Техническа спецификация по обособена позиция № 8 с предмет:

„Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“

1. **Платформа за управление на идентичността на потребителите**

Общи изисквания	
REQ.1.	Тип лиценз: вечен (perpetual), с включени 60 месеца поддръжка
REQ.2.	Брой лицензи: • 1 брой базова система за управление и контрол на цифровите идентичности и достъпа до информация, включени 60 месеца поддръжка на системата; • допълнителни лицензи за модул за 8000 потребителя за функции за контрол на достъпа до информация (access management), включени 60 месеца поддръжка на модула; • допълнителни лицензи за модул за 8000 потребителя за функции за управление и контрол на цифровите идентичности (identity management), включени 60 месеца поддръжка на модула; • допълнителни лицензи за модул за 8000 потребителя за функции за защитено вписване на потребителите в системите (secure login), включени 60 месеца поддръжка на модула;
REQ.3.	Да може да се управлява създаването на акаунти.
REQ.4.	Да може да се управлява промяната на правата, свързани с акаунт.
REQ.5.	Да може да се управлява де-активирането на акаунти (account revocation).
REQ.6.	Да разполага с автоматизирани работни процеси (workflows) за заявяване и одобрение на права за достъп до ресурси.
REQ.7.	Да предоставя възможност, потребителите сами да заявяват и сменят пароли – услуга тип „Password Self-Service”.
REQ.8.	Да предоставя възможност за заявяване и одобрение на услуга за самообслужване.
REQ.9.	Да могат да се наблюдават дейностите на потребителите.
REQ.10.	Да извършва одит на правата за достъп.
REQ.11.	Да предоставя отчети за доказване на съответствие със законови и нормативни документи.
REQ.12.	Да разполага с централизирано хранилище за съхранение на информация за цифрови идентичности, прости роли, композитни роли, упълномощавания, права на достъп.
REQ.13.	Да извършва одит на дейностите, свързани с даване / промяна / отнемане на права и да предосатвя отчети.
REQ.14.	Да могат да се наблюдават централизирано дейностите, свързани с даване / промяна / отнемане на права.
REQ.15.	Да предоставя управление на роли.
REQ.16.	Да предоставя управление на атестации на роли.
REQ.17.	Да предоставя управление на функциите по самообслужването на потребителите (self-service).
REQ.18.	Де е възможно първоначално конфигуриране на решението в среда без мрежова свързаност и след проверка на функционалността – внедряване в реална продукционна среда.

REQ.19.	Да предоставя графично представяне на компонентите на решението за управление на цифрови идентичности (ЦИ) и наблюдение на взаимодействието им и съвместната им работа.
REQ.20.	Да предоставя възможност за модифициране и тестване на средата на решението за управление на ЦИ.
REQ.21.	Да предоставя възможност за пренасяне от тестовата среда в реалната продукционна среда на част от решението или на цялото решение.
REQ.22.	Да предоставя възможност за съвместна работа и споделяне на няколко екипа по внедряване.
REQ.23.	Да извършва анализиране, обогатяване и разширяване на ЦИ. Контролиране на източниците на ЦИ в рамките на организацията.
REQ.24.	Да извършва асоцииране на атрибутите на базата данни с ЦИ на приложенията към базата с данни с ЦИ на решението за управление на ЦИ (schema map attributes association).
REQ.25.	Да извършва анализ на данните за ЦИ, намиране на противоречия, изчистване на данни за ЦИ, осъществяване на съответствие между подобни величини между приложните системи и решението за управление на ЦИ.
REQ.26.	Да позволява дефиниране и конфигуриране на профили за анализиране на един или повече набори от данни.
REQ.27.	Да предоставя метрични данни за сравнение на стойности на атрибути за определяне на съответствието между форматите на данни за ЦИ в приложните системи и в системата за управление на ЦИ.
REQ.28.	Да предоставя профили на съответствието за сравнение на стойности в един или повече набори от данни за ЦИ.
REQ.29.	Да може да открива дублиране на стойности в един набор от данни за ЦИ.
REQ.30.	Да може да открива съответствие между стойности в два различни набора от данни за ЦИ.
REQ.31.	Да предоставя дефиниране на набори от разрешения за достъп, свързани с една или повече приложни системи.
REQ.32.	Да предоставя събиране на идентификатори на акаунти от свързаните системи и свързаните с тях разрешения за достъп.
REQ.33.	Да предоставя централизирано разрешение на достъп на потребителите до свързаните приложни системи.
REQ.34.	Да разполага с вградени роли с различни нива на достъп към модула за управление на роли.
REQ.35.	Да позволява откриване на прости роли, композитни роли, профили.
REQ.36.	Да позволява съпоставяне на прости роли, композитни роли, профили - от различни приложни системи към системата за управление на ЦИ.
REQ.37.	Да предоставя централизирано управление на прости роли, композитни роли и профили, в различните свързани приложни системи.
REQ.38.	Да предоставя автоматизирано средство за изваждане на информация за роли от свързаните системи и връзка с централното хранилище на ЦИ и да разполага с изглед (dashboard) за даване / промяна / отнемане на права.
REQ.39.	Да може да се управлява централизирано чрез уеб-браузър. Централизирано наблюдение, конфигуриране и администриране на системата.

REQ.40.	Да предоставя информация в реално време за здравето на системата и нейните компоненти.
REQ.41.	Да предоставя синхронизиране, трансформиране, разпределяне и обмен на информация за ЦИ в рамките на организацията между свързани системи и системата за управление на ЦИ.
REQ.42.	Да предоставя контрол върху потоците от данни между свързаните системи.
REQ.43.	Да позволява определяне на кои данни да се споделят.
REQ.44.	Да позволява определяне на коя система е авторитарния източник на съответната порция данни.
REQ.45.	Да позволява определяне на това как данните да се интерпретират и трансформират, за да съответстват на изискванията на другите системи.
REQ.46.	Да предоставя синхронизиране на пароли между различни системи.
REQ.47.	Да предоставя автоматизирано създаване на нови потребителски акаунти в свързаните системи.
REQ.48.	Да предоставя автоматизирано премахване на стари потребителски акаунти в свързаните системи.
REQ.49.	Да предоставя отчет за доказване, че точните хора имат разрешен достъп до точните ресурси.
REQ.50.	Да предоставя отчет за доказване, че хората с отнети права нямат права за достъп в системите, за които са им отнети правата на достъп.
REQ.51.	Да предоставя отчет за доказване, че всеки служител има права за достъп до всички ресурси, които се изискват от неговата позиция.
REQ.52.	Да предоставя проследяване на всички дейности свързани с даване / промяна / отнемане на права.
REQ.53.	Да предоставя записване на всички дейности свързани с даване / промяна / отнемане на права.
REQ.54.	Да има възможност за предоставяне на данни за дейностите по даване / промяна / отнемане на права, както и за цифровите идентичности в организацията за целите на вътрешен или външен одит.
REQ.55.	Да предоставя предварително зададени отчети за информация свързана с ЦИ.
REQ.56.	Да предоставя възможност за изработване на специфични отчети, търсения и справки за информация свързана с ЦИ.
REQ.57.	Да предоставя централна мета-директория за съхранение на данни за ЦИ. Метадиректорията да има възможност да е свързана с всички източници на данни за ЦИ и да може да обменя данни за ЦИ със източниците на ЦИ на свързаните системи.
REQ.58.	Да предоставя автоматизиране на обработването и синхронизирането на промените на данните, които настъпват, както в централната мета-директория, така и в отделните системи. Автоматизацията да работи на базата на събития (event-based).
REQ.59.	Да предоставя стандартно вградени драйвери за свързване на външни системи към централната мета-директория и системата за управление на ЦИ.
REQ.60.	Да предоставя възможност за разработване на специфични драйвери за свързване на специфични системи към системата за управление на ЦИ и централната мета-директория.
REQ.61.	Да предоставя възможност за свързване с отдалечени сървъри и системи.

REQ.62.	Да предоставя централизирано хранилище за събиране на всичката информация свързана с ЦИ, правата за достъп и действията за даване / отнемане / промяна на права за достъп.
REQ.63.	Да предоставя възможност за извършване на търсения - както стандартни, така и специфични, дефинирани от потребителя относно: ЦИ, правата за достъп и действията за даване / отнемане / промяна на права за достъп.
REQ.64.	Да предоставя вградени справки за доказване на съответствия с вътрешни / нормативни / законови актове.
REQ.65.	Да предоставя възможност за създаване на специфични отчети.
REQ.66.	Да предоставя автоматизирана услуга за събиране на данните свързани с ЦИ.
REQ.67.	Да предоставя автоматизирана услуга за събиране на данни за свързани системи / акаунти за съответна система / права на достъп / стойности на величини / профили на потребители.
REQ.68.	Да предоставя автоматизирана услуга за регистриране на събития и събиране на одитни записи за дейностите свързани с роли и даване / отнемане / промяна на права, както и за дейности свързани с отчети относно вмъкване, модификация, изтриване или създаване на график за отчет.
REQ.69.	Да предоставя провизиране на потребители, на базата на бизнес-ролята им в организацията.
REQ.70.	Да предоставя автоматизирани работни процеси за одобрение и провизиране.
REQ.71.	Да предоставя атестационен процес на потребители, потребителски профили, роли, задължения.
REQ.72.	Да предоставя откриване и управление на конфликтиращи се роли.
REQ.73.	Да предоставя възможност за самообслужване от страна на потребителите – управление на лични данни, промяна на пароли и секретна лична информация, заявяване на достъп до системи и ресурси.
REQ.74.	Да предоставя надзор над работните процеси за заявяване и одобрение на права.
REQ.75.	Да предоставя уеб-базирана услуга на потребителите за самообслужване.
REQ.76.	Да предоставя автоматизирано провизиране на потребители, на базата на ролята им в организацията.
REQ.77.	Да предоставя персонализиран изглед на потребителите относно разрешения, задачи, заявки.
REQ.78.	Да предоставя самообслужване за нулиране / смяна на пароли.
REQ.79.	Да предоставя възможност за свързване с външни програми за управление на забравени пароли.
REQ.80.	Да предоставя вграден механизъм за единствен доставчик на информация за еднократно вписване (Single Sign-On).
REQ.81.	Да разполага с Common Criteria сертификат от ниво EAL3+.
REQ.82.	Да разполага със сертификати: RHEL 6/7 (за 32 и 64 битови системи).
REQ.83.	Да предоставя защита на уеб-базираните ресурси, като осигурява достъп само на оторизирани потребители до предварително зададени ресурси.
REQ.84.	Да може да осигурява достъп на следните групи потребители: вътрешни служители, външни партньори, външни потребители.

REQ.85.	Да предоставя скриване на адресите на защитените ресурси, както от вътрешни, така и от външни потребители.
REQ.86.	Да може да осигурява достъп до ресурси на оторизирани потребители, без значение, както на местонахождението на потребителя, така и на вида/типа устройство, от което се извършва достъпа.
REQ.87.	Да предоставя управление на множество пароли на един и същ потребител.
REQ.88.	Да може да осигурява достъп само до предварително дефинирани ресурси, в зависимост от позицията/ролята на потребителя в организацията.
REQ.89.	Да предоставя защита на личните данни и да може да осигурява поверителността на потребителите.
REQ.90.	Да разполага с вградени ресурси за изграждане на строга автентификация с повече от един фактор.
REQ.91.	Да предоставя възможност за използване на едни и същи данни за вписване за достъп до услуги от външни доставчици на услуги.
REQ.92.	Да предоставя автоматизирано създаване на потребителски акаунти в системите на федерираните партньори или доставчици на услуги.
REQ.93.	Да предоставя достъп до множество уеб-приложения с еднократна автентикация (с една парола) тип „Single Sign-On”, на базата на стандарти.
REQ.94.	Да позволява изграждането и налагането на политики за права за достъп.
REQ.95.	Да предоставя автоматизиране на даването и отнемането на права за достъп, на базата на ролята на потртебителя в организацията и политиките за достъп, свързани с ролята.
REQ.96.	Да предоставя следния модел за автоматизиране на процеса по даването и отнемането на права за достъп:
REQ.97.	Автентикация на потребител -> присъединяване на роля -> преглед на политиките за достъп, свързани с ролята -> налагане на политиките -> осигуряване на достъп до предварително зададени ресурси, в зависимост от ролята.
REQ.98.	Да предоставя възможност за споделяне на информация за цифрова идентичност между различни източници на информация за ЦИ – както вътрешни за организацията, така и външни.
REQ.99.	Да предоставя възможност на външни потребители да получават оторизиран достъп до вътрешни за организацията уеб-ресурси.
REQ.100.	Да поддържа следните стандарти за федериране на ЦИ: Liberty Alliance, WS-Federation, WS-Trust, SAML.
REQ.101.	Да предоставя възможност за идентифициране на риска, свързан с броя на опитите за вписване (login), управление на риска, предприемане на действия, базирани на нивото на риска.
REQ.102.	Да предоставя възможност за определяне на коя бизнес информация или лична информация от корпоративната директория да може да бъде споделяна.
REQ.103.	Да предоставя функция за вмъкване на идентичност (identity injection) чрез извличане на информация от директориина услуга и на тази база – възможност за вмъкване на информация в HTML хедъри, възможност за търсене в стрингове или автентификационни хедъри.

REQ.104.	Да предоставя функция за федериране на идентичност чрез асоцииране на акаунти между доставчик на идентичност и доставчик на услуга.
REQ.105.	Да се поддържат следните протоколи за федериране на идентичност: Liberty, SAML 1.1, SAML 2.0, Oauth.
REQ.106.	Да предоставя следните методи за автентикация на потребителите: • Чрез потребителско име / парола, • RADIUS • Автентикация на базата на токени, • Автентикация чрез X.509 дигитални сертификати, • Kerberos • Риск-базирана автентикация, • Time-Based One-Time Password (TOTP) • „Social authentication“ метод • OpenID Connect
REQ.107.	Да предоставя контрол на правата на потребителите.
REQ.108.	Да предоставя възможност за динамично налагане на политиките за оторизация.
REQ.109.	Да предоставя потребителски портал с възможност за конфигуриране на елементите в него за всеки потребител персонално, където потребителят да може да достъпва и управлява автентификациите си, федерациите и данните на профила си.
REQ.110.	Да предоставя възможност потребителския портал и уеб-страницата за вписване в него да могат да се ребрандират с логото и данните на организацията.
REQ.111.	Да предоставя възможност за интегриране със следните системи за съхраняване на данните за идентификацията и правата на потребителите: • Informix 10 и Informix 12; • IBM Domino 8.5 и IBM Domino 9; • IBM DB2 10; • MS Active Directory реализирана върху MS Windows Server 2008 R2; • MySQL 5.0 -5.5; • CoachDB 10; • LDAP базирани хранилища; • PostgreSQL 8.x и 9.x;
Гаранция и поддръжка:	
REQ.112.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.113.	Получаване на нови версии на софтуера - минимум 5 (пет) години.

2. **Система системата за управление на привилегированите потребители**

Общи изисквания	
REQ.114.	Тип лиценз: вечен (perpetual), с включени 60 месеца поддръжка

REQ.115.	Брой лицензи: софтуерни лицензи за 300 бр. за управление на привилегированите потребители (privileged access management), с включени 60 месеца поддръжка на модула
REQ.116.	Да поддържа управление на правата за достъп до: Windows, Linux, Unix системи; виртуални сървъри; облачни услуги; бази от данни; приложения.
REQ.117.	Да предоставя запис на всички Windows, Linux и Unix команди, извършени от привилегированите потребители на системите.
REQ.118.	Да предоставя видеозапис на сесиите до всички физически и виртуално базирани среди, изискващи удостоверяване на достъпа.
REQ.119.	Да предоставя възможност за търсене във видеозаписите.
REQ.120.	Да предоставя възможност за съхраняване на пароли, ключове и друга чувствителна информация в единно защитено хранилище.
REQ.121.	Да може да извършва корелация на команди, спрямо разрешени такива.
REQ.122.	Да предоставя пълен регистър на възникналите събития, с възможност за одитиране.
REQ.123.	Да може да извършва проверка на пароли за облачни услуги.
REQ.124.	Да поддържа x11 протокол.
REQ.125.	Да предоставя защита на паролите в единно защитено хранилище.
REQ.126.	Да предоставя възможност за допълнителна дву-факторна и стъпкова автентификация.
REQ.127.	Да предоставя поддръжка на допълнителни методи за автентификация чрез – еднократна парола, смартфон, глас, SMS.
REQ.128.	Да поддържа функция за еднократно вписване (Single Sign-On) за Linux и Unix сървъри.
REQ.129.	Да поддържа използването на защитен RDP прокси протокол за отдалечени сесии.
REQ.130.	Да поддържа използването на AD и LDAP автентификация.
REQ.131.	Да предоставя криптирана база от данни за съхранение на данните за вписване на привилегированите потребители.
REQ.132.	Да предоставя възможност за задаване и налагане на политики за управление на достъпа.
REQ.133.	Да предоставя възможност за автоматично идентифициране на привилегированите акаунти.
REQ.134.	Решението да се управлява чрез централизирана уеб-базирана конзола.
REQ.135.	Решението да разполага с интерфейс за управление на политиките за достъп от тип „drag-and-drop“.
REQ.136.	Да предоставя възможност за използване на съществуващи LDAP директории като място за съхранение на данните за вписване на привилегированите потребители.
REQ.137.	Да предоставя възможност за автоматично прилагане на политики за достъп на Windows групи.
REQ.138.	Да предоставя йерархична структура за изграждане на правила за достъп.
REQ.139.	Да предоставя риск-базиран контрол на сесиите на привилегированите потребители и оцветяване на рисковите сесии, с цел непосредствен контрол.
REQ.140.	Да извършва и предоставя анализ на поведението на привилегированите потребители в реално време.
REQ.141.	Да извършва и предоставя анализ на действията с клавиатура от привилегированите потребители.

REQ.142.	Да предоставя възможност за възпроизвеждане на UNIX, Linux and Windows сесиите на привилегированите потребители.
REQ.143.	Да предоставя одит в реално време на всички Windows хостове.
REQ.144.	Да предоставя автоматични отчети на база предварително зададени правила.
REQ.145.	Да предоставя механизми за защита, които да осигуряват невъзможност за промяна, подмяна или унищожаване на събрани одитни видеозаписи и данни.
REQ.146.	Да предоставя възможност за създаване на работни процеси.
REQ.147.	Да предоставя възможност за FTP одит.
REQ.148.	Да предоставя възможност за задаване на ACL ограничения.
Гаранция и поддръжка:	
REQ.149.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.150.	Получаване на нови версии на софтуера - минимум 5 (пет) години.