

Příloha č. 4 - Technická specifikace

Účelem systému pro řízení a kontrolu přístupu osob je zajištění kontroly vstupu osob do různých prostor a místností v budově Zadavatele. Tento systém umožní Zadavateli dohled nad pohybem rezidentních uživatelů a efektivní správu oprávnění k přístupu. Zadavatel tak bude schopen reagovat na provozní potřeby uživatelů a současně bude schopen omezit přístup, tak aby zvýšil celkovou úroveň zabezpečení budovy a částečně tak naplnil ochranu měkkých cílů.

Systém pro řízení a kontrolu přístupu osob musí umožňovat centrálně z několika počítačů současně spravovat a auditovat oprávnění jednotlivých uživatelů pro přístup a musí umožnit zpětný audit aktivity uživatelů.

Tento dokument uvádí minimální technické požadavky a požadovaný způsob implementace systému pro řízení a kontrolu přístupu osob v budově Zadavatele. Tento dokument popisuje, jak dodavatel systém nastaví a provede.

1. Obecný popis a požadavky na systém pro řízení a kontrolu přístupu osob

- 1.1.a) Systém pro řízení a kontrolu vstupu (dále také jako „SŘKP“) bude modulární řešení, které umožní kombinovat různé technologie pro řízení a kontrolu vstupu dveřmi a jinými mechanickými zábrannými prostředky.
- 1.1.b) Zadavatel požaduje, aby SŘKP podporoval a zahrnoval kombinaci minimálně těchto technologií pro řízení a kontrolu vstupu:
 - i. Elektromechanické (mechatronické) zámkové vložky,
 - ii. Elektromechanické (mechatronické) visací zámky,
 - iii. Bezdrátová elektronická zámková kování,
 - iv. Bezdrátové elektronické zámkové vložky,
 - v. Elektronické přístupové kontroléry a snímače identifikačních karet,
 - vi. Klíčový depozit,přičemž požadavky a způsob implementace na jednotlivé technologie pro řízení a kontrolu dveří a mechanických zábranných prostředků jsou popsány níže.
- 1.1.c) SŘKP musí být napříč různými technologiemi a včetně obslužného software řešen jako jeden unifikovaný a provázaný celek, který bude spravován, dohledáván a administrován z jednotného obslužného software.
- 1.1.d) SŘKP a obslužný software bude provozován na IT infrastruktuře Zadavatele, přičemž Zadavatel poskytne jak IT infrastrukturu pro provoz obslužného software, tak i komunikační síť LAN pro vzájemné propojení jednotlivých komponent v systému.
- 1.1.e) Veškerý software nutný pro provoz systému a všech technologií bude implementován na infrastruktuře Zadavatele tj. On-premise. Systém nesmí pro svůj plnohodnotný provoz vyžadovat spojení přes internet a nesmí využívat cloudové služby.
- 1.1.f) Systém musí být možné instalovat na stávající mechanické zábranné prostředky. Předmětem plnění není výměna mechanických zábranných prostředků nebo jejich částí.
- 1.1.g) Dodavatel poskytne záruku na dodané výrobky a obslužný software po dobu 36 měsíců.
- 1.1.h) Po trvání záruční doby bude dodavatel poskytovat v rámci ceny plnění veškerý update a upgrade obslužného software. Dodavatel se zavazuje, že provede minimálně jeden upgrade před koncem záruční doby.
- 1.1.i) Dodavatel se zavazuje poskytovat technickou podporu po dobu instalace a záruky v českém jazyce.

- 1.1.j) Dodavatel se zavazuje poskytovat školení pověřených osob minimálně 2x za rok po dobu 36 měsíců (po dobu poskytování podpory) a nutnost proškolení pověřených osob při aktualizaci systému.

1.2. Rozsah systému

Systém musí být navržen tak, aby byl dostatečně kapacitně dimenzován a aby byl schopen plnit všechna níže uvedená kapacitní a kvantitativní kritéria současně.

- 1.2.a) Systém a veškeré jeho komponenty (včetně zařízení pro obsluhu mechanických zábranných prostředků) musí být dimenzovány pro minimálně 10 000 uživatelů.
- 1.2.b) Systém a veškeré jeho komponenty (včetně zařízení pro obsluhu mechanických zábranných prostředků) musí být dimenzovány pro minimálně 10 000 uživatelských a návštěvních karet.
- 1.2.c) Systém musí umožnit kompletní obsluhu, administraci a konfiguraci z neomezeného počtu pracovních stanic.
- 1.2.d) Systém musí podporovat a implementovat minimálně 20 půdorysných mapových podkladů, ve kterých bude možné vizualizovat jednotlivé prvky SKV a jejich stavy.
- 1.2.e) Systém musí být dimenzován a koncipován tak, aby byl schopen obsloužit minimálně 2000 elektromechanických zámkových vložek.

2. Obslužný software

2.1. Systémové a architektonické požadavky:

- 2.1.a) Systém bude využívat architekturu server – klient
- 2.1.b) Veškerá data ze všech připojených technologií SŘKP budou ukládána do databáze.
- 2.1.c) Obslužný software a všechny jeho softwarové komponenty musí být možné provozovat na redundantním serverovém řešení v režimu HA (high availability) nebo FT (fault tolerant).
- 2.1.d) Databáze bude provozována na Microsoft SQL serveru verze 2019 nebo novější
- 2.1.e) Prostředky pro provoz MS SQL serveru a aplikačního serveru poskytne zadavatel na vlastní infrastrukturu.
- 2.1.f) Obslužný software bude využívat asynchronní komunikaci mezi jednotlivými softwarovými komponentami pro zajištění rychlých odezev.
- 2.1.g) Obslužný software umožní provoz současně ze všech klientských pracovišť. Architektura obslužného software musí být koncipována jako nezávislá na počtu připojených klientských aplikací, respektive uživatelů. Případné licenční podmínky musí být součástí celkové nabídky.
- 2.1.h) Klientské aplikace budou realizovány formou Windows desktop aplikace, tedy tlustými klienty.
- 2.1.i) Obslužný software a všechny jeho softwarové komponenty musí být možné upgradovat centrálním způsobem na všech pracovních stanicích najednou.
- 2.1.j) Obslužný software bude včetně veškerých podpůrných nástrojů lokalizován v českém jazyce.

2.2. Funkce software

Obslužný software bude sloužit pro kompletní administraci celého řešení včetně všech technologií pro řízení a kontrolu vstupu dveřmi a jinými mechanickými zábrannými prostředky. Obslužný software musí umožňovat:

- 2.2.a) dohled a monitoring systému v reálném čase v podobě textového výpisu událostí v systému,
- 2.2.b) dohled a monitoring systému v reálném čase v grafické formě v mapových podkladech,
- 2.2.c) dohled a monitoring aktuální stavů jednotlivých prvků systému,
- 2.2.d) správu uživatelů, karet, klíčů,
- 2.2.e) správu (přidání/odebrání/editace) oprávnění uživatelů na průchod před mechanické zábranné prostředky.
- 2.2.f) Reporting a audit historie událostí.
- 2.2.g) Audit nastavených oprávnění,
- 2.2.h) Zasílání notifikací ze systému.

2.3. Funkce pro dohled a monitoring systému

Obslužný software bude prezentovat události a stavy připojených technologií pro řízení a kontrolu vstupu. Pro dohled a monitoring systému budou v obslužném software dostupné minimálně tyto funkce:

Zajištění ergonomie operování systému a možnost parametrizace systému vhodně pro aplikaci Zadavatele musí systém umožňovat zobrazení informací a ovládacích prvků v panelech a musí umožňovat uživatelské uspořádání pracovní plochy:

- 2.3.a) Systém musí umožňovat zobrazení informací a ovládacích prvků v panelech (oknech).
- 2.3.b) Systém musí podporovat flexibilní uživatelské uspořádání pracovní plochy - operátoři musí mít možnost uživatelské změny panelů, jejich rozložení a rozmístění na pracovní ploše systému následovně:
 - i. jednotlivé panely lze libovolně umístit na pracovní ploše,
 - ii. panely lze skrývat,
 - iii. panely lze řadit do záložek,
 - iv. panely lze zobrazit vícekrát a různým nastavením,
 - v. rozložení panelů lze uložit jako operátorské nastavení a vyvolat na libovolné pracovní stanici,
 - vi. rozložení panelů lze sdílet mezi operátory.

Software musí podporovat zobrazení aktuálních událostí v systému v textové formě:

- 2.3.c) Software musí umožňovat prezentování událostí ve formě textového výpisu.
- 2.3.d) V textovém výpisu musí být možné události řadit podle různých kritérií například podle času, konkrétního zařízení, operátora atd.
- 2.3.e) Události, které jsou operátorovi v software prezentovány, jsou filtrovány na základě oprávnění přihlášeného operátora,
- 2.3.f) Operátor má možnosti využít uživatelské filtry událostí, které vyfiltrují jen požadované události, dle různých kritérií například podle času, konkrétního zařízení, operátora atd., aby byla zajištěna ergonomie v systému.

Software musí podporovat zobrazení aktuálních událostí a ovládacích prvků v mapových a grafických podkladech.

- 2.3.g) Systém musí umožnit zobrazení stavů prvků do půdorysného mapového podkladu.
- 2.3.h) Systém musí podporovat prezentování stavu prvků formou ikon nebo obecných polygonů, definovaných administrátorem.

- 2.3.i) Společné grafické objekty - systém musí umožňovat namapovat více fyzických prvků na jeden grafický objekt a umožnit tak zobrazit stav více prvků, například v celé budově nebo areálu pomocí jedné ikony nebo polygonu.
- 2.3.j) Systém musí umožňovat přibližování a oddalování (zoom) grafického podkladu a prvků.
- 2.3.k) Systém musí umožňovat posuv grafického podkladu a prvků v případě, že se grafický podklad nevejde do panelu (okna).
- 2.3.l) Při přiblížení grafického podkladu do takové míry, kdy se celý podklad nevejde do panelu (okna) musí systém zobrazit orientační mapku, která prezentuje operátorovi jaká část je z grafického podkladu zobrazována.
- 2.3.m) Systém musí podporovat vektorové (zvětšitelné bez ztráty kvality a rozlišení) i bitmapové (zvětšitelné se ztrátou rozlišení a kvality) grafické podklady.
- 2.3.n) Systém musí podporovat využití více mapových podkladů (například samostatné mapy pro jednotlivé objekty).

Software bude nabízet možnosti pro diagnostiku a monitoring aktuálních stavů v systému ve formě zobrazení struktury systému, která bude obsahovat jednotlivé prvky SKV a dle charakteru prvku budou zobrazeny i jeho stavy, například stav komunikace nebo napájení. Systém musí přehledně prezentovat stavy zařízení (stav komunikace, stav napájení):

- 2.3.o) Systém bude prezentovat prvky systému a jejich stavy ve formě stromové struktury systému, ze které vyplývá architektura systému a nadřazenost nebo podřazenost jednotlivých komponent systémů včetně hardwarových zařízení.
- 2.3.p) Systém bude prezentovat prvky systému a jejich stavy ve formě struktury vytvořené na základě fyzického umístění zařízení, kdy je možné stromově zobrazit budovy, patra budov, místnosti a v nich jednotlivé prvky SKV, tak aby byl možné ergonomicky zobrazit kde se jaké zařízení nebo prvek SKV nachází.
- 2.3.q) Stromová struktura fyzických umístění prvků musí být plně konfigurovatelná, aby ji bylo možné definovat pro konkrétní areál nebo budovu a tato struktura musí přesně odpovídat členění budovy zadavatele.
- 2.3.r) Systém musí prezentovat stavy všech softwarových komponent nutných pro provoz systému a stavy všech obsluhovaných hardwarových zařízení určených pro online provoz, aby byla možná diagnostika, nebo vyvolání ovládacího panelu zařízení.

2.4.Zpracování mapových podkladů

Obslužný software bude podporovat mapové podklady, které budou sloužit pro prezentaci stavů a událostí z prvků SKV. **Současně budou mapové podklady sloužit pro vizuální prezentaci jednotlivých prvků SKV a přístupových bodů, aby umožnily uživatelsky přívětivou správu a přidělování oprávnění přímo z mapového podkladu.**

- 2.4.a) Software bude prezentovat události a stavy systému v mapových podkladech. Dodavatel přepracuje mapové podklady tak, aby byly měly zcela jednotný vzhled, jednotné tloušťky čar a jednotnou reprezentaci okenních výplní a dveří. Mapové podklady budou půdorysné.
- 2.4.b) Mapové podklady budou zpracovány ve vektorovém grafickém formátu, který umožní bezetrátové přibližování a zvětšování. Zadavatel požaduje zpracování mapových podkladů v barevném schématu, které je vhodné pro trvalé operování systému. Využití surových nebo graficky očištěných stavebních výkresů (odmazání některých prvků a vyčištění vrstev) je nepřípustné.
- 2.4.c) Minimální počet zpracovaných mapových podkladů je 20, jejichž zpracování musí být zahrnuto v ceně plnění.

2.5. Workflow a incident management

Systém musí být vybaven funkcemi pro sledování a evidenci postupu řešení incidentů. Systém musí umožnit definovat události, které vyžadují potvrzení o zahájení řešení operátorem, sledování a zaznamenání postupu jejich řešení a uzavření incidentu s jednoznačným zjištěním o příčině vzniku incidentu.

Dodavatel navrhne jaké události a z jakých zařízení budou zařazeny do incident managementu, tedy systému detailního odbavení mimořádných událostí. Dodavatel sestaví výčet zařízení a událostí a navrhne Zadavateli zařazení do incident managementu.

Dále dodavatel navrhne výčet možných příčin vzniku incidentů, které budou v systému nastaveny a operátoři budou muset vybrat vybranou příčinu, aby bylo jednoznačné, jaký byl důvod vzniku incidentu.

2.6. Správa uživatelů, karet, klíčů

Software musí být schopen zajistit funkcionality pro komplexní evidenci a správu osob, identifikačních medií (karet a klíčů). Software musí umožnit systémově přidělovat a spravovat oprávnění na prvky SŘKV, které umožňují vstup přes mechanické zábranné prostředky. Proto software musí plnit tyto požadavky:

- 2.6.a) Správu databáze (uživatelů, karet, klíčů a jejich uživatelů, předmětů a přidělených oprávnění) musí být možné realizovat z jakékoliv pracovní stanice v systému se stejnými funkcionalitami a možnostmi v závislosti na oprávnění operátora.

Software musí umožňovat správu těchto entit:

- 2.6.b) Správa (přidávání/mazání/editace) uživatelů (držitelů karet a klíčů),
- 2.6.c) Správa (přidávání/mazání/editace) identifikačních medií – karet,
- 2.6.d) Správa (přidělování/odebírání) elektromechanických klíčů uživatelům,

Systém bude umožňovat správu identifikačních karet v rozsahu minimálně těchto funkcí:

- 2.6.e) Systém musí evidovat přístupová média (karty) a umožnit jejich správu (přidání, úprava).
- 2.6.f) Systém musí umožňovat i hromadné vložení většího počtu karet.
- 2.6.g) Systém nesmí umožnit smazání karty z důvodu zachování historie událostí vztahených ke kartě. Místo smazání (fyzického odstranění z databáze) musí systém nabízet jiné nástroje, jak označit kartu, která nemá být používána (např. označit ji jako zničená, ztracená atd.).

Správa uživatelů musí být možná na úrovni jednotlivých osob ale i skupin, aby bylo možné nad uživateli provádět hromadnou správu a podle příslušnosti ve skupinách uživatele filtrovat.

- 2.6.h) Software umožní definici skupin uživatelů – systém musí umožnit definovat skupiny, do kterých lze přidělovat jednotlivé držitele karet a následně s nimi pracovat a provádět hromadné operace.
- 2.6.i) Systém musí podporovat definici neomezeného množství atributů, které je možné uživateli v systému přidělit a vyplnit jejich hodnoty například (osobní číslo, číslo oddělení, název oddělení, společnost, rezident/návštěva/dodavatel/úklid atd.) a podle těchto hodnot databázi uživatelů filtrovat.
- 2.6.j) Nad filtrovaným seznamem uživatelů musí být možné provádět hromadné operace jako například přidat nebo odebrat oprávnění.

Systém musí být vybaven funkcionalitami pro kontrolu vkládaných údajů do databáze osob. Tyto funkce mají zajistit vložení korektních a validních údajů do databáze v případě že systém administruje více osob z různých organizačních jednotek.

- 2.6.k) systém musí umožnit nakonfigurovat kontroly obsahu datových polí v databázi. Kontroly umožní odhalit chyby a neplatně zadané informace do databáze a předcházet tak chybám a nekonzistencím v obsahu databáze.
- 2.6.l) konfiguraci a aplikaci validátorů (kontrol) na vybraná datová pole v databázi,
- 2.6.m) konfigurovat různá validační kritéria (například maska/regulární výraz u textových polí, nebo hodnota se musí/nesmí rovnat zadané hodnotě, nebo hodnota je povinná, nebo obsahuje část textu, u číselných a datumových datových polí kontrolovat operátory větší/menší než, obsah datového pole musí být jedinečný)
- 2.6.n) svázání datových polí, kdy obsah jednoho datového pole může vynutit vyplnění dalších polí, například pokud je vyplněno, že osoba je zaměstnanec, systém začne požadovat pořízení fotografie nebo telefonního čísla, pokud je osoba dodavatel, uvedené kontroly fotografie a telefonního čísla se neprovádí.
- 2.6.o) různé druhy reakcí systému na vložení nevalidních dat - vložení dat, které nesplňují podmínky, může operátora: 1) upozornit na nevalidní obsah pole a přesto umožnit uložení zadaných dat nebo 2) zabránit uložení dokud nedojde k nápravě.

Systém musí podporovat hromadný (dávkový) import uživatelů pro uvedení systému do provozu. Dodavatel provede ve spolupráci se zadavatelem prvotní import všech uživatelů do systému, jak bude probíhat postupná výměna zámků tak, aby systém byl funkční a obsluhovatelný. To znamená, že při výměně jednotlivého zámku za nový předá nový klíč příslušnému uživateli a do systému zaeviduje příslušná práva. Konkrétní seznam osob obdrží od Zadavatele.

Systém musí umožňovat hromadný import dat o uživateli z jiných systémů včetně fotografií.

2.7. Parametrizace databáze uživatelů a karet a jejich atributů

Odporovatelnost systému, přehlednost auditu přidělených oprávnění a možnost systematicky třídit a filtrovat uživatele v databázi dle potřeb Zadavatele a jeho organizačních jednotek je podmíněna vysokou mírou adaptace software tak, aby obsahoval potřebné a relevantní informace u jednotlivých uživatelů. Proto se vyžadují tyto funkce:

- 2.7.a) Systém musí umožnit přidělit uživatelům různé atributy, jejichž význam může být přizpůsoben. Atributem je editovatelné pole, které může dle potřeb obsahovat různá data o uživateli.
- 2.7.b) Atributů může být u uživatelů neomezené množství.
- 2.7.c) Atributy budou mít definovatelný charakter obsahu, aby bylo možné zadat požadované hodnoty atributu. Systém musí nabízet tyto typy atributů:
 - (a) text,
 - (b) číslo,
 - (c) výběr z předdefinovaných hodnot,
 - (d) datum a čas,
 - (e) obrázek,
 - (f) logický (ano/ne)
- 2.7.d) Atributů může být neomezené množství a jeden typ atributu může být použit vícekrát

Zadavatelem odhadovaný počet a význam atributů, který bude požadován, ale očekává se jeho adaptace při implementaci systému, dle provozních potřeb

Uživatel	Typ atributu	Název atributu
	Text	Jméno uživatele
	Text	Příjmení uživatele
	Dle potřeby (číslo nebo text)	ID uživatele / osobní číslo
	Obrázek	Fotka uživatele
	Výběr z předdefinovaných hodnot	Název společnosti
	Výběr z předdefinovaných hodnot	Oddělení
	Výběr z předdefinovaných hodnot	Vztah k ČRO

Karta/klíč	Typ atributu	Název atributu
	Číslo	PIN
	Číslo	Číslo karty
	Text	UID karty

Návštěvník	Typ atributu	Název pole
	Text	Jméno návštěvníka
	Text	Příjmení návštěvníka
	Číslo	Číslo OP nebo PASu
	Text	Společnost / Firma

Návštěva (událost)	Typ atributu	Název atributu
	Výběr z předdefinovaných hodnot	Jméno a příjmení navštíveného
	Výběr z předdefinovaných hodnot	Místo návštěvy (budova)
	Čas	Předpokládaná doba trvání návštěvy
	Výběr z předdefinovaných hodnot	Účel návštěvy

2.7.e) Konfigurovatelná atributy se promítnou do všech částí software, kde jsou dostupná a využitelná, například reportování událostí, správa uživatelů, audit oprávnění.

2.8. Správa oprávnění uživatelů na průchod před mechanické zábranné prostředky.

Software bude umožňovat přehlednou a ergonomickou správu oprávnění. S ohledem na uvažovaný rozsah SKV, který bude přesahovat 2000 prvků, na které se budou přidělovat oprávnění je vyžadováno, aby software byl vybaven funkcemi pro ergonomickou správu oprávnění a audit přidělených oprávnění upřesněných takto:

2.8.a) Systém musí podporovat tyto formy oprávnění:

- i. oprávnění na jednotlivé prvky SŘKP (elektromechanické zámkové vložky) s časovou zónou, která specifikuje časové období, kdy oprávnění platí.

- ii. skupinová oprávnění, kdy skupina je tvořena jedním nebo více prvky SKV s časovou zónou, která specifikuje časové období, kdy oprávnění platí.
- 2.8.b) Rozbor skupinových oprávnění – software musí umožnit operátorovi snadno a rychle zjistit, jaká je definice (obsah) skupinových oprávnění například formou nápovědy nebo rozbalovacího seznamu.
- 2.8.c) Expirace oprávnění – systém umožňuje přidělení časově omezeného oprávnění (skupinové oprávnění, jednotlivé snímače, ovládání střežení, klíče a předměty, skupiny klíčů a předmětů) od-do s přesností na dny. Po expiraci je oprávnění automaticky deaktivováno.
- 2.8.d) Software musí umožnit přidělit jednomu uživateli i více než jeden elektromechanický klíč.

Systém musí umožnit správu oprávnění uživatelů i z mapového podkladu. Vzhledem k rozsahu systému není dostačující správa oprávnění z běžných výčtových seznamů, které umožní vybrat určitá oprávnění reprezentované textově. Systém tedy musí umožňovat:

- 2.8.e) Software musí umožnit správu (přidání, odebrání) oprávnění z výčtu oprávnění v textové formě.
- 2.8.f) Software musí umožnit správu (přidání, odebrání) oprávnění z grafického mapového podkladu budovy nebo areálu.

Při implementaci systému dodavatel zpracuje půdorysné podklady budov a areálů, do kterých budou zaneseny grafické ikony reprezentující prvky SŘKP (snímače karet, zámkové vložky atp.), na které lze přidělovat uživatelům oprávnění.

- 2.8.g) Ikona prvku SŘKP musí být v mapovém podkladu jednoznačně identifikovatelná například tak, že se zobrazí název prvku přístupového systému po najetí kurzorem na grafický prvek.
- 2.8.h) Operátor bude mít při běžné správě oprávnění možnost zobrazit si mapové podklady budovy nebo areálu, ve kterých budou zobrazeny prvky SŘKV. Při výběru uživatele budou v mapovém podkladu vizuálně odlišeny prvky přístupových systémů, na které držitel již má přidělené oprávnění.
- 2.8.i) Software musí operátorovi umožňovat provést tyto úkony z mapového podkladu:
 - i. Přidat oprávnění uživateli kliknutím nebo funkcí drag & drop na ikonu reprezentující prvek přístupových systémů,
 - ii. Odebrat oprávnění kliknutím na ikonu reprezentující prvek přístupových systémů,
 - iii. Zobrazit prvky, na které má uživatel již přidělené oprávnění
 - iv. Zobrazit rozpad skupinových oprávnění na jednotlivé přístupové prvky, to umožní přehledně zobrazit, které prvky dané skupinové oprávnění zahrnuje.
- 2.8.j) Z mapového podkladu software bude umožňovat přidat i odebrat oprávnění na prvky přístupových systémů více a uživatelům karet najednou.

2.9. Reporting a Audit

Software musí poskytovat funkce pro reportování a audit tj. funkce umožňující prohlížení událostí (i v historii), výpis a audit nastavení systému. Operátorské prostředí pro reportování musí být přehledné, s funkcemi pro snadné a rychlé filtrování podle dostupných atributů uživatelů. Reportované informace, jejich výběr a rozsah musí být systém schopen ergonomicky spravovat, proto musí systém vytvářet a využívat tzv. reportovací sestavy. Ty umožní operátorům rychlý přístup k potřebným informacím díky tomu, že obsahují operátorem předdefinovanou a modifikovatelnou definici reportovaných informací.

- 2.9.a) Reportovací sestavy musí být prezentovány formou tabulkového výpisu.

- 2.9.b) Tabulkový výpis musí umožnit ekvivalentní export a následný import do tabulkových procesorů jako například MS Excel.
- 2.9.c) Tabulkový výpis umožní přímo v software filtrování.
- 2.9.d) Reportovací sestavy musí být prezentovány i graficky.
- 2.9.e) Sestavy s událostmi musí umožňovat zobrazit informace v neomezeném časovém období.
- 2.9.f) Systém musí umožňovat generování těchto sestav:
 - i. události (zprávy SŘKP, poplachy, poruchy, výpadky komunikace, činnost operátorů),
 - ii. přehled činnosti operátorů – činnost operátorů je logována, systém musí umožnit výpis činnosti operátorů (správa karet, změny konfigurace, ovládání zařízení),
 - iii. historie návštěv - sestava historie návštěv umožňuje procházení jednotlivých návštěv (událostí) a jejich detailů (hodnocení návštěvy, navštívené osoby, navštěvující osoby atd.),
 - iv. Přidělená oprávnění ke kartám – systém musí umožnit sestavit seznam karet a osob s vybranými oprávněními, které jsou ke kartě přiřazené. Oprávnění jsou těchto typů: 1) pro přístupový systém, 2) pro manipulaci s předměty, 3) pro ovládání systému uživateli.
 - v. Karty - sestava oprávnění karty umožňuje vypsat kompletní nastavení a oprávnění vybrané karty nebo karet. Sestava obsahuje všechny dostupné informace o kartě (základní parametry karty, informace o držiteli i všechna přidělená oprávnění).

2.10. Notifikace ze systému

Software musí umožňovat zasílání notifikací prostřednictvím e-mailu a SMS. Vzhledem k plánovanému rozsahu řešení je nutná customizace notifikací a dynamické přidělování adresátů dle předdefinované struktury odpovědností.

- 2.10.a) Systému musí zasílat SMS a e-mailové notifikace.
- 2.10.b) Obsah notifikací musí být customizovatelný dle potřeb aplikace.
- 2.10.c) Do obsahu zpráv bude možné vkládat automaticky doplňovaná data, zpráv a událostí například datum a čas zprávy, ke které se notifikace vztahuje, událost, která je předmětem zprávy, jméno a příjmení uživatele, číslo klíče atd.
- 2.10.d) Odeslání notifikační zprávy je podmíněno splněním podmínek, které musí být možné konfigurovat například datum a čas, zařízení nebo prvek SŘKP, kterého se notifikace týká uživatel, kterého se notifikace týká atd.
- 2.10.e) Software dále umožní asociovat konkrétní prvky SŘKP s konkrétními uživateli například dveře a/nebo elektromechanická vložka u kanceláře určitého uživatele může být asociována s tímto uživatelem. Pak je možné nastavit asociaci vložek s větším počtem uživatelů a dynamicky tak určit adresáty zpráv o aktivitě na dveřích jejich kanceláře.

2.11. Přihlašování do obslužného software

Minimální kritéria pro parametry hesla musí být konfigurovatelné a musí být možné nastavit minimální parametry hesel tak, aby byly dodrženy veškeré legislativní požadavky v oblasti zabezpečení IT systémů a informačních technologií. Software musí v oblasti přihlašování a požadavků na hesla splňovat tato kritéria:

- 2.11.a) Požadavky na délku hesla musí být nastavitelné.
- 2.11.b) Požadavky na komplexitu hesla musí být nastavitelné.
- 2.11.c) Délka hesla musí být nastavitelná na minimálně 8 znaků.
- 2.11.d) Komplexita hesla bude nastavena tak, aby heslo obsahovalo alespoň jedno velké písmeno.
- 2.11.e) Komplexita hesla bude nastavena, tak aby heslo obsahovalo alespoň jednu číslici.

- 2.11.f) V případě neúspěšného přihlášení uživatele z důvodu chybně zadaných údajů software nezobrazuje, která část přihlašovacích údajů je špatná.
- 2.11.g) Hesla nesmí být uložena v otevřené podobě ani pomocí reverzibilního šifrování.

2.12. Podpora

- 2.12.a) Systém musí být vybaven integrovanou interaktivní nápovědou, která je dostupná v uživatelském prostředí obslužného software.

2.13. Ochrana osobních údajů v SŘKP a obslužném software

Základní funkce systému v oblasti ochrany osobních údajů. Systém musí umožňovat:

- 2.13.a) vynucení síly hesla – operátoři jsou systémem nuceni dodržovat administrátorem definovanou sílu (délka, komplexita) hesla,
- 2.13.b) detailní logování operátorské činnosti,
- 2.13.c) zobrazení a export historie operátorské činnosti,
- 2.13.d) evidovat zpracovávané osobní údaje ve formě tzv. systém listu, který obsahuje legislativou stanovené informace o rozsahu zpracovávaných osobních údajů a identifikaci zpracovatele osobních údajů,
- 2.13.e) tisk systém listu na žádost subjektu osobních údajů (osob, jejichž údaje jsou zpracovávány),
- 2.13.f) automatické udržování délky záznamů v systému – systém musí být schopen automaticky a v definované periodě provádět odstranění záznamů (nejen s osobními údaji) z databázi systému tak, aby byly dodrženy, příslušným úřadem schválené lhůty pro uchování osobních údajů.

Funkce umožňující uplatnění práv subjektu (osob, jejichž údaje jsou zpracovávány). Systém musí umožnit:

- 2.13.g) vygenerování a tisk subject listu, ten obsahuje všechny osobní údaje (informace o subjektu, jeho kartách, oprávněních a celou historii osoby a jí přidělených karet),
- 2.13.h) anonymizaci osobních údajů; smazání držitele nesmí z důvodu zachování historie smazat osobní údaje, pokud je vyžadováno odstranění osobních údajů, anonymizace odstraní osobní údaje, ale informace o anonymním držiteli jsou zachovány.

3. Elektromechanické zámkové vložky a visací zámky

Pro obsluhu stávajících dveří a jiných mechanických zábranných prostředků s instalovaným kováním je navržen elektromechanický nebo také mechatronický systém zámkových vložek, které kombinují jak mechanické vlastnosti vložek a klíčů tak i možnost nastavení elektronických oprávnění, která dále umožňují omezit přístup. Požadavky na elektromechanické vložky a klíče jsou popsány v požadavcích v této části.

3.1. Obecné požadavky na elektromechanické zámkové vložky a klíče

- 3.1.a) Jeden typ elektromechanických klíčů musí podporovat jak elektromechanické (mechatronické) zámkové vložky tak i visací zámky.
- 3.1.b) Elektromechanické vložky zámků musí být možné přímo instalovat záměnou ve stávajících dveřích, katrech dle ČSN EN 1303 (165191) a instalace nevyžaduje žádné stavební nebo mechanické úpravy dveří, kování nebo zámků

- 3.1.c) Pro průchod dveřmi z elektromechanickými vložkami budou sloužit klíče, které budou umožňovat průchod na základě jejich mechanického zpracování (mechanických práv) a na základě elektroniky, která umožní nastavit další práva.
- 3.1.d) V klíčích budou integrovány jednoznačné identifikační elektronické prvky, které umožní identifikovat klíče v systému a software a přidělovat na konkrétní klíče oprávnění a vyčítat z klíče historii událostí a průchodech vložkami.
- 3.1.e) certifikace zámkového systému Národním bezpečnostním úřadem
- 3.1.f) 3. bezpečnostní třída vložky dle ČSN EN 1627 (nebo vyšší)
- 3.1.g) Zneplatnění elektronických přístupových práv konkrétního klíče je možné provést přímou distribucí "zakázaných klíčů" do dotčených vložek pomocí dodaného nástroje (např. servisního klíče).
- 3.1.h) Časové omezení platnosti přístupových práv od jednotek minut až po neomezenou expiraci
- 3.1.i) Nastavitelná hodnota časového plánu platnosti přístupových práv (denní/týdenní rozvrh včetně začátku a konce platnosti)

3.2. Provedení a minimální požadavky na elektromechanické zámkové vložky

- 3.2.a) Rozměry elektro mechanických vložek musí odpovídat rozměrům uvedeným ve výkazu výměr.
- 3.2.b) V zamykacím systému bude možné definovat minimálně deset skupin mechanických práv včetně generálního klíče:
 - (a) SK I – generální klíč – přístup ke všem dodaným vložkám a zámkům zadavatele
 - (b) SK II – skupinový klíč - přístup pouze k vložkám dané podskupiny
 - (c) SK X – skupinový klíč - přístup pouze k vložkám dané podskupiny
- 3.2.c) cylindrické vložky odpovídají rozměrům Europrofilu dle DIN 18252:2018
- 3.2.d) Mechatronické cylindrické vložky pro svůj provoz nevyžadují trvalé připojení napájení (externí zdroj napájení ani baterie)
- 3.2.e) stupeň krytí cylindrické vložky IP 51 (anebo vyšší)
- 3.2.f) Tělo vložky / klíče je opatřeno jedinečným identifikačním/sériovým číslem, přičemž zadavatel obdrží seznam dodaných identifikačních čísel pro každou jednotlivou dodávku

3.3. Provedení a minimální požadavky na elektromechanické klíče

- 3.3.a) profil klíče (mechanického i mechatronického) je jedinečný pro zákazníka
- 3.3.b) klíč pro ovládání mechatronických vložek je mechanický s integrovaným čipem v jeho těle
- 3.3.c) klíč je napájen uživatelsky vyměnitelnou baterií
- 3.3.d) Klíč má ve své paměti uložen seznam vložek, které je oprávněn odemknout a tento seznam je zároveň aktualizovatelný.
- 3.3.e) Ukládání informací o událostech (tj. úspěšné/neúspěšné odemknutí/zamknutí konkrétní cylindrické vložky) v paměti klíče (záznam min. 1000 posledních událostí)

4. KLÍČOVÝ DEPOZIT

Nedílnou součástí systému je komplexní dodávka dvou samostatných sestav klíčových depozitů, které je určeny pro bezpečné a přehledné uložení a správu fyzických mechatronických klíčů. Zadavatel požaduje dodání dvou depozitů v konfiguraci umožňující uložení min. 20ks mechatronických klíčů, z nichž každý bude možno vložit do samostatné cylindrické půlvložky - zámkové pozice v depozitu. Každý depozit bude vybaven dvěma konstrukčními typy půlvložek: a) mechatronická cylindrická půlvložka v počtu 10ks a b) mechanická cylindrická půlvložka v počtu 10ks ve zbývajících pozicích. Hlavním

účelem depozitu je uložení vytipovaných (např. generálních) klíčů, které není povoleno vynášet mimo areál provozovatele. Depozity musí být součástí výše uvedeného komplexního přístupového systému za účelem jednotné centrální administrace uživatelů, správy přístupových oprávnění, evidence a nepřetržitému dohledu.

4.1. Obecné požadavky na Depozity

- 4.1.a) Depozity musí umožňovat přiřazení oprávnění na jednotlivé mechatronické klíče, skupiny klíčů včetně auditu jejich použití.
- 4.1.b) Všechna data o pohybu mechatronických klíčů musí být uchovávána v zabezpečené databázi a dostupná pro auditní účely.
- 4.1.c) Komunikace mezi depozity a obslužným softwarem musí být šifrovaná.
- 4.1.d) Depozit musí být provozuschopný 24/7 a umožnit správu uživatelů v reálném čase.
- 4.1.e) Všechna oprávnění musí být spravována z centrálního rozhraní.
- 4.1.f) Musí být umožněna správa mechatronických klíčů z jednoho rozhraní spolu s depozitem.
- 4.1.g) Depozit musí kontinuálně monitorovat vlastní stav (napájení, komunikace, funkčnost modulů) a generovat výstrahy či upozornění v případě provozních chyb.
- 4.1.h) Depozit musí být navíc vybaven:
 - i. Snímačem RFID karet nebo čipů.
 - ii. Elektronicky zajištěnými odolnými dveřmi, za kterými budou jednotlivé mechatronické klíče pevně uzamčeny v integrovaných ½ vložkách.

4.2. Provedení a minimální požadavky na depozitní zařízení

- 4.2.a) Každá pozice v depozitu musí umožnit mechanické zasunutí a uzamčení mechatronického klíče do cylindrické mechanické, případně mechatronické půlvložky, která bude speciálně vytvořena pro vybraný uživatelský klíč MKS.
- 4.2.b) Depozit musí být připraven pro bezpečné uložení mechatronických klíčů s blokadí výdeje bez autorizace.
- 4.2.c) Depozit musí být vybaven dotykovým displejem (min. 7") a akustickou signalizací
- 4.2.d) Musí být součástí integrovaná kamera, která bude snímat jednotlivé operace s depozitem.
- 4.2.e) Záznam o všech manipulacích musí být dostupný a exportovatelný.
- 4.2.f) Depozit musí umožnit automatické odhlášení uživatele po dokončení operace.
- 4.2.g) Každá pozice pro mechatronický klíč musí být vybavena LED indikací stavu (obsazeno/volno).

4.3. Obslužný software a řízení událostí

- 4.3.a) Musí zobrazovat aktuální provozní události a umožnit jejich filtrování dle oprávnění operátora.
- 4.3.b) Musí umožnit rezervaci mechatronických klíčů a přístupových oprávnění v čase (časová okna, kalendář).
- 4.3.c) Musí být možné přikládat k incidentům komentáře, fotografie a dokumenty.
- 4.3.d) Uživatelské rozhraní musí být přehledné, v českém jazyce, a zobrazovat:
 - i. stav zařízení (online/offline),
 - ii. vydané mechatronické klíče,
 - iii. upozornění a výstrahy.
- 4.3.e) Musí být umožněna **vzdálená správa**, včetně možností jako:
 - i. vzdálené otevření pozice,
 - ii. zablokování výdeje mechatronických klíčů,

- iii. konfigurace přístupů,
 - iv. aktualizace depozitu.
- 4.3.f) Software musí umět generovat upozornění formou notifikace přímo z depozitu v případě:
- i. překročení výpůjční doby,
 - ii. nevrácení mechatronického klíče,
 - iii. pokusu o neoprávněný přístup,
 - iv. technické poruchy zařízení.

4.4. Rozšíření depozitu

- 4.4.a) Depozit musí být technologicky a softwarově připraven k rozšíření o modulární řešení pro bezpečné uložení a správu střelných zbraní a příslušenství (např. zásobníků).
- 4.4.b) Depozit musí disponovat možností rozšíření jednoho nebo více speciálních zbraňových depozitních modulů, které budou plně integrovány do jednotného obslužného softwaru.
- 4.4.c) Rozšiřující moduly pro zbraně musí umožňovat uložení krátkých i dlouhých zbraní v souladu s bezpečnostními požadavky, a to minimálně dle:
 - i. třídy S1 dle ČSN EN 14450+A1,
 - ii. nebo třídy RC2 dle ČSN EN 1627.
- iii. Každá schránka musí být připravena k osazení senzory pro vícestupňovou kontrolu obsahu, zejména:
 - 1. RFID čtečkou pro identifikaci zbraně,
 - 2. váhovým senzorem pro detekci hmotnosti zbraně a zásobníku,
 - 3. optickým senzorem pro přítomnost,
 - 4. a integrovanou kamerou s přísvitkem pro vizuální kontrolu v reálném čase.
- 4.4.d) Modulární schránky musí mít možnost výměny profilovaného dna dle typu ukládané zbraně a příslušenství.
- 4.4.e) Rozšíření depozitu o další moduly pro mechatronické klíče musí být v budoucnu dostupné v ocelovém konstrukčním provedení s certifikací RC2.

4.5. TECHNICKÉ POŽADAVKY

- 4.5.a) Napájení zařízení: AC200–240 V, 50–60 Hz
- 4.5.b) Požadované konstrukční rozměry depozitu včetně ovládacího panelu: výška max. 810 mm, šířka max. 460 mm, hloubka max. 200 mm
- 4.5.c) Provozní teplota zařízení musí být v rozsahu +5 °C až +45 °C.
- 4.5.d) Depozit musí umožňovat definici minimálně 200 časových zón. Tyto časové zóny musí umožnit i určení přesného dne a hodiny, kdy je mechatronický klíč zpřístupněn.
- 4.5.e) Interní vyrovnávací paměť událostí musí mít kapacitu minimálně 10 000 záznamů.

4.6. PROVOZNÍ DOHLED

- 4.6.a) Software musí zobrazovat, zda je depozit připojený k síti a komunikuje.
- 4.6.b) V případě poruchy musí být možné provést vzdálené zásahy (restart, úprava oprávnění)
- 4.6.c) Zařízení musí být navrženo pro nepřetržitý provoz 24/7.
- 4.6.d) Musí obsahovat záložní napájecí zdroj (baterii) s minimální výdrží 24 hodin při výpadku sítě.
- 4.6.e) Záložní baterie musí být umístěna uvnitř zařízení.

- 4.6.f) Depozit musí v případě výpadku sítě automaticky přejít do offline režimu, při kterém musí zajistit vydávání a vrácení mechatronických klíčů a předmětů dle přednastavených pravidel.
- 4.6.g) Po obnovení spojení musí dojít k automatické synchronizaci dat s obslužným software, kdy veškeré události na depozitu musí být synchronizovány do centrálního software.