

Klasifikace: Veřejný dokument



Technická specifikace

**Příloha č. 1 zadávací
dokumentace pro zadávací řízení
„Nasazení MFA a pořízení nosičů
certifikátů“**

Obsah

1	Seznam zkratk	4
2	Úvod	8
2.1	Záměr SŽ v oblasti MFA a nosičů uživatelských certifikátů	8
2.2	Předmět plnění veřejné zakázky	9
2.3	Oblasti, které nejsou předmětem plnění veřejné zakázky	14
2.4	Požadované funkcionality a vlastnosti řešení	15
2.4.1	Požadované vlastnosti systémů správy životního cyklu uživatelských certifikátů a správy životního cyklu nosičů certifikátů a obslužného SW koncových stanic	15
2.4.2	Požadované vlastnosti nosičů certifikátů	15
2.4.3	Požadavky na personalizaci nosičů certifikátů a technologie personalizačního pracoviště	15
2.4.4	Distribuce nosičů certifikátů a přístupových kódů	17
2.4.5	Integrace s bezpečnostními a provozními systémy Zadavatele	17
2.4.6	Licence	18
2.4.7	Další technické podmínky	19
3	Současný stav a popis prostředí	19
4	Požadavky na plnění	19
4.1	Před-implementační analýza	19
4.2	Implementace systému správy životního cyklu uživatelských certifikátů pro prostředí UAS a správy životního cyklu nosičů certifikátů	21
4.3	Implementace MFA s využitím uživatelských certifikátů (pro UAS)	22
4.4	Napojení systému správy životního cyklu uživatelských certifikátů (UAS) a nosiče certifikátů na další definované systémy Zadavatele	23
4.5	Ověřovací (pilotní provoz), dokumentace řešení, školení	24
4.6	Úvodní dodávka fyzických nosičů (karet)	26
4.7	Dodávka a implementace technologií personalizačního pracoviště	27
4.8	Zajištění přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů pro prostředí UAS	28
4.9	Technická podpora řešení	28
4.10	Služby na vyžádání	29
4.11	Průběžná dodávka fyzických nosičů (karet) a spotřebního materiálu personalizačního pracoviště	30
4.12	Ukončení smlouvy a exit plán	31
4.12.1	Exit plán	31

4.12.2	Součinnost stran	32
5	Fáze plnění a akceptační milníky	32

1 Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

Zkratka	Popis
AD, MS AD	Microsoft Active Directory
ADFS	Active Directory Federation Service
AS-IS	Současný stav
AKB	Architekt kybernetické bezpečnosti
API	Rozhraní pro programování aplikací (Application Programming Interface)
CA	Certifikační autorita
MKB	Manažer kybernetické informační bezpečnosti
ČSN	Česká státní norma
DC	Domain controller. Řadič domény s Active Directory
DR	Disaster Recovery (obnova po havárii)
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
EPS	Elektronické protipožární systémy
EZS	Elektronické zabezpečovací systémy
GPA	Garant primárního aktiva
GPdA	Garant podpůrného aktiva
HA	Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance
Harmonogram	Harmonogram stanovený ve Smlouvě o dílo, konkrétně v její příloze „Harmonogram“

HLD	Přehledový vysokoúrovňový design (High Level Design)
HR	Lidské zdroje
HW	Hardware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IDM	Správa identit a přístupů (Identity and Access Management)
IdP	Identity Provider (v případě SŽ zajišťuje služby IdP systém Microsoft Active Directory)
IS	Informační systém
ISVS	Informační systémy veřejné správy
ITSM	IT Service Management
KII	Kritická informační infrastruktura
LDAP	Lightweight Directory Access Protocol
LLD	Nízko úrovňový design (Low Level Design)
MB	Mega Byte
MCAS	Microsoft Cloud App Security
MD	Člověkodenní, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day)
MDM	Správa mobilních zařízení (Mobile Device Management)
MFA	Vícefázové ověření (Multifactor Authentication)
MPLS	Multiprotocol Label Switching / Multiprotokolové přepojování
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
On-premise	On-premise software je takový software, který lze instalovat a provozovat v prostorách organizace, která jej využívá
OS	Operační Systém
OTP	Jednorázové heslo (One Time Password)

OT	Operational Technology / Operační technologické sítě a prvky
PAM	Správa privilegovaných přístupů (Privileged Access Management)
PIM	Správa privilegovaných identit (Privileged Identity Management)
PD	Pracovní Den
PKI	Infrastruktura správy a distribuce veřejných klíčů (Public Key Infrastructure); informační systém, produkuje a využívá digitální certifikáty
RDP	Protokol na přenos vzdálené plochy (Remote Desktop Protocol)
RPO	Recovery Point Objective – cílový bod zotavení
RTO	Recovery Time Objective – cílová doba zotavení
s2s VPN	Site to site VPN
SLA	Dohoda o úrovni poskytovaných služeb (Service Level Agreement)
SSH	Zabezpečený protokol pro připojení k serverům
SSO	Systém jednotného přihlášení (Single Sign-On)
SW	Software
SŽ	Správa železnic, státní organizace
Token	Dedikované HW úložiště soukromého klíče uživatele – zpravidla čipová karta.
UAS	Uživatelsko-aplikační síť
VPN	Virtuální privátní síť (Virtual Private Network)
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů
ZoKB	Zákon 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Seznam zkratk pro specifické aplikace SŽ:

Zkratka	Popis
ASVC	Automatické stavění vlakových cest
DŘT	Dispečerská řídicí technika
DDTS	Dálková diagnostika technologických systémů
CDP	Centrální dispečerské pracoviště
CDS	Centrální dispečerský systém
DŽDC	Dispečer železniční dopravní cesty
DŽIN	Dispečer železniční infrastruktury
ED	Elektro dispečer
GVD	Grafikon vlakové dopravy
SSZT	Správa sdělovací a zabezpečovací techniky
ST	Správa tratí
SŽE	Správa železniční energetiky
TechDS	Technologický a dohledový systém
TDCDP	Traťový dispečer dálkového ovládání zabezpečovacího zařízení na CDP
VS	Vlakové soupravy

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace veřejné zakázky „Nasazení MFA a pořízení nosičů certifikátů“ v prostředí SŽ (dále jen „veřejná zakázka“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

2.1 Záměr SŽ v oblasti MFA a nosičů uživatelských certifikátů

Záměrem veřejné zakázky je zavedení prostředků pro identifikaci uživatelů a jejich vysoce bezpečné ověření (autentizaci) při přístupu k ICT/OT/IoT aktivům SŽ. Implementace systému vícefaktorové autentizace (MFA) s využitím uživatelských certifikátů vydaných důvěryhodnými interními certifikačními autoritami je v souladu s dlouhodobou koncepcí bezpečné identifikace a autentizace uživatelů a zvýšení zabezpečení přístupů k aktivům SŽ.

Autenticita uživatelů bude ověřována bezpečným systémem vůči autentizačním službám typu Identity Provider (v aktuálním prostředí SŽ: vůči systému Microsoft Active Directory, ADFS a Entra ID). SŽ v rámci tohoto projektu plánuje zavedení systému

- vizuální identifikace uživatelů s využitím potištěných zaměstnaneckých karet (plastových, popř. elektronických fyzických nosičů);
- elektronické identifikaci uživatelů s využitím bezkontaktních, popř. kontaktních čipů fyzického nosiče vůči systémům fyzické bezpečnosti (přístupové systémy), popř. dalších interních systémů SŽ;
- autentizace uživatelů založeném na interních uživatelských certifikátech vystavených důvěryhodnou interní certifikační autoritou a uložené na bezpečném fyzickém nosiči certifikátu¹.

Hlavními cíli projektu Nasazení MFA a pořízení nosičů certifikátů jsou zejména:

- zvýšení bezpečnosti ICT prostředí SŽ, ochrana před zneužitím uživatelských účtů a oprávnění;
- zajištění vysoce bezpečné autentizace uživatelů vůči systému poskytující autentizační služby (konkrétně Active Directory, ADFS, a Entra ID), v této veřejné zakázce v prostředí UAS. Systémy poskytující autentifikační služby budou na sobě nezávislé a budou poskytovat pro uživatele s předmětnou identitou navzájem nezávislé přístupové profily ke koncovým zařízením v prostředí.
- zajištění systematické a strukturované správy prostředků bezpečné identifikace a autentizace uživatelů (uživatelských certifikátů, fyzických nosičů, případně dalších prostředků);

¹ SŽ nepředpokládá, že by uvedená metoda byla jedinou metodou MFA a může být v rámci jiných aktivit doplněna dalšími autentizačními metodami.

- procesů pro správu celého životního cyklu uživatelských certifikátů a jejich nosičů, podpora těchto procesů odpovídajícím IT systémem s vysokou mírou automatizace a definovanou bezpečnostní segregací rolí při správě certifikátů;
- splnění legislativních požadavků (ZoKB, VoKB);
- naplnění platných interních předpisů SŽ.

Součástí projektu bude i návrh a implementace procesů bezpečné autentizace uživatelů i při nedostupnosti nosiče certifikátu (alternativní způsoby autentizace, náhradní pracovní postupy apod.).

SŽ požaduje pořízení identifikačních a autentizačních prostředků (nosičů certifikátu) ve formě plastových karet velikosti běžné platební karty. SŽ požaduje pořízení tří typů těchto prostředků (karet):

Na pořizované identifikační prostředky a nosiče certifikátů SŽ klade další požadavky, zejména:

- musí obsahovat kontaktní část (čip) technicky odpovídající požadavkům na QSCD prostředek² pro uložení/generování uživatelských certifikátů a jejich privátních klíčů s využitím k bezpečné autentizaci uživatelů vůči systému poskytující autentizační služby (konkrétně Active Directory);
- musí být osazeny bezdrátovou (bezkontaktní) částí kompatibilní se systémy využívající bezdrátové technologie pro identifikaci uživatelů (např. systémy fyzické bezpečnosti, docházkový systém apod.); zajištění hardwarové a softwarové kompatibility nosičů certifikátů a obslužného SW pro hlavní používané OS (Windows, Linux, macOS);
- možnost potisku nosiče definovanými optickými identifikačními údaji (vhodnou technologií tisku), včetně překrytí ochrannou fólií a umístění ochranného prvku pro ověření autenticity nosiče formou hologramu;
- definovaná fyzická odolnost nosičů certifikátů i jejich případného potisku.

Technické požadavky na nosiče certifikátů jsou uvedeny v příloze č. 4.

2.2 Předmět plnění veřejné zakázky

Cílem veřejné zakázky je uzavření smlouvy, jejímž předmětem bude zejména:

- poskytnutí služeb před-implementační analýzy, detailního návrhu řešení a prováděcího projektu,
- dodávka identifikačních a autentizačních prostředků (fyzických nosičů certifikátů) s technickými parametry definovanými v příloze č. 4, včetně služeb potisku (personalizace) fyzického nosiče v následujících variantách:

Typ A: plastová karta pro vizuální identifikaci (potisk, ochranné prvky);

² SŽ požaduje nosič certifikátu (čipovou kartu) technicky splňující požadavky QSCD, přičemž SŽ nepožaduje, aby prostředek (čipová karta) byla certifikována jako kompatibilní a akceptovaný prostředek některé z akreditovaných certifikačních autorit v ČR vydávající kvalifikované certifikáty (v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce);

Typ B: smart karta s vnitřním čipem (bezkontaktní bezdrátová komunikace) pro identifikaci uživatelů, včetně možnosti potisku a ochranných prvků pro vizuální identifikaci jako u typu A;

Typ C: hybridní smart karta s kontaktním (viditelným) čipem pro ukládání uživatelských certifikátů a bezpečnou autentizaci uživatelů, s bezdrátovým čipem pro bezkontaktní identifikaci identické s typem B a možností potisku a ochranných prvků pro vizuální identifikaci jako u typu A;

- dodávka technologií personalizace fyzických nosičů, implementace ochranných prvků a ochranné vrstvy nosičů s parametry uvedenými v příloze č. 5,
- dodávka, implementace a podpora systému pro správu životního cyklu uživatelských certifikátů vydávaných interními důvěryhodnými CA a umístěnými na nosiči certifikátů (pro prostředí UAS), včetně systému správy životního cyklu nosičů certifikátů,
- integrace dodaného systému se službami IdP (AD) pro zajištění bezpečné identifikace a autentizace uživatelů s využitím uživatelských certifikátů (pro prostředí UAS),
- dodávka, implementace a podpora klientského SW pro koncové stanice (pro zajištění bezpečné autentizace uživatelů s využitím uživatelských certifikátů), včetně intuitivního výběru certifikátu pro příslušné prostředí (UAS),
- propojení (integrace) procesů vydávání fyzického nosiče certifikátu na systémy využívající nosič pro identifikaci uživatele pomocí bezdrátové technologie certifikátu (např. přístupové systémy fyzické bezpečnosti), včetně návrhu a realizace způsobu předávání a aktualizace dat,
- zajištění školení pracovníků Zadavatele na dodané technologie a konkrétní implementaci,
- služby na vyžádání.

Plnění bude obsahovat následující poptávané oblasti:

Fáze 1: Před-implementační analýza

Zpracování před-implementační analýzy pro zavedení systému bezpečné identifikace a ověřování uživatelů, správy životního cyklu osobních uživatelských certifikátů, správy životního cyklu nosičů certifikátů, způsobu napojení na související systémy a nastavení obslužných procesů a procesů obnovy.

Součástí před-implementační analýzy bude dále návrh procesů pro řešení nestandardních nebo problémových stavů vydaných certifikátů nebo jejich nosičů (např. zapomenutí nosiče uživatelem, zničení nosiče, kompromitace přístupových PIN kódů apod.), včetně návrhu propojení těchto procesů s již zavedenými procesy Zadavatele.

Před-implementační analýza zahrnuje i revizi konfigurace stávající implementace interních CA a jejich využití v dalších částech implementace, včetně identifikace případných nutných doplnění (např. šablony).

Součástí před-implementační analýzy bude i návrh procesu přechodu uživatelů ze současného stavu využití zaměstnaneckých karet a k využití nových zaměstnaneckých karet včetně využití MFA s využitím osobních uživatelských certifikátů, včetně návrhu adopční kampaně.

Před-implementační analýza bude obsahovat také detailní návrh řešení a prováděcí projekt včetně harmonogramu dalších kroků, definici požadavků na nezbytnou součinnost Zadavatele a návrh metodiky akceptačních funkčních a výkonových testů a testovacích scénářů testů obnovy řešení.

Součástí před-implementační analýzy bude i zpracování exit plánu.

Fáze 2: Implementace systému správy životního cyklu uživatelských certifikátů a správy životního cyklu nosičů certifikátů pro prostředí UAS

Zadavatel požaduje na základě schválených výstupů před-implementační analýzy dodávku a provedení implementace systému správy životního cyklu uživatelských certifikátů pro prostředí UAS.

Dodavatel dále provede dodávku a implementaci systému správy životního cyklu nosičů certifikátů.

Po provedení implementace provede dodavatel v souladu s metodikami definovanými v rámci před-implementační analýzy akceptační funkční, výkonové a zátěžové testy a odstraní případné neshody.

Dodavatel dále poskytne součinnost při provedení bezpečnostních testů a podle metodiky a scénářů definovaných v před-implementační analýze provede testy obnovy implementovaných systémů; případné neshody dodavatel odstraní.

Fáze 3: Implementace MFA s využitím uživatelských certifikátů (prostředí UAS)

Na základě výstupů předchozích fází provede dodavatel implementaci vysoce bezpečné autentizace uživatelů vůči systému poskytující autentizační služby (konkrétně Active Directory, ADFS a Entra ID) založené na uživatelských certifikátech v prostředí UAS.

Fáze 4: Napojení systémů správy životního cyklu uživatelských certifikátů a nosičů certifikátů na další definované systémy Zadavatele

Dodavatel zajistí procesní, datové nebo aplikační propojení

- systému správy životního cyklu uživatelských certifikátů pro prostředí UAS
- systému správy životního cyklu nosičů certifikátů

se systémy definovanými touto technickou specifikací v čl. 2.4.5, popř. se systémy identifikovanými v rámci před-implementační analýzy, způsobem definovaným v před-implementační analýze.

Dodavatel provede:

- propojení (integraci) procesů vydávání fyzického nosiče certifikátu se systémy využívající nosič pro identifikaci uživatele (především pomocí bezdrátové technologie, např. přístupové systémy fyzické bezpečnosti),
- procesní, datovou a/nebo aplikační integraci systému správy životního cyklu uživatelských certifikátů pro prostředí UAS na další systémy definované touto zadávací dokumentací a před-implementační analýzou.

Fáze 5: Ověřovací (pilotní) provoz, dokumentace řešení, školení

Po provedení implementace řešení provede dodavatel v souladu s metodikami definovanými v rámci před-implementační analýzy akceptační funkční, výkonové a zátěžové testy a odstraní případné neshody.

Dodavatel dále poskytne součinnost při provedení bezpečnostních testů a podle metodiky a scénářů definovaných v před-implementační analýze provede testy obnovy implementovaných systémů; případné neshody dodavatel odstraní.

Po provedení akceptačních a bezpečnostních testů a odstranění případných neshod dodavatel převede řešení do pilotního (ověřovacího) provozu v délce minimálně 2 kalendářních týdnů pro skupinu uživatelů definovanou v rámci před-implementační analýzy a v rámci pilotního provozu dodavatel odstraní případné provozní závady.

Po vyhodnocení pilotního provozu bude řešení převedeno do produkce a dodavatel zajistí technickou podporou řešení.

V rámci této fáze dodavatel vybuduje také testovací prostředí systému správy uživatelských certifikátů a MFA s plnou funkcí produkčního prostředí.

Fáze 6: Úvodní dodávka fyzických nosičů (karet)

Pro pilotní provoz (Fáze 5) a zajištění přechodu k novému řešení (Fáze 6) dodavatel zajistí dodávku příslušného množství fyzických nosičů identifikačních a autentizačních prostředků uvedených v příloze č. 4, včetně ochranných obalů.

Zadavatel předpokládá následující dodávky fyzických nosičů (karet). Termíny a množství dodávek mohou být upřesněny v před-implementační analýze:

1. Fyzické nosiče pro pilotní provoz

Pro pilotní provoz zajistí dodavatel následující množství fyzických nosičů:

- **Typ B: 40 ks**
- **Typ C: 40 ks**

Pro pilotní provoz budou dodány fyzické nosiče bez personalizace³ a včetně ochranných obalů.

2. Úvodní dodávka personalizovaných fyzických nosičů

Pro přechod k novému řešení (Fáze 6) zajistí dodavatel úvodní dodávku následujícího množství fyzických nosičů:

- **Typ A: 0 ks**
- **Typ B: 1.500 ks**
- **Typ C: 9.000 ks**

Nosiče budou dodány včetně jejich personalizace, ochranných prvků pro ověření autenticity nosiče a ochranných obalů

Fáze 7: Dodávka a implementace technologií personalizačního pracoviště

V této fázi dodavatel zajistí dodávku nezbytných technologií personalizačního pracoviště (HW i SW), jejich implementaci a integraci s příslušnými systémy a procesy Zadavatele identifikovanými v před-implementační analýze.

Současné vybavení a funkce personalizačního pracoviště jsou uvedeny v příloze č. 5.

Fáze 8: Zajištění přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů

Na základě návrhu procesu a harmonogramu přechodu ze současného stavu na využití nových identifikačních a autentizačních prostředků (nosičů certifikátů) pro identifikaci a vícefaktorovou autentizaci (MFA) uživatelů s využitím osobních uživatelských certifikátů, definovaného v před-implementační analýze, zajistí dodavatel potřebnou součinnost při realizaci tohoto přechodu pro prostředí UAS.

Fáze 9: Technická podpora řešení

Pro implementované řešení poskytne dodavatel službu technické podpory implementovaného řešení v délce 24 měsíců. Technická podpora je poskytována od převedení řešení do produkce, tj. od ukončení Fáze 5.

Fáze 10: Služby na vyžádání

Dodavatel poskytne zadavateli služby konzultace na vyžádání. Služby mohou být čerpány především pro rozšiřování a rozvoj systému správy životního cyklu uživatelských certifikátů.

Fáze 11: Průběžná dodávka fyzických nosičů (karet) a spotřebního materiálu personalizačního pracoviště

³ Zadavatel předpokládá personalizaci fyzických nosičů z pilotního provozu v personalizačním pracovišti, popř. využití nepersonalizovaných nosičů pro potřeby řešení nestandardních situací (vydání dočasného náhradního identifikačního / autentizačního prostředku apod.).

Dodavatel zajistí dodávky fyzických nosičů, a ochranných obalů na základě dílčích objednávek Zadavatele. Nosiče budou dodávány bez personalizace, která bude zajišťována Zadavatelem s využitím personalizačního pracoviště.

Příloha č. 4 zadávací dokumentace určuje maximální objem plnění v dodávkách fyzických nosičů všech typů, jejich ochranných prvků, ochranných obalů a spotřebního materiálu personalizačního pracoviště. Množství fyzických nosičů, poměr jednotlivých typů a množství souvisejících ochranných prvků, obalů a spotřebního materiálu definované přílohou č. 4 zadávací dokumentace je nutno vnímat jako maximální a Zadavatel tento rozsah není povinen využít. Dodavatel bere na vědomí, že bez jakékoli sankce či poplatku Zadavatele, nemusí být uvedené množství úplně využito.

2.3 Oblasti, které nejsou předmětem plnění veřejné zakázky

Pro vyloučení pochybností Zadavatel uvádí, že následující oblast **není** předmětem plnění veřejné zakázky:

- hardware pro provoz systému správy životního cyklu uživatelských certifikátů
- licence Microsoft, které SŽ nakupuje v rámci centrálních nákupů
- čtečky kontaktních čipů nosičů certifikátů

Pro provoz systému správy životního cyklu uživatelských certifikátů Zadavatel poskytne dostatečné HW zdroje formou virtuálních strojů, virtuálních serverů s podporovanými operačními systémy, popř. databázových serverů podle technických a výkonnostních specifikací dodavatele stanovených v před-implementační analýze.

Zadavatel vyčlení pro dodávané řešení maximálně 6 virtuálních strojů, přičemž celkové použití zdrojů pro řešení nepřesáhne:

- 48 vCPU
- 224 GB RAM
- 2TB diskového prostoru

v součtu pro všechny takto poskytnuté virtuální stroje.

Omezení na maximálně 6 virtuálních strojů a související celkové využití zdrojů je uvedeno pro dodané řešení. Pro vytvoření testovacího prostředí budou poskytnuty zdroje definované v před-implementační analýze s odpovídajícími nižšími technickými nároky vyplývajícími z charakteru testovacího prostředí.

Uvedená omezení pro poskytnutí zdrojů mohou být na základě schválené před-implementační analýzy překročena pouze z důvodu požadavků SŽ (např. požadavky na vysokou dostupnost řešení, distribuci řešení v různých lokalitách apod.).

Virtuální stroje⁴ budou poskytnuty v souladu přílohou č. 17 (Platforma SŽ).

2.4 Požadované funkcionality a vlastnosti řešení

2.4.1 Požadované vlastnosti systémů správy životního cyklu uživatelských certifikátů a správy životního cyklu nosičů certifikátů a obslužného SW koncových stanic

Seznam požadovaných funkčních a nefunkčních vlastností systému správy životního cyklu uživatelských certifikátů, systému správy životního cyklu nosičů certifikátů a middleware/obslužného SW koncových stanic je uveden v příloze č. 3.

2.4.2 Požadované vlastnosti nosičů certifikátů

Seznam požadovaných funkčních a nefunkčních vlastností nosičů certifikátů je uveden v příloze č. 4.

Součástí dodávky nosičů certifikátů musí být i vhodný obal (pouzdro) pro ochranu nosiče certifikátu a jeho personalizaci před poškozením.

Součástí dokumentace dle požadavku Poz-6 uvedenému v kapitole 4.5 musí být i kompletní podrobná dokumentace čipů nosiče certifikátů (kontaktních i bezkontaktních), podporované formáty a protokoly, zejména detailní popis struktury a formátu dat ukládaných na kontaktní části nosiče z důvodu zajištění kompatibility s případným budoucím systémem bezpečného startu a ochrany pracovních stanic s OS Windows (pre-boot authentication).

2.4.3 Požadavky na personalizaci nosičů certifikátů a technologie personalizačního pracoviště

Zadavatel požaduje zajištění dodávky nosičů certifikátů včetně personalizace, zejména pro zajištění přechodu ze současného stavu na využití nových fyzických nosičů pro identifikaci uživatelů a nasazení MFA s využitím osobních uživatelských certifikátů (Fáze 6).

Současně Zadavatel požaduje dodávku technologií pro personalizaci nosičů (karet) a doplnění nebo vybudování personalizačního pracoviště včetně dodávky a konfigurace příslušného hardware a software tak, aby byl schopen personalizovat nosiče vlastními silami, zejména pro menší množství vydávaných nosičů, řádově cca stovky kusů měsíčně.

2.4.3.1 Požadavky na personalizaci nosičů

Požadavky na personalizaci nosičů (společné pro službu personalizace u dodavatele nebo v interním personalizačním pracovišti):

⁴ Virtuálními stroji jsou myšleny virtuální servery s podporovanými OS, databázové servery, popř. samostatné virtuální stroje.

- oboustranný barevný potisk retransferovou technologií tisku
- oboustranná laminace ochrannou fólií s ochranným prvkem (hologram) se zachování přístupu ke kontaktnímu čipu nosiče

2.4.3.2 Požadavky na trvanlivost potisku

Potisk včetně ochranného prvku (hologramu) musí zůstat zřetelný a jasně čitelný minimálně po dobu **24 měsíců** od předání nosiče uživateli a používání nosiče běžným způsobem jako autentizačního a identifikačního prostředku (tj. nošení v ochranném obalu, vysouvání nosiče z obalu a používání nosiče ve čtečce kontaktní části pro autentizaci a elektronické podpisy mnohokrát denně apod.).

2.4.3.3 Požadavky na technologie personalizačního pracoviště

Požadavky na technologie personalizačního pracoviště (zejména tiskárny karet, laminace apod.):

- požadované maximální denní množství personalizace karet: do 100ks / pracovní den (8 hodin)
- personalizační technologie musí být schopna číst identifikátor bezkontaktního čipu nosiče
- tiskárna pro tisk přístupových kódů karet (PIN/PUK) do diskretní zóny PINového formuláře
- požadovaná záruka na jakost dodaných technologií personalizačního pracoviště: 24 měsíců od převedení pracoviště do produkce

Pro dodané technologie personalizačního pracoviště je dodavatel povinen zajistit i **pozáruční servis a dodávky spotřebního materiálu v déle doby trvání smlouvy této veřejné zakázky.**

2.4.3.4 Zdroj dat pro personalizaci nosičů

Všechna potřebná data pro personalizaci nosičů certifikátů (identita, osobní údaje, pracovní zařazení, fotografie apod.) jsou obsažena v personálním systému Zadavatele (SAP HR).

2.4.3.5 Vizuální vzhled (grafický design) personalizovaných nosičů

U vizuálního vzhledu personalizovaných nosičů se Zhotovitel bude řídit pravidly grafického manuálu SŽ.

Jednotný vizuální styl Správy železnic je zpracován v Grafickém manuálu jednotného vizuálního stylu, který je umístěn veřejně na webových stránkách organizace

<https://www.spravazeleznic.cz/press/logomanual>

Zadavatel upozorňuje, že písmo Styrene je licenční a podmínky pro jeho získání jsou uvedeny v Grafickém manuálu jednotného vizuálního stylu Správy železnic, v kapitole 2. A. Pokud dodavatel použije toto písmo při personalizaci fyzických nosičů, tyto licence pro výrobu/personalizaci zajistit. Cena licencí písma musí být v tomto případě součástí nabídkové ceny.

Zaměstnanecké karty jsou popsány v kapitole 8.1. v grafickém manuálu SŽ (viz příloha č. 18)

Vzory šablon zaměstnaneckých karet obsahem přílohy č. 21.

Zadavatel upozorňuje, že vizuální vzhled nosiče může být po dobu trvání smlouvy měněn v závislosti na změnách interních předpisů nebo grafického manuálu.

2.4.3.6 Vazby na systémy pro bezkontaktní identifikaci uživatelů

Personalizační pracoviště zajišťuje i datovou vazbu pro systémy identifikace uživatelů pomocí bezdrátových technologií (založené na standardech MIFARE® DESFire®). Konkrétně zajišťuje datové vstupy do přístupového systému ASSET (s dalšími vazbami na docházkový systém a HR modul SAP).

2.4.4 Distribuce nosičů certifikátů a přístupových kódů

Distribuci připravených (personalizovaných) nosičů s vydanými certifikáty a související přístupové kódy (PIN/PUK vytištěné v diskrétní zóně PINového formuláře) zajistí Zadavatel vlastními silami po celou dobu trvání smlouvy.

2.4.5 Integrace s bezpečnostními a provozními systémy Zadavatele

2.4.5.1 Integrace s nástroji pro bezpečnostní monitoring

Systémy

- správy životního cyklu uživatelských certifikátů
- správy životního cyklu nosičů certifikátů
- vícefaktorové autentizace (MFA)

musí být integrovány do stávajících bezpečnostních dohledových nástrojů – konkrétně je požadována integrace minimálně s nástrojem typu SIEM a Log management nástroj.

V rámci integrace s nástrojem typu SIEM je požadován minimálně záznam aktivit ve formě strukturovaných logů, které jsou dále v čase blízkém reálnému přenášeny a vyhodnocovány v SIEM nástrojích a ukládány pro případnou zpětnou analýzu, včetně napojení na nástroj Log management.

V dokumentaci řešení dodavatel uvede strukturu logů (nebo odkaz na jednoznačnou dokumentaci), aby bylo možné vytvořit korelační pravidla pro SIEM.

Rozsah a struktura logů musí být v souladu s požadavky ZoKB a VoKB.

2.4.5.2 Integrace s nástroji podpory uživatelů (Service Desk)

Zadavatel požaduje, aby systémy

- správy životního cyklu uživatelských certifikátů
- správy životního cyklu nosičů certifikátů

byly integrovány s nástrojem podpory uživatelů (Service Desk) pro zajištění kvalitní podpory procesů správy životního cyklu uživatelských certifikátů a nosičů certifikátů i z hlediska zapojení koncových uživatelů (žádosti, řešení nestandardních stavů, informace o blížící se expiraci vydaných certifikátů apod.).

Rozsah a způsob integrace s nástrojem Service Desk (JIRA) bude definován v před-implemenční analýze.

2.4.5.3 Integrace s přístupovými systémy fyzické bezpečnosti

Systémy

- správy životního cyklu uživatelských certifikátů
- správy životního cyklu nosičů certifikátů

musí být integrovány se stávajícími systémy Zadavatele v oblasti řízení fyzické bezpečnosti a přístupů, zejména:

- přístupový systém: identifikace zaměstnance pomocí bezkontaktního nosiče v rámci přístupového systému (fyzická bezpečnost);
- použití služebního vozidla: identifikace zaměstnance pomocí bezkontaktního nosiče, umožnění použití služebního vozidla; případně dalších systémů identifikovaných v rámci před-implemenční analýzy.

2.4.5.4 Procesy správy životního cyklu uživatelských certifikátů, segregace rolí a schvalovací workflow

Dodavatel navrhne procesy správy životního cyklu certifikátů i jejich nosičů v souladu se Zadavatelem provozovaným systémem PKI a doplní systém PKI zejména o

- definici rolí a oprávnění – návrh rolí musí respektovat „best practice“ požadavky na bezpečnostní segregaci rolí a role by měly být založené na doménových skupinách AD
- šablony, podle kterých budou vydávány uživatelské certifikáty, včetně dokumentace šablon. Součástí plnění musí být nejen šablony pro vydávání certifikátů běžných koncových uživatelů, ale i šablony pro operátory (např. Enrollment Agent, Key Recovery Agent apod.)
- navrhnout a implementaci bezpečnostního konceptu životního cyklu certifikátů, způsob autorizace žádostí o prvotní certifikát a autorizace žádosti o následný certifikát, Návrh schvalovacích procesů v rámci životního cyklu certifikátů musí být zpracován s ohledem na zajištění bezpečnosti schvalování, zejména pro privilegované účty a role.

2.4.6 Licence

Nezbytnou součástí plnění je i dodávka SW licencí pro všechny dodané SW části plnění. Dodavatel zajistí dodávku SW licencí tak, aby implementované řešení převedené do produkčního prostředí bylo plně licencováno – licence musí vždy plně pokrývat implementované části řešení převedené do produkce.

Zadavatel požaduje, aby SW licence systému správy životního cyklu uživatelských certifikátů, správy životního cyklu nosičů certifikátů,

middleware a obslužného SW koncových stanic byly tzv. perpetuální, tj. bez časového omezení platnosti licence.

2.4.6.1 Licence pro testovací prostředí

Zadavatel požaduje, aby licence, které jsou součástí plnění, současně pokryly možnost instalace samostatného testovacího prostředí systému správy životního cyklu uživatelských certifikátů a MFA, s plnou funkcí jako je systém převedený do produkce. Licence musí být využitelné v testovacím prostředí UAS a v rozsahu minimálně pro 100 testovacích uživatelů.

2.4.6.2 Zdrojové kódy

Pro části řešení vyvinuté v rámci této veřejné zakázky pro potřeby Zadavatele (tj. části, které nejsou součástí standardních produktových SW modulů, např. integrační rozhraní k systémům Zadavatele apod.) požaduje Zadavatel dodávku dokumentovaných zdrojových kódů za účelem možné budoucí podpory a rozvoje řešení interními pracovníky Zadavatele a za účelem provedení případné bezpečnostní analýzy kódů.

2.4.7 Další technické podmínky

2.4.7.1 Jazyk uživatelského prostředí

— Zadavatel požaduje, aby uživatelské rozhraní dodaných a implementovaných systémů a SW podpory koncových stanic bylo v českém jazyce.

U rozhraní určeného pro správce dodaného a implementovaného SW připouští zadavatel anglický nebo český jazyk.

3 Současný stav a popis prostředí

Současný stav ICT prostředí Zadavatele v oblastech z hlediska budoucího systému správy privilegovaných přístupů je uveden v Příloze č. 2.

4 Požadavky na plnění

Plnění veřejné zakázky se skládá z níže uvedených částí:

4.1 Před-implementační analýza

Poz-1	Před-implementační analýza
Popis	Dodavatel zpracuje před-implementační analýzu pro zavedení systému bezpečné identifikace a ověřování uživatelů, správy životního cyklu osobních uživatelských certifikátů, správy životního cyklu nosičů

certifikátů, napojení na související systémy a nastavení obslužných procesů a procesů obnovy.

Před-implementační analýza musí obsahovat minimálně následující části (pro prostředí UAS):

- Základní popis řešení, technologií a technických konceptů;
- Identifikace předpokladů úspěšné implementace MFA s využitím osobních uživatelských certifikátů a stavu jejich splnění pro prostředí UAS;
- Analýzu současného stavu implementace systému PKI (interních CA), návrh na jejich případné technologické (softwarové) doplnění s ohledem na procesy správy životního cyklu osobních uživatelských certifikátů a implementaci MFA založené na uživatelských certifikátech;
- Základní architekturu řešení (HLD) s jejím vysvětlením;
- Detailní návrh architektury řešení systému správy životního cyklu osobních uživatelských certifikátů;
- Detailní návrh technického řešení implementace systému správy životního cyklu osobních uživatelských certifikátů, včetně požadavků na HW zdroje, ukládání dat, síťové prostředí apod.;
- Revize stávajícího systému šablon vydávajících CA a jejich doplnění o potřebné šablony pro vydávání osobních uživatelských certifikátů, šablony pro operátory a další šablony v navrhovaném řešení nezbytné;
- Detailní návrh obslužných procesů systému správy životního cyklu osobních uživatelských certifikátů, včetně definování rolí a jejich bezpečnostní segregace, a detailní návrh schvalovacích procesů/workflow, detailní návrh automatizace anonymizace osobních údajů, detailní návrh řešení registračních autorit, detailní návrh notifikačních procesů;
- Detailní návrh procesů zálohování a obnovy systému správy životního cyklu osobních uživatelských certifikátů;
- Detailní návrh procesů pro řešení nestandardních nebo problémových stavů vydaných certifikátů nebo jejich nosičů (např. zapomenutí nosiče uživatelem, zničení nosiče, kompromitace přístupových PIN kódů, zablokování přístupových kódů, odebrání nosiče uživateli apod.), včetně návrhu propojení těchto procesů s již zavedenými procesy Zadavatele.
- Detailní návrh technického řešení implementace systému správy životního cyklu nosičů certifikátů, technického řešení personalizačního pracoviště včetně návrhu technologií potisku a ochrany nosiče certifikátů (včetně případné implementace vizuálních ochranných prvků);
- Detailní návrh řešení uživatelského rozhraní pro práci s certifikáty a nosiči certifikátu (uživatelský portál – samoobsluha, obslužný SW koncových stanic apod.)
- Detailní návrh řešení obnovy uživatelského šifrovacího certifikátu ze zálohy
- Integrace s IDM
- Detailní návrh procesů správy životního cyklu nosičů certifikátů, včetně návrhu na procesní, datové a aplikační propojení na

Výstupy	<p>systemy využívající funkcionality nosiče certifikátů (viz kap. 2.4.5)</p> <ul style="list-style-type: none"> ▪ Detailní návrh řešení SW podpory (middleware) využití certifikátů (osobních uživatelských certifikátů) na koncových stanicích pro OS Windows 10 a vyšší a macOS 13 a vyšší; ▪ Detailní návrh integrační architektury s bezpečnostními a infrastrukturními systémy zadavatele (zejména SIEM, log management, AD, SMTP, NTP apod.) ▪ Detailní návrh harmonogramu a detailní prováděcí projekt implementace řešení pro prostředí UAS; ▪ Detailní návrh požadavků na součinnost ze strany Zadavatele při implementaci řešení pro prostředí UAS; ▪ Podklady pro analýzu rizik implementace systémů bezpečné identifikace a ověřování uživatelů pomocí osobních uživatelských certifikátů pro prostředí UAS; ▪ Návrh metodiky a plánu provedení akceptačních funkčních, výkonových a zátěžových testů řešení, včetně návrhu testů obnovy a zotavení pro vybrané typy událostí/závad (včetně výkonnostních parametrů obnovy a zotavení – RPO, RTO apod.) ▪ Definování skupiny uživatelů pro ověřovací (pilotní) provoz ▪ Detailní návrh procesu a harmonogramu přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů, včetně provedení adopční kampaně a definování součinnosti dodavatele a Zadavatele při realizaci tohoto přechodu ▪ Detailní návrh zajištění dodávek nosičů certifikátů, jejich personalizace a souvisejících logistických procesů. ▪ Exit plán zpracovaný de požadavků uvedených v kap. 4.12.1 - 4.12.2
	<p>Výstupem před-implementační analýzy bude soubor dokumentů pokrývajících výše uvedené oblasti (pro prostředí UAS).</p> <p>Zadavatel požaduje zpracování dokumentace odpovídající požadavkům ISMS a ITSM. Požadavky na dokumentaci jsou uvedeny v interním předpisu č.j. 509/2025-SŽ-SŽT-NKB (viz příloha č. 19).</p>

4.2 Implementace systému správy životního cyklu uživatelských certifikátů pro prostředí UAS a správy životního cyklu nosičů certifikátů

Poz-2	Implementace systému správy životního cyklu uživatelských certifikátů pro prostředí UAS a správy životního cyklu nosičů certifikátů
-------	--

Popis	<p>Na základě schválených výstupů před-implementační analýzy provede dodavatel dodávku a implementaci systému správy životního cyklu uživatelských certifikátů vydávaných interní CA pro prostředí UAS a systému správy životního cyklu nosičů certifikátů⁵ včetně nastavení příslušných souvisejících procesů a integrace s nástroji bezpečnostního monitoringu a podpory uživatelů.</p> <p>Součástí dodávky bude i řešení SW podpory (middleware) využití osobních uživatelských certifikátů na koncových stanicích pro OS Windows 10 a vyšší a macOS 13 a vyšší. Dodavatel dodá příslušný SW, včetně dokumentace. Vlastní distribuci a instalaci SW na koncové stanici provede Zadavatel vlastními silami. Při distribuci a implementaci SW podpory koncových stanic poskytne dodavatel Zadavateli nezbytnou součinnost a technickou pomoc při řešení nestandardních stavů.</p> <p>Po provedení implementace provede dodavatel v souladu s metodikami definovanými v rámci před-implementační analýzy akceptační funkční, výkonové a zátěžové testy a odstraní případné neshody.</p> <p>Dodavatel dále poskytne součinnost při provedení případných bezpečnostních testů Zadavatelem a odstraní případné neshody⁶.</p>
Výstupy	<p>Výstupem bude:</p> <ul style="list-style-type: none"> ▪ implementovaný systém správy životního cyklu uživatelských certifikátů vydávaných interní CA pro prostředí UAS, včetně příslušných šablon pro interní CA ▪ nastavené procesy správy životního cyklu uživatelských certifikátů ▪ implementovaný systém správy životního cyklu nosičů certifikátů ▪ nastavené procesy správy životního cyklu nosičů certifikátů a jejich personalizace ▪ nastavené procesy řešení nestandardních stavů nebo problémových stavů uživatelských certifikátů a jejich nosičů ▪ integrace implementovaných systémů se systémy bezpečnostního monitoringu (s nástrojem typu SIEM a Log management nástrojem) a s nástrojem podpory uživatelů (Service Desk) ▪ dodávka řešení SW podpory (middleware) využití osobních uživatelských certifikátů na koncových stanicích ▪ protokoly z akceptačních funkčních, výkonnostních a zátěžových testů a protokol odstranění případných neshod ▪ protokol o provedení bezpečnostních testů a odstranění případných neshod.

4.3 Implementace MFA s využitím uživatelských certifikátů (pro UAS)

⁵ Pro systém správy životního cyklu uživatelských certifikátů a systém správy životního cyklu nosičů certifikátů Zadavatel připouští možnost implementovat je jako jeden systém.

⁶ Metodiku bezpečnostních testů definuje Zadavatel, provedení bezpečnostních testů zajistí Zadavatel za součinnosti dodavatele.

Poz-3	Implementace MFA s využitím uživatelských certifikátů pro prostředí UAS
Popis	<p>Na základě výstupů předchozích frází provede dodavatel implementaci vysoce bezpečné autentizace uživatelů vůči systému poskytující autentizační služby (konkrétně Active Directory, Entra ID, ADFS) založené na uživatelských certifikátech v prostředí UAS.</p> <p>Po provedení implementace provede dodavatel v souladu s metodikami definovanými v rámci před-implementační analýzy akceptační funkční, výkonové a zátěžové testy a odstraní případné neshody.</p>
Výstupy	<p>Výstupem bude:</p> <ul style="list-style-type: none"> ▪ implementovaná metoda MFA bezpečné autentizace uživatelů s využitím osobních uživatelských certifikátů vydávaných interní CA vůči ActiveDirectory (ADFS) pro prostředí UAS ▪ implementovaná metoda MFA bezpečné autentizace uživatelů s využitím osobních uživatelských certifikátů vůči Entra ID systému M365 ▪ protokoly z akceptačních funkčních, výkonnostních a zátěžových testů a protokol odstranění případných neshod.

— 4.4 Napojení systému správy životního cyklu uživatelských certifikátů (UAS) a nosiče certifikátů na další definované systému Zadavatele

Poz-4	Napojení systému správy životního cyklu uživatelských certifikátů (pro prostředí UAS) a nosiče certifikátů na další definované systému Zadavatele
Popis	<p>Na základě před-implementační analýzy a výstupů předchozích fází dodavatel zajistí</p> <ul style="list-style-type: none"> ▪ propojení (integraci) procesů vydávání fyzického nosiče certifikátu se systémy využívající nosič pro identifikaci uživatele (především pomocí bezdrátové technologie, např. přístupové systémy fyzické bezpečnosti, viz kap. 2.4.5) ▪ procesní, datovou a/nebo aplikační integraci systému správy životního cyklu uživatelských certifikátů pro prostředí UAS na systémy definovanými touto zadávací dokumentací a způsobem stanoveným v před-implementační analýze.
Výstupy	Výstupem této fáze bude implementované napojení systému správy životního cyklu uživatelských certifikátů (pro prostředí UAS) a nosiče

certifikátů na další systémy Zadavatele stanovené v před-implementační analýze.

4.5 Ověřovací (pilotní provoz), dokumentace řešení, školení

Poz-5	Ověřovací (pilotní) provoz pro prostředí UAS
Popis	<p>Na základě výstupu předchozích fází, včetně provedení akceptačních testů jednotlivých částí řešení, převede dodavatel řešení implementované podle požadavků Poz-2, 3 a 4 do pilotního (ověřovacího) provozu v délce minimálně 2 kalendářních týdnů pro skupinu uživatelů definovanou v rámci před-implementační analýzy. V rámci pilotního provozu dodavatel odstraní případné provozní závady.</p> <p>Součástí pilotního provozu bude i ověření funkčnosti procesů zálohování a obnovy řešení.</p> <p>Po vyhodnocení pilotního provozu bude řešení převedeno do produkce a dodavatel v souladu s požadavkem odst. 4.9 této technické specifikace zajistí technickou podporou řešení.</p> <p>V rámci této fáze dodavatel vybuduje také testovací prostředí systému správy uživatelských certifikátů a MFA (prostředí UAS) s plnou funkcí produkčního prostředí. HW zdroje formou virtuálních strojů a síťové prostředí pro testovací prostředí zajistí SŽ podle specifikace dodavatele. Virtuální stroje budou poskytnuty v souladu s přílohou č. 17 zadávací dokumentace (Platforma SŽ).</p>
Výstupy	<p>Výstupem této fáze bude:</p> <ul style="list-style-type: none"> ▪ dokument vyhodnocení pilotního provozu ▪ testovací prostředí systému správy uživatelských certifikátů a MFA pro prostředí UAS.

Poz-5a	Dokumentace implementovaných systémů a souvisejících procesů
Popis	<p>Jako součást plnění zpracuje dodavatel dokumentaci implementovaných systémů minimálně v následujícím rozsahu:</p> <ol style="list-style-type: none"> Produktová dokumentace ke všem dodávaným SW a HW produktům, Detailní popis architektury, instalační a implementační dokumentace, dokumentace k napojení souvisejících systémů, dokumentace k integraci s prostředím SŽ (AD, ADFS, Entra ID, ServiceDesk, SIEM, Log management apod.), Podrobná dokumentace procesů, Administrátorské příručky, popis konfigurace, instalační procedury, dokumentace DR řešení,

	<p>e) Uživatelské příručky,</p> <p>f) Podrobná dokumentace k nosiči certifikátu (kontaktní i bezkontaktní části), včetně podrobného popisu datových struktur a formátu ukládaných certifikátů, využitých standardů a protokolů,</p> <p>g) Dokumentace ke všem logům – zejména popis struktury logů, seznam událostí s jejich charakteristikou a strukturou.</p> <p>Dokumentace uvedená výše v b) až e) této technické specifikace je požadována v českém jazyce. Produktová dokumentace od výrobců standardního SW a HW je akceptovatelná v anglickém nebo českém jazyce.</p> <p>Dokumentace bude zpracována pro implementaci řešení pro prostředí UAS.</p> <p>Pravidelná aktualizace dokumentace bude prováděna v rámci technické podpory řešení, a to pravidelně při aktualizacích (patchování, upgrade) implementovaného řešení.</p>
Výstupy	<p>Dokumentace implementovaného řešení pro prostředí UAS.</p> <p>Zadavatel požaduje zpracování dokumentace odpovídající požadavkům ISMS a ITSM. Požadavky na dokumentaci jsou uvedeny v interním předpisu č.j. 509/2025-SŽ-SŽT-NKB (viz příloha č. 19).</p>

Poz-5b Školení pracovníků Zadavatele					
Popis	Požadovanou součástí plnění je zajištění školení IT specialistů na implementované řešení (viz následující tabulka).				
		Typ školení	Název – obsah školení	Počet osob proškolených osob	Rozsah (v MD)
	1.	Administrace a provoz systému správy životního cyklu uživatelských certifikátů a MFA	Školení zaměřená na základní správu a provoz systému správy životního cyklu uživatelských certifikátů a souvisejícího systému MFA	Minimálně 5 maximálně 8	2 MD
	2.	Administrace a provoz systému správy životního cyklu nosičů certifikátů – nestandardní stavy a náhradní postupy	Školení zaměřená na pokročilou správu a provoz systému správy životního cyklu nosičů certifikátů, včetně personalizačního centra, na řešení nestandardních a problémových stavů a souvisejících procesů a náhradních pracovních postupů Školení v oblasti zálohování a obnovy implementovaných systémů	Minimálně 5 maximálně 8	2 MD

3	Integrační rozhraní	Školení v oblasti integračních rozhraní a napojování definovaných systémů.	Minimálně 3 maximálně 5	0,5MD
4	Uživatelské rozhraní	Školení v oblasti SW podpory koncových stanic (pro OS Windows a macOS) Školení v oblasti uživatelského rozhraní implementovaného řešení určeného koncovým uživatelům, včetně souvisejících metodických postupů/procesů	Minimálně 5 Maximálně 10	1MD
5	Personalizační pracoviště	Školení v oblasti používání technologií personalizačního pracoviště (potisk karet, ochranné fólie, ochranné prvky)	Minimálně 3 Maximálně 5	0,3MD

Školení č. 1, 2, 3 a 5 proběhnou v rámci pilotního provozu implementace řešení, školení č. 4 proběhne po uvedení řešení do produkce.

Školení proběhne v prostorách SŽ. Konkrétní termíny a místo školení určí SŽ. Školení proběhne v českém nebo slovenském jazyce.

Školení poskytne určeným pracovníkům komplexní informace v takovém rozsahu, aby tito pracovníci dokázali samostatně a dlouhodobě spravovat a provozovat dodané řešení a zajistit technickou a metodickou podporu koncových uživatelů.

Školitel bude disponovat certifikací výrobce dodávané technologie, resp. výrobců všech technologií, ze kterých bude složena dodávka (pokud výrobci takové certifikace vystavují). Certifikát je možno nahradit čestným prohlášením o způsobilosti daného školitele, založeném na prokazatelné odborné praxi a realizovaných projektech. Certifikát a/nebo čestné prohlášení předloží dodavatel SŽ nejpozději pět (5) pracovních dní přede dnem konání školení.

Výstupy

Protokoly o provedených školení pracovníků Zadavatele na dodané technologie a konkrétní implementaci.

4.6 Úvodní dodávka fyzických nosičů (karet)

Poz-7	Úvodní dodávka fyzických nosičů (karet)
Popis	<p>Pro pilotní provoz (Fáze 5) a zajištění přechodu k novému řešení (Fáze 6) dodavatel zajistí dodávku příslušného množství fyzických nosičů typu A, B a C včetně jejich ochranných obalů.</p> <p>1. Fyzické nosiče pro pilotní provoz (viz kap. 4.5)</p> <p>Pro pilotní provoz zajistí dodavatel následující množství fyzických nosičů certifikátů:</p>

	<ul style="list-style-type: none"> ▪ Typ B: 40 ks ▪ Typ C: 40 ks <p>Pro pilotní provoz budou dodány fyzické nosiče bez personalizace a včetně ochranných obalů.</p> <p>2. Úvodní dodávka personalizovaných fyzických nosičů</p> <p>Pro přechod k novému řešení (Fáze 6) zajistí dodavatel úvodní dodávku následujícího množství fyzických nosičů:</p> <ul style="list-style-type: none"> ▪ Typ A: 0 ks ▪ Typ B: 1.500 ks ▪ Typ C: 9.000 ks <p>Nosiče budou dodány včetně jejich personalizace, ochranných prvků a ochranných obalů.</p> <p>Předpokládaný harmonogram dodávek fyzických nosičů, jejich personalizace (u dodavatele), ochranných prvků a ochranných obalů je definován před-implementační analýzou a může být upravován podle skutečného průběhu plošného nasazení řešení v celé organizaci Zadavatele.</p>
Výstupy	Dodávka fyzických nosičů, jejich personalizace (mimo nosiče pro pilotní provoz), ochranných prvků a ochranných obalů nosičů v souladu s průběžně aktualizovaným harmonogramem plánu dodávek.

4.7 Dodávka a implementace technologií personalizačního pracoviště

Poz-8	Dodávka a implementace technologií personalizačního pracoviště
Popis	<p>Dodavatel zajistí dodávku a implementaci nezbytných technologií pro personalizaci nosičů, tj. doplnění nebo vybudování personalizačního pracoviště a nastavení příslušných procesů personalizace nosičů.</p> <p>Zadavatel preferuje využití stávajícího vybavení personalizačního pracoviště a jeho doplnění o nezbytné technologie, tak aby byly splněny požadavky na funkčnost personalizačního pracoviště definované v kap. 2.4.3 včetně datových, popř. integračních vazeb definovaných v před-implementační analýze (minimálně na přístupový systém ASSET).</p> <p>Součástí dodávky personalizačních technologií bude i úvodní dodávka spotřebního materiálu pro personalizaci minimálně 500ks nosičů.</p> <p>Současné technologické vybavení a funkce zajišťované personalizačním pracovištěm jsou uvedeny v příloze č. 5.</p>

Výstupy	<p>Vybudované/doplněné personalizační pracoviště nosičů certifikátů, včetně implementovaných technologií a nastavení procesů personalizace fyzických nosičů a datových, popř. integračních vazeb na další systémy identifikované v rámci před-implementační analýzy.</p> <p>Dodaný spotřební materiál pro personalizaci minimálního definovaného množství fyzických nosičů.</p>
---------	---

4.8 Zajištění přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů pro prostředí UAS

Poz-6	Zajištění přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů pro prostředí UAS
Popis	<p>Na základě procesu a harmonogramu přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů definovanému v před-implementační analýze poskytne dodavatel nezbytnou odbornou součinnost při realizaci adopční kampaně a přechodu na MFA s využitím osobních uživatelských certifikátů (rolloutu řešení) pro prostředí UAS v celé organizaci Zadavatele.</p> <p>Maximální souhrn těchto služeb bude činit 10 MD za celou dobu trvání Fáze 8, čerpání bude probíhat dle konkrétních potřeb zadavatele.</p> <p>Dodavatel je povinen zahájit poskytování služeb Fáze 8 do 3 (tří) pracovních dní od doručení závazného požadavku Zadavatele na poskytnutí služby</p>
Výstupy	Výstupem tohoto bude poskytnutá odborná součinnost při realizaci procesu přechodu k MFA s využitím osobních uživatelských certifikátů pro prostředí UAS.

4.9 Technická podpora řešení

Pro implementovaný systém požaduje Zadavatel poskytování služby technické podpory v délce 24 měsíců.

Služby jsou rozděleny na pravidelně vykonávané a individuálně, samostatně objednávané činnosti.

Poz-9a	Průběžně prováděné a pravidelné měsíční činnosti
Popis	<p>Průběžně prováděné a pravidelné měsíční činnosti zahrnují:</p> <ul style="list-style-type: none"> Provádění údržby systému: min. 1x měsíčně, Kontrola provozních systémových logů s následným řešením případných incidentů,

	<ul style="list-style-type: none"> ▪ Zajištění služeb servisní podpory pro řešení SW vad, včetně identifikace a analýzy neshod, ▪ Vedení systémové dokumentace včetně změnových požadavků, ▪ Provoz kontaktního místa prostřednictvím webové aplikace, emailu a telefonní hot-line v českém jazyce zdarma nebo za běžný účastnický tarif, <p>Vypracování protokolu o údržbě s detailním popisem veškerých nalezených nedostatků a postupu pro jejich odstranění: 1x měsíčně.</p>
Výstupy	Výstupem tohoto bude poskytnutí služby technické podpory prováděné průběžně nebo pravidelně měsíčně v termínech stanovených SŽ.

Poz-9b	Pravidelné půlroční činnosti
Popis	Průběžně prováděné a pravidelní půlroční činnosti zahrnují: <ul style="list-style-type: none"> ▪ Kontrola záloh, případná obnova v test prostředí, ▪ Pravidelná profylaxe technologií personalizace nosičů certifikátů a včetně návrhu řešení nalezených problémů.
Výstupy	Výstupem tohoto bude poskytnutí služby technické podpory prováděné jednou za půl roku v termínech stanovených SŽ.

Poz-9c	Individuálně objednávané činnosti technické podpory řešení
Popis	Individuálně objednávané činnosti technické podpory zahrnují zejména: <ul style="list-style-type: none"> ▪ Instalace nejnovějších opravných balíčků a relevantních nových verzí SW, dle doporučení výrobce, ▪ Konfigurace požadavků na změnu dle potřeb SŽ, ▪ Řešení provozních incidentů uživatelů, které nejsou způsobeny prokazatelnou vadou SW nebo implementace, ▪ Diagnostika implementovaných systémů, resp. závad, v místě plnění nebo prostřednictvím vzdáleného přístupu dle žádosti správce aplikace.
Výstupy	Výstupem tohoto bude poskytnutí služby technické podpory prováděné na žádost SŽ v termínech dle příslušného SLA.

Technická podpora bude poskytována v souladu ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 5 závazného návrhu smlouvy, který tvoří přílohu č. 11 zadávací dokumentace) podle servisního modelu B3.

4.10 Služby na vyžádání

Poz-10	Služby na vyžádání
---------------	---------------------------

Popis	<p>Dodavatel poskytne zadavateli služby konzultace na vyžádání. Služby mohou být čerpány především pro rozvoj a úpravy systému správy životního cyklu uživatelských certifikátů, popř. SW koncových stanic.</p> <p>Maximální souhrn těchto služeb bude činit 20 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb zadavatele.</p> <p>Dodavatel je povinen zahájit poskytování služeb na vyžádání do 10 (deseti) pracovních dní od doručení závazného požadavku Zadavatele na poskytnutí služby.</p>
Výstupy	<p>Výstupem tohoto bude poskytnutí služby konzultace, implementace a konfigurace systému správy životního cyklu uživatelských certifikátů na vyžádání podle potřeb Zadavatele.</p>

4.11 Průběžná dodávka fyzických nosičů (karet) a spotřebního materiálu personalizačního pracoviště

....

Poz-11	Průběžná dodávka fyzických nosičů (karet) a spotřebního materiálu personalizačního pracoviště
Popis	<p>v této fázi dodavatel zajistí dodávky fyzických nosičů, ochranných prvků a ochranných obalů na základě dílčích objednávek Zadavatele. Nosiče budou dodávány bez personalizace, která bude zajišťována Zadavatelem s využitím personalizačního pracoviště.</p> <p>Dodavatel zajistí dodávky spotřebního materiálu personalizačního pracoviště na základě dílčích objednávek Zadavatele.</p> <p>Dodavatel je povinen dodat nosiče, popř. spotřební materiál do 15 (patnácti) pracovních dnů od doručení objednávky Zadavatele.</p> <p>Předpokládaný harmonogram dodávek fyzických nosičů, ochranných prvků a ochranných obalů je definován před-implementační analýzou a může být upravován podle skutečného průběhu plošného nasazení řešení MFA založeném na uživatelských certifikátech v celé organizaci Zadavatele.</p> <p>Příloha č. 4 zadávací dokumentace určuje maximální objem plnění v dodávkách fyzických nosičů všech typů, jejich ochranných prvků, ochranných obalů a spotřebního materiálu personalizačního pracoviště. Množství fyzických nosičů, poměr jednotlivých typů a množství souvisejících ochranných prvků, obalů a spotřebního materiálu definované přílohou č. 4 zadávací dokumentace je nutno vnímat jako maximální a Zadavatel tento rozsah není povinen využít.</p>
Výstupy	<p>Dodávka fyzických nosičů, ochranných prvků, ochranných obalů a spotřebního materiálu personalizačního pracoviště v souladu s dílčími objednávkami Zadavatele.</p>

4.12 Ukončení smlouvy a exit plán

V případě uplynutí smluvního období nebo předčasného ukončení smlouvy požaduje zadavatel součinnost dodavatele k zajištění hladkého přechodu na nový systém.

4.12.1 Exit plán

Exit plán bude zpracován Dodavatelem v rámci fáze 1 – před-implementační analýza (Zadavatel mu k tomu poskytne nezbytnou součinnost, která je blíže vymezena níže v kap. 4.12.2). Tento plán bude obsahovat konkrétní kroky, odpovědnosti, harmonogram a požadavky na součinnost obou stran při ukončení smluvního vztahu, včetně předání dat, dokumentace a zajištění kontinuity služeb.

Zpracovaný exit plán se po akceptaci Zadavatelem stane pro obě strany **závazným dokumentem**.

Veškeré požadavky na součinnost při ukončení smlouvy jsou vymezeny v této technické specifikaci a dále budou konkretizovány v samotném exit plánu.

V rámci kap. 4.12.2.3 je uvedeno, že Dodavatel poskytne součinnost v rozsahu **5 MD**. Tento rozsah je určen **výhradně pro činnosti spojené s ukončením smlouvy**, včetně realizace kroků uvedených v exit plánu. **Nejedná se o nadstandardní službu**, a proto není naceňována zvlášť a její cena je (stejně jako cena za zpracování exit plánu) již zahrnuta v celkové ceně za před-implementační analýzu (fáze 1). Pokud by v budoucnu vznikla potřeba rozšíření tohoto rozsahu, bude řešeno formou dodatku ke smlouvě.

V rámci přechodu na nový systém požaduje Zadavatel následující podklady a součinnost.

Při ukončení smlouvy je dodavatel povinen předat následující výstupy:

- kompletní export všech konfiguračních dat systému MFA (např. nastavení politik, seznamy zařízení, přístupová pravidla, integrační body – AD, Radius, SAML),
- auditní logy a záznamy o autentizačních událostech za posledních 18 měsíců,
- dokumentace k provoznímu nastavení, integračním vazbám a bezpečnostním opatřením,
- přehled provedených změn v infrastruktuře během implementace,
- dokumentace typu Low-Level Design (L-LD) a provozní manuály,
- přehled licencí a jejich aktuální stav,
- export osobních údajů v souladu s čl. 28 GDPR a jejich bezpečné předání.

Exit plán bude nedílnou součástí smlouvy a bude obsahovat:

- harmonogram přechodu včetně milníků a odpovědností,
- varianty přechodu (např. převzetí provozu jiným dodavatelem, migrace na nový systém),
- zajištění provozní kontinuity po dobu přechodného období,
- podpora při transformaci dat a testování v případě migrace na nový systém.

4.12.2 Součinnost stran

4.12.2.1 Zadavatel:

Zajistí technické prostředky potřebné pro migraci (např. servery, úložiště).

Zajistí přístupy k systémům pro možnost analýzy a exportu dat.

Poskytne dodavateli provozní dokumentaci (stávající konfigurace, bezpečnostní politiky, seznam používaných technologií).

Určí odpovědné osoby dle RACI matice.

4.12.2.2 Nový dodavatel:

Aktivně se zapojí do převzetí systému a validace dat.

Zajistí kompatibilitu s novým řešením.

4.12.2.3 Stávající dodavatel:

Poskytne konzultační podporu v rozsahu až 5 MD.

Odpovídá za úplnost a správnost předaných dat.

Spolupracuje při řešení incidentů během přechodného období.

Exit plán bude zpracován jako součást před-implementační analýzy (Fáze 1). Cena za jeho zpracování je zahrnuta v ceně před-implementační analýzy. Harmonogram zpracování exit plánu se řídí harmonogramem analýzy, tj. 10 týdnů od zahájení plnění. Exit plán bude akceptován společně s výstupy analýzy a následně se stane nedílnou přílohou smlouvy.

5 Fáze plnění a akceptační milníky

Služby musí být dodány v níže uvedených fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) musí být Zadavatelem akceptována nejpozději v termínu uvedeném v Harmonogramu, tj. v příloze č. 15 zadávací dokumentace. Zadavatel akceptuje výstupy dané Fáze, jestliže je Dodavatel provedl v šíři a kvalitě požadované ve výzvě k podání nabídek této veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky dodávky.

Fáze	Prostředí	Popis	Kapitola obsahující požadavky	Akceptační milník
Fáze 1	UAS	Před-implementační analýza	4.1	AM.0
Fáze 2	UAS	Implementace systému správy životního cyklu uživatelských certifikátů (pro UAS) a správy životního cyklu nosičů certifikátů	4.2	AM.1
Fáze 3	UAS	Implementace MFA s využitím uživatelských certifikátů (UAS)	4.3	
Fáze 4	UAS	Napojení systémů správy životního cyklu uživatelských certifikátů a nosičů certifikátů na další definované systémy Zadavatele (UAS)	4.4	
Fáze 5	UAS	Ověřovací (pilotní) provoz (UAS), dokumentace řešení, školení	4.5	
Fáze 6	UAS	Úvodní dodávka nosičů certifikátů a jejich personalizace	4.6	
Fáze 7	UAS	Dodávka a implementace technologií personalizačního pracoviště	4.7	
Fáze 8	UAS	Zajištění přechodu ze současného stavu na využití nových nosičů certifikátů a MFA s využitím osobních uživatelských certifikátů	4.8	
Fáze 9	UAS	Technická podpora řešení	4.9	
Fáze 10	UAS	Služby na vyžádání	4.10	
Fáze 11	UAS	Průběžné dodávky fyzických nosičů (karet) a spotřebního materiálu personalizačního pracoviště	4.11	