

ПРИЛОГ 2

ПОЗИВА ЗА ПОДНОШЕЊЕ ПОНУДЕ ЗА НАБАВКУ РЕШЕЊА ЗА УПРАВЉАЊЕ ДИГИТАЛНИМ ИДЕНТИТЕТИМА И ПРИСТУПОМ, број: С32-2-4812 од 17.09.2026.године

Функционални захтеви ИАМ решења:

Предмет набавке је испорука и имплементације решења за управљање дигиталним идентитетима и приступом - Identity and Access Management (IAM).

1. Имплементација ИАМ решења мора обухватити:
 - (1) Анализу тренутних процеса управљања дигиталним идентитетима и приступом, идентификација недостатака и регулаторна усклађеност;
 - (2) Имплементација новог ИАМ решења и интеграција са ресурсима (10 апликација) које ће бити дефинисане у оквиру фазе Анализе.
2. Резултат Анализе (1) мора да буде:
 - 2.1. Извештај о процени ИАМ у организацији (*IAM Assessment Report*)
 - 2.2. План имплементација са архитектуром препорученог ИАМ решења
3. Понуђач мора да успостави робустан оквир за управљање ИАМ решењем и идентитетима у банци усклађен са регулативом Републике Србије и другим релевантим међународним стандардима као што су GDPR, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27701, PSD2, EBA ICT, PCI DSS и сл.
4. Извршити свеобухватну процену тренутног стања управљања дигиталним идентитетима, управљања приступом, аутентификацијом, привилегованим приступом и могућности управљања животним циклусом идентитета у организацији у свим окружењима: локално, *Cloud* и хибридно.
5. Процена и документоване зрелост управљања ИАМ-ом, организационе одговорности, структуре одговорности, процесе доношења одлука и постојеће оперативне моделе, укључујући идентификацију недостатака, ризика и могућности за побољшање.
6. Процена ефикасности модела контроле приступа, укључујући контролу приступа засновану на улогама (RBAC), контролу приступа засновану на атрибутима (ABAC), поделу дужности (SoD), управљање привилегованим приступом и процедуре приступа у хитним случајевима (*break-glass*).
7. Процена контроле безбедности идентитета, укључујући механизме аутентификације, вишефакторску аутентификацију (MFA), једнократну пријаву (SSO), протоколе федерације, услуге директорија, управљање привилегованим приступом, евидентирање, праћење и могућности заштите од претњи идентитетима.
8. Провести процене ризика повезаних с идентитетима, које обухватају ризике *cyber* безбедности, инсајдерске претње, прекомерне привилегије, налоге без овлашћења, сукобе података о идентитету (SoD), ризике приступа трећих страна, ризике од преваре идентитета и оперативне слабости.
9. Процена пракси заштите приватности и личних података повезаних са дигиталним идентитетима, укључујући класификацију података о идентитетима, задржавање, минимизирање, закониту обраду, могућност ревизије и захтеве за приватност већ у дизајну.
10. Дизајнирати и успоставити оквир управљања ИАМ-ом за организацију, укључујући тела управљања, оперативни модел, RACI матрице, власништва над контролама, путеве ескалације, управљање изузецима и структуре доношења одлука.
11. Развити или унапредити политике, стандарде, процедуре и смернице повезане са ИАМ-ом које обухватају управљање приступом, аутентификацију, привилеговани приступ, стандарде лозинки, MFA, прегледе приступа, SoD,

приступ трећих страна, управљање животним циклусом идентитета и евидентирање ревизије.

12. Креирати и документовати целокупне процесе управљања и оперативне процесе IAM-a, укључујући токове рада, одобрења, контролне тачке, SLA, KPI, KRI и захтеве за ревизорске доказе.
13. Успоставити периодичне процесе сертификације и ресертификације приступа, укључујући управљање прегледима корисничког приступа, прегледима привилегованог приступа, валидацијом SoD-a и праћењем санације и корекција.
14. Преглед и оптимизација управљања привилегованим налозима, административним приступом, дељеним налозима, сервисним налозима и приступом у хитним случајевима, укључујући контроле праћења, одобравања, одговорности и сегрегације.
15. Дефинисати процесе праћења усклађености и спремности за ревизију, укључујући методологије тестирања контрола, захтеве за прикупљање доказа, механизме извештавања, праћење санације и континуирано праћење усклађености.
16. Израдити препоруке и дизајне циљног стања за принцип нултог поверења (*Zero Trust*) за идентитете, управљање идентитетима у *Cloud*-у, интеграцију хибридних идентитета и модерне стратегије аутентификације.
17. Организовати радионице, интервјуе са заинтересованим странама и радне сесије са пословним, безбедносним, ревизорским, HR и IT тимовима како би се валидирани захтеви, структуре управљања, ризици и дизајн процеса.
18. Израдити приоритетни план IAM-a, укључујући краткорочне, средњорочне и дугорочне иницијативе, редослед имплементације, приоритете за санацију ризика, побољшања управљања и препоруке за побољшање зрелости.
19. Израдити извештаје за руководство, укључујући извештаје о процени, документацију о управљању, дијаграме процеса, процене зрелости, регистре ризика, мапирање усклађености и презентације за менаџмент.
20. Подржати осигурање квалитета и периодичне прегледе управљања током животног циклуса имплементације IAM-a како би се осигурала усклађеност са циљевима безбедности, усклађености, управљања, приватности и оперативним циљевима.
21. Понуђач мора израдити предлог IAM GRC контролног оквира који повезује функционалности IAM решења са релевантним регулаторним, безбедносним и ревизорским захтевима, укључујући Закон о информационој безбедности Републике Србије, Закон о заштити података о личности Републике Србије, GDPR, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, PCI DSS, EBA ICT смернице, PSD2 и друге применљиве захтеве за финансијски сектор. Коначну применљивост предложених контрола потврђује Наручилац.
22. Понуђач мора израдити нацрт Матрице применљивости IAM контрола, која повезује IAM процесе, техничке контроле, власнике контрола, учесталост извршења, очекиване доказе, начин тестирања контроле и статус имплементације. Матрица представља препоруку за Наручиоца и основ за интерно усвајање, ажурирање и даљу примену.
23. Понуђач мора израдити IAM Risk & Control Matrix као препоруку за управљање ризицима повезаним са идентитетима и приступом. Матрица треба да обухвати најмање ризике прекомерних овлашћења, неажурних налога, orphan налога, shared налога, сервисних налога без власника, SoD конфликта, неадекватног privileged access модела, кашњења у деактивацији налога, недовољне MFA покривености и недовољног ревизорског трага. Вредновање ризика и прихватање резидуалног ризика врши Наручилац.
24. Понуђач мора, на основу постојећег организационог и контролног оквира Наручиоца, предложити модел власништва над IAM контролама и процесима. Предлог треба да обухвати релевантне организационе улоге, укључујући власнике апликација, власнике пословних улога, власнике података, IT,

- информациону безбедност, Compliance, DPO, интерну ревизију и руководство. Коначну одлуку о власништву, именовању и одговорностима доноси Наручилац.
25. Понуђач мора израдити предлог RACI матрице за кључне IAM процесе, укључујући креирање корисника, измену приступа, престанак приступа, привилеговани приступ, приступ трећих страна, ресертификацију приступа, управљање SoD конфликтима и управљање изузецима. RACI матрица се усаглашава са Наручиоцем и примењује након интерног одобрења од стране Наручиоца.
 26. Понуђач мора предложити процес управљања IAM изузецима, укључујући критеријуме за одобравање, временско ограничење, власника ризика, компензационе контроле, периодични преглед, евидентирање и извештавање. Одлуке о одобравању изузетака, прихватању ризика и примени компензационих контрола доноси Наручилац.
 27. Понуђач мора предложити методологију периодичног тестирања IAM контрола, укључујући начин узорковања, очекиване доказе, критеријуме успешности, евидентирање налаза и праћење корективних мера. Спровођење тестирања и прихватање резултата врши се у сарадњи са Наручиоцем.
 28. Понуђач мора дефинисати препоручени сет ревизорских доказа које IAM решење и повезани процеси треба да омогуће, укључујући захтеве за приступ, одобрења, измене права, деактивације налога, резултате ресертификације, SoD конфликте, приступ привилегованим налозима, break-glass приступ, MFA догађаје, административне логове и извештаје о изузецима. Наручилац одређује коначан формат, период чувања и интерне власнике доказа.
 29. Понуђач мора предложити IAM KPI/KRI модел за праћење ефикасности, ризика и усклађености IAM процеса. Предлог треба да обухвати показатеље као што су број orphan налога, број SoD конфликта, проценат завршених ресертификација, просечно време одобравања приступа, просечно време деактивације налога, MFA покривеност, број IAM изузетака и број отворених remediation активности. Коначни сет KPI/KRI показатеља усваја Наручилац.
 30. Понуђач мора израдити IAM Audit Readiness пакет као подршку Наручиоцу за интерну ревизију, екстерну ревизију, регулаторни надзор и провере усклађености. Пакет треба да садржи препоручене контролне листе, матрице доказа, тестне сценарије, шаблоне извештаја и препоруке за санацију налаза. Одговорност за званично достављање доказа ревизији или регулатору остаје на Наручиоцу.
 31. IAM решење мора да има подршку процесу управљања животним циклусом идентитета:
 - придруживање (*Joiner*)
 - промена (*Mover*)
 - одлазак (*Leaver*)
 - self-service портал за кориснике
 - делегирани захтеви од стране овлашћених особа
 32. Решење мора бити имплементирано у локалном дата центру, on-premises.
 33. Решење мора да има подршку за импорт организационих јединица, организационе хијерархије, корисника и атрибута.
 34. Подршка за потпуни ревизорски траг (*audit trail*), праћење промена над корисницима, улогама, њиховим атрибутима и правима приступа.
 35. Подршка за интеграцију са Security Information and Event Management (*SIEM*) решењем IBM QRadar.
 36. Подршка за интеграцију са Privileged Access Management (*PAM*) решењем CyberArk.
 37. Решење мора да има подршку за Role-Based Access Control (*RBAC*) моделе, омогућавајући корисницима без техничких компетенција да учествују у процесу животног циклуса идентитета.
 38. Подршка за визуелизацију целе хијерархије улога и права.

39. Подршка за аутоматско додељивање правила која се могу конфигурисати до нивоа појединачних атрибута.
40. Подршка за дефинисане нивое одобравања управљања идентитетима и приступом усклађени са процесима.
41. Решење мора имати подршку за аутоматско двосмерно усклађивање (*reconciliation*) како би се кориснички налози синхронизовали и консолидовали, те осигурали конзистентност и безбедност.
42. Решење мора имати подршку дефинисања ауторитативног извора током усклађивања (*reconciliation*), глобално или за сваки атрибут.
43. Подршка за двосмерну консолидацију налога у информативном моду пружајући извештај о разликама између IAM решења и управљаних система (апликација) без икаквих промена.
44. Решење мора имати подршку за синхрони и асинхрони начин повезивања са управљаним системима.
45. Подршка за ресертификацију корисника укључујући њихове улоге, права и нарушавање "Separation of Duties (SoD)" политика.
46. Подршка за ресертификацију улога укључујући њихове власнике, менаџере, зависност са другим улогама, повезане организационе јединице и права која садрже.
47. Решење треба да обезбеди аутоматски одабир опсега ресертификације улога према менаџеру, власнику улоге, ризику, врсти улоге и захтевима лиценце.
48. Решење мора имати подршку за управљање и провођење поделе дужности (SoD).
49. Решење мора имати визуелизацију и управљање SoD матрицама које приказују односе између различитих SoD класа.
50. Решење мора имати стандардне извештаје о кршењима SoD политика.
51. IAM решење мора бити интегрисано са апликацијама где корисници нису аутентификовани путем Active Directory (AD).
52. IAM решење мора бити скалабилно како би подржало раст броја корисника и апликација у организацији.
53. Решење мора подржати високу доступност (*High Availability*) и опоравак услед катастрофе (*Disaster Recovery*).
54. Решење треба да обезбеди MFA за све AD аутентификације, укључујући NTLM, Kerberos, LDAP и LDAPS.
55. MFA решење мора да буде у могућности да се интегрише са Entra ID-ом (Azure AD).
56. MFA решење треба да подржава RADIUS аутентификацију.
57. MFA решење треба да подржава FIDO2.
58. MFA решење треба да подржава TOTP.
59. MFA решење мора да нуди грануларни *role-based* приступ за администраторе.
60. MFA решење мора да буде у стању да примени правила сегментације на кориснике и групе.
61. MFA решење мора да буде у стању да понуди полисе засноване на ризику.
62. MFA решење треба да понуди полисе засноване на ризику које могу блокирати приступ у реалном времену.
63. MFA решење треба да понуди полисе засноване на ризику које могу покренути MFA у реалном времену.
64. MFA решење треба да подржава полисе приступа засноване на сегментацији идентитета.
65. MFA решење треба да обезбеди полисе које имају за циљ да спрече заобилажење IAM/PAM-а.
66. MFA решење мора да буде у могућности да блокира покушаје приступа које врше shadow администратори.
67. MFA решење треба да обезбеди заштиту од MFA bombing TTP.

68. MFA решење треба да има могућност да обузда напад и да обезбеди да се не прошири на додатне ресурсе у случају инцидента.
69. MFA решење треба да обезбеди аутентификационе логове.
70. MFA решење треба да може да прилагоди приказ логова тако да приказују додатне податке.
71. MFA решење треба да има могућност да изведе логове у SIEM IBM QRadar.
72. MFA решење мора да буде у могућности да открије активност идентитета међу следећим IdP-има: AD, Entra AD, Okta.
73. MFA решење треба да буде у стању да произведе извештаје о процени ризика.
74. MFA решење мора да буде у могућности да направи извештај о мапирању сервисних налога за потребе onboarding-a у PAM.
75. MFA решење треба да буде у могућности да производи прилагођене извештаје о аутентификацији и евиденцији покушаја приступа.
76. MFA решење мора да подржава мобилну push нотификацију као фактор аутентификације.
77. MFA решење мора да подржава биометријску аутентификацију путем мобилног уређаја, укључујући отисак прста и препознавање лица.
78. MFA решење треба да подржава офлајн аутентификацију када мобилни уређај нема интернет конекцију.
79. MFA решење мора да имплементира заштиту од MFA *fatigue* напада кроз ограничење броја push нотификација у дефинисаном временском прозору.
80. MFA решење мора да захтева експлицитну корисничку потврду унутар push нотификације која садржи контекстуалне информације о захтеву за аутентификацију, укључујући локацију, уређај и апликацију.
81. MFA решење треба да подржава number matching као механизам за спречавање MFA bombing напада.
82. MFA решење мора да подржава enrollment и de-enrollment мобилних уређаја као фактора аутентификације.
83. MFA решење мора да омогући администраторима да даљински опозову регистровани уређај корисника.
84. MFA решење мора да детектује и блокира аутентификацију са роотованих или јаилбрејкованих уређаја.
85. MFA решење треба да подржава регистрацију више уређаја по кориснику.
86. MFA решење мора да изложи REST API за интеграцију са екстерним системима и апликацијама.
87. MFA решење мора да обезбеди REST API документацију и да подржава стандардне механизме аутентификације API приступа у складу са OAuth2 стандардом.
88. MFA решење мора да подржава on-premises deployment без зависности од екстерних cloud сервиса.
89. MFA решење треба да подржава hybrid deployment модел у којем основне компоненте могу бити on-premises, а управљање cloud-based.
90. Сви подаци везани за аутентификацију корисника морају бити заштићени током преноса "in transit" (TLS 1.2 или новији).
91. Механизам енкрипције мора да омогући енкрипцију података на нивоу колоне базе података (*column-level encryption*) без измене апликативног кода.
92. Механизам енкрипције мора да ради транспарентно тако да крајњи корисници и апликације не смеју примећивати разлику у раду.
93. Механизам енкрипције мора да подржава енкрипцију података без потребе за ангажовањем развојних програмера (девелопера).
94. Механизам енкрипције мора да подржава централизовано управљање кључевима и политикама путем јединствене управљачке конзоле.
95. Механизам енкрипције мора да подржава аутоматски ротацију кључева (*key rotation*) без прекида рада система (*zero downtime*).

96. Механизам енкрипције мора да подржава грануларну контролу приступа на нивоу колоне, са могућношћу доделе јединствених кључева по колони.
97. Механизам енкрипције мора да подржава маскирање података (*data masking*) са различитим нивоима видљивости према улози корисника.
98. Механизам енкрипције мора да подржава свеобухватно логовање и ревизију (*audit log*) сваког приступа енкриптованим подацима и кључевима.
99. Механизам енкрипције мора да буде сертификовано према стандарду FIPS 140-2 до нивоа Level 3 кроз управљачки сервер или HSM интеграцију.
100. Механизам енкрипције мора да подржава следеће базе података: Oracle, Microsoft SQL Server, IBM DB2 и Teradata.
101. Механизам енкрипције мора да подржава следеће оперативне системе: Microsoft Windows, Linux, Solaris, HP-UX и IBM AIX.
102. Механизам енкрипције мора да подржава следеће алгоритме и методе енкрипције: AES (*Advanced Encryption Standard*), RSA, ECC (*Elliptic Curve Cryptography*), FPE (*Format-Preserving Encryption*) FF3.
103. Механизам енкрипције мора да подржава централизовану администрацију кључева из јединствене конзоле за све окружења (*on-premises*).
104. Механизам енкрипције мора да подржава аутоматску ротацију кључева и поново-ковање (*re-keying*) енкриптованих података без прекида рада апликација.
105. Механизам енкрипције мора да подржава опцију енкрипције локално на серверу базе података или на управљачком серверу кључева како кључеви никад не напуштају сигурну енклаву.
106. Механизам енкрипције мора да подржава грануларност кључева на нивоу појединачне колоне у бази података.
107. Механизам енкрипције мора да подржава механизме лод баланцинга за дистрибуцију енкрипције на кластер управљачких сервера.
108. Механизам енкрипције мора да обезбеди сепарацију дужности (*Separation of Duties*) тако да администратори базе података не смеју имати приступ кључевима нити некриптованим подацима.
109. Механизам енкрипције мора да се инсталира на сваком серверу базе података са подршком за ручну и тиху (*silent*) инсталацију.
110. Механизам енкрипције мора да подржава деплоумент у физичким, виртуелним и *Cloud* окружењима без измене пословних процеса или апликација.
111. Механизам енкрипције мора да подржава *Cloud* и виртуелизована окружења како би организација задржала потпуну контролу над подацима и кључевима у *Cloud*-у.
112. Механизам енкрипције мора да буде транспарентан према свим постојећим апликацијама без потребе за изменама апликативног кода.
113. Механизам енкрипције мора подржавати механизам заштите података у складу са Законом о заштити података о личности Републике Србије, General Data Protection Regulation (GDPR) EU регулативом и PCI DSS (*Payment Card Industry Data Security Standard*).
114. Механизам енкрипције мора да подржава контролу приступа засновану на улогама (*Role-Based Access Control*).
115. Механизам заштите података мора се испоручити као виртуелно или хардверско решење.
116. Понуђач мора провести пенетрационо теситање након имплементације продукционог IAM окружења ради идентификације слабости у IAM архитектури и процене отпорности на ескалацију привилегија и злоупотребе идентитета.
117. Пенетрационо тестирање треба да обухвати изворе идентитета (IdP), управљање приступом, MFA механизме, животни циклус корисника (*provisioning/deprovisioning*), API механизме повезане са аутентификацијом и ауторизацијом, администраторске интерфејсе, привилеговане приступе и друге

механизме усклађене са методологијама као што су OWASP, NIST SO 800-115 и сл.

118. За потребе имплементације IAM решења Наручилац ће обезбедити серверску инфраструктуру на виртелном окружењу (Hypervisor: VMware vSphere/ESXi или Microsoft Hyper-V) са следећим минималним ресурсима за примарну локацију, и то:

CPU: 120, RAM: 528 GB, Storage: 1 TB. Тип Storage је *block storage* са PersistentVolume backed by NVMe или SSD.

Обука за понуђено решење:

План обуке за IAM решење треба да буде структуриран тако да осигура темељно разумевање управљања идентитетом и приступом на свим нивоима корисника. Обука треба да се проводи у формату сесија уживо.

Потребно је обезбедити обуке за следеће групе корисника:

1. Обука техничких администратора: полазници ће бити корисници који администрирају систем.
2. Обука кључних корисника: полазници ће бити одабрана група крајњих корисника који ће користити систем за тражење приступа у име, одобравање захтева, вршење сертификације и извршавање мануелних задатака.
3. Обука крајњих корисника: полазници ће бити одабрана група крајњих корисника који ће користити систем искључиво за тражење приступа и преглед свог личног приступа и података.

Приступ обуци треба да имати за циљ да осигура несметан и успешан прелазак на ново IAM решење.

Испорука и имплементација

Понуђач је у обавези да изврши испоруку и имплементацију решења у року од 12 (дванаест) месеци од ступања уговора на снагу.

Место испоруке и имплементације је на локацији Наручиоца у Београду.

Техничка подршка

Понуђач је у обавези да пружи техничку подршку у трајању од 24 месеца по принципу 8x5 (од понедељка до петка, од 8:30 то 16:30 часова) у складу са параметрима датим у наставку.

Приоритет проблема дефинише Наручилац, а верификује понуђач, у тренутку пријаве кvara. Време оцива техничке подршке зависи од класификације пријављеног нивоа приоритета инцидента.

Критичан: Потпуни прекид продукционог окружења. Продукционо IAM решење није функционално или утиче на продукцију у толикој мери да се квалитет продукције не може гарантовати кроз наставак рада.

Озбиљан: Кључна компонента решења није доступна што значајно утиче на продукционо окружење или компоненту која није критична за продукционо окружење.

Низак: Мањи утицај на продукционо окружење, функцију или део функционалности који не ради исправно. Функционална ограничења, проблеми и грешке у корисничком интерфејсу или грешке у документацији.

Дефиниције времена:

Време одзива: време које протекне од тренутка када Наручилац пријави проблем (отвори сервисни захтев) до тренутка када техничка подршка Понуђача контактира Наручиоца у циљу размене информација у вези проблема и почетка рада на његовом отклањању.

Време опоравка: време које протекне од тренутка пријаве проблема (подизања сервисног захтева) до тренутка потпуног решења проблема или опоравка основних функционалности неопходних за рад сервиса или мрежну управљивост.

Време затварања случаја: време које протекне од тренутка пријаве проблема (подизања сервисног захтева) до тренутка када су успостављене све функционалности, односно стање као пре проблема (коначно решење).

У случају да је сервисни захтев узрокован отказом опреме која није предмет одржавања, онда претходни временски интервали нису применљиви.

Ескалациона табела приоритета:

	Време одзива	Време опоравка	Време затварања случаја
Критичан ниво	1h	2h	7 дана
Озбиљан ниво	4h	6h	14 дана
Низак ниво	8h	72h	30 дана

Сервисни захтеви приоритета Критичан ниво се обавезно пријављују и телефонским позивом. У случају потребе за истовременом пријавом више проблема, сваки сервисни захтев се засебно пријављује.