Екз. № 2

МИНИСТЕРСТВО НА ОТБРАНАТА
НА РЕПУБЛИКА БЪЛГАРИЯ

Т Е Х Н И Ч Е С К А С П Е Ц И Ф И К А Ц И Я

„КРИПТОГРАФСКО СРЕДСТВО ЗА ЗАЩИТА НА НАЦИОНАЛНА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ ДО НИВО НА КЛАСИФИКАЦИЯ ДО „ЗА СЛУЖЕБНО ПОЛЗВАНЕ “ВКЛЮЧИТЕЛНО”

ТС А 69 3802 21-ВО

СОФИЯ
2021 г.

1. НАИМЕНОВАНИЕ НА ПРОДУКТА

„Криптографско средство за защита на национална класифицирана информация до ниво на класификация до „За служебно ползване“ включително”

2. СЪСТАВ И ОПИСАНИЕ НА ПРОДУКТА

2.1. Състав на криптографското средство:

2.1.1. Основен модул/корпус;

2.1.2. Интерфейсни и захранващи кабели и адаптери;

2.1.3. Захранващ модул (допуска се същият да е и в състава на основния модул/корпус);

2.1.4. Устройство за зареждане на криптографски ключове;

2.1.5. Елементи за монтаж в комуникационен шкаф.

Предмет на настоящата техническа спецификация (ТС) е доставка, монтиране в транспортни платформи и/или работни места, интегриране, инсталиране и гаранционна поддръжка, с възможност за експлоатация на изделие (криптографското средство/оборудване), предназначено за защита на класифицираната информация (глас, съобщения и данни) до ниво на класификация национално „За служебно ползване“, включително, съгласно ЗЗКИ, обменяна в комуникационна среда посредством криптиране на IP virtual private networks (VPNs) със скорост на криптиране до 1 Gbit/s.

3. ТАКТИКО-ТЕХНИЧЕСКИ ИЗИСКВАНИЯ КЪМ ПРОДУКТА

3.1. Изисквания по предназначение

3.1.1. Изделието да осигурява криптиране на мрежов IP трафик през Internet Protocol Security (IPSEC) или еквивалентно/и – ESP (Encapsulated Security Payload) протокол или еквивалентно/и по Стандарт RFC 2406 - IP Encapsulating Security Payload (ESP) или еквивалентно/и, като позволява изграждането на сигурни Виртуални Частни Мрежи (англ. Virtual Private Network (VPNs) и защитава мрежовият трафик от подслушване и манипулации;

3.1.2. Изделието да включва режим на работа: IPSEC RFC 2406 или еквивалентно/и в транспортен режим (ESP);

3.1.3. Изделието да включва алгоритми за криптиране на пакета с данни:

3.1.3.1. Advanced Encryption Standard (AES) или еквивалентно/и с 256 битов ключ;

3.1.3.2. троен AES или еквивалентно/и със сумарен ключ от 768 бита;

3.1.3.3. петорен AES или еквивалентно/и със сумарен ключ от 1280 бита.

3.1.4. Изделието да включва алгоритъм за удостоверяване на пакетите:

3.1.4.1. SHA256[1] или еквивалентно/и в режим Hash-based Message Authentication Code (HMAC) или еквивалентно/и с използване на произволни битове като маска.

3.1.5. Изделието да включва тип на криптиране и удостоверяване:

3.1.5.1. IPSec ESP RFC 2406 или еквивалентно/и;

3.1.5.2. AES256 или еквивалентно/и в режим GCM (от англ. Galois/Counter Mode — брояч с удостоверяване Галуа);

3.1.5.3. CBC (Cipher Block Chaining mode) + HMAC - SHA256 или еквивалентно/и.

3.1.6. Изделието да включва режим на криптиране на данни:

3.1.6.1. „Верижно Блоково Шифроване“ CBC (Cipher Block Chaining mode) или еквивалентно/и;

3.1.7. Изделието да включва (позволява) скорост на криптиране:

3.1.7.1. 50 Mbit/s;

3.1.7.2. 100 Mbit/s;

3.1.7.3. 250 Mbit/s.

---

[1] Алгоритъм, който генерира 256-битова хеш стойност от произволно количество входни данни.

3.1.8. Изделието да включва (позволява) IP рутиране, изградено върху GRE (Generic Routing Encapsulation) протокол или еквивалентно/и;

3.1.9. Изделието да включва реализация на защитна стена;

3.1.10. Хардуерната платформа на изделието да включва:

3.1.10.1. Не по-малко от един 64 битов процесор с вграден хардуерен AES ускорител, ниска консумация на ток, пасивно охлаждане;

3.1.10.2. Не по-малко от 1 (един) wide area network (WAN) порт, тип Ethernet или еквивалентно/и със скорост до 1Gbit/s;

3.1.10.3. Не по-малко от 1 (един) local area network (LAN) порт, тип Ethernet или еквивалентно/и със скорост до 1Gbit/s;

3.1.10.4. VGA (Video Graphics Array) или еквивалентно/и порт;

3.1.10.5. Не по-малко от два USB или еквивалентно/и порта.

3.1.11. Изделието да включва IP протоколи на външният WAN интерфейс:

3.1.11.1. IPV4 или еквивалентно/и;

3.1.11.2. IPV6 или еквивалентно/и.

3.1.12. Изделието да позволява работа с топологии на свързване на защитените мрежи:

3.1.12.1. Рутер;

3.1.12.2. Мост (bridge);

3.1.12.3. Възможност за изграждане на защитени мрежи с висока наличност.

3.1.13. Изделието да позволява трафик контрол (англ. Shaping (шейпинг) или еквивалентно/и;

3.1.14. Изделието да позволява зареждане на IPSec ключове и конфигурации без мрежа от USB устройство на което е записана информацията от ключов център;

3.1.15. Възможност за импортиране на предварително генерирани ключове в Центъра за управление, както и разпространение на ключовете с флаш памет/USB носител.

3.1.16. Възможност за отдалечено управление на криптиращите устройства посредством Център за управление;

3.1.17. Изделието да включва индикация за работоспособност от вграден LCD дисплей;

3.1.18. Изделието да позволява:

3.1.18.1. Криптирано съхраняване и зареждане на ключове и конфигурации (криптирани);

3.1.18.2. Тампер-защита;

3.1.18.3. Ключ за старт/стоп.

3.1.19. Електрическо захранване: (100 – 240) V/(50 – 60) Hz;

3.2. Изисквания, свързани с експлоатацията на продукта

3.2.1. Режим на работа;

Непрекъснат режим на работа (захранване) 24/7 (двадесет и четири) часа в денонощието/седем дни в седмицата.

3.3. Изисквания за устойчивост към външни въздействащи фактори

3.3.1. Допустими параметри на околната среда (при работа):

3.3.1.1. Температура на околната среда: от минус 10 °C до +60 °C;

3.3.1.2. Влажност: 95 % (RH) до +50 °C.

3.3.2. Допустими параметри на околната среда (при съхранение):

3.3.2.1. Температура на околната среда: от минус 25 °C до +70°C;

3.3.2.2. Влажност: 65 % (RH) до +50 °C.

3.3.3. Изисквания по електромагнитна защита:

3.3.3.1. Монтирането, интегрирането, инсталирането, експлоатацията и техническата поддръжка на продукта (оборудването), предмет на техническата спецификация, не трябва да влошават електромагнитните характеристики на транспортните платформи и/или работни места, на които/където е монтирана същата.

3.4. Изисквания по отношение опазването на околната среда

Не се изисква

3.5. Други специфични изисквания

3.5.1. Изисквания по експлоатацията, удобство за техническото обслужване и ремонт;

3.5.1.1. Дейностите по монтиране, експлоатацията, техническото обслужване и ремонта на продукта (оборудването), предмет на техническата спецификация, не трябва да влошават експлоатационните характеристики на същата и възможностите за техническо обслужване и ремонт.

3.5.2. Сертификация на продукта;

3.5.2.1. Продуктът (оборудването), предмет на техническата спецификация, да е одобрено от Националният орган по криптографска сигурност на Република България, за защита на класифицирана информация до ниво на класификация национално „За служебно ползване“, включително, съгласно ЗЗКИ.

3.5.3. Провеждане на изпитвания за работоспособност – съгласно искането на Заявителя;

3.5.4. Изпълнителят да е оторизиран от Производителя на оборудването, предмет на ТС да предлага, доставя, интегрира, инсталира и поддържа продукта (оборудването), предмет на техническата спецификация, за гаранционния срок и извънгаранционно обслужване на територията на Република България;

3.5.5. Монтирането, интегрирането и другите необходими дейности свързани с експлоатацията на изделието (оборудването), предмет на техни-

ческата спецификация, да е съгласно изискванията за сертифициране на същото от националния орган по криптографска сигурност на Република България, за защита на класифицирана информация до ниво на класификация национално „За служебно ползване“, включително, съгласно ЗЗКИ;

3.5.6. Продуктът (оборудването), предмет на техническата спецификация, да е нов/о, неупотребяван/о и е произведен/о не по-рано от годината предхождаща доставката;

3.5.7. Продуктът (оборудването), предмет на техническата спецификация, да е в текущата продуктова линия на Производителя.

4. ИЗИСКВАНИЯ КЪМ ВИДОВЕТЕ ОСИГУРЯВАНЕ

4.1. Обучение и средства за обучение

4.1.1. Обучение на личен състав

Изпълнителят да провежда обучение и запознава служители и администратори по криптографска сигурност на Възложителя, с права същите да провеждат обучение за работа, администриране, обслужване и техническа експлоатация на оборудването, предмет на техническата спецификация – съгласно искането на Заявителя;

4.2. Осигуряване на експлоатационна документация

4.2.1. Да бъде предоставена експлоатационна документация – инструкция за експлоатация и контролни листи;

4.2.2. Да бъде предоставена техническа документация - техническо описание и примерни схеми на свързване.

4.3. Осигуряване на техническа помощ;

4.3.1. В рамките на гаранционния срок Изпълнителят да осигури основна точка за контакт и консултации, като комуникацията с нея да се извършва по избор, чрез стационарен телефон, мобилен телефон, факс, електронна поща и писмено уведомление;

4.3.2. В рамките на гаранционния срок в основната точка за контакт Изпълнителят[2] да осигури приемане/регистриране (завеждане) на уведомления за възникнали аварии (откази и/или повреди), заявки за услуги, диагностика и ремонт, доклади за състоянието на оборудването и друга кореспонденция по извършването на техническото поддържане на криптографското оборудване, предмет на настоящата техническа спецификация;

4.3.3. В рамките на гаранционния срок основната точка за контакт да работи:

4.3.3.1. По схемата 8/5 (осем часа през работното време, в работните дни от седмицата) – за консултация със специалист на Изпълнителя;

4.3.3.2. Консултацията да обхваща следните дейности:

4.3.3.2.1. Консултиране и дистанционна помощ по ежедневната дейност на представители на Възложителя за работата на оборудването;

4.3.3.2.2. Консултиране при възникнала авария за диагностициране на проблем/и и предложения за възможни незабавни мерки по отстраняването му/им;

4.3.3.2.3. Консултациите да се завеждат/отчитат (зададен въпрос от Потребителя, даден отговор или препоръчано действие от Изпълнителя, както и получените резултати от предприетите действия) в дневници, заведени при Потребителя и Изпълнителя.

4.4. Осигуряване на оборудване за поддръжката и ремонта, резервни части, инструменти и принадлежности;

Изисква се

4.5. Осигуряване на тестово и метрологично оборудване;

Изисква се

---

[2] Навсякъде в техническата спецификация където се записва Изпълнител/Възложител да се счита и за представители на същите.

4.6. Други изисквания към видовете осигуряване.

Не се изисква

5. ИЗИСКВАНИЯ КЪМ ОПАКОВКАТА, МАРКИРОВКАТА, ЕТИКЕТИРАНЕТО

5.1. Изделието да бъде доставено в оригиналната транспортна опаковка устойчива на удар, вибрации и повишена влажност;

5.2. Допълнителните принадлежности да са доставени в подходящи опаковки за съхранение, недопускащи механично и физикохимично въздействие;

5.3. Изделието да бъде маркирано по подходящ начин, указващ, наличието на контролирано съдържание в опаковката.

6. ИЗИСКВАНИЯ ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

6.1. За изпълнение на дейностите по настоящата техническа спецификация, на Изпълнителя ще бъде необходимо посещение на режимни формирования и/или обекти от МО и БА/транспортни платформи, по смисъла на чл. 162 от ППЗЗКИ, както и зони за сигурност клас I и клас II, за което следва да се предприемат необходимите мерки за това, при спазване на ЗЗКИ и съпътстващата го нормативна и поднормативна база;

6.2. При допускане на специалисти на Изпълнителя на територията на военните формирования да се спазват всички изисквания на пропускателния режим, установени в регламентиращите документи.

7. ГАРАНЦИОНЕН СРОК

7.1. Гаранционният срок на изделието (оборудването) **при експлоатация**, предмет на техническата спецификация, да бъде не по-кратък от 24 (двадесет и четири) месеца, считано от датата на подписване на двустранния протокол след приемни изпитвания за работоспособност – съгласно искането на Заявителя;

7.2. Гаранционният срок на изделието (оборудването) **при съхранение**, предмет на техническата спецификация, да бъде не по-кратък от 36 (тридесет и шест) месеца, считано от датата на подписване на двустранния протокол.

8. ОЦЕНЯВАНЕ НА СЪОТВЕТСТВИЕТО

8.1. Оценяване на съответствието на продукта (оборудването), предмет на техническата спецификация, с изискванията на договора се извършва от комисия, с председател представител на Възложителя, с участие на представители на Заявителя/Потребителя и Изпълнителя по договора. В случаите, когато Възложител е министъра на отбраната, председател на комисията е представител на Институт по отбрана „Професор Цветан Лазаров“;

8.2. Изпълнителят представя на комисията следните документи:

8.2.1. Документ, че продуктът (оборудването), предмет на техническата спецификация, е одобрено от националният орган по криптографска сигурност на Република България, за защита на класифицирана информация до ниво на класификация национално „За служебно ползване“, включително, съгласно ЗЗКИ;

8.2.2. Декларация съдържаща текст, че доставения продукт е нов, неупотребяван и е произведен не по-рано от годината предхождаща доставката;

8.2.3. Гаранционна карта за продукта (оборудването), предмет на техническата спецификация, с идентифициращия го сериен номер (номер, партида или друго, идентифициращо продукта/оборудването), издадена от Изпълнителя;

8.2.4. Декларация за съответствие с изискванията на договора, съгласно БДС EN ISO/IEC 17050-1:2010 или еквивалентно/и, издадена от Изпълнителя, за съответствие на извършената доставка с изискванията на договора;

8.3. Документите по т. 8.2, които са на чужд език, да са съпроводени с превод на български език.