Приложение № 2
към рамков договор № 93-00-97 от 03.07.2020 г.

ЗАЯВКА по Рамков договор № 93-00-97 от 03.07.2020 г. (вх. № ПО-16-875/03.07.2020 г. на ИО АД)	☒
ЗАЯВКА по Рамков договор № 93-00-97 от 03.07.2020 г. (вх. № ПО-16-875/03.07.2020 г. на ИО АД), (актуализирана)	☐ [1]

Позиция от ПГ-2026 г.:	*№ по ред от ПГ*	*11*
Описание на проект съгласно ПГ:	*„Техническа поддържка на SSL сертификат за удостоверяване автентичността на сайтовете на АВ и Code Signing сертификат за удостоверяване на автентичността на софтуерния код.“* [2]	
CPV код	*79811000-2*	
Рег. номер на писмо от МИДТ за утвърждаване на проекта /становище по проекта	*МИДТ-Рег. №-18-00-267-1/19.11.2026*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) евро без ДДС***, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*		*Общо 856,00 евро без ДДС, разделени като следва:* *1 бр. Sectigo Code Signing сертификат на стойност – 718,00 евро без ДДС* *1 бр. SSL сертификати от вида: Essential Wildcard на стойност - 138,00 евро без ДДС*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*		*На части:* *След подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предаването и приемането на всеки един сертификат, посочени в таблица 1 от ТП и издадена фактура.*
Плащане с акредитив или авансово ДА/НЕ		*НЕ*
Документи за плащане с акредитив или авансово		*НЕ*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**		*Срок на валидност на SSL сертификата - 12 месеца, считано от момента, в който удостоверителят подпише сертификата.* *Срок на валидност на Code Signing*

[1] Отбелязва се в случай че заявката е актуализирана
[2] Съгласувано между страните – изпълнението на заявката стартира от момента, в който удостоверителят подпише сертификатите, което може да е преди датата на подписване на заявката.

	сертификата – 36 месеца, считано от момента, в който удостоверителят подпише сертификата.
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*НЕПРИЛОЖИМО*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*На части::* *С подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предаването и приемането на всеки един от свертификатите, посочени в таблица 1 към ТП.*
Приложения: (*напр: технически параметри, образци на отчетни документи***)**	*Технически параметри (ТП)*
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):		*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		*Подпис:*
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 ПГ, 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.*

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за

„Техническа поддържка на SSL сертификати за удостоверяване автентичността на сайтовете на АВ и Code Signing сертификат за удостоверяване на автентичността на софтуерния код.“

Гр.София, 2026 г.

1. *Обща информация*

Реализирането на заявката ще допринесе за осигуряване онлайн сигурността на следните домейни за нуждите на АВ:
- registryagency.bg
За нуждите на АВ е необходимо да бъде подновен и сертификата, удостоверяващ автентичността на софтуерния код.

2. *Предмет*

Предметът на заявката е осигуряване на техническа поддържка на SSL сертификат за удостоверяване автентичността на сайта на АВ и Code Signing сертификат за удостоверяване на автентичността на софтуерния код, в съответствие с характеристиките, описани в Таблица № 1:

Таблица 1:

№	Тип	Вид	Брой	Предназначение	Срок на валидност	Крайна дата на валидност на текущ сертификат
1	Валидация по Домейн (Domain Validation)	Essential Wildcard / SSL	1	registryagency.bg	12 месеца	29.08.2026
2	Code Signing	Sectigo Code Signing Certificate	1	За удостоверяване на автентичността на софтуерния код	36 месеца	10.08.2026

3. *Минимални изисквания към изпълнението на дейността*

- Всички браузъри който са обновени с актуални ROOT сертификати на издателите да удостоверяват защитената връзка със сайтовете на Агенцията по вписванията без да дават съобщение за грешка, без да са необходими допълнителни действия от страна на служители на АВ или от страна на интернет потребителите.

- Оказване на съдействие при генерирането на заявка за подписване на сертификат CSR – Certificate Signing Request;

- Удостоверяване на автентичността на софтуерния код

- Доставка на сертификатите заедно със съпътстващата документация.

4. *Място за изпълнение на услугата:*

Мястото за изпълнение на услугата е гр. София, улица „Елисавета Багряна" № 20.

5. Изисквания към мрежовата и информационната сирурност[3]

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 (АВ) 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 (АВ), 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 (АВ). 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 (АВ), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Бенефициера (АВ). 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 (АВ) 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 (АВ).

4. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Заявката(„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 съответната администрация;

(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 (АВ);

(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 (АВ), лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на съответната администрация от страна на Бенефициера (АВ) и на

[3] 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 Бенефициера (АВ), които са предмет на защита съгласно приложимото законодателство в областта.

Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.