# Technická specifikace – Část 5 Aktivita 2 Zavedení systému jednotného přihlašování a dvou faktorové autentizace

Obsah

[1) Popis požadavků na řešení 3](#_Toc197343327)

[a) Minimální technické parametry softwarového nástroje pro jednotné přihlašování a dvoufaktorovou autentizaci (dle čl. 2.1.5.2. písm. a) zadávací dokumentace) 3](#_Toc197343328)

[b) Minimální technické parametry stacionárních čteček bezkontaktních karet (dle čl. 2.1.5.2. písm. b) zadávací dokumentace) 6](#_Toc197343329)

[c) Minimální technické parametry autentizačních předmětů (dle čl. 2.1.5.2. písm. c) zadávací dokumentace) 6](#_Toc197343330)

# Popis požadavků na řešení

## Minimální technické parametry softwarového nástroje pro jednotné přihlašování a dvoufaktorovou autentizaci (dle čl. 2.1.5.2. písm. a) zadávací dokumentace)

|  |
| --- |
| **Požadavek na funkcionalitu** |
| Obecné požadavky |
| Klientská část řešení musí podporovat Windows Desktop OS (Windows 10 a novější), Linuxové OS tenkých klientů a v případě mobilních klientských zařízení minimálně operační systémy rodiny Windows, iOS a Android. |
| Řešení bude ve výchozím stavu navrženo a dodáno jako vysoce dostupné, s odolností vůči výpadku jednoho serverového prvku, s minimálně dvěma vzájemně zastupitelnými prvky. Při výpadku jednoho prvku zůstává řešení plně funkční, zbylý funkční prvek/prvky nadále poskytují plnou funkčnost. K překlopení na funkční prvek/prvky musí dojít automaticky, bez nutnosti ručního zásahu, maximálně v jednotkách sekund. Všechny prvky si vzájemně replikují nastavení a data, v případě výpadku prvku tedy nedojde ke ztrátě nastavení či dat. Všechny prvky řešení musí být spravovány jako jeden celek, jednotnou správou z webové konzoly, napříč datovými centry, případně cloudy. |
| Serverová část řešení bude nasazena ve formě virtuálních strojů (podpora minimálně VMware vSphere, Microsoft Hyper-V). Virtuální stroje musí být možné, a ze strany výrobce podporované, provozovat v cloudu (podpora minimálně Microsoft Azure). Řešení musí být možné nasadit také v hybridním režimu, kdy jeden nebo více virtuálních strojů je provozováno v místním datovém centru a další virtuální stroj nebo stroje v cloudu, formou SaaS. |
| Řešení musí umožnovat definovat práva na činnosti ve správcovských nástrojích na základě členství v Active Directory skupinách. Řešení musí být schopno definovat různé úrovně administrátorských přístupů – delegování administrativních oprávnění – vytvořením kombinací (sad) oprávnění. |
| Řešení musí být integrováno na jednu nebo více instancí adresářových služeb Microsoft Active Directory Directory Services (AD DS). Identita – uživatelský účet – uživatele dodaného řešení musí odpovídat identitě v AD DS. Změny v AD DS (změny stavu účtu, atributů, členství ve skupinách) musí být automaticky synchronizovány s dodaným řešením. Řešení nesmí modifikovat schéma Active Directory. Dodané řešení musí být možné integrovat na další adresářové (LDAP) služby jiných výrobců. |
| Komunikace mezi jednotlivými komponentami řešení v rámci HTTPS komunikace musí být šifrována TLS protokolem minimálně verze 1.2, uložená citlivá data – zejména přihlašovací údaje uživatelů – musí být chráněna FIPS 140-2 validovaným šifrováním AES 256. |
| Více-faktorová autentizace |
| Řešení musí umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci, minimálně: kontaktní čipové karty (smart karty), bezkontaktní karty a předměty včetně karet NXP Mifare DesFire, bezkontaktní FIDO bezpečnostní karty a kontaktní FIDO USB klíče, USB tokeny, bezkontaktní RFID předměty, biometrické prvky (otisk prstu), login/heslo (s vazbou i bez vazby na adresářovou službu), a jejich vzájemné kombinace. Vyžádání druhého faktoru musí být možné definovat dynamicky, na základě splnění podmínky (např. uplynutí časového intervalu). |
| Řešení musí pro vybrané uživatele poskytnout funkci tzv. „Push“ autentizace a/nebo autentizace pomocí OTP (One-Time Password) pro přihlášení ke koncovým zařízením s Windows OS a do VPN prostřednictvím mobilní aplikace (podporované mobilní OS: minimálně Android a iOS). |
| Řešení musí umožnit volbu parametrů autentizačního PIN kódu pro více-faktorové ověřování (podobně, jako u hesla např. v Active Directory). Délku PINu v rozmezí alespoň od 4 do alespoň 16 znaků, musí umožnit exspiraci PIN kódu po definovaném časovém intervalu, musí umožnit použití jak čistě numerického PINu, tak PINu obsahujícího čísla a písmena a speciální znaky. Řešení dále musí umožnit vynucení historie PINu a zamezit uživateli, aby si při obnově PINu zvolil dříve jím použitý PIN kód (je požadováno, aby si systém pamatoval alespoň 8 posledních PINů). Řešení musí volitelně umožnit vynutit nastavení, které uživateli zamezí nastavit si snadno uhodnutelný PIN (minimálně nedovolit opakování stejných po sobě jdoucích znaků, jako např. „1111“ a jednoduchou číselnou řadu, jako např. „1234“). |
| Řešení musí obsahovat technologii pro automatizaci přihlašovacího procesu, která uživateli umožní přihlášení do vzdálené plochy s využitím již zadaných přihlašovacích pověření, bez nutnosti opakovaně zadávat přihlašovací údaje, potvrzovat připojovací dialogy, znovu použít autentizační předmět, znovu zadávat PIN kód. Tato technologie musí podporovat nejběžnější produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, VMware Horizon). |
| Řešení musí umožňovat režim redukovaného uživatelského rozhraní, tzv. "appliance mode", na tenkých klientech. V tomto režimu je běžné uživatelské rozhraní tenkého klienta nahrazeno přihlašovací obrazovkou pro více-faktorovou autentizaci. |
| Řešení musí umožnit nastavení různých kombinací přihlašovacích faktorů pomocí politik, a tyto politiky aplikovat na skupiny uživatelů, skupiny koncových zařízení, typy koncových zařízení s rozlišením alespoň koncová stanice s Windows/mobilní zařízení/server vzdálené plochy. |
| Řešení musí zajistit funkčnost více-faktorové autentizace pomocí bezkontaktních karet a předmětů i v případě, kdy klientské zařízení není připojeno k síti (je offline) nebo není dostupná serverová strana řešení. |
| Řešení musí poskytnout funkce více-faktorové autentizace na koncových (klientských) zařízeních používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce více-faktorové autentizace na koncovém (klientském) zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být více-faktorové ověření provedeno jménem konkrétního uživatele, tedy přihlašování musí být prováděno uživatelským Active Directory účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény. |
| Single Sign-On (SSO) |
| Řešení musí poskytovat funkci automatického přihlášení SSO (Single Sign-On) alespoň do následujících aplikací:  Fons Enterprise (Stapro), OpenLims (Stapro), EnvisLims (DSSoft), Helios Nefrit (Asseco), ShiftMaster (Ivar ID Poděbrady), WebKredit (Anete), IceWarp mail (Icewarp)  V případě webových aplikací musí být pro funkci SSO podporovány minimálně tyto prohlížeče: Microsoft Edge Chromium verze 120 a vyšší, Google Chrome verze 120 a vyšší. Dále musí být pro webové aplikace podporována autentizace pomocí protokolů SAML a OpenID Connect. |
| Řešení musí poskytovat funkci Single Sign-On do aplikací (popsaných v předchozím bodu) z koncových (klientských) zařízení používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce SSO do aplikací (popsaných v předchozím bodu) na koncovém zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být funkce SSO poskytovány jménem konkrétního uživatele, tedy přihlašování do aplikací musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény. |
| Řešení musí zajišťovat funkčnost SSO pro aplikace, jejichž klientská strana běží jak na fyzických stanicích, tak ve virtuální ploše – VDI, dále pro virtualizované aplikace a server vzdálené plochy. Řešení musí poskytnout plnou funkčnost SSO pro nejběžnější technologie virtualizace aplikací a desktopů na trhu (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, VMware Horizon). |
| Přihlašovací údaje do jednotlivých aplikací musí být dostupné jen příslušnému uživateli. Přihlašovací údaje do jednotlivých aplikací a systémů musí být šifrovány, a musí být ukládány na serverovou stranu řešení, aby byly dostupné na každé koncové stanici, ke které se uživatel přihlašuje. Systém musí umožnit, aby pro kritické aplikace bylo přihlášení pomocí SSO vynucováno. |
| Řešení musí umožnit funkci SSO přihlašování do aplikací jak identitou (účtem) z Active Directory, tak účtem spravovaným danou aplikací. Řešení musí dále poskytovat funkcionalitu Identity Provider (IdP). |
| Řešení musí obsahovat integrovaný správce hesel (Password Manager) pro všechny uživatele, s možností uživatelské správy. IT správce musí mít možnost nastavit, zda uživatel může přihlašovací údaje editovat nebo jen zobrazit, a dále, zda může zobrazit heslo v čitelné podobě. Funkce zobrazení hesla v čitelné podobě musí být možné dodatečně zabezpečit (např. vyžádáním hesla, PINu apod.). |
| Řešení musí obsahovat grafické uživatelské rozhraní pro vytváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní a uživatelsky přívětivé, bez nutnosti psát kód, programovat, používat řádkové příkazy a umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace uživatelsky, vlastními silami, bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu těchto aplikací. |
| Samoobslužný reset hesla |
| Řešení musí poskytnout integraci na funkci samoobslužného resetu hesla Active Directory účtu a musí umožnit vyvolání této funkce z přihlašovací obrazovky klientské stanice, bez nutnosti se předem přihlásit. |

## Minimální technické parametry stacionárních čteček bezkontaktních karet (dle čl. 2.1.5.2. písm. b) zadávací dokumentace)

|  |
| --- |
| **Čtečky karet** |
| Požadované parametry stacionárních čteček bezkontaktních karet, resp. tokenů:   * 500KS * Pracovní frekvence: 13,56 MHz * Podpora bezkontaktních karet/předmětů: rodina NXP Mifare® * Rozhraní: připojitelná přes USB * Typ: externí * Napájení: přes USB rozhraní * Formát: stolní * Přenos dat: zabezpečený, přes API (nesmí simulovat klávesnici) * Kompatibilita OS: Windows 10 a vyšší |

## Minimální technické parametry autentizačních předmětů (dle čl. 2.1.5.2. písm. c) zadávací dokumentace)

|  |
| --- |
| Autentizační předměty |
| * 700 ks - karet * 280 ks – náramků * 20 ks - tokenů   Požadované parametry bezkontaktních tokenů:  TOKEN   * Pracovní frekvence: 125 kHz a 13,56 MHz * Standardy bezkontaktních předmětů: EM4102/EM4200 a NXP Mifare® minimálně S50, 1kb * Formát: přívěšek (fob) * Provedení: plastový, mechanicky odolný, možnost potisku nebo gravírování   KARTA   * Dodaná čipová karta musí být ve velikosti bankovní karty * Dodaná karta bude obsahovat bezkontaktní čipy dle ISO/IEC 14443 a odvozených norem. Karta musí obsahovat vysokofrekvenční čip 13.56 MHz, minimálně NXP MIFARE S50, 1kb pro bezkontaktní dvou-faktorové přihlašování ke koncovým (klientským) zařízením a zároveň 125 KHz čip EM420x pro stávající systémy (stravovací, přístupový). * Dodaná karta obsahuje výše uvedené kontaktní a bezkontaktní čipy v jednom ověřovacím předmětu. * Požadované parametry karty: * formát: ID-1 * provedení umožňující potisk karty   NÁRAMEK   * Dodaný čipový náramek bude obsahovat bezkontaktní čip/čipy dle ISO/IEC 14443 a odvozených norem. * Náramek musí obsahovat vysokofrekvenční čip 13.56 MHz, minimálně NXP MIFARE S50, 1kb pro bezkontaktní dvou-faktorové přihlašování ke koncovým (klientským) zařízením. * Požadované parametry bezkontaktního náramku: * materiál: voděodolný, silikonová guma * potisk náramku: název organizace (Zadavatele), rytý, vylitý barvou |