Názov predmetu zákazky: Centrálny manažment identít (CMI)

Predmetom zákazky je dodanie softvérového nástroja pre Centrálny manažment identít (ďalej aj „nástroj“ alebo „CMI“ príp. "IDM") pre 1000 používateľov v zmysle požiadaviek uvedených nižšie vrátane súvisiacich služieb inštalácie, konfigurácie a zaškolenia

Popis súčasného stavu na strane verejného obstarávateľa

V podmienkach verejného obstarávateľa v súčasnosti neexistuje jednotný centralizovaný systém na správu identít. Aktuálna agenda správy identít sa rieši cez Microsoft Active Directory, kde sú zapojené pracovné stanice používateľov a oprávnenia pre prístup k aplikačnej vrstve sú riešené prostredníctvom definovaných oprávnení cez group membership.

1. Špecifikácia predmetu zákazky Centrálny manažment identít

Verejný obstarávateľ má momentálne 300 interných zamestnancov, 50 pracovníkov na dohodu, 40 externistov. Počet 1000 ráta s rezervou pri rastúcom počte zamestnancov. Verejný obstarávateľ požaduje aby nástroj pre správu identít pre minimálne 1000 používateľov spĺňal nasledujúce funkčné požiadavky:

Základné požiadavky na CMI

1. Musí byť lokálne integrovateľný do existujúceho IT prostredia verejného obstarávateľa (t. j. pre všetky prevádzkované platformy, systémy a aplikácie).
2. Musí podporovať import zamestnaneckých údajov a organizačnej štruktúry s existujúcim modulom Asseco SPIN/ Kros Olymp. Požadovaná periodicita synchronizácie údajov je 1x za 24 hodín.
3. Musí podporovať integráciu s MS Active Directory a s existujúcim dochádzkovým systémom Aktion Next.
4. Musí umožňovať automatické vytváranie a vypínanie identít podľa ich stavu v module Asseco SPIN/ Kros Olymp. Aktuálne sa v rámci realizácie projektu počíta iba so systémami uvedenými v opise predmetu zákazky. Musí umožňovať automatické notifikácie priameho nadriadeného pri vzniku novej identity podriadeného zamestnanca a bezpečné doručenie jeho iniciálneho hesla.
5. Musí umožňovať doplnenie informácii ako mail, telefón, pracovne zaradenie pre každú identitu.
6. Musí podporovať evidenciu súhlasov GDPR.
7. Musí podporovať implementáciu do cloudového prostredia.
8. Musí umožňovať automatické notifikácie IT oddelenia (distribučná skupina) o vzniku novej identity na overenie prípadne doplnenie požadovaných oprávnení.
9. Musí umožňovať automatické pridelenia oprávnení (provisioning/deprovisioning) odvodeného od úrovne zaradenia do organizačnej štruktúry (napr. group membership „HR“ pre všetkých zamestnancov HR oddelenia použitý na zdieľanie HR dokumentov).

10. Musí umožňovať efektívnu a jednoduchú tvorbu procesných schvaľovaní (workflow schvaľovania) na základe definovaných požiadaviek prístupu v súlade s organizačnou štruktúrou a následným automatizovaným priradením/odobratím práv a privilégií entite.
11. Musí umožňovať používateľskú tvorbu reportov a dashboardov.
12. Musí umožňovať časové povolenie prístupu identity k zdrojom.
13. Musí umožňovať podporu okamžitého zakázania identity (hodinová výpoveď) a dočasné povolenie identity (neskoré predlženie pomeru v Asseco SPIN1/ Kros Olymp).
14. Musí umožňovať podporu zakladania dodatočných užívateľov priamo do nástroja IDM (externisti, dodávatelia a pod.).
15. Musí byť schopný zamedziť vytvoreniu duplicitných identít.
16. Musí umožňovať jednotný login, generovať heslo podľa voliteľnej politiky hesla do IDM a AD.
17. Musí mať k dispozícii samoobslužný portál pre používateľskú správu hesiel a používateľského profilu/ identity:
    a. musí byť lokalizovaný minimálne do Anglického jazyka. Preferovaný je slovenský jazyk, ale minimálne požiadavky spĺňa aj Angličtina.
    b. musí zaznamenávať históriu vykonaných udalostí používateľom,
    c. musí používateľovi ponúkať mechanizmus na obnovenie zabudnutého hesla aj formou kontrolných otázok, zaslania overenia na registrovaný email, alebo zariadenie
    d. musí používateľovi ponúkať mechanizmus na vyžiadanie dodatočných oprávnení z katalógu rolí a oprávnení.
    e. musí poskytovať možnosť hlásenia chýb a problémov
    f. musí poskytovať možnosť zadávať žiadosti o softvérové licencie
    g. musí poskytovať funkcie samoobslužnej správy, ktoré umožňujú používateľom a povereným správcom vytvárať, aktualizovať a odstraňovať informácie o účte uložené v profile používateľa, ako sú atribúty identity, používateľské meno a heslo, preferencie používateľa a nastavenia ochrany osobných údajov
    h. musí poskytovať používateľský generátor hesiel
18. Musí ponúkať automatické a plnohodnotné auditovanie, monitorovanie, zaznamenávanie činností, reportovanie a notifikácie pokrývajúce aktivity správcov a používateľov v celom nástroji minimálne v rozsahu podľa platnej legislatívy SR.
19. Musí poskytovať informácie vo forme zostáv a reportov pre poskytnutie informácii na analýzu mapovania prístupov používateľov k zdrojom, pokročilú analýzu a klasifikáciu rizík, analýza partnerských skupín, detekcia anomálií, monitorovanie privilegovaného prístupu, proaktívnu analytika entít a prístupov, a podrobnú analýzu oddelenia povinností (SoD).
20. Musí poskytovať možnosť využitia 2FA pre mobilne zariadenia. To znamená, že pokiaľ súčasťou softvérového balíčku CMI nie je služba 2FA/MFA, tak je potrebné ho dodať ako separátny softvérový balíček tvoriaci súčasť plnenia zo strany (úspešného) uchádzača. Požiadavky na 2FA respektíve MFA sú nasledovné.
    - Natívna integrácia s ponúkaným CMI riešením.
    - Podpora minimálne 1000 užívateľov
    - Musí podporovať hardvérové a softvérové tokeny.

- Musí podporovať operačné systémy IOS a Android, pre mobilné OTP
- Musí podporovať push notifikácie a biometrickú autentifikáciu
- Musí podporovať autentifikáciu on-premise ale aj do cloudových app. V prípade on- premise riešenia musí byt implementované v režime aktiv/ aktiv.
- Musí podporovať nasledovne protokoly:
  - Rádius pre autentifikáciu
  - SAML/OIDC pre autentifikáciu
  - REST API pre administráciu – správa tokenov a užívateľov
  - Agent integrácie pre autentifikáciu pre desktopy s OS Windows a Linux
- Musí podporovať virtuálne platformy. Napríklad HyperV a VMware
- Musí mat self- service konzolu pre užívateľov
- Musí podporovať HA konfiguráciu pre autentifikačný server
- Musí poskytovať automatizovanú distribúciu softvérových tokenov
- Nástroj musí umožňovať použiť hybridnú architektúru. To znamená podpora Saas aplikácii spolu s lokálnymi zdrojmi a to VPN, Servery, stolové počítače-laptopy, pričom databáza používateľov (AD-LDAP) zostávajú on-premise.
- Nástroj musí podporovať pred definovane funkcie výkazov a to:
  - zoznam všetkých užívateľov
  - zoznam užívateľov s počtom neúspešných prihlásení
  - zoznam užívateľov, ktorý sa neprihlásili a nepoužili 2FA/MFA od definovaného dátumu.
  - Automatické posielanie reportov mailom na základe auditného plánu a to len špecifickým užívateľom.
- Nástroj musí poskytovať možnosť viacerých rolí, ako je administrátor, audítor, helpdesk agent, bezpečnostný administrátor.
- Prístup pre administrátora je len s možnosťou 2FA/MFA.
- V prípade uzamknutia účtu musí byť táto informácia automaticky poslaná na helpdesk support ponúkaného nástroja v rámci organizácie verejného obstarávateľa.

21. Musí poskytovať autorizačné služby s metódou riadenia a pridelenia oprávnení minimálne RBAC, DAC, MAC. Musí ponúkať proaktívnu kontrolu dodržiavania nastavených bezpečnostných a prevádzkových pravidiel.
22. Musí byť schopný zohľadniť kroky životného cyklu identít a organizačnej štruktúry (nástup, výstup, zmena útvaru, zmena pracovnej pozície, vznik/zmena/zrušenie útvaru).
23. Musí ponúkať možnosť SMTP a SMS notifikácií v procese životného cyklu zamestnancov a v procese manuálnej správy.
24. Musí ponúkať možnosť re-certifikácie (pravidelného auditu) prístupových oprávnení.
25. Musí ponúkať možnosť zamedzenia priradenia konfliktných oprávnení (kontrola SOD medzi rolami v žiadosti / voči už priradeným roliam užívateľa).
26. Musí ponúkať vysokú dostupnosť.
27. Musí poskytovať manažment minimálne 1000 identít s možnosťou škálovateľnosti v počte miliónov identít.
28. Musí zabezpečiť dostatočný výkon pre spracovanie overení identít a poskytnutých oprávnení v definovanom rozsahu

Uvedené konektory/ integračné rozhrania sú požadované vzhľadom na to, že nimi verejný obstarávateľ disponuje a využíva ich pre zabezpečenie fungovania úradu/ rezortu.

Požiadavky na Spracovanie udalostí a synchronizácia používateľských údajov medzi komponentmi CMI

1. Nástroj musí mať mechanizmy na spracovanie a spracovanie udalostí zodpovedné za regulovanú synchronizáciu informácií o používateľoch a pripravené konektory na spracovanie a synchronizáciu používateľských účtov, ktoré v čase ich výberu a nákupu podporujú tieto systémy:
   - Databázy: Oracle, MS SQL Server, My SQL, Sybase, Postgress a ďalšie prostredníctvom ovládačov ODBC.
   - Adresárové a doménové služby: Microsoft Active Directory, LDAP v.3
   - Poštové systémy: Microsoft Exchange
   - Groupware systémy: MS SharePoint
   - Operačné systémy: Microsoft Windows Server 2003/2008/2012 a vyššie, Red Hat
2. Nástroj musí mať funkciu "poistky"(Fuse) na zastavenie spracovania požiadaviek, keď počet zistených zmien prekročí prah definovaný používateľom. Prahové hodnoty by sa mali vyjadriť ako percento zmien. Spracovanie systému pri aktivácii poistiek nesmie meniť údaje.
3. Nástroj musí umožniť nastavenie "poistiek" pre spracované informácie samostatne pre každý typ operácie, napr. pre Nové, Aktualizované a Vymazané záznamy. Informácie o spustení poistky by sa mali zaznamenať v denníku auditu systému.
4. Nástroj musí byť vybavený mechanizmom na obojsmernú výmenu informácií:
   - Výmena musí mapovať udalosť, ktorá nastala v jednom systéme, na udalosť v druhom systéme.
   - Udalosť, ktorá nastane v nadradenom (zdrojovom) module, napr. vytvorenie používateľského účtu, sa musí odzrkadliť analogickou udalosťou vytvorením účtu s príslušným heslom v príslušných pripojených systémoch,
   - Podobne, ak je používateľský účet zablokovaný v nadradenom systéme - táto udalosť sa musí prejaviť príslušnou akciou (zablokovaním) v pripojených systémoch,
5. Nástroj musí umožňovať integráciu len na čítanie (read only) , t. j. automatické čítanie údajov o účtoch a oprávneniach z integrovaného systému a vydávanie príkazov správcom na úpravu týchto údajov prostredníctvom úloh CMI, e-mailových oznámení alebo príkazov pre Service Desk. Spôsob objednávania zmien by mal byť konfigurovateľný v CMI.
6. Nástroj musí mať možnosť prideľovať a delegovať administratívne oprávnenia týkajúce sa možnosti konfigurovať a spravovať tok a replikáciu informácií o používateľoch v nástroji pre správu identít (CMI).
7. Nástroj musí prezentovať informácie o identite a účtoch a oprávneniach vlastnených používateľom v spravovaných systémoch, pričom oprávnenia sa prezentujú v zmysle priameho pridelenia a nepriameho pridelenia, napr. prostredníctvom iných oprávnení alebo rolí. Nástroj musí byť schopný rozlišovať medzi stavom pridelenia oprávnení.

8. Nástroj musí umožňovať zmenu hesiel v pripojených systémoch ako je AD.
9. Nástroj musí byť vybavený možnosťou prideľovať a delegovať práva (na úlohy, požiadavky, zobrazenie údajov atď.) v nadradených právach udelených v CMI inému používateľovi. Náhradník preberá všetky práva od zastupovanej osoby.

Požiadavky na správu prístupu a zabezpečenie zodpovednosti za používanie účtu

1. Ponúkaný nástroj CMI musí umožňovať správu viac ako jedného používateľského účtu (prihlasovacie meno/heslo) v rámci každého z integrovaných systémov (aplikácií)
2. CMI musí umožňovať správu ďalších používateľských účtov (operátor, správca atď.). Proces riadenia by sa mal realizovať na základe modulu Workflow.
3. Oprávnenia (prístup) k pripojeným systémom sa musia udeľovať na základe rolí alebo oprávnení prijatých v procese podávania žiadosti.
4. Nástroj musí umožňovať vytváranie profilov oprávnení pre používateľov spolu s cestami pre akceptovanie týchto profilov určenými používateľmi alebo skupinami používateľov.
5. Nástroj musí umožniť zmenu organizačného útvaru alebo pozície zamestnancom vrátane spustenia procesov kontroly oprávnení automatického odňatia/priznania oprávnení alebo spustenia kontroly oprávnení vyplývajúcich z takejto zmeny.
6. Nástroj musí poskytovať možnosť monitorovať a vykazovať pridelené roly k používateľským identitám, najmä tie, ktoré poskytujú prístup k privilegovaným účtom.
7. Nástroj musí umožniť prezentáciu informácií o tom, prostredníctvom ktorého z účtov v spravovanom systéme má používateľ pridelené konkrétne oprávnenie.
8. Udelenie oprávnení k účtom môže byť časovo neobmedzené alebo časovo obmedzené (platí dátum skončenia platnosti takéhoto oprávnenia).

Požiadavky na Elektronické mechanizmy toku informácií/požiadaviek (Workflow)

1. Nástroj musí mať zabudované mechanizmy na implementáciu akceptačných a schvaľovacích pracovných postupov pre roly a prístup a oprávnenia v prepojených systémoch.
2. Modul Workflow musí byť neoddeliteľnou súčasťou CMI a musí byť od toho istého výrobcu.
3. Modul Workflow musí poskytovať možnosť vytvárať jednostupňové alebo viacstupňové rozvetvené pracovné postupy akceptácie na súčasné (v jednej aplikácii) udelenie a zrušenie prístupu do akéhokoľvek systému/zdroja pomocou priameho priradenia a nepriameho priradenia pomocou objektov rolí....
4. Modul Workflow musí poskytovať úplnú podporu procesu od žiadosti až po realizáciu zmeny vyplývajúcej zo žiadosti. Napr. žiadosť o pridelenie členstva používateľa v skupine AD sa môže považovať za úplnú až po tom, ako nástroj prečíta, že používateľský účet je priradený k skupine. Tento mechanizmus by mal fungovať pre obojsmerné integrované systémy aj systémy určené len na čítanie.

5. Modul Workflow musí byť webový a musí umožňovať používateľom pracovať s nástrojom aspoň pomocou špecifických prehliadačov definovaných nižšie v časti „Nefunkčné požiadavky“.
6. Modul pracovného postupu musí byť neoddeliteľnou súčasťou dodaného nástroja a jeho používanie nesmie vyžadovať druhé prihlásenie.
7. Modul Workflow by mal obsahovať mechanizmus umožňujúci osobe vydávajúcej rozhodnutie delegovať spracovanie všetkých pridelených procesov na inú osobu na určitý čas (tzv. zastupovanie). Funkcie dostupné z úrovne správcu a používateľa pre všetkých používateľov.
8. Modul Workflow musí obsahovať mechanizmus umožňujúci osobe vydávajúcej rozhodnutie delegovať vybraný proces (alebo procesy) na inú osobu.
9. Modul Workflow musí mať funkcionalitu na definovanie procesu akceptácie takým spôsobom, aby bolo možné v jednej aplikácii spracovať čiastočnú akceptáciu, napr. akceptovať len 2 z 3 požadovaných objektov, pričom účinok rozhodnutia musí byť zmapovaný v audit trail aj v reportoch.
10. Mechanizmus pracovného postupu musí poskytovať možnosť udeliť oprávnenia jednej osobe alebo skupine osôb.
11. Mechanizmy pracovného postupu musia poskytovať možnosť prideliť udelenie prístupových práv alebo rolí na presne definované a vybrané obdobie počas akceptácie.
12. Modul Workflow musí poskytovať grafické prostredie, prístupné prostredníctvom špecifických prehliadačov, ako sú definované nižšie v časti „Nefunkčné požiadavky“, bez potreby inštalácie dodatočného softvéru alebo tzv. plug-inov, v ktorom bude možné graficky vykonávať operácie konfigurácie a plánovania procesu a cesty prijatia.
13. Modul Workflow musí poskytovať používateľom (iniciátorom) možnosť sledovať proces schvaľovania udeľovania práv. Priebeh aplikácie musí byť k dispozícii v grafickej podobe, ako aj vo forme následných úloh.
14. Modul Workflow musí mať funkcionalitu, ktorá umožní vykonať zmeny v procese schvaľovania. Uplatnené zmeny by sa mali zohľadniť pri začatí nového procesu.
15. CMI musí mať možnosť konfigurovať modul pracovného toku a obmedziť vybraným používateľom možnosť iniciovať žiadosti
16. Modul Workflow musí mať možnosť vytvárať vlastné formuláre na udeľovanie žiadostí a schválení.

Požiadavky na mechanizmus udeľovania práv používateľom prostredníctvom rolí

1. Nástroj musí poskytovať možnosť definovať roly spojené so špecifickými oprávneniami používateľov v pripojených systémoch a aplikáciách
2. Nástroj musí upozorniť na výskyt potenciálneho porušenia z dôvodu oddelenia oprávnení už vo fáze definovania/modifikácie rolí.
3. Definícia a modifikácia rolí musí mať proces schvaľovania rolí pred ich zverejnením a sprístupnením na použitie
4. Rola (vyššej úrovne) musí umožňovať pokrytie oprávnení v niekoľkých samostatných aplikáciách
5. Nástroj musí byť schopný udeliť, zrušiť a upraviť roly pridelené používateľovi

6. Spracovanie rolí musí zahŕňať možnosť definovať vzájomne sa vylučujúce roly na ktorejkoľvek úrovni hierarchie oprávnení a nástroj musí mať možnosť kontrolovať (akceptovať) udeľovanie rolí, ktoré sa vzájomne vylučujú z dôvodu oddelenia povinností.
7. Nástroj musí mať zabudovaný mechanizmus na varovanie pred udelením rolí používateľovi, ktoré boli definované ako vzájomne sa vylučujúce.
8. Spracovanie rolí musí umožňovať definovanie hierarchických rolí, t. j. musí byť možné definovať roly v CMI ako súčet iných rolí
9. Nástroj musí byť schopný udeliť používateľovi určitú rolu na určité časové obdobie.
10. Nástroj musí poskytovať používateľovi možnosť zobraziť informácie o pridelených rolách na portáli používateľa. Táto možnosť sa vzťahuje na priame priradenia aj na nepriame priradenia prostredníctvom hlavnej úlohy.
11. Nástroj musí poskytovať používateľovi, ako aj jeho nadriadenému možnosť požiadať o rolu a sledovať stav tejto žiadosti.
12. Nástroj musí mať možnosť vytvárať prehľady/súhrny všetkých rolí, ktoré boli dané alebo odobraté používateľovi (vrátane všetkých údajov o zamestnancoch/ kontraktoroch). V správe by mali byť uvedené aj osoby, ktoré tieto operácie prijali, spolu s dátumami jednotlivých operácií.
13. Nástroj musí umožňovať podávanie žiadostí o rolu zamestnancovi aj jeho nadriadenému. Nadriadený musí mať možnosť požiadať o pridelenie úloh pre svojich podriadených. Každý nadriadený má prístup k zoznamu svojich priamych podriadených.
14. Nástroj musí byť schopný vytvárať pokročilé (viacstupňové schvaľovacie) pracovné postupy so schválením žiadosti o pridelenie roly
15. Nástroj musí mať grafickú konzolu podporovanú špecifickými prehliadačmi na čítanie aktuálnych rolí používateľov.
16. Poskytnutý nástroj správy identít musí podporovať procesy pridávania, modifikácie a odstraňovania rolí na základe procesu akceptácie
17. Nástroj musí mať mechanizmus na simuláciu účinkov procesu zmeny roly vo forme prezentácie toho, aké zmeny sa uskutočnia v oprávneniach používateľov po vykonaní požiadavky na zmenu roly.

Požiadavky na pravidlá kompatibility a oddelenia privilégií

1. Nástroj na riadenie identít (CMI) musí mať mechanizmus, ktorý umožňuje vytvárať pravidlá na dohľad nad dodržiavaním predpisov a oddelením práv.
2. Vytváranie pravidiel zhody musí byť možné z rozhrania systému správy identít prostredníctvom grafického rozhrania (bez potreby používať externé programovacie knižnice alebo zadávať kód).
3. Mechanizmus pravidiel musí umožňovať vytváranie pravidiel oddelenia oprávnení vo forme definícií dvojíc vzájomne sa vylučujúcich oprávnení a súborov vzájomne sa vylučujúcich oprávnení. Musí byť možné definovať vylúčenie na rôznych úrovniach, napr. rola v CMI a privilégium v riadenom systéme (napr. skupina AD).
4. Mechanizmus oddelenia oprávnení musí podporovať vnorenie oprávnení. Ak je pravidlo oddelenia definované pre dve oprávnenia, nástroj musí zistiť porušenie

pravidla aj v prípade, že sú pridelené ľubovoľne vnorené roly obsahujúce konfliktné oprávnenia.

5. Mechanizmus pravidiel musí umožňovať vytváranie pravidiel, ktoré overujú, či majú prístup k určitým oprávneniam len určité osoby. Napríklad je možné definovať pravidlo, ktoré detekuje používateľov s právami špecifickými pre účtovné oddelenie a nepatriacich do účtovného oddelenia.
6. Mechanizmus pravidiel musí umožňovať vytváranie pravidiel členstva v rolách s voliteľným mechanizmom automatického udeľovania a odoberania rolí, t. j. v závislosti od konfigurácie definovaného pravidla:
    - Používateľom, ktorí spĺňajú pravidlo o členstve v role a nemajú pridelenú rolu, sa má rola prideliť automaticky alebo sa má zobraziť upozornenie na porušenie pravidla.
    - Používateľom, ktorí majú rolu a nespĺňajú pravidlo členstva, sa má rola automaticky odobrať alebo sa má zobraziť upozornenie na porušenie pravidla.
7. Mechanizmus pravidiel musí umožňovať vytváranie pravidiel overujúcich, či používatelia majú všetky práva vyplývajúce z rolí, ktoré im boli pridelené, spolu s voliteľným mechanizmom automatického udeľovania práv, t. j. v závislosti od konfigurácie konkrétneho pravidla sa používateľom roly, ktorí nemajú práva zadané v role, majú práva udeliť automaticky alebo sa má zobraziť upozornenie na porušenie pravidla.
8. Nástroj musí umožňovať vytváranie pravidiel, ktoré zisťujú udeľovanie oprávnení v spravovanom systéme obchádzaním aplikácie v systéme správy identít. Musí byť možné nakonfigurovať reakciu na takúto udalosť, napr. automatické zrušenie oprávnenia.
9. Množiny osôb a objektov rolí a privilégií používaných v pravidlách musia byť definovateľné enumeratívne, ako aj prostredníctvom špecifických kritérií objektov a prostredníctvom asociácií, napr. určené osoby, osoby so špecifickými hodnotami atribútov, osoby so špecifickými rolami, osoby s rolami so špecifickými parametrami.
10. Nástroj musí prepočítavať pravidlá v reálnom čase a upozorňovať na výskyt porušenia pravidiel v dôsledku vykonávanej činnosti aspoň v prípade:
    - žiadosť o udelenie alebo zrušenie práv
    - žiadosť o zmenu definície roly
11. Nástroj riadenia identít musí mať zabudované aspoň tieto typy recertifikácie, pripravené na použitie ihneď po inštalácii:
    - Prehľad práv používateľov
    - Preskúmanie úlohy (rozhodnutie o ponechaní alebo deaktivácii úlohy)
    - Prehľad definícií rolí - prehľad oprávnení pridelených rolám
    - Kontrola účtov (bežných~~, osirelých~~ a zdieľaných účtov)
12. V rámci recertifikačnej kampane musí mať kontrolór k dispozícii aspoň tieto činnosti: ponechať si nárok, odobrať nárok, odobrať nárok po stanovenom čase.
13. V rámci recertifikácie používateľských oprávnení musí byť možné skontrolovať všetky úrovne/typy oprávnení - roly CMI, oprávnenia spravovaného systému, skupiny, aplikačné roly v závislosti od úrovne integrácie so spravovaným systémom.

Požiadavky na protokolovanie, monitorovanie, podávanie správ, zodpovednosť v rámci CMI

1. Nástroj musí mať zabudovaný a integrovaný modul na podávanie správ a audit, ktorý poskytuje ten istý výrobca, ktorý vyrába CMI.
2. Nástroj musí zhromažďovať a uchovávať informácie o používateľoch a ich účtoch a oprávneniach v pripojenom IS, ako aj o všetkých operáciách a súboroch priamo alebo nepriamo (prostredníctvom aplikácií) spojených s identitou
3. Nástroj musí byť schopný automaticky spúšťať predpripravené správy o identitách používateľov na pravidelnej báze v určitom definovanom čase a musí byť schopný automaticky posielať tieto správy elektronickou poštou (e-mailom).
4. Nástroj musí mať možnosť vytvárať správy o požiadavkách na pracovné postupy a o pridelených rolách a profiloch (oprávneniach) používateľov.
5. Musí byť možné zobraziť informácie a preddefinované harmonogramy pre generovanie správ
6. Nástroj musí poskytovať možnosť samostatne definovať šablóny správ a exportovať ich do súborov xls (alebo xlsx), csv, pdf, xml, html a rtf. Definícia šablón musí byť dostupná pomocou nástroja zabudovaného do CMI a pomocou jednotného rozhrania.
7. Musí byť možné upravovať a modifikovať štandardné šablóny správ poskytované výrobcom CMI len pomocou nástrojov zabudovaných do systémového rozhrania.
8. Nástroj musí umožniť zobrazenie historických údajov v reálnom čase týkajúcich sa žiadostí, oprávnení a rolí, o ktoré používateľ požiadal. CMI musí umožniť vykazovanie týchto údajov definovateľným spôsobom
9. Nástroj musí byť schopný odhaliť operácie vytvárania alebo modifikácie používateľských účtov a/alebo skupín v MS Active Directory, ktoré sa vykonávajú mimo nástroja pre správu identít (obchádzajú ho). Po zistení uvedených operácií musí byť nástroj schopný vykonať každú z týchto činností (spoločne alebo samostatne):
    - odoslať e-mailové oznámenie určenej osobe so základnými informáciami o účte.
    - spustenie pracovného postupu s konkrétnym procesom definovaným v CMI na automatické odstránenie takýchto neoprávnených zmien a operácií v službe MS AD.
10. Musí byť tiež možné získať údaje zo systémov a aplikácií (napr. pomocou konektorov plochých súborov), ktoré nie sú priamo spravované v CMI.
11. CMI musí zaznamenávať zmeny v identite používateľa (zmena mena, ID zamestnanca)
12. CMI musí zaznamenávať a uchovávať informácie o vykonaných požiadavkách na pracovný postup a pridelených rolách, profiloch používateľov
13. CMI musí umožniť vykazovanie podľa jednotlivých parametrov identity, žiadostí a typov dokumentov priradených k identitám priamo alebo nepriamo prostredníctvom žiadostí
14. Všetky akcie používateľa (zobrazenie/editácia/odstránenie) definované správcom CMI musia byť uložené v systémových protokoloch prístupných z aplikácie.

Systémové požiadavky na Centrálny manažment identít

1. CMI musí byť možné spustiť aspoň na týchto operačných systémoch:
    - Red Hat Enterprise Linux Server verzia 6.5 alebo vyššia

- SUSE Linux 12.2

2. CMI musí poskytovať integrácie s týmito systémami:
   - modulom Asseco SPIN
   - Kros Olymp
   - MS Active Directory
   - Existujúcim dochádzkovým systémom Aktion Next
   - Multifaktorovú autentifikáciu
   - RSA Archer

   Tieto integrácie musia byt aj súčasťou dodávky riešenia
3. CMI musí zaručiť možnosť spustiť komponenty zodpovedné za synchronizáciu (konektory) na lokálnom serveri CMI.
4. CMI musí zaručiť bezpečnosť a integritu prenášaných údajov medzi CMI a konektormi spustenými na vzdialených serveroch.

Požiadavky na správu hesiel v informačných systémoch

1. CMI musí umožniť zmenu hesla v súvisiacich systémoch, t. j.
   - AD (prihlásenie do systému Windows)
   - ~~SAP~~
   - Existujúcim dochádzkovým systémom Aktion Next
2. CMI musí umožniť používateľom meniť heslá v súvisiacich systémoch samostatne, bez účasti správcov IS pomocou špecializovaného nástroja (portálu).
3. CMI musí umožniť identifikáciu identity prostredníctvom súboru definovateľných podporných otázok.
4. CMI musí vynútiť zmenu hesla v súvisiacom systéme v rámci definovaného času odozvy v závislosti od IT prostredia verejného obstarávateľa - nie však dlhšie ako trojnásobok času na vykonanie operácie v zdrojovom systéme.
5. Každá žiadosť o zmenu hesla v pridružených systémoch musí byť potvrdená formou e-mailovej správy do poštovej schránky používateľa a uložená v záznamoch CMI.

Nefunkčné požiadavky

1. Vyhľadávanie v databáze CMI - nesmie byť dlhšie ako 5 sekúnd
   - Vytvorenie identity v CMI na základe údajov zo zdrojového systému - nesmie byť dlhšie ako 3 minúty
   - Vytvorenie účtu v zdrojovom systéme pomocou CMI vykonané počas štandardnej prevádzky systému bez hromadných operácií spustených na pozadí atď. - nie dlhšie ako trojnásobok času vykonávania v zdrojovom systéme
   - Udelenie/odstránenie oprávnení/blokovanie konta v integrovanom systéme pomocou CMI vykonané počas štandardnej prevádzky systému bez hromadných operácií atď. prebiehajúcich na pozadí. - nie viac ako 3-násobok času vykonávania v zdrojovom systéme
2. Ponúkaný CMI musí byť dostupný a podporovaný výrobcom v týchto prehliadačoch:
   - Microsoft Edge
   - Mozilla Firefox v30+

- Google Chrome v31+
- Apple Safari v10.x+

3. Ak uchádzač poskytuje dodatočné licencie pre CMI, poskytnuté licencie musia umožňovať neobmedzené používanie. To znamená použitie perpetuálnych licencií. Táto požiadavka sa nevzťahuje na open source
4. CMI musí podporovať Perpetuálne licencie a nie subscription. Táto požiadavka sa nevzťahuje na open source
5.
6. CMI musí zabezpečiť nepretržitú dostupnosť systému 24 hodín denne, 7 dní v týždni.
7. CMI musí umožniť prístup ku všetkým systémovým prostriedkom a modulom, ktoré sú k dispozícii používateľovi prostredníctvom jednotnej webovej konzoly bez potreby dodatočného overovania.
8. CMI musí informovať používateľa, keď sa vykonávajú operácie, ktoré spôsobujú, že používateľské rozhranie čaká na pripravenosť.
9. Rozsiahly systém oprávnení na údaje a funkcie (používateľ vidí len konkrétne údaje o zamestnancoch, ku ktorým má pridelené oprávnenia)
10. CMI a všetky jeho komponenty by mali byť prevádzkované na hardvérovej/softvérovej štandardnej platforme. ~~Minimálne požiadavky sú nasledovne:~~
    ~~2x procesor Intel Xeon 2,6 Ghz, 20M Cache~~
    ~~Minimálne 48GB RAM~~
    ~~Minimálne 800GB SSD disky~~
    ~~2x 1Gbit Ethernet~~
    ~~Remote management~~
    ~~**Dodanie hardvér NIE je súčasťou predmetu zákazky.**~~
11. CMI musí v každom svojom module umožňovať jednotné vyhľadávanie objektov podľa jednotlivých zbieraných parametrov (napr. pre používateľa priezvisko, meno, číslo atď.
12. Nástroj musí umožňovať používanie šifrovania prenosu údajov, napr. SSL
13. Nástroj musí mať možnosť integrácie so systémami triedy SIEM (štandardizovaný systémový log).
14. Nástroj musí mať možnosť podporovať mechanizmy uchovávania údajov (vymazanie po určitej časovej perióde) – účet, aplikácie, oprávnenia.
15. CMI nástroj musí byt štandardný a široko používaný v rámci vertikál Industry, ako je napríklad Healthcare, Automotive, Manufacturing, Finance.
16. Ponúkaný nástroj CMI musí obsahovať v rámci softwarového licenčného balíčka aj licenciu na internú databázu používanú pre CMI softvérové riešenie.
17. Ponúkaný nástroj CMI musí byť iba softvérového charakteru a nie v podobe hardvérového apliance.
18. Nástroj musí podporovať out of the box reportingu pre štandardné frameworky. To znamená, že nástroj musí poskytovať pred definované reporty na štandardné rámce.
19. Natívna funkcia zastupiteľnosti v rámci organizácie, na schvaľovanie požiadaviek
20. Centrálne úložisko musí poskytovať možnosť prideliť lokálne administrátorské práva iným používateľom. Riadenie musí prebiehať prostredníctvom definovateľných administratívnych rolí.
21. Centrálne úložisko informácii (CUI), respektíve databáza musí byt centrálne spravovaná.

22. Centrálne úložisko informácií sa musí spravovať pomocou webového nástroja na správu.
23. CMI musí mať zabudované centrálne úložisko informácií (Databázu) o používateľoch a ich oprávneniach v IS spolu s informáciami o ich príslušnosti k organizačnej jednotke, aby bolo možné používateľa jednoznačne identifikovať.
24. CMI musí umožňovať šifrovanie poverení a hesiel počas prenosu aj ukladania (napr. SSL).
25. Nástroj musí podporovať SCIM na programovanie a mazanie identít.
26. Nástroj musí podporovať natívnu integráciu na RSA Archer. Je to z dôvodu, že verejný obstarávateľ disponuje týmto kľúčovým systémov v oblasti kybernetickej bezpečnosti. Natívna integrácia musí spĺňať nasledovné požiadavky:
    - RSA Archer vie cez natívnu integráciu zbierať a vymieňať údaje o používateľských účtoch a roliach v rámci GRC riešenia.
    - Tak isto vie zbierať informácie o užívateľských prístupoch, atribútoch identít, porušení pravidiel,
    - Integrácia bude poskytovať podrobné údaje o aplikáciách z RSA Archer, ako sú nároky a prístupy.
    - Integrácia dodá funkcionality poskytnutia a zrušenia účtov v RSA Archer.
    - Nasledovné atribúty musia byť zbierané cez natívnu integráciu z nástroja RSA Archer:
        a. Užívateľky účet a prislúchajúce atribúty, a to emailová adresa, meno účtu, status účtu, Meno užívateľa, Priezvisko užívateľa, pridelený identifikátor užívateľa, Oddelenie, na ktorom pracuje, posledný dátum prihlásenia, Spoločnosť, telefónne číslo, status uzamknutia účtu, status vypnutia účtu.
        b. Skupina a prislúchajúce atribúty, ako Meno skupiny a Identifikátor skupiny.
        c. Rola a prislúchajúce atribúty, ako je Identifikátor role, Meno role, popis role, alias role, dátum poslednej zmeny.

Ďalšie požiadavky na predmet dodávky:

1. Úspešný uchádzač musí k ponúkanému nástroju pre správu identít dodať dokumentáciu pre správu nástroja CMI, školenie IDM administrátora a užívateľskú príručku.
2. Nástroj musí obsahovať grafické webové rozhranie pre správu CMI bez nutnosti inštalácie „hrubého“ klienta.
3. Výrobca musí zabezpečovať vydávanie aktualizácií a opráv v závislosti na publikovaných a oznámených zraniteľnostiach.
4. Komunikácia medzi serverom a klientami musí byť šifrovaná.
5. Požaduje sa dodávka dvoch inštancií - testovaciu a produkčnú.
6. Verejný obstarávateľ požaduje v ponuke uviesť presný názov ponúkaného produktu.
7. Verejný obstarávateľ požaduje v rámci ponuky vypracovať a predložiť návrh vo vysokej dostupnosti .
8. Verejný obstarávateľ požaduje pre On-Prem riešenie špecifikovať HW komponenty, ktoré však nepredstavujú súčasť predmetu zákazky.
9. Nástroj musí mať možnosť post implementačnej podpory a podporné služby pre produkt a jeho prevádzku.

10. Úspešný uchádzač poskytne odborné školenie minimálne pre dvoch administrátorov a všetkých užívateľov, a to vo fáze nasadenia nastroja do produkcie.
11. Zabezpečovanie vydávanie a aktualizácií a opráv Diela v závislosti na publikovaných a oznámených zraniteľnostiach počas obdobia záručnej doby.
12. Uchádzač v ponuke uvedie názov produktov, na ktorých ponúka CMI, vrátane produktových identifikátorov.
13. Úspešný uchádzač poskytne high level architektúru CMI a popis ako bude prebiehať integrácia.
14. Verejný obstarávateľ v rámci ponuky uviesť odhad množstvo človekodní a rolí (MD a profily), ktoré je potrebné zabezpečiť na strane verejného obstarávateľa.
15. Úspešný uchádzač dodá v rámci plnenia predmetu zákazky administrátorskú príručku v Anglickom Jazyku, preferované je v Slovenčine. Tak isto dodá inštalačnú príručku v Slovenskom Jazyku.

16. <u>Bezpečnostný projekt</u>

Úspešný uchádzač dodá počas implementácie aj bezpečnostný projekt, ktorý bude vypracovaný na základe požiadaviek zo Zákona č. 95/2019 Z.z. o informačných technológiách verejnej správe a o zmene a doplnení niektorých zákonov a vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Minimálne požadované súčasti v rámci bezpečnostného projektu sú nasledovné

- Návrh bezpečnostnej architektúry.
- Zoznam a klasifikácia aktív Zoznam a analýza zákonov, ktoré sa vzťahujú na tento projekt a aké požiadavky z toho vyplývajú
- Zoznam Log informácii, aké generuje CMI nastroj a vytvoriť odporúčania na Use Case pre nástroj SIEM
- Vytvorenie Rizikovej analýzy kvalitatívnou metódou, ako je požadované vo vyhláške ÚPVII č. 179/2020 Z.z. a podľa odporúčania NBU. https://www.nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf
- Vytvorenie zoznam Rizík s vysokou úrovňou.
- Vykonanie bezpečnostnej analýzy zameranej na bezpečnosť CMI nástroja a jeho integrácií.
- Vykonanie skenovanie zraniteľností. Túto aktivitu vykoná verejný obstarávateľ vlastným nástrojom, Výsledky budú priložené ako príloha bezpečnostného projektu.
- Vykonanie Data Privacy Impact analýzy. (DPIA)
- Vytvorenie Business Impact analýzy (BIA)
- Vytvorenie Plánov zálohy a plánov obnovy.
- Vytvorenie Business continuity plánu pre CMI nástroj a jeho komponenty. Vytvorenie R&R dokumentu, na rozdelenie úloh medzi verejným obstarávateľom a úspešných uchádzačom ako zhotoviteľom.

- Vytvorenie dokumentu podľa OWASP v4.0.2. a výsledku zhody. Pokiaľ má úspešný uchádzač príp. výrobca ponúkaného nástroja takúto analýzu už vypracovanú v rámci software developmentu, môže byť použitá aj táto.

Lehota dodávky:

Lehota dodávky je najneskôr do 6 mesiacov na nadobudnutia účinnosti zmluvy.

Zoznam výrazov a skratiek:

Odborný výraz	Vysvetlenie výrazu
MD	ManDay alebo človekodeň.
NCZI	Národné centrum zdravotníckych informácií
HW	Hardvér
SW	Softvér
On-Prem	V priestoroch organizácie alebo datacentra NCZI
CUI	Centrálne úložisko informácii
CMI	Centrálny manažment identít. Tak isto to je IDM.
SIEM	Security Incident and Event Management
SSL	Secure Sockets Layer
AD	Active Directory
IDM	Identity manažment
2FA	Dvojfaktorová autentifikácia
MFA	Multifaktorová autentifikácia
SCIM	System for Cross-domain Identity Management
Verejný obstarávateľ	Národné centrum zdravotníckych informácií