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-2024 г.:	*№ по ред от ПГ*	*1.3*
Описание на дейност/проект съгласно ПГ:	*Поддръжка на 200 бр. лицензи за многофакторна автентикация (Cisco Duo Essentials)*	
CPV код	*48514000-4*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
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*	*13 950.00 лв. лв. без ДДС*	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно след подписване на приемо-предавателен протокол по чл. 6 от договора и издадена фактура на стойност 13 950 лв. без ДДС или 16 740 лв. с ДДС;*	
Плащане с акредитив или авансово ДА/НЕ	*НЕ*	
Документи за плащане с акредитив или авансово	*неприложимо*	
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*До 4 месеца след подписване на заявката*	
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Съгласно изискванията на Техническите параметри*	
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*С подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на съответната поддръжка.*	
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически параметри*	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		

[1] Отбелязва се в случай че заявката е актуализирана

ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		*Подпис:*
Съгласувал за съответствие на заявката с ПГ		*Подпис:*
Ръководител на проект/дейност по заявката (напр: представител на дирекцията – Заявител):		*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Координатор от „Информационно обслужване“ АД по заявката		*Подпис:*
Ръководител на проект/дейност по заявката		*Подпис:*
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		*Подпис:*

ПРИЛОЖЕНИЕ № 1

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА:

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

гр. София 2024 г.

I. ПРЕДМЕТ

В предмета на заявката се включва поддръжка на закупените лицензии, 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, като поддръжката ще е валидна до 12 декември 2024г.

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.

Необходимо е да бъде осигурена техническа поддръжка и правото на ползване за 36 месеца на софтуерни продукти Cisco Duo Essentials.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Таблица 1

1. Система за двуфакторна автентикация	
	Спецификация – минимални изисквания
	Основни функции
	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 повъняване;* • *Биометрични сензори (Touch ID).*
	Системата трябва да се интегрира с Microsoft Windows за осигуряване на двуфакторна автентикация към Remote Desktop (RDP) или локални влизания (local logon).

	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.
	Системата трябва да осигурява възможности за вписване и управление на потребителският профил без намесата на администратор.
	Системата трябва да осигурява защита и осигурява достъп чрез двуфакторна автентикация на приложения в мрежата на възложителя.
	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.
	Системата трябва да осигурява „offline" автентикация, например когато мобилният телефон с приложението нямат достъп до интернет.
	Системата трябва да поддържа SAML конектор за облачни приложания като Google Apps, Amazon Web Services, Box, Salesforce и Microsoft Office 365.
	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.
	Системата трябва да позволява на потребителите да не се иска допълнителна автентикация ако наскоро е правена такава, като времето трябва да е конфигурируем параметър.
	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.
	Системата трябва да позволява на прилагането на различни политики на специфични потребителски групи достъпващи определено приложение.
	Системата трябва да позволява достъпа до специфични приложения без VPN достъп.

	Автентикацията да е подсигурена с асиметрични ключове.
	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 устройсва);* • *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:
	Софтуера може да бъде реализиран като облачно и/или локално инсталирано приложение или приложения.
	Софтуера да има инсталирани и лицензирани с постоянен лиценз операционна система и база данни, които поддържат гореописаните функции.
	Софтуера да е окомплектован със съответните лицензи и права за използване според условията на производителя за минимум 200 потребителя.
	Гаранция и поддръжка:
	Срок на техническа поддържка директно от производителя – минимум 1 (една) година.
	Получаване на нови версии на софтуера - – минимум 1 (една) година

III. СРОК НА ИЗПЪЛНЕНИЕ. УСЛОВИЯ НА ДОСТАВКА

1. Срокът за доставката на поддръжката е до 4 месеца .

IV. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. Мястото на извършване на поддръжката е сградата на Администрацията на Министерския съвет, в гр. София, п. к. 1594, бул. „Княз Александър Дондуков” № 1.