

Приложение № 2
към рамков договор № МС-117/09.10.2024 г.

ЗАЯВКА по Рамков договор № МС-117 от 09.10.2024 г. (ПО-16-3093/09.10.2024 г. на ИО АД)		☒
ЗАЯВКА по Рамков договор № МС-117 от 09.10.2024 г. (актуализирана)		☐ ¹
Позиция от ПГ-2026 г.:	<i>№ по ред от ПГ</i>	<i>1.1</i>
Описание на дейност/проект съгласно ПГ:	<i>Поддръжка на 200 бр. лицензи за многофакторна автентикация (Cisco Duo Essentials)</i>	
CPV код	<i>48514000-4</i>	
Рег. номер на писмо от МИДТ за утвърждаване на проекта /становище по проекта	<i>МИДТ Рег.№ 03-00-256/09.09.2026</i>	
Изискване за достъп до класифицирана информация ДА/НЕ	<i>НЕ</i>	
Стойност: (стойността следва да съответства на заложената в План-графика) без ДДС, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово	<i>18 060,00 евро без ДДС, разпределени както следва:</i> <i>За 2026 г. - 6 020,00 евро без ДДС</i> <i>За 2027 г. - 6 020,00 евро без ДДС</i> <i>За 2028 г. - 6 020,00 евро без ДДС</i>	
Начин за плащане: (еднократно, на части, периодично, авансово или др.)	<i>На части:</i> <i>след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на поддръжката на лицензите и издадени фактури, както следва:</i> <i>през 2026 г. за период от 12 месеца;</i> <i>през 2027 г. за период от 12 месеца;</i> <i>през 2028 г. за период от 12 месеца.</i>	
Плащане с акредитив или авансово	<i>НЕ</i>	

¹ Отбелязва се в случай че заявката е актуализирана

ДА/НЕ		
Документи за плащане с акредитив или авансово	<i>неприложимо</i>	
Срок на изпълнение: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	<i>До 1 месец след подписване на заявката</i>	
Гаранционен срок: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	<i>Съгласно изискванията на Техническите параметри</i>	
Отчитане: (периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)	<i>С подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на поддръжката на лицензите</i>	
Приложения: (напр: технически параметри, образци на отчетни документи)	<i>Технически параметри</i>	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:		
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):		<i>Подпис:</i>
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		<i>Подпис:</i>

Ръководител на договора от страна на БЕНЕФИЦИЕРА:		Подпис:
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		Подпис:
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		Подпис:

Забележка: С една заявка могат да се възлагат повече от един проект по ППГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА:

„Поддръжка на 200 бр. лицензи за многофакторна автентикация (Cisco Duo Essentials) за нуждите на Администрацията на Министерския съвет (АМС)“

гр. София, 2026 г.

I. ПРЕДМЕТ

В предмета на заявката се включва поддръжка на закупените лицензи, използвани от АМС за многофакторна автентикация с последващ контрол на отдалечения достъп до ресурси (хардуер и софтуер) до вътрешната мрежа. АМС използва Cisco Duo Essentials за 200 потребителя.

За да се обезпечи непрекъсваемостта на работата на тези системи и имайки предвид нуждата от надеждна поддръжка е необходимо да се поднови правото на ползване и поддръжка на изброените софтуерни продукти за срок от 36 месеца.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Таблица 1

Система за двуфакторна автентикация– Cisco Duo Essentials със следните минимални изисквания	
Основни функции	
1.	Системата трябва да осигурява двуфакторна автентикация на защитен VPN достъп за 200 потребители. Системата трябва да поддържа следните методи за автентикация за осигуряване на гъвкави и достъпни опции за всички типове потребители: • U2F (Universal 2nd Factor) токени; • Хардуерни токени; • Мобилни пароли (6-цифрен код); • SMS; • Обратно телефонно позвъняване; • Биометрични сензори (Touch ID)
2.	Системата трябва да се интегрира с Microsoft Windows за осигуряване на двуфакторна автентикация към Remote Desktop (RDP) или локални влизания (local logon)
3.	Системата трябва да осигурява унифицирано приложение за "push" известия и OTP (One-time password) базирана автентикация към мобилен телефон с Android и iOS операционни системи
4.	Системата трябва да осигурява възможности за вписване и управление на потребителският профил без намесата на администратор
5.	Системата трябва да осигурява защита и достъп чрез двуфакторна автентикация на приложения в мрежата на възложителя

6.	Системата трябва да поддържа интеграция с VPN концентратори за отдалечен достъп на основните производители като CA SiteMinder, Oracle Access Manager, Juniper, Cisco, Palo Alto Networks, F5, Citrix и други
7.	Системата трябва да осигурява „offline“ автентикация, например когато мобилният телефон с приложението няма достъп до интернет
8.	Системата трябва да поддържа SAML конектор за облачни приложения като Google Apps, Amazon Web Services, Box, Salesforce и Microsoft Office 365
9.	Системата трябва да поддържа Microsoft и OpenLDAP директорийни услуги, както и облачно базирани такива в Microsoft Azure. Трябва да се поддържа възможността да се импортират потребители, телефонни номера и групи посредством синхронизация с директорийната услуга. Потребителската информация трябва да може да се обновява регулярно и автоматично, така че да може последните промени в потребителският статус да влязат в действие. Синхронизираната информация не трябва да съдържа актуални потребителски пароли
10.	Системата трябва да позволява на потребителите да не се иска допълнителна автентикация, ако наскоро е правена такава, като времето трябва да е конфигурируем параметър
11.	Политиките трябва да се управляват централизирано и прилагат глобално или споделено между приложенията, така че да не се налага една политика да се прилага на няколко места
12.	Системата трябва да позволява на прилагането на различни политики на специфични потребителски групи достъпващи определено приложение
13.	Системата трябва да позволява достъпа до специфични приложения без VPN достъп
14.	Автентикацията да е подсигурана с асиметрични ключове
15.	Системата да поддържа разширение със следните функции при необходимост с допълнителен лиценз: • Идентификация на рискови устройства; • Идентификация на корпоративни и лични устройства (десктоп, лаптоп, мобилни устройства); • Проверка на състоянието от гледна точка сигурност на корпоративни и лични устройства (Windows, Macs, iOS and Android); • Установяване на инсталация на приложения за сигурност на трети производители;

	• Контрол на достъпа базиран на тип (роля) на потребителя; • Системата трябва да осигурява контрол на достъпа базиран локация или мрежа използвана от потребителя; • Системата трябва да поддържа контекстуална автентикация на база разпознатото устройство
Управление и наблюдение:	
16.	Софтуерът може да бъде реализиран като облачно и/или локално инсталирано приложение или приложения
17.	Софтуерът да има инсталирани и лицензирани с постоянен лиценз операционна система и база данни, които поддържат гореописаните функции
18.	Софтуерът да е окомплектован със съответните лицензи и права за използване според условията на производителя за минимум 200 потребителя
Гаранция и поддръжка:	
19.	Срок на техническа поддръжка директно от производителя – 36 (тридесет и шест) месеца
20.	Получаване на нови версии на софтуера - 36 (тридесет и шест) месеца

- Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или официален негов представител за право на разпространение на предлаганите продукти на територията на Република България
- Заявки за обслужване (тикети) за доставения хардуер се подават чрез осигурена от Изпълнителя онлайн система за управление на заявки (СУЗ). Всички заявки, получени чрез електронна поща или телефон следва да бъдат регистрирани в СУЗ

III. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

Услугите по поддръжка се предоставят отдалечено, при необходимост от оказване на съдействие на място е гр. София, п. к. 1594, бул. „Княз Александър Дондуков“ № 1

IV. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ²

² Изискванията към мрежовата и информационната сигурност са приложими, в случай, че по време на изпълнение на заявката Изпълнителят (подизпълнителите, когато е приложимо) имат достъп до информация и активи на Възложителя/ Бенефициера/АМС/МИДТ, които са предмет на защита съгласно приложимото законодателство в областта.

1. Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.
2. Във връзка с мрежовата и информационната сигурност на Бенефициера/Възложителя/ АМС/МИДТ и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:
 - (а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Бенефициера/Възложителя/ АМС/МИДТ ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.
 - (б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Бенефициера/Възложителя/ АМС/МИДТ. За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Бенефициера/Възложителя/ АМС/МИДТ, подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера/Възложителя/ АМС/МИДТ. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.
 - (в) Определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна на Бенефициера при възникване на инцидент по МИС.
 - (г) Осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на извършения анализ и оценка на риска, с цел да се гарантира необходимото ниво на сигурност. Имплементираните смекчаващи механизми трябва да са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.
3. Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на Услугата на трети страни без изричното писмено съгласие на Бенефициера/Възложителя/ АМС/МИДТ.
4. При неспазване на изискванията за сигурност на информацията Изпълнителят дължи неустойка съгласно уговореното в договора.

5. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:
- (а) При изпълнението на задълженията си, осъществяват комуникация с лицата, които ще имат достъп до системите на Бенефициера/Възложителя/ АМС/МИДТ;
 - (б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);
 - (в) При получена информация, лица по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Бенефициера/Възложителя/ АМС/МИДТ;
 - (г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Бенефициера/Възложителя/ АМС/МИДТ, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на АМС от страна на Бенефициера/Възложителя/ АМС/МИДТ и на Изпълнителя извършват анализ и набеязват мерки за отстраняване на допуснатата нередност в определен срок.