů PAM v obdobné roli:	**[VYPLNÍ ÚČASTNÍK]**

Architekt řešení:	
Jméno a příjmení fyzické osoby:	**[VYPLNÍ ÚČASTNÍK]**
Informaci, v jakém pracovněprávním či jiném vztahu je daná fyzická osoba vůči účastníkovi, tj. zejména zda je poddodavatelem účastníka.	**[VYPLNÍ ÚČASTNÍK]**
Délka dosavadní praxe s tvorbou architektury pro implementaci IdM a/nebo PAM v obdobné roli a s tvorbou architektury v souvislosti se zavedením systémů pro kybernetickou bezpečnosti:	**[VYPLNÍ ÚČASTNÍK]**

Senior projekt manager:	
Jméno a příjmení fyzické osoby:	**[VYPLNÍ ÚČASTNÍK]**
Informaci, v jakém pracovněprávním či jiném vztahu je daná fyzická osoba vůči účastníkovi, tj. zejména zda je poddodavatelem účastníka.	**[VYPLNÍ ÚČASTNÍK]**
Stručný popis referenčního projektu, a rozsah zapojení dané fyzické osoby včetně označení její role:	**[VYPLNÍ ÚČASTNÍK]**
Název a IČO společnosti, kde byl referenční projekt realizován. Kontaktní osoba společnosti pro účely ověření uvedených informací (jméno, telefon a e-mail).	**[VYPLNÍ ÚČASTNÍK]**
Délka dosavadní praxe z oblasti řízení projektů týkajících se implementace softwarových řešení v obdobné roli:	**[VYPLNÍ ÚČASTNÍK]**
Seznam získaných relevantních certifikátů: ***Kopie certifikátů požadovaných zadavatelem musí být přiloženy v nabídce***	**[VYPLNÍ ÚČASTNÍK]**

Přílohu tohoto seznamu budou tvořit kopie zadavatelem požadovaných certifikátů v souladu se zadávací dokumentací

Bezpečnostní expert:	
Jméno a příjmení fyzické osoby:	**[VYPLNÍ ÚČASTNÍK]**

Informaci, v jakém pracovněprávním či jiném vztahu je daná fyzická osoba vůči účastníkovi, tj. zejména zda je poddodavatelem účastníka.	**[VYPLNÍ ÚČASTNÍK]**
Stručný popis referenčního projektu, a rozsah zapojení dané fyzické osoby včetně označení její role:	**[VYPLNÍ ÚČASTNÍK]**
Název a IČO společnosti, kde byl referenční projekt realizován. Kontaktní osoba společnosti pro účely ověření uvedených informací (jméno, telefon a e-mail).	**[VYPLNÍ ÚČASTNÍK]**
Délka dosavadní praxe z oblasti kybernetické bezpečnosti v obdobné roli:	**[VYPLNÍ ÚČASTNÍK]**
Seznam získaných relevantních certifikátů: ***Kopie certifikátů požadovaných zadavatelem musí být přiloženy v nabídce***	**[VYPLNÍ ÚČASTNÍK]**

Přílohu tohoto seznamu budou tvořit kopie zadavatelem požadovaných certifikátů v souladu se zadávací dokumentací

Integrátor IdM/PAM:	
Jméno a příjmení fyzické osoby:	**[VYPLNÍ ÚČASTNÍK]**
Informaci, v jakém pracovněprávním či jiném vztahu je daná fyzická osoba vůči účastníkovi, tj. zejména zda je poddodavatelem účastníka.	**[VYPLNÍ ÚČASTNÍK]**
Stručný popis referenčního projektu, a rozsah zapojení dané fyzické osoby včetně označení její role: *(účastník doplní tolik řádků, kolik významných zakázek předkládá)*	**[VYPLNÍ ÚČASTNÍK]**
Název a IČO společnosti, kde byl referenční projekt realizován. Kontaktní osoba společnosti pro účely ověření uvedených informací (jméno, telefon a e-mail).	**[VYPLNÍ ÚČASTNÍK]**

SEZNAM PODDODAVATELŮ

Název veřejné zakázky:

„Služby poskytování implementace a podpory IDM a PAM“

Název účastníka (vč. právní formy):	**[VYPLNÍ ÚČASTNÍK]**
Sídlo:	**[VYPLNÍ ÚČASTNÍK]**
IČO:	**[VYPLNÍ ÚČASTNÍK]**

1) V souladu s požadavkem zadavatele uvedeném v zadávací dokumentaci k výše uvedené veřejné zakázce, uvádím seznam poddodavatelů, s jejichž pomocí budu plnit předmět zakázky.

A)
Poddodavatel **[VYPLNÍ ÚČASTNÍK]**
se sídlem **[VYPLNÍ ÚČASTNÍK]**
zastoupený **[VYPLNÍ ÚČASTNÍK]**
IČO: **[VYPLNÍ ÚČASTNÍK]**
Druh a rozsah služeb, které bude poddodavatel poskytovat: **[VYPLNÍ ÚČASTNÍK]**
Procento celkových nákladů plnění, které bude poddodavatel realizovat: [VYPLNÍ ÚČASTNÍK]

B)
Poddodavatel **[VYPLNÍ ÚČASTNÍK]**
se sídlem **[VYPLNÍ ÚČASTNÍK]**
zastoupený **[VYPLNÍ ÚČASTNÍK]**
IČO: **[VYPLNÍ ÚČASTNÍK]**
Druh a rozsah služeb, které bude poddodavatel poskytovat: **[VYPLNÍ ÚČASTNÍK]**
Procento celkových nákladů plnění, které bude poddodavatel realizovat: [VYPLNÍ ÚČASTNÍK]

C)
Poddodavatel **[VYPLNÍ ÚČASTNÍK]**
se sídlem **[VYPLNÍ ÚČASTNÍK]**
zastoupený **[VYPLNÍ ÚČASTNÍK]**
IČO: **[VYPLNÍ ÚČASTNÍK]**
Druh a rozsah služeb, které bude poddodavatel poskytovat: **[VYPLNÍ ÚČASTNÍK]**
Procento celkových nákladů plnění, které bude poddodavatel realizovat: [VYPLNÍ ÚČASTNÍK]

(účastník přidá počet poddodavatelů dle potřeby)

2) Tímto jako účastník výše uvedené veřejné zakázky čestně prohlašuji, že nemám v úmyslu zadat žádnou část uvedené veřejné zakázky žádnému poddodavateli.[1]

[1] V případě, že účastník nemá v úmyslu zadat žádnou část zakázky žádnému poddodavateli, seznam poddodavatelů dle bodu 1) nevyplňuje a pole proškrtne.

PROHLÁŠENÍ O ZACHOVÁNÍ MLČENLIVOSTI

[DOPLNÍ DODAVATEL]

se sídlem: [DOPLNÍ DODAVATEL]

IČO: [DOPLNÍ DODAVATEL]

společnost zapsaná v obchodním rejstříku vedeném [DOPLNÍ DODAVATEL] soudem v [DOPLNÍ DODAVATEL]

oddíl [DOPLNÍ DODAVATEL], vložka [DOPLNÍ DODAVATEL]

zastoupená: [DOPLNÍ DODAVATEL]

(dále jen „**Dodavatel**“)

vědom si svých závazků v tomto prohlášení obsažených a s úmyslem být tímto prohlášením vázán, deklaruje následující:

1. ÚČEL PROHLÁŠENÍ

1.1 Státní tiskárna cenin, s. p., se sídlem Růžová 943/6, Nové Město, 110 00 Praha 1, IČO: 00001279, vedená u Městského soudu v Praze pod sp. zn. ALX 296 (dále jen „**Zadavatel**") oznámila odesláním formuláře Oznámení o zahájení zadávacího řízení svůj úmysl zadat veřejnou zakázku s názvem „**Služby poskytování implementace a podpory IDM a PAM“** (dále jen „Veřejná zakázka“) dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“). Dodavatel s úmyslem účastnit se Veřejné zakázky požaduje náhled do těch částí zadávací dokumentace k Veřejné zakázce, které obsahují informace, jež Zadavatel považuje za důvěrné /nejedná se o důvěrné informace ve smyslu zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti/ a vyžaduje jejich ochranu (dále jen „**Důvěrné informace**“). Z tohoto důvodu předkládá Dodavatel prohlášení o ochraně důvěrných informací (dále jen „**Prohlášení**“).

1.2 Účelem Prohlášení je závazek Dodavatele, že Důvěrné informace dle Prohlášení použije pouze způsobem a k účelu v Prohlášení stanoveným.

1.3 Nedohodnou-li se Zadavatel a Dodavatel jinak, Dodavatel není oprávněn nakládat s Důvěrnými informacemi, pokud prohlášení není účinné alespoň v části specifikované v odst. 7.1 Prohlášení.

2. DŮVĚRNÉ INFORMACE

2.1 Nedohodnou-li se Dodavatel a Zadavatel jinak, jsou veškeré informace, které byly Zadavatelem Dodavateli poskytnuty a jsou uvedené v příloze č. 1 Prohlášení, považovány za Důvěrné informace, jejichž použití podléhá Prohlášení.

3. UŽITÍ DŮVĚRNÝCH INFORMACÍ

3.1 Veškeré Důvěrné informace zůstávají výhradním vlastnictvím Zadavatele a Dodavatel je oprávněn tyto užít jen pro účely své účasti v zadávacím řízení na plnění Veřejné zakázky.

3.2 Dodavatel se zavazuje zachovat důvěrnost Důvěrných informací a zpřístupnit je třetím osobám pouze za podmínek stanovených v tomto Prohlášení.

3.3 Svým zaměstnancům a orgánům je Dodavatel oprávněn Důvěrné informace zpřístupnit jen v rozsahu, v jakém je pro tu-kterou osobu nezbytně nutné, aby se s Důvěrnými informacemi seznámila pro účely účasti Dodavatele v zadávacím řízení na zadání Veřejné zakázky. Tyto osoby musí být poučeny o důvěrném charakteru předávaných informací a zavázány k mlčenlivosti.

3.4 Dodavatel je oprávněn zpřístupnit Důvěrné informace třetím osobám jen s předchozím písemným souhlasem Zadavatele anebo při splnění podmínek uvedených v článku 4 Prohlášení.

4. PODDODAVATELÉ

4.1 Pokud Dodavatel zvažuje sdílet při přípravě nabídky na realizaci Veřejné zakázky a/nebo při eventuálním plnění Veřejné zakázky Dodavatelem Důvěrné informace se třetími osobami (dále jen „**Poddodavatelé**“) je povinen zajistit a prokázat Zadavateli, že před zpřístupněním Důvěrných informací Poddodavateli, že:

4.1.1 Poddodavatel deklaroval vlastním jménem a na vlastní účet prohlášení s v podstatě stejným obsahem, jako je obsah Prohlášení; tento předpoklad se považuje za splněný, pokud bude Zadavateli doručeno vyhotovení takového prohlášení o ochraně Důvěrných informací podepsané osobou oprávněnou zavazovat Poddodavatele; nebo

4.1.2 Dodavatel uzavřel s Poddodavatelem dohodu o ochraně informací, na základě, které budou Důvěrné informace poskytnuté Dodavateli a sdílené s Poddodavatelem podléhat ochraně i ze strany Poddodavatele za stejných podmínek, jako jsou stanoveny Prohlášením; tento předpoklad se považuje za splněný, pokud bude Zadavateli doručeno jedno vyhotovení takovéto dohody o ochraně informací podepsané osobami zastupujícími Poddodavatele a Dodavatele.

To neplatí, pokud Zadavatel již udělil písemný souhlas podle odst. 3.4 Prohlášení.

4.2 Za Poddodavatele se považuje jakákoliv třetí osoba spolupracující s Dodavatelem dle odst. 4.1 bez ohledu na to, zda:

4.2.1 spolupráce probíhá v rámci konsorcia Dodavatele a takovéto třetí osoby, jehož členové odpovídající Zadavateli společně a nerozdílně, nebo

4.2.2 spolupráce je založena na poddodavatelském vztahu takovéto třetí osoby vůči Dodavateli, nebo

4.2.3 spolupráce je založena na poddodavatelském vztahu Dodavatele vůči takovéto třetí osobě, nebo

4.2.4 Dodavatel a třetí osoba zvolili eventuální jinou formu spolupráce.

5. SPLNĚNÍ ÚČELU PROHLÁŠENÍ

5.1 Dodavatel se zavazuje, že po splnění účelu Prohlášení dle článku 1 anebo na písemnou výzvu Zadavatele bezodkladně zničí dokumenty získané od Zadavatele,

jakož i jakékoliv kopie, které v souvislosti s plněním předmětu a účelu Prohlášení pořídil.

6. PORUŠENÍ POVINNOSTÍ

6.1 Dodavatel odpovídá za porušení povinností pro nakládání s Důvěrnými informacemi dle článku 3 Prohlášení, které způsobil jeho Poddodavatel, jako by toto porušení způsobil sám Dodavatel. V případě, že Poddodavatel předložil Zadavateli prohlášení dle odst. 4.3.1 Prohlášení, odpovídají za porušení Prohlášení Dodavatel i Poddodavatel společně a nerozdílně.

6.2 Poruší-li Dodavatel jakoukoliv povinnost dle článku 3 anebo 4 anebo 5 Prohlášení, vznikne Zadavateli právo požadovat zaplacení smluvní pokuty Dodavatelem ve výši 200.000 Kč za každé porušení takové povinnosti, Dodavatel má povinnost smluvní pokutu zaplatit ve lhůtě a způsobem stanovenými v písemné výzvě Zadavatele k zaplacení smluvní pokuty.

6.3 Povinnost Dodavatele zaplatit smluvní pokutu dle Prohlášení se nedotýká nároku Zadavatele na náhradu škody způsobené porušením povinnosti, která ke vzniku nároku na smluvní pokutu vedla, a to v plné výši.

7. ZÁVĚREČNÁ USTANOVENÍ

7.1 Povinnost chránit Důvěrné informace zavazuje Dodavatele bez ohledu na případný zánik účinnosti Prohlášení po dobu patnácti (15) let od platnosti Prohlášení. Ustanovení o odpovědnosti a smluvních pokutách budou považována za účinná i pro případy porušení povinnosti dle předchozí věty.

7.2 Veškeré povinnosti vyplývající z Prohlášení přecházejí, pokud to povaha těchto povinností nevylučuje, na právní nástupce Dodavatele.

7.3 Kontaktní osoba Dodavatele pro komunikaci se Zadavatelem:

Jméno a příjmení: [DOPLNÍ DODAVATEL]

Adresa: [DOPLNÍ DODAVATEL]

Telefon: [DOPLNÍ DODAVATEL]

E-mail: [DOPLNÍ DODAVATEL]

7.4 Nedílnou součást Prohlášení tvoří Příloha č. 1 Specifikace Důvěrných informací

Dodavatel prohlašuje, že s obsahem Prohlášení souhlasí a na důkaz toho k němu připojuje svůj podpis.

Dodavatel

V [DOPLNÍ DODAVATEL] dne [DOPLNÍ DODAVATEL]

.....

[DOPLNÍ DODAVATEL]

[DOPLNÍ DODAVATEL]

PŘÍLOHA č. 1 Specifikace Důvěrných informací

Důvěrné informace jsou veškeré následující skutečnosti, informace a dokumenty:

Příloha č. 6 zadávací dokumentace

Obsahem neveřejné přílohy zadávací dokumentace jsou exporty dat a nastavení koncových systémů, a to včetně definic rolí jednotlivých uživatelů. .