**Príloha č. 1**

# Opis predmetu zákazky

Predmetom zákazky je vypracovanie štúdie realizovateľnosti/uskutočniteľnosti vrátane návrhu procesného a technického riešenia zabezpečenia manažmentu celého životného cyklu správy privilegovaných účtov naprieč všetkými IT organizačnými útvarmi banky (ďalej aj „Štúdia“) a konzultačnej podpory v predpokladanom objeme maximálne 96 osobohodín na obdobie 24 mesiacov od odovzdania a prevzatia Štúdie.

V súčasnosti je v Národnej banke Slovenska (ďalej aj „NBS) pokrytá správa privilegovaných účtov manuálne, z tohto dôvodu verejný obstarávateľ požaduje pripraviť Štúdiu procesného a technického riešenia pre oblasť správy riadenia privilegovaných účtov, ktorá pokryje celý životný cyklus privilegovaného účtu (role) poskytne rozhrania pre všetky (príp. aj iné) IS aj tie novovznikajúce .

## 1. Požiadavky na obsah a rozsah Štúdie:

1.1 Vypracovať Štúdiu na bezproblémovú implementáciu procesov a nástrojov pre manažment správy privilegovaných účtov (napr. Administrátor, root) technických účtov, personalizovaných administrátorských účtov v podmienkach NBS.

1.2 Očakávané základné aktivity v rámci vypracovania Štúdie sú:

1.2.1 Zmapovanie a zhodnotenie (AS IS) súčasného stavu v oblasti správy privilegovaných účtov v NBS (tzn. procesy, role, postupy, štandardy atď.) a existujúcej IT infraštruktúry

1.2.2 Zber, sumarizácia a analýza (aj očakávaných/predpokladaných) požiadaviek na budúce riešenie správy privilegovaných účtov.

1.2.3 Príprava návrhu vhodného riešenia pre PAM (ďalej len Správa privilegovaných účtov - Privilege Acces Mananagment) využívania (chápeme ako interne poskytovanú službu odborom OIT v NBS) a informačnú architektúru a s tým súvisiace procesy, politiky a nástroje.

1.2.4 Vypracovanie viacerých návrhov riešenia pre PAM ich porovnanie a vypracovanie komplexného technického návrhu celobankového riešenia pre všetky IS v NBS a pre preferované riešenie, vrátane tzv. Cost – Benefit Analýzy (ďalej aj „CBA“).

1.2.5 Vypracovanie plánu implementácie všetkých (vyššie uvedených) navrhovaných zmien do praxe.

1.3 Výstupom bude Štúdia , ktorá bude obsahovať:

1.3.1 Zhodnotenie súčasného stavu používania správy privilegovaných účtov technického riešenia a jeho IT podpory v NBS.

1.3.2 Návrh riešenia v NBS v oblasti správy privilegovaných účtov, vrátane plánu jej implementácie.

1.3.3 Definíciu rolí, prípadné zlúčenie rolí , vrátane identifikácie nezlučiteľných rolí.

1.3.4 Definíciu a základné vlastnosti a funkcionality správy privilegovaných účtov.

1.3.5 Stratégiu využívania správy privilegovaných účtov, informačná architektúra, politiky a procesy, organizačne popísať workflow – toky.

1.3.6 Návrh personálneho zabezpečenia prevádzky.

1.3.7 Vypracovanie CBA (Cost Benefit Analýza) a TCO (Celkové náklady na vlastníctvo - finančný odhad), vrátane odhadu pre vhodný licenčný model v prostredí NBS.

1.3.8 Porovnanie minimálne 3-toch produktov nasadených v rutinnej prevádzke a posúdenie vhodnosti pre potreby NBS.

1.3.9 Popis procesov vo forme BPMN, technologická a aplikačná vrstva vo forme Archimate.

1.4 Verejný obstarávateľ požaduje vypracovanie Štúdie od úspešného uchádzača do troch mesiacov odo dňa nadobudnutia účinnosti zmluvy. Výstupy budú dodané elektronicky v niektorom z bežných formátov MS Office (MS Word, MS Excel).

## 2. Popis jednotlivých častí zákazky

2.1 Zhodnotenie súčasného stavu v NBS:
Táto časť bude zameraná na mapovanie a zhodnotenie aktuálneho (AS-IS) stavu správy privilegovaných účtov, jednotlivých oblastí týkajúcich sa životného cyklu (systémy, procesy, organizácia, technológie...) v NBS ako základného východiska pri prípravu ďalších krokov.

2.1.1 V jej rámci sa uskutočnia potrebné analytické aktivity a stretnutia s odbornými pracovníkmi s cieľom získať všetky potrebné informácie o aktuálnej situácii, očakávaných externých a interných požiadavkách, bariérach, rozhraniach na iné IS a možných obmedzeniach

2.1.2 Rovnako bude v tejto časti vykonané zhodnotenie stavu systémov, technológie a infraštruktúry, ktoré sú aktuálne používané v NBS.

Ďalšou oblasťou, ktorá bude v tejto časti analyzovaná a zohľadnená pri návrhu riešenia je aj relevantná legislatíva (externá, interná, EU...), týkajúca sa problematiky riešenej Štúdiou. Výstupom tejto časti bude analýza existujúceho stavu, identifikácia požiadaviek, očakávaných potrieb a obmedzení, prípadných bariér pre túto oblasť, vrátane zhodnotenia existujúcej architektúry, procesu, rozhraní, technológie a infraštruktúry.

2.2 Základné predpoklady a ciele:
Táto časť bude zameraná na návrh priorít a cieľov NBS v oblasti správy privilegovaných účtov detailný popis predpokladov a tiež aj z nich vyplývajúcich kritérií na výber (dizajn) potrebného riešenia. Rovnako bude potrebné pripraviť aj návrh štandardného procesu a pracovné toky. Úspešný uchádzač tu tiež popíše očakávané prínosy, ktoré by mohli byť prostredníctvom centrálnej správy privilegovaných účtov dosiahnuté, rovnako aj prípadné identifikované nevýhody.

Výstupom tejto časti bude:

a) návrh priorít a cieľov, bariér a rizík ich dosiahnutia,
b) návrh kritérií pre výber vhodného technického riešenia,

2.3 Návrh odporúčaného riešenia:
Táto časť bude zameraná na vypracovanie návrhu komplexného technického riešenia, ktoré bude spĺňať požiadavky a kritéria definované v predchádzajúcich krokoch. Úspešný uchádzač v rámci Štúdie porovná/zhodnotí viacero alternatívnych riešení, avšak vo výsledku musí odporučiť len jedno, to najvýhodnejšie riešenie pre NBS. Odporúčané riešenie bude v tejto časti podrobne popísané (aplikačná architektúra, technologická, dátová a bezpečnostná architektúra, rozhrania...) tak, aby bolo možné oceniť, prípadne jeho dodávku (napr. prieskumom trhu). V tejto časti tiež úspešný uchádzač popíše všetky relevantné predpoklady na jeho prevádzku v budúcnosti (dostupnosť, úroveň podpory a pod.).

Výstupom tejto časti bude detailný popis odporúčaného procesného a technického riešenia pre NBS, ktoré bude možné následne (bez úprav) použiť ako Opis predmetu zákazky v procese obstarávania tohto diela, porovnanie tohto riešenia so súčasným stavom (tzv. Gap analýza) a podrobný plán implementácie navrhovaného riešenia, ktorý bude obsahovať popis potrebných implementačných aktivít (vytvorenie) a zmien, vrátane potrebných úprav interných riadiacich aktov a postupov, odporúčaný časový harmonogram, potrebné organizačné zabezpečenie, spôsob mitigácie rizík / riešenie závislostí a prípadnú potrebu organizácie školiacich (a podobných) aktivít. .

2.4 Analýza nákladov a prínosov odporúčaného riešenia:
Táto časť bude zameraná na prípravu tzv . CBA odporúčaného riešenia, ktorá porovná na časovej osi (pre obdobie 4-6 rokov, podľa navrhovanej stratégie) vyčíslené predpokladané (TCO – Total Cost of Ownership) náklady na zavedenie riešenia (prípadne vývoj, licencie, HW...) a vyvolané náklady riešenia s kvantifikovanými identifikovanými potenciálnymi (kvantitatívne, aj kvalitatívne) benefitmi navrhovaného riešenia. Rovnako úspešný uchádzač v rámci CBA vyčísli aj cash flow v jednotlivých rokoch.

Výstupy jednotlivých častí budú dodané vo formáte MS Office, vrátene architektonických modelov vo formáte Archimate, detailný popis pre procesy vo formáte bpmn.

## 3. Opis projektu

Vypracovanie štúdie realizovateľnosti pre implementáciu procesov a nástrojov na zabezpečenie kompletného cyklu manažmentu správy privilegovaných účtov (napr. Administrátor, root) technických účtov, administrátorských účtov v podmienkach NBS.

**Cieľom projektu je :**

1) Zaintegrovať do štúdie realizovateľnosti všetky zákaznícke služby IT ( Informačné systémy ) a technické služby IT ( infraštruktúra IS ) pod spoločnú správu privilegovaných účtov, bez možnosti priameho prístupu k dotknutým systémom, iba cez správu privilegovaných účtov. Výnimkou sú služby, ktoré musia mať samostatné riešenie vyplývajúcich z osobitného účelu alebo vyplývajúcej osobitnej politiky z ECB
2) Vytvoriť stratégiu využívania správy privilegovaných účtov ( chápeme ako poskytovanú službu v NBS) a s tým súvisiace procesy, politiky a nástroje. Elektronická správa privilegovaných účtov zabezpečí celý životný cyklus ( Vrátane nahradenia papierových obálok k privilegovaným účtom a rieši zastupovanie administrátorov) a nahradí súčasné postupy správy administrátorských hesiel a to najmä :
   a) Prijatie alebo vytvorenie požiadavky na privilegovaný účet (role).
   b) Kontrola a schválenie privilegovaných účtov (role).
   c) Sprístupňovanie, prideľovanie oprávnení v prípade potreby, bez znalosti potreby hesla. (Riešenie prístupu k systémom aj v prípade nedostupnosti povereného personálu).
   d) Sledovanie životného cyklu privilegovaných účtov od vzniku až po exspiráciu administrátorského účtu.
   e) Ukončenie platností privilegovaných účtov (role).
3) Zadefinovať informačný proces pre vytvorenie a správu privilegovaného účtu (workflow) , proces a schvaľovacie pracovné toky.
4) Zefektívnenie a zjednodušenie práce administrátorov (Odbúravanie papierovej formy a dokladovania).
5) Zvýšenie komfortu, (Vypracovanie scenára pre homeoffice, Integrácia Správy privilegovaných účtov cez 2FA).
6) Poskytnutie rozhrania pre IS a rozšírenie integrácie na všetky poskytované technické služby IT (nielen na OIT).
7) Vypracovanie prevádzkových postupov v prípade nefunkčnosti Správy privilegovaných účtov
8) Zrušenie archivácie hesiel v obálkach (v papierovej forme).

**Zdôvodnenie projektu**

Realizovanie tohto projektu je potrebné pre zefektívnenie súčasnej práce v NBS pri správe s privilegovanými účtami. Ide najmä o zvýšenie bezpečnosti spravovaných služieb IT prostredníctvom centralizovaného riadeného prístupu k privilegovaným účtom. Pôjde aj zvýšenie produktivity, zlepšenie kooperácie, zníženie papierového a manuálneho balastu a obálok na správu privilegovaných účtov, ktoré bude dostupné pre všetky IS v NBS.

Napr. sa ide o:

- skrátenie času potrebného na doručenie obálky s prístupom na privilegovaný účet
- urýchlenie a zjednodušenie prístupu k požadovaným privilegovaným účtom
- zníženie nákladov na papierové uchovávanie a likvidáciu obálok s privilegovanými účtami

- kontrola životného cyklu a výmeny hesla k privilegovaným účtom
- úspora nákladov na FTE v zjednodušení procesov na uchovávanie hesiel k privilegovaným účtom
- lepší prehľad nad kontrolou a dodržaním procesu
- automatizáciu zabezpečenia tejto činnosti v NBS
- úsporu – odbúranie likvidácie obálok s privilegovanými účtami a manuálnej správy privilegovaných účtov

**Požadované výstupy:**

1) Definícia rolí, prípadné zlúčenie rolí , vrátane identifikácie nezlučiteľných rolí.
2) Definícia vlastností a funkcionality správy privilegovaných účtov.
3) Stratégia využívania správy privilegovaných účtov, informačná architektúra, politiky a procesy, organizačne popísať workflow – toky.
4) Návrh personálneho zabezpečenia prevádzky.
5) Definovať finančné zabezpečenie a možné scenáre harmonogramu realizácie projektu v podmienkach NBS (Plán nasadania harmonogramu podľa navrhovaných postupov).
6) Vypracovanie CBA (Cost Benefit Analýzy) a TCO (Celkových náklady na vlastníctvo - finančný odhad), podľa šablóny ktorá sa nachádza v prílohe , vrátane odhadu pre vhodný licenčný model v prostredí NBS.
7) Porovnanie minimálne 3-toch produktov nasadených v rutinnej prevádzke a posúdenie vhodnosti pre potreby NBS.
8) Popis procesov vo forme BPMN, technologická a aplikačná vrstva vo forme Archimate.

**Obmedzenia a predpoklady:**

Obmedzenia sú spojené hlavne s:

1) rezistenciou pracovníkov voči zmene a pokračovanie v zaužívaných postupoch,
2) nedostatočnou motiváciou interných pracovníkov administrátorov,
3) nesplnením očakávaní a zjednodušenia procesov,
4) nedostatočnou angažovanosťou pri realizácií projektu ako aj v období po jeho ukončení a do riadneho adaptovania a stabilizovania procesov.

**Zainteresované strany:**

Medzi zainteresované strany patria nasledovné útvary :
OIT , Ostatné organizačné útvary v NBS.

**Požiadavky na systém:**

1) riadenie prístupu ku všetkým privilegovaným účtom (nielen pre admin účty Administrátor, root a technické účty, ale aj pre personalizované admin účty) s použitím 2FA,
2) riešenie uchováva heslo (ktoré je anonymizované pre správcu) správca nepozná heslo k cieľovému systému len ho použije (zavolá ho v rámci bežného pracovného postupu pri použití),
3) vytváranie auditných záznamov o využívaní privilegovaných účtov,
4) vysoká dostupnosť systému najneskôr do 2-och hodín,
5) zabezpečiť ukladanie hesiel v centrálnej databáze,
6) podporovať roly podľa aktuálne používaného procesu (nastaviteľné prístupy k heslám podľa rolí),
7) možnosť nastavenia viacerých politík pre komplexnosť hesla a pravidelnosť výmeny hesiel privilegovaných účtov (čas exspirácie) pre rôzne skupiny admin účtov (technické účty a účty správcov),
8) systém musí mať vlastné zálohovanie / archivovanie alebo podporovať externé zálohovacie systémy (napr. NetBackup) pri zachovaní vysokej bezpečnosti (minimálne 1 predchádzajúci rok).
9) Podpora 2FA (v súčasnosti NBS využíva smart card login (PKI), RSA SecurID) v závislosti od kritickosti systému.

10) Podpora 2FA – podľa kritickosti systému. Požiadavky na štandardnú úroveň autentifikácie (dvojfaktorová autentizácia, napr. heslo/PIN skombinované s jednorazovým heslom ) (HOTP/TOTP a pod., nie však SMS kódy), alebo heslo/PIN skombinované so softvérovým alebo hardvérovým certifikátom. Prípustná je aj autentizácia certifikátom, kde prístup k súkromnému kľúču je chránený heslom/PIN a ktorý uzamkne kľúč po niekoľkých neúspešných pokusoch. Vhodné príklady: ESCK PKISW certifikát, MS authenticator. Pokročilá úroveň autentifikácie je dvojfaktorová autentizácia, napr. heslo/PIN skombinované s tokenom, kde token je fyzicky oddelené zariadenie (iné ako zariadenie z ktorého sa používateľ prihlasuje aj na ktoré sa prihlasuje). Vhodné príklady: RSA SecurID token, HW certifikát vydaný ESCB-PKI alebo všeobecne dôveryhodnou CA.
11) možnosť pridať dodatočné informácie o účtoch (napr. názov systému, DB, zariadenia),
12) reporty o účtoch (názov systému, posledná zmena hesla, čas exspirácie a pod.),
13) možnosť notifikácie pri zmene hesla k privilegovanému účtu. dostupnosť systému cez web rozhranie,
14) možnosť ukladať okrem hesiel aj certifikátov, PIN kódy, súbory so secret informáciami,
15) v prípade výpadku HTP dostupnosť na ZTP, požitie aj v prípade režimu práce s homeoffice,
16) využitie jump servera pre kontrolovaný prístup do infraštruktúry (aj pre externých používateľov) a odstránenie anonymity vo využívaní zdieľaných admin účtov (root, admin, backup),
17) možnosť rozšírením licencií (modulov) riešiť privilegovaný prístup pre celé prostredie NBS,
18) dodávateľ môže v rámci Štúdie navrhnúť rozšírenie požiadaviek na systém pre správu privilegovaných účtov o vhodné doplnenia, vychádzajúc z najnovším preverených postupov tkz „ best practises “.

**Požiadavky na integráciu s ďalšími prevádzkovanými službami IT**

1) s AD - minimálne v rozsahu, že vie načítať AD kontá správcov a technické účty
2) so skenerom zraniteľností (Tenable.sc) - systém musí byť podporovaný skenerom zraniteľností Tenable.sc a umožniť využitie účtov spravovaných v systéme na skenovanie zraniteľností (Windows, SSH, Oracle credentials a pod.). (naplnenie požiadavky je možné dohľadať v dokumentácii Tenable.sc.)
3) s Monitoringom bezpečnosti IT (systém slúžiaci na zber a vyhodnocovanie auditných a bezpečnostných udalostí v informačných systémoch a infraštruktúrach IS) – logovanie auditných záznamov o využívaní privilegovaných účtov, prístupu k heslám
4) s Monitoringom infraštruktúry IT (centrálne systémy pre operačný monitoring infraštruktúry IT a informačných systémov

**Požiadavky na procesy**

1) Popísať proces pre riadenie rolí (privilegovaných identít) a autorizačných pravidiel .
2) Popísať procesy na pravidelné automatizované zmeny hesla privilegovaných prístupov.
3) Popísať schvaľovací proces vytváraní privilegovaných prístupov, zmeny vlastníkov privilegovaných prístupov, ako aj modifikácie, blokovania, odobratia či prenosy privilegovaných prístupov.
4) Popísať proces životného cyklu privilegovaných prístupov v navrhovanom riešení
5) Popísať prevádzkový proces k správe privilegovaných prístupov pre administrátorov

**Charakteristika prostredia NBS**:

Služby IT zahŕňajú okrem iných aj systémy s OS Linux, Windows, aktívne sieťové prvky, komponenty VMware infraštruktúry, databázové systémy (napr. Oracle, MS SQL) atď.

**Vysvetlenie pojmu privilegovaný účet**

Pojem privilegovaný účet označuje účet (account) v informačnom systéme, ktorý má špecifické oprávnenia, t.j. účty typu root v Linux/UNIX systémoch, účty typu Administrator vo Windows systémoch, systémové účty používané aplikáciami alebo zdieľané účty (technologické účty), ktoré nie sú viazané na jedinú fyzickú osobu. S týmito účtami pracujú privilegovaní používatelia. Pojem

privilegovaný používateľ označuje fyzickú osobu, ktorá používa privilegované účty. Ide o pracovníkov prevádzky, dodávateľov alebo vývojárov. Cieľový systém označuje systém, na ktorý sa privilegovaný používateľ pripája prostredníctvom privilegovaných účtov.

**Čo nie je cieľom projektu :**

Cieľom projektu nie je :

1) Dodanie systému správy privilegovaných účtov pre SWIFT, dodanie systému pre 2FA.
2) Skomplikovanie systému riadenia správy privilegovaných účtov.
3) Predimenzované riešenie.

Úspešný uchádzač je povinný vypracovať Štúdiu tak, aby mohla byť použitá ako podklad vo verejnej súťaži na realizáciu zákazky, ktorej predmetom bude procesné a technické riešenie zabezpečenia manažmentu celého životného cyklu správy privilegovaných účtov naprieč všetkými IT organizačnými útvarmi banky a aby spĺňala požiadavky pre vypracovanie opisu predmetu zákazky stanovené príslušnými ustanoveniami zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Technické požiadavky nesmú byť diskriminačné a nesmú sa odvolávať na konkrétneho výrobcu, výrobný postup, obchodné označenie, patent, typ, oblasť alebo miesto pôvodu alebo výroby, ak by tým dochádzalo k znevýhodneniu alebo k vylúčeniu určitých záujemcov alebo tovarov, ak si to nevyžaduje predmet zákazky. Takýto odkaz možno použiť len vtedy, ak nemožno opísať predmet zákazky dostatočne presne a zrozumiteľne, a takýto odkaz musí byť doplnený slovami "alebo ekvivalentný".