# Zajištění fyzického zabezpečení datového centra

## Dálkový Monitorovací Systém – Remote Monitoring Systém (RMS)

RMS systém bude realizován autonomními monitorovacími jednotkami pracujícími samostatně nezávisle na sobě s možností vzájemného propojení do jedné skupiny. Jednotky budou nepřetržitě monitorovat teplotu vstupu každého racku a současně monitorovat fyzický vstup do racku pomocí dveřních čidel na dveřích.

V případě překročení, nastavených mezních hodnot nebo otevření dveří racku, bude monitoring informovat uživatele prostřednictvím přednastavených komunikačních kanálů podle důležitosti incidentu. Monitoring bude poskytovat možnost informovat uživatele pomocí:

- SNMP do nadřazeného systému

- SMS prostřednictvím stávající GSM brány NXS-9750 4G (dual modem)

- E-mail

- sepnutím kontaktu

Všechny jednotky budou uživatelsky nastavitelné přes WEB rozhraní. Musí v budoucnu umožnit uživateli upravovat nastavení nebo doplnit systém monitoringu o další čidla, GSM kartu a rozšiřující modulu podle aktuálních potřeb, bez nutnosti zásahu odborné firmy.

Instalace jednotlivých komponent RMS dle lokality bude provedena takto:

* Primární serverovna – budova F
  + 1x monitorovací jednotka včetně 19“ držáku – TYP 1
  + 2x teplotní čidlo
  + 24x dveřní magnetický kontakt
* Sekundární serverovna – budova S
  + 1x monitorovací jednotka včetně 19“ držáku – TYP 1
  + 2x teplotní čidlo
  + 12x dveřní magnetický kontakt
* Podružné datové rozvaděče – 24x
  + 1x monitorovací jednotka včetně 19“ držáku – TYP 2
  + 2x teplotní čidlo
  + 4x dveřní magnetický kontakt

Ve všech lokalitách, bude jedno teplotní čidlo naistalováno dovnitř datového rozvaděče a druhé vně dat. rozvaděče. Cílem je snímání teploty vzduchu v dat. rozvaděči a v místnosti serveroven nebo jednotlivých podružných dat. rozvaděčů.

Všechny monitorovací jednotky budou nakonfigurovány tak aby je bylo možné vzdáleně konfigurovat přes webové rozhraní. Dále budou nastaveny tak aby posílaly upozornění, v případě otevření, některého z dveřních kontaktů nebo při překroční hraniční teploty v dat. rozvaděči či v místnosti. Tyto upozornění budou zasílány na zvolený e-mail.

## Specifikace minimálních požadavků technického řešení

### *RMS řešení s monitorovací jednotkou – TYP 1 – 2ks*

|  |  |
| --- | --- |
| **Požadovaná funkcionalita (technické parametry)** | **Specifikace minimálních požadavků pro aktuální instalaci a funkčnost při plánovaném budoucím rozšíření (GSM karta)** |
| Monitorovací jednotka 1U, 19“ | Monitoring prostředí a technologií |
|  | Podpora minimálně 100 čidel |
|  | Podpora minimálně 700 senzorů |
| Čidlo teplota | Rozsah měření:  Teplota -10 až 80°C, tolerance ±0,5 °C |
| Dveřní kontakt | Suchý kontakt, IP68 |
| Komunikační protokoly: | Síťové protokoly:  DHCP; HTTP; HTTPS; DynDNS; SSL; SNMP v1, v2c, v3; SMTP; FTP; Syslog; RADIUS; OpenVPN  VPN:  Dostupná přes LAN a GSM/LTE kartu |
| Alarmy a notifikace: | Podporované typy:  E-mail, FTP log, Syslog, SMTP, SNMP Traps, SMS/Provolání, Web-to-SMS  Minimální počet příjemců E-mailu: 20  Minimální počet příjemců SMS nebo provolání: 20 |
| Virtuální čidla: | PING  IP kamera  SNMP Get  Uživatelské klíče: RFID karty  Programovatelná logická schémata  Časovače  Triggers  SNMP trap  Výpočet hodnoty z více vstupních údajů  Modbus TCP/IP |
| Napájení: | Externí adaptér 12V  Možnost rozšíření o redundantní napájení (2 zdroj/baterie) |
| Výstupy: | 2x výstupní relé 12V/0,25A |
| Vstupy: | 8x analogové vstupy pro čidla  1x vstup pro digitální čidla prostředí, možnost řetězení až 16 čidel (až 32 senzorů)  16x DI suchý kontakt  Modbus TCP/IP |
| Kamery | 1x USB  1x IP |
| Interní čidla | 1x teplota (tolerance ±1 °C)  1x napájecí napětí (tolerance 1%) |
| Další konektory: | 1x Ethernet 10/100Mbit  1x USB |
| Externí úložiště | 1x SD slot, 32GB |
| Provozní podmínky | Teplota -10 až 80°C  Vlhkost 0 až 90%, nekondenzující |
| Instalace a konfigurace | Fyzická instalace monitorovací jednotky a čidel  Konfigurace jednotky   * Nastavení LAN rozhraní * Základní konfigurace systému * Vytvoření půdorysu místnosti a vložení jako podklad pro znázornění fyzického umístění čidel (2D nebo 3D) * Nastavení prahových hodnot pro senzory * Konfigurace logických filtrů * Konfigurace oznámení SNMP, E-mail |
| Záruka | 2 roky |

### *RMS řešení s monitorovací jednotkou – TYP 2 – 24ks*

|  |  |
| --- | --- |
| **Požadovaná funkcionalita (technické parametry)** | **Specifikace minimálních požadavků pro aktuální instalaci a funkčnost při plánovaném budoucím rozšíření (GSM karta)** |
| Monitorovací jednotka 1U, 19“ | Monitoring prostředí a technologií |
|  | Podpora minimálně 100 čidel |
|  | Podpora minimálně 700 senzorů |
| Čidlo teplota | Rozsah měření:  Teplota -10 až 80°C, tolerance ±0,5 °C |
| Dveřní kontakt | Suchý kontakt, IP68 |
| Komunikační protokoly: | Síťové protokoly:  DHCP; HTTP; HTTPS; DynDNS; SSL; SNMP v1, v2c, v3; SMTP; FTP; Syslog; RADIUS; OpenVPN  VPN:  Dostupná přes LAN a GSM/LTE kartu |
| Alarmy a notifikace: | Podporované typy:  E-mail, FTP log, Syslog, SMTP, SNMP Traps, SMS/Provolání, Web-to-SMS  Minimální počet příjemců E-mailu: 20  Minimální počet příjemců SMS nebo provolání: 20 |
| Virtuální čidla: | PING  IP kamera  SNMP Get  Uživatelské klíče: RFID karty  Programovatelná logická schémata  Časovače  Triggers  SNMP trap  Výpočet hodnoty z více vstupních údajů  Modbus TCP/IP |
| Napájení: | Externí adaptér 12V  Možnost rozšíření o redundantní napájení (2 zdroj/baterie) |
| Výstupy: | 2x výstupní relé 12V/0,25A |
| Vstupy: | 4x analogové vstupy pro čidla  1x vstup pro digitální čidla prostředí, možnost řetězení až 16 čidel (až 32 senzorů)  4x DI suchý kontakt  Modbus TCP/IP |
| Kamery | 1x USB  1x IP |
| Interní čidla | 1x teplota (tolerance ±1 °C)  1x napájecí napětí (tolerance 1%) |
| Další konektory: | 1x Ethernet 10/100Mbit  1x USB 2.0 typ mikro |
| Externí úložiště | 1x SD slot, 32GB |
| Provozní podmínky | Teplota -10 až 80°C  Vlhkost 0 až 90%, nekondenzující |
| Instalace a konfigurace | Fyzická instalace monitorovací jednotky a čidel  Konfigurace jednotky   * Nastavení LAN rozhraní * Základní konfigurace systému * Vytvoření půdorysu místnosti a vložení jako podklad pro znázornění fyzického umístění čidel (2D nebo 3D) * Nastavení prahových hodnot pro senzory * Konfigurace logických filtrů * Konfigurace oznámení SNMP, E-mail |
| Záruka | 2 roky |

## Elektronická Zabezpečovací Signalizace (EZS)

Vnitřní objektová ochrana serveroven, prostřednictvím EZS je řešena jako prostorová ochrana prostoru primární a sekundární serveroveny v objektu, kde jsou instalovány pohybové PIR, audio detektory, siréna, EPS stropní detektory a dále magnetické kontakty na vstupních dveřích a oknech. Přístup zajištuje čtečka a elektromotorický zámek vstupních bezpečnostních dveří. Elektromotorický zámek je součástí řešení bezpečnostních dveří viz aktivita „Zajištění fyzického zabezpečení datového centra“.

Centrální ústředna s GSM a IP komunikací je umístěna uvnitř primární serverovny na stěně vedle podružného silového HR. Je určena pro řízení zabezpečení i sekundární serverovny. Objekty jsou propojeny optickým kabelem a komunikují mezi sebou pomocí optických převodníků po sběrnici RS 485 EZS kript. Klávesnice LCD pro ovládání a zaarmování systému je uvnitř prostoru SV vedle vstupních dveří. V návrhu je též možnost zapnutí systému, či ovládání systému přes mobilní aplikaci. Totéž řešení rozmístění prvků je navrženo pro sekundární serbverovnu. S výjimkou audio čidla a magnetu pro okno.

EZS ústředna je ovládána pomocí SW na PC nebo mobilní aplikací, popřípadě LCD klávesnicí s čtečkou přímo v místě serverovny.

Na celé řešení, EZS, požadujeme záruku v délce trvání 24 měsíců.

## Specifikace minimálních požadavků technického řešení

*EZS ústředna (stupeň. č2 střední rizika):*

* Deska ústředny
* 16 zón
* 8 výstupů
* GSM TF komunikátor
* obousměrný IP port RS 485
* sběrnice RS 485,
* rozdělení až na 8 podsystémů
* možnost variability velkého sortimentu příslušenství

*PIR detektory (stupeň č. 2 střední rizika):*

* infradetektor pohybu dosah 11x12 m
* nastavitelná citlivost
* teplotní kompenzace
* NC kontakt
* možnost výměnných čoček pro dlouhý dosah

Požární detektory (certif. ZÚS - pro požární bezp. staveb):

* Optickouřový detektor
* automatická kompenzace zaprášení
* nastavitelná citlivost
* samoresetovací

*Magnetické kont. (stupeň č.2 střední rizika):*

* čtyřdrátový plastový kontakt
* temper smyčka
* povrchová montáž
* pracovní mezera 30 mm.

*Komunikační modul (stupeň č. 2 střední rizika):*

* universální kom. GSM

*Software:*

* grafický řídící a monitorovací program pro monitorování ústředen EZS
* min. s českou jazykovou mutací
* pro operační systém Windows

*Software mobilní:*

* software pro ovládání, přes mobilní aplikaci, EZS ústředny
* je určen pro správu systému

*Modul:*

* interface umožní připojit, na sběrnici, EZS ústřednu
* kontrola systému zapínání a vypínání
* kontrola vstupu a režimů

*Čtečka:*

* bezkontaktní
* čtecí dosah 3 cm
* formát Wiegand
* signalizace tříbarevná
* medium karta – přívěšek
* signalizace zvuková
* MIFARE, OSDP, Wiegand

*Siréna:*

* zálohovaná

## Klíčový depozit

Předmět celého řešení klíčového depozitu je jeho dodávka a montáž technologického řešení.

Systém klíčového depozitu (dále jen KPD) bude obsahovat úložné prostory pro 96 klíčů na RFID přívěscích s možností budoucího rozšíření dle potřeb klienta. Očekávané rozměry boxu jsou 69x95x20 cm, avšak tyto rozměry bude možné modulovat dle potřeby.

Poptávané řešení musí zahrnovat kompletní zprovoznění zařízení, včetně montáže a proškolení obsluhy. V ceně musí být rovněž zahrnut obslužný software, který umožní správu a ovládání systému.

KPD je určen k bezpečnému a řízenému uložení a výdeji klíčů pouze oprávněným osobám. Autorizace uživatele proběhne na základě přihlašovacího PIN kódu nebo bezkontaktní ID karty pomocí snímače karet. Dodávka bude zahrnovat veškerý potřebný software pro provoz a správu klíčového depozitu.

Jednotlivé údaje a oprávnění zaměstnanců zadá dodavatelem při instalaci celého řešení. Po proškolení musí být zadavatel schopen svými silami kvalifikovaně provádět administraci a správu klíčového depozitu.

Klíčový depozit bud koncipován jako “stand-alone“ zařízení. Zařízení zvládne fungovat autonomně bez přístupu k energii po dobu 24 hodin od výpadku. Ke správě držitelů karet a oprávnění se bude využívat vzdáleného počítače, který umožní administraci systému. Navrhované řešení bude spravováno přes počítačovou síť LAN. Zařízení musí umožnit případný požadavek na integraci do integrovaného bezpečnostního systému EISS. V případě integrace klíčového depozitu do systému EISS musí, objednatel, získat systémové řešení certifikované do čtvrté bezpečnostní třídy.

*Zásadní vlastnosti KPD:*

* Zvýšení zabezpečení: Zavedení pravidel, kdy klíče zůstávají v budově – snížení rizika ztráty klíčů.
* Snížení nákladů: Přenesení nákladů za ztracený klíč na odpovědnou osobu, redukce nákladů na evidenci, vydávání a správu klíčů, nepřetržitá dostupnost a evidence klíčů 24/7.
* Technologická integrace: Možnost využít stávající přístupové karty zákazníka pro snadné ovládání depozitů. Zařízení bude možné vybavit snímačem karet. Dále bude možné depozity propojit se systémem EISS, který umožní rozšířit funkčnost na depozitu.
* Celkové řešení: Depozitní systém bude navržen pro hromadnou správu a reporting. Bude obsahovat obslužný software, který umožňuje efektivní správu přístupů, záznamů a monitorování v reálném čase.
* Přizpůsobení firemní identitě: Bude mít možnost volby vzhledu zařízení, barevného provedení podle specifikace objednatele a umístění nemocničního loga na zařízení.
* Bez dodatečných poplatků za údržbu: Zařízení bude dodáno kompletně funkční a plně připravené k používání, aniž by byla v budoucnu nutná jakákoliv dodatečná údržba či servisní poplatky.

V místě instalace, Objednatel, zajistí následující součinnost:

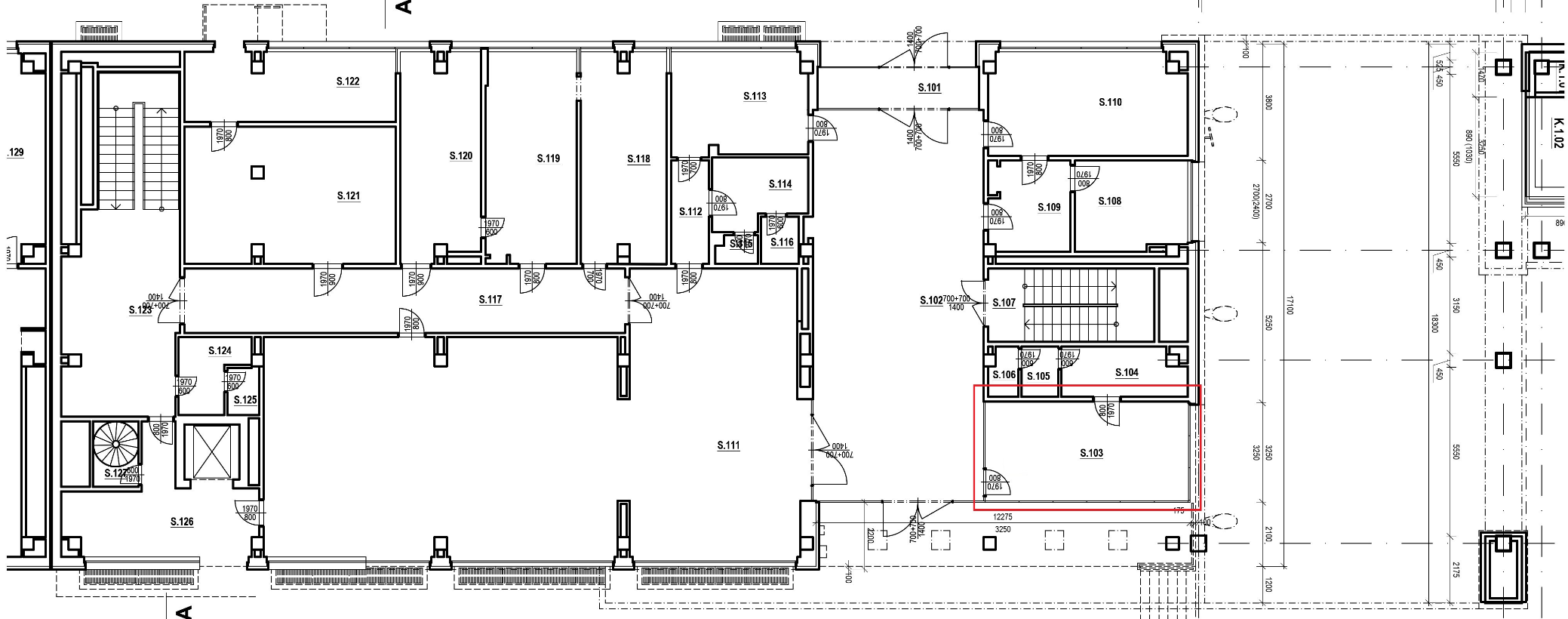
1. PC, nebo virtuální stroj pro instalaci softwarového vybavení depozitu (server).

2. Vzdálený přístup k PC se serverem prostřednictvím internetu po celou dobu realizace.

3. Revidovaný přívod 230V v místě instalace klíčového depozitu.

4. Port LAN v místě instalace depozitu, konektivita PC s klíčovým depozitem.

5. Vzdálený přístup ke všem technickým prostředkům pro realizaci klíčového depozitu před, během i po dobu trvání záruky.



*Obr. Místo instalace klíčového depozitu (viz také soubor Místnost pro instalaci klíčového depozitu.jpg)*

Na celé řešení, KPD, požadujeme záruku v délce trvání 24 měsíců.

## Specifikace minimálních požadavků technického řešení

|  |  |
| --- | --- |
| **Číslo požadavku** | **Specifikace minimálních funkčních a technických požadavků** |
| 1 | KPD musí umožňovat bezpečnou správu a synchronizaci uživatelů a identifikátorů (ID karet, otisků prstů, PINů) mezi depozity a IBŘS, dále přiřazování oprávnění na klíče, skupiny klíčů a předměty včetně jejich auditu. |
| 2 | KPD musí umožňovat přenos všech provozních událostí a poplachů do IBŘS pro zajištění okamžité reakce operátora a pro zpětné prohlížení událostí, monitoring aktuálního stavu KPD s návazností na ostatní bezpečnostní systémy integrované v IBŘS. |
| 2 | KPD musí být vybaven optickou signalizací stavu obsazenosti u jednotlivých pozic klíčů a schránek pomocí LED indikátorů. |
| 3 | KPD musí umožňovat monitoring aktuálního stavu klíčového depozitu, včetně stavů klíčů, obsazenosti schránek apod., v reálném čase prostřednictvím grafického rozhraní v IBŘS. |
| 4 | Systém musí být modulární a flexibilní, aby bylo možné nasadit pouze požadované funkce podle potřeb provozovatele. |
| 5 | Veškerá data o klíčích, předmětech a jejich manipulaci musí být uložena v zabezpečené databázi. |
| 6 | KPD musí disponovat možností rozšíření o konstrukční moduly pro bezpečné ukládání krátkých a dlouhých zbraní, včetně munice v samostatných schránkách se senzory identifikujícími stav přítomnosti zbraně či zásobníku v depozitu. |
| 7 | KPD musí disponovat možností kombinace způsobů ukládání klíčů a předmětů v rámci jednoho zařízení pro maximální flexibilitu. |
| 8 | KPD musí být provozuschopný v režimu 24/7 a umožnit správu uživatelů a jejich oprávnění v reálném čase. |
| 9 | KPD musí umožňovat zálohování energie na minimálně 24 hodin pro zajištění provozu zařízení při výpadku napájení. |
| 10 | KPD musí zajišťovat bezpečné uložení identifikačních karet ve formátu "ISO/IEC 7810" a zároveň umožňovat jejich přidělování, evidenci a sledování v IBŘS. |
| 11 | KPD musí umožňovat nastavení víceúrovňého zabezpečení přístupu, s využitím RFID identifikátorů, PIN kódů nebo biometrie. |
| 12 | Veškerá komunikace mezi KPD a obslužným software včetně IBŘS musí být šifrovaná. |
| 13 | KPD musí automaticky odhlašovat uživatele po dokončení operace, aby bylo zajištěno bezpečné ukončení procesů obsluhy. |
| 14 | KPD musí být vybaven systémem detekce neoprávněné manipulace se zařízením, např. proti odtržení od stěny. |
| 15 | Dvířka KPD musí být k dispozici v různých konstrukčních variantách, například z tvrzeného skla se zvýšenou odolností nebo z oceli. |
| 16 | KPD musí být vybaven funkcí odesílání notifikací provozních stavů a událostí (odebrání, vrácení klíče, předmětu či zbraně, jejich nevrácení ve stanovené lhůtě) prostřednictvím IBŘS, SMS nebo e-mailu. |
| 17 | Veškeré záznamy o manipulaci s klíči a předměty musí být uchovávány pro auditní účely. |
| 18 | KPD musí umožňovat sledování přítomnosti předmětů a klíčů pomocí optických senzorů, váhových senzorů nebo RFID. |
| 19 | Systém musí umožňovat rozšíření o další geograficky oddělené depozity, které budou společně a centrálně řízeny z prostředí IBŘS. |
| 20 | KPD musí podporovat uživatelskou administraci, např. přidání nebo odebrání klíčů a předmětů, bez omezení a přerušení provozu. |
| 21 | KPD musí umožnit rezervace klíčů a předmětů s časovým omezením, včetně řízení přístupu dle oprávnění. |
| 22 | KPD musí disponovat systémem pro pevné uzamčení klíčů v depozitu, které odolá hrubé síle. |
| 23 | KPD musí podporovat nouzový režim pro vyzvednutí klíčů pomocí servisního klíče, přičemž každá operace musí být zaznamenána v systému. |
| 24 | KPD musí disponovat možností umístění zákazníckého loga (např. na prosklených dvěřích). Musí umožňovat také různé varianty barevného provedení povrchové úpravy dle palety RAL. |
| 25 | KPD musí být možné vybavit různými typy nabíjecích systémů přímo ve schránkách (např. USB-C, 230V, micro USB apod.) |
| 26 | KPD musí umožňovat konstrukční zabudování DIN cylidrických vložek přímo do segmentů v zabezpečené vnitřní části depozitu. Do těchto cylidrických vložek musí být možné vložit a mechanicky uzamknout jednotlivé. Mechanické uvolnění klíčů v cylidrických vložkách je možné pouze na základě platné autorizace. |
| 27 | KPD musí podporovat napojení na Active Directory prostřednictvím IBŘS ve dvou úrovních: a) Single Sign On (SSO), b) Synchrozniace uživatelů - držitelů karet. |
| 28 | KPD musí umožnit vytvoření přístupových oprávnění pro více uživatelů na jeden klíč nebo předmět podle časových zón. |
| 29 | KPD musí podporovat propojení na systémy požárně bezpečnostního zařízení, aby v případě vyhlášení poplachu mohly být zpřístupněny klíče či jiné důležité předměty. |
| 30 | KPD musí disponovat možností archivace všech událostí s možností snadného filtrování podle klíče, předmětu, času nebo uživatele. |
| 31 | KPD musí umožňovat vzdálenou správu. |
| 32 | KPD musí splňovat certifikace pro uložení zbraní nebo jiných předmětů dle třídy S1 (ČSN EN 14450+A1) nebo RC2 (ČSN EN 1627). |
| 33 | KPD musí disponovat možností výběru různych velikostí barevného dotykového displeje pro ovládání. Velikost displeje až 21 palců. |
| 34 | KPD musí umožňit osazení akustické signalizace s vazbou na provozní stavy. |
| 35 | KPD musí umožňovat přímou instalaci alkoholtesterů. Na základě výsledku alkoholtestu je možné podmínit proces vydání/vrácení klíčů a předmětů. |
| 36 | KPD musí umožňovat osazení a zabudování kamery pro pořízení snímků během procesu autorizace fyzické obsluhy depozitu. Vizuální snímky musí být zaznamenány v historii událostí IBŘS. |