ПРИЛОЖЕНИЕ №6

РЕПУБЛИКА БЪЛГАРИЯ

ДЪРЖАВНА АГЕНЦИЯ „ТЕХНИЧЕСКИ ОПЕРАЦИИ”

1000 София, ул.„6-ти септември” №29, тел.: +359 2 982 4971; факс: +359 2 946 1339

ДЪРЖАВНА АГЕНЦИЯ
“ТЕХНИЧЕСКИ ОПЕРАЦИИ”
Изх.№ 31-6927
дата: 15.05.2015 г

УТВЪРЖДАВАМ:.. .....

ЗАМ.–ПРЕДСЕДАТЕЛ НА
ДЪРЖАВНА АГЕНЦИЯ
„ТЕХНИЧЕСКИ ОПЕРАЦИИ”

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

„Доставка на криптографски средства за защита на информацията”

гр. София, 2015 г.

1. **Пълно наименование:**

„Доставка на криптографски средства за защита на информацията".

2. **Състав и описание:**

Количество и състав на необходимите криптографски средства за защита на информацията (хардуерни криптиращи устройства) съгласно таблица 1:

таблица 1 – Състав и количество на необходимото оборудване и услуги

№	Наименование на продукта	Коли-чество	Мярка
1.	Хардуерно криптиращо устройство минимум 90Mbps (доставка, конфигуриране и обучение)	2	бр.
2.	Хардуерно криптиращо устройство минимум 10Mbps (доставка, конфигуриране и обучение)	9	бр.

Забележка: Заложените количества по т. 2 в таблица 1 са минимално изискуеми за съответния етап, като е възможна промяна в зависимост от разполагаемия бюджет.

2.1. Избраният участник за изпълнител да организира и осигури обучение на минимум 5 служители на Възложителя при производителя. Обучението следва да бъде проведено от производителя на криптиращите устройства най–късно до датата на въвеждането в експлоатация на хардуерните криптиращи устройства. На преминалите обучението служители да бъдат издадени сертификати от производителя.

2.2. Избраният участник за изпълнител да достави и въведе в експлоатация (тества и конфигурира) на място, при възложителя, хардуерните криптиращи устройства, както и да осигури последваща поддръжка на устройствата.

2.3. Оферираните криптиращи устройства трябва да са в текущата продуктова линия на производителя (прилага се съответен документ доказващ, че техниката е в текущата продуктова линия на производителя).

2.4. Всички криптиращи устройства да преминат поекземплярна проверка и одобрение във връзка с чл. 68 от Наредбата за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация и чл. 4 от Наредбата за криптографската сигурност на класифицираната информация.

2.5. Въвеждането в експлоатация на хардуерните криптиращи устройства става след получаването на одобрението по т. 2.4 и последващото подписване на протокол за отразяване на дейностите по тестване и конфигуриране.

3. Технически изисквания към продукта:

3.1. Хардуерно криптиращо устройство минимум 90Mbps:

№	Минимални изисквания
1.	Наличие на отделен сесиен ключ за всеки криптиран тунел
2.	Наличие на хардуерен генератор на случайни числа
3.	Поддръжка на минимум 100 криптирани IP VPN тунела
4.	Възможност за въвеждане на криптографски ключове от потребителя
5.	Разделени нива на достъп до менюто на криптографското средство
6.	Възможност за локално и отдалечено блокиране на криптографското средство
7.	Защитен криптографски модул
8.	Минимална скорост на криптиране 90Mbps
9.	Изграждане на различни типове криптографски мрежи
10.	Възможност за криптиране на данни, глас и видео в реално време
11.	Да поддържа приоритизация на пакетите
12.	Да поддържа DHCP услуги (раздаване на адреси), статично или динамично рутиране от страна на вътрешния комуникационен интерфейс
13.	Да поддържа DHCP услуги (приемане на адреси) и NAT от страна на външния комуникационен интерфейс
14.	Да поддържа задаване на статични адреси за комуникационните интерфейси
15.	Да притежава локален потребителски интерфейс за управление и наблюдение

16.	Да притежава комуникационни интерфейси тип: минимум 100BASE-TX, RJ45
17.	Да притежава интерфейси за управление и въвеждане на ключове, посредством външен носител
18.	Да позволява отдалечено управление
19.	Да може да извършва автоматична самодиагностика
20.	Електрическото захранване да работи минимум в интервал 150 ÷ 230 VAC / 50Hz с възможност за „hot-plug" замяна без спиране на криптографското средство
21.	Да притежава автономно охлаждане
22.	Външен размер подходящ за монтиране в 19" комуникационен шкаф
23.	Работна температура на околната среда от 0°C до +50°C
24.	Температура на съхранение в интервал от –25°C до +70°C
25.	Влажност 5% до 95%, некондензираща
26.	Да разполага с крепежни елементи за монтаж в комуникационен шкаф 19" с дълбочина до 800 mm (разстояние между шините)
27.	Гаранционен срок – минимум 3 години

3.2. Хардуерно криптиращо устройство минимум 10Mbps:

№	Минимални изисквания
1.	Наличие на отделен сесиен ключ за всеки криптиран тунел
2.	Наличие на хардуерен генератор на случайни числа
3.	Поддръжка на минимум 100 криптирани IP VPN тунела
4.	Възможност за въвеждане на криптографски ключове от потребителя
5.	Разделени нива на достъп до менюто на криптографското средство
6.	Възможност за локално и отдалечено блокиране на криптографското средство
7.	Защитен криптографски модул
8.	Минимална скорост на криптиране 10Mbps
9.	Изграждане на различни типове криптографски мрежи
10.	Възможност за криптиране на данни, глас и видео в реално време
11.	Да поддържа приоритизация на пакетите
12.	Да поддържа DHCP услуги (раздаване на адреси), статично или динамично рутиране от страна на вътрешния комуникационен интерфейс

13.	Да поддържа DHCP услуги (приемане на адреси) и NAT от страна на външния комуникационен интерфейс
14.	Да поддържа задаване на статични адреси за комуникационните интерфейси
15.	Да притежава локален потребителски интерфейс за управление и наблюдение
16.	Да притежава комуникационни интерфейси тип: минимум 10/100BASE-TX, RJ45
17.	Да притежава интерфейси за управление и въвеждане на ключове, посредством външен носител
18.	Да позволява отдалечено управление
19.	Да може да извършва автоматична самодиагностика
20.	Електрическото захранване да работи минимум в интервал 150 ÷ 230 VAC / 50Hz с възможност за „hot-plug" замяна без спиране на криптографското средство
21.	Да притежава автономно охлаждане
22.	Външен размер подходящ за монтиране в 19" комуникационен шкаф
23.	Работна температура на околната среда от 0°C до +50°C
24.	Температура на съхранение в интервал от –25°C до +70°C
25.	Влажност 5% до 95%, некондензираща
26.	Да разполага с крепежни елементи за монтаж в комуникационен шкаф 19" с дълбочина до 800 mm (разстояние между шините)
27.	Гаранционен срок – минимум 3 години

Хардуерните криптиращи устройства по т. 3.1. да са съвместими с хардуерните криптиращи устройства по т. 3.2.

Хардуерните криптиращи устройства трябва да отговарят на минималните технически изисквания, посочени в т. 3.1. и 3.2, като се допускат предложения със завишени параметри.

4. Място за изпълнение:

– за доставката: гр. София, ул. „6-ти септември" №29 – сграда на МВР.

– за обучението – при производителя на криптографските средства;

– за конфигурирането на криптографските средства – при възложителя.

5. Изисквания за качество и стандарти

5.1. Всички компоненти да са нови, неупотребявани и оригинални продукти от актуалния каталог на съответния производител към датата на изготвяне на оферта. Продуктите да не са рециклирани, ремаркетирани или със занижено качество по друг начин.

5.2. Криптиращите устройства да притежават CE маркировка и да отговарят на стандарти БДС EN 55022 class B, БДС EN 55024 и БДС EN 60950-1 или техни еквиваленти.

5.3. Производителят на криптиращите устройства да притежава система за управление на качеството по БДС EN ISO 9001:2008 или еквивалент.

6. Изисквания за гаранция

6.1. Минималния гаранционен срок е 3 години от въвеждането в експлоатация на криптиращото устройство (след тестване и конфигуриране). Гаранционното обслужване е за сметка на изпълнителя и включва поддръжка по телефона, диагностика и профилактика на място, обновяване на фърмуера на устройствата, поддържане в наличност на резервни части и ремонт или подмяна на дефектирали компоненти или устройства.

6.2. При критични проблеми, които нарушават работоспособността на устройствата или основната им функционалност за реализиране на мрежова свързаност и защита на информацията, да се гарантира максимално време за диагностика на проблема на място при клиента до 4 часа след съобщаване за проблема и максимално време за отстраняване на проблема чрез ремонт или подмяна – до 12 часа (включително в неработни дни).

6.3. При всички останали проблеми да се гарантира максимално време за диагностика на проблема на място при клиента до 1 работен ден след съобщаване за проблема и максимално време за отстраняване на проблема чрез ремонт или подмяна – до 5 работни дни.

6.4. Да се гарантират минимум 5 години извънгаранционно обслужване. Извънгаранционното обслужване е за сметка на клиента и включва поддръжка по телефона, диагностика и профилактика на място, поддържане в наличност на резервни части и ремонт или подмяна на дефектирали компоненти или устройства.

7. Изисквания към опаковката и етикетирането

Криптографските средства да се доставят с пълен комплект документация и аксесоари. Където е посочено да се доставят и допълнителни компоненти и аксесоари. Всички документи на чужд език да се съпровождат с превод на български език.

8. Специфични изисквания за сигурност

Криптиращите устройства и криптоалгоритъмът да са одобрени от Органа по криптографска сигурност за криптиране до ниво на класификация на информацията минимум „ПОВЕРИТЕЛНО”.