МИНИСТЕРСТВО НА ВЪТРЕШНИТЕ РАБОТИ
ДИРЕКЦИЯ "УПРАВЛЕНИЕ НА СОБСТВЕНОСТТА И СОЦИАЛНИ ДЕЙНОСТИ"
гр. София 1301, ул. "Княз Борис I" № 124
УРИ 5785опн-6-5785мпр-42/16.08.2017г.

ДОГОВОР ЗА ОБЩЕСТВЕНА ПОРЪЧКА

Днес, ...2017 г., в гр. София, след проведена процедура, открита с Решение № 5785мпр-19 от 24.03.2015 г. на възложителя, между:

МИНИСТЕРСТВО НА ВЪТРЕШНИТЕ РАБОТИ, с адрес: гр. София, ул. "6-ти септември" № 29, ИН по ДДС BG 000695235, представлявано от Георги Стоянов – заместник - директор на ДУССД – МВР (съгласно Заповед № 8121з – 200/02.02.2017 г., наричано по-долу за краткост Възложител, от една страна,

и

„С ЕНД Т-ОСИ" ДЗЗД, със седалище и адрес на управление: гр. София, бул. „Искърско шосе" № 7, Търговски център „Европа", сграда 6, ет. 3, код по БУЛСТАТ 177143204, представлявано от Злати Стойчев Петров, в качеството на представляващ, наричана по-долу Изпълнител от друга страна и на основание чл.41, ал.1 от ЗОП (отм.), за възлагане на обществена поръчка, с предмет: „Разширение на системите за публичен частен ключ (PKI), изградени за обслужване на процеса на издаване на документи за самоличност с електронен носител, включително изграждане на единна точка за контакт (SPOC) и връзка с ICAO – PKD върху системата за граничен контрол", и Решение № 5785опм-6-5785мпр-11/23.02.2017 г. на Възложителя за определяне на Изпълнител, се сключи настоящият договор, като страните се споразумяха за следното:

I. ПРЕДМЕТ НА ДОГОВОРА.

Чл.1.(1) Възложителят възлага, а Изпълнителят приема да достави срещу възнаграждение хардуерни и софтуерни средства за разширение на системите за публичен частен ключ (PKI), изградени за обслужване на процеса на издаване на документи за самоличност с електронен носител, включително изграждане на единна точка за контакт (SPOC) и връзка с ICAO – PKD върху системата за граничен контрол, както следва:

Арт.1. HSM	- 9 броя;
Арт.2. Сървъри	- 6 броя;
Арт.3. LAN комутатори	- 3 броя;
Арт.4. SAN комутатори	- 3 броя;
Арт.5. Дисков масив	- 2 броя;
Арт.6. Диск-базирано архивиращо устройство	- 2 броя;
Арт.7. Софтуер и лицензи	- 1 брой,

съгласно техническата спецификация - Приложение №1 и Техническа оферта – Приложение № 2, неразделна част от този договор.

(2) Настоящият договор включва следните дейности:

1.Разширение на съществуващите системи на CSCA/ CSRA и CVCA/CVRA, с цел осигуряване на новата функционалност към системата за Граничен контрол;

2. Разширение на системите за PKI – изграждане на DV, DVRA и IS;

3. Изграждане на National Public Key Directory (NPKD), SPOC и връзка с IKAO-PKD;

4. Разработване на програмни средства за транспортиране на заявки за сертификати, получаване, актуализация и съхранение на сертификати;

5. Разработване на програмни средства, за работа със сертификати при изпълнение на EAC (Разширен контрол за достъп на Системата за проверка до биометричните данни, съхранени в електронния носител на информация (чип), вграден в документа на национални и чужди документи за пътуване).

(3) Изпълнителят приема да извърши всички услуги, съпътстващи доставката - разопаковане, монтаж, инсталация, конфигуриране, тестване, внедряване и гаранционно

2784

обслужване на доставените по предходната алинея технически и програмни средства, включително и да обучи служители на МВР за работа с тях.

II. СРОК, НАЧИН И МЯСТО НА ИЗПЪЛНЕНИЕ.

Чл.2.(1) Настоящият договор влиза в сила от датата на подписването му. Изпълнението на договора се извършва на две фази:

(2) Фаза 1.Дейности по разширение на съществуващите системи:

1. Етап 1 - Изготвяне на проект на техническо решение, съгласно техническата спецификация - до 30 (тридесет) календарни дни след подписване на договора;

2. Етап 2 - Доставка на необходимите технически и програмни средства и реализиране на включеното по Етап 1– до 90 (деветдесет) календарни дни след приемане на етап 1.

3. Етап 3. Внедряване на включеното във фаза 1 на разширението и обучение – до 30 (тридесет) календарни дни след приемане на етап 2.

(3) Фаза 2. Дейности, осигуряващи изискванията по разширение на системите за PKI:

1. Етап 1. Изготвяне на проект на техническо решение, отговарящо на техническата спецификация – до 30 (тридесет) календарни дни след приемане на Етап 3 от Фаза 1.

2. Етап 2. Доставка на необходимите технически и програмни средства и реализиране на разширението в тестова среда – до 60 (шестдесет) календарни дни след приемане на етап 1.

3. Етап 3. Внедряване на включеното в Етап 1 и Етап 2 на Фаза 2, обучение и цялостно внедряване на проекта – до 60 (шестдесет) календарни дни след приемане на етап 2.

(4) Изпълнението на всеки етап започва след писмено уведомление за готовност от страна на възложителя. Уведомлението се изпраща в срок до 7 (седем) календарни дни от датата на подписване на договора, или от датата на приемане на предходен етап. Приемането на всеки етап се извършва с протокол на комисия, назначена със заповед на възложителя. Приключването на Етап 3 се извършва с протокол, утвърден от Възложителя.

Чл.3.Място на изпълнение: Дирекция „Комуникационни и информационни системи" - МВР, гр. София, ул. „Теодосий Търновски" № 42.

III. ПРИЕМАНЕ И ОБУЧЕНИЕ. ГАРАНЦИОННО ОБСЛУЖВАНЕ.

Чл.4.(1) Приемането на доставката се извършва на посоченото в чл.3 от договора място, след подписан от представители на страните приемо- предавателен протокол за доставка;

(2) Приемо- предавателният протокол се подписва само срещу протокол за съответствие, подписан от представители на възложителя. За времето от подписването на приемо-предавателният протокол до изготвянето и подписването на протокола за съответствие, се подписва протокол за временно съхранение и отговорно пазене;

(3) Изпълнителят се задължава, доставеното оборудване да не е използвано преди това и да е в производствената листа на производителя за 2014 година.

(4) Изпълнителят се задължава, цялото оборудване да отговаря на параметрите и техническите характеристики от Техническата оферта на Изпълнителя, приложена към договора и е в пълно съответствие с Техническата спецификация на Възложителя.

(5) Изпълнителят се задължава, доставката да се придружава със съответната документация, съгласно техническата спецификация.

Чл.5.(1). Гаранционният срок е стандартен фирмен и е 36 (тридесет и шест) месеца.

(2) Гаранционното обслужване е на място, в режим 24/7, като:

1. Времето за реакция е максимално до 4 (четири) часа от момента, в който потребителят е заявил наличие на технически проблем;

2. Времето за отстраняване е до 24 (двадесет и четири) часа. Ако ремонтът изисква повече от 24 часа, изпълнителят предоставя еквивалентно устройство за временна замяна. В този случай, гаранционния срок на взетото за ремонт устройство се удължава с времето за отстраняване на повредата;

(3) При подмяна на носител на информация не се допуска неговото изнасяне от МВР;

(4) Гаранционно обслужване на софтуера включва актуализиране / надстройване на софтуера в отговор на каквито и да са установени несъответствия във функционирането на системното и приложното програмно осигуряване, както и при промени в европейски стандарт CSN 36 9791, Решения на Европейската комисия C(2008) 8657 от 22.12.2008, C(2009) 7476 от 5.10.2009, C(2002) 3069 , C(2009) 3770 от 20.5.2009, C(2011) 5478 от 4.8.2011.

Чл.6.(1) След изпълнението на всеки етап се изготвят протоколи - изпълнение на инсталиране и конфигуриране; пускане на оборудване и софтуер в експлоатация; проведени тестове; проведено обучение.

(2) За установяване на отклоненията и недостатъците се съставя протокол, подписан от представители на Възложителя и Изпълнителя.

Чл.7. Изпълнителят приема да обучи до 30 служители на МВР – представители на Възложителя по предварително съгласувани график и теми.

IV. ЦЕНИ. УСЛОВИЯ И НАЧИН НА ПЛАЩАНЕ.

Чл.8.(1) Възложителят се задължава да заплати на Изпълнителя цена в размер на 2 497 117.00(словом: два милиона четиристотин деветдесет и седем хиляди сто и седемнадесет) лева без ДДС или 2 996 540.40 (словом: два милиона деветстотин деветдесет и шест хиляди петстотин и четиридесет и 0,40) лева с вкл. ДДС, съгласно Ценовата оферта на Изпълнителя, Приложение №14, неразделна част от договора.

(2) В цената по предходната алинея са включени всички транспортни разходи, такси, пощенски услуги и комуникации.

(3) Разходите за доставка на технически и програмни средства, разопаковане, монтаж, инсталация, конфигуриране, тестване, внедряване, обучение, актуализиране на софтуера и гаранционно обслужване са за сметка на изпълнителя.

Чл.9.(1) Плащането на изпълнените дейности се извършва по банков път, по сметка на изпълнителя, след приключване на Фаза 2, Етап 3 (т. 12.3 от Приложение №1 „Техническа спецификация“), срещу представени от изпълнителя оригинална фактура и протокол за изпълнението на горецитирания етап, утвърден от възложителя.

(2) Банковата сметка на Изпълнителя е:

Банка – Обединена Българска Банка АД

Банкова сметка: BG33UBBS80021083565130

Банков код: UBBSBGSF

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ.

Чл.10.(1) Изпълнителят се задължава:

1. да изпълни доставката, като транспортирането и разтоварването до мястото за изпълнение са за сметка на изпълнителя;

2. да инсталира, конфигурира и интегрира доставеното хардуерно и софтуерно оборудване, както и да обучи служители на Възложителя за работа с тях.

3. да достави техническите средства, като същите са окомплектовани с всички необходими аксесоари, осигуряващи работата им и свързването им към други системи, като

например: токозахранващи кабели, входни устройства, захранващи адаптери, токозахранващи удължители, кабели за вътрешно и междинно свързване, адаптери, монтажни китове и т.н.

4. За всяка единица доставен артикул, изпълнителят гарантира, че същата е напълно съвместима със спецификациите на другите артикули, включени в Приложение 1 „ Техническа спецификация“.

5. Изпълнителят е отговорен за предоставяне на гаранционно обслужване. За всички технически проблеми се задължава да има разкрито помощно бюро (хелп деск) за техническа поддръжка. Достъпът до помощното бюро е осигурен чрез телефонен номер, факс и e-mail в РБългария, които да не поставят потребителите пред необходимост да заплащат разговори по международни тарифи или по такива за разговори на големи разстояния

6. да изпълни поръчката, съгласно приложените към договора ценова и техническа оферти.

7. За срока на действие на договора, Изпълнителят осигурява:

а) достъп до сайта на производителя с възможност за изтегляне на обновления за програмните продукти;

б) достъп до сайта на производителя с възможност за изтегляне на нови версии за програмните продукти;

в) възможност за регистриране на проблеми и консултации денонощно директно към производителя - по телефон и електронна поща;

г) консултации и системна помощ на място за програмните продукти.

(2) Изпълнителят има право да:

1. иска от Възложителя необходимото съдействие за изпълнение на поръчката;

2. получи договореното възнаграждение по реда и при условията на настоящият договор;

Чл.11.(1) Възложителят се задължава:

1. да заплати цената на договора по реда и при условията в него:

2. да не възпрепятства Изпълнителя и да не нарушава оперативната му самостоятелност във връзка с изпълнението на договора;

3. да уведомява писмено Изпълнителя в предвидените в този договор случаи.

(2) Възложителят има право:

1. да оказва текущ контрол при изпълнението на договора:

2. да иска от Изпълнителя да изпълни възложената поръчка в срок и без отклонение.

3. да откаже приемането и заплащането на част или цялото възнаграждение, когато Изпълнителят се е отклонил от изискванията на договора.

VI. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ НА ДОГОВОРА.

Чл.12.(1) Гаранцията за добро изпълнение се определя от Възложителя в размер на 5% от общата стойност на договора без ДДС или 124 855.85 лева (словом: сто двадесет и четири хиляди осемстотин петдесет и пет и 0.85).

(2) Изпълнителят сам избира формата на гаранцията. Гаранцията за изпълнение на договора се представя от Изпълнителя под формата на парична сума или банкова гаранция.

(3) Гаранцията, представена във вид на парична сума, се внася по IBAN: BG09 BNBG96613300146201, BIC код: BNBGBGSD, банка БНБ, на името на Министерство на вътрешните работи. Всички банкови разходи свързани с обслужването на превода на гаранцията, включително при нейното възстановяване са за сметка на изпълнителя.

(4) Когато гаранцията за изпълнение на договора е под формата на банкова гаранция, то тя е безусловна, неотменяема, представена преди подписването на договора, покриваща 100 % стойността на гаранцията за изпълнението му, със срок на валидност - срока за изпълнение на

договора, плюс срока на гаранционната поддръжка, плюс 30 дни.

(5) Когато поръчката не бъде изпълнена в договорения краен срок, Изпълнителят е длъжен да удължи срока на банковата гаранция или да предостави на Възложителя нова банкова гаранция с валидност - срокът на изпълнение на поръчката, плюс срока на гаранционната поддръжка плюс 30 дни..

(6) При точно и пълно изпълнение на договора, Възложителят освобождава 75% от внесената гаранция за изпълнение по ал.1 или 93 641.89 лева /деветдесет и три хиляди шестстотин четиридесет и един и 0.89/ в срок от 20 (двадесет) работни дни след подписан протокол, утвърден от Възложителя за изпълнението на Фаза 2, Етап 3 , без да се дължат лихви на изпълнителя. Останалите 25 % или 31 213,96 лева /тридесет и една хиляди двеста и тринадесет и 0.96/ се задържат като обезпечение на дейностите по гаранционното обслужване и се възстановяват в срок от 20 /двадесет/ работни дни след изтичане на срока, посочен в чл.5, ал.1 от договора. При прекратяване на договора, гаранцията за изпълнение се възстановява в пълен размер в срок от 20 /двадесет/ работни дни след прекратяването му, без да се дължат лихви на изпълнителя.

(7) Възложителят задържа гаранцията за изпълнение на договора, ако в процеса на неговото изпълнение възникне спор между страните, до приключването му с влязло в сила съдебно решение или споразумение.

(8) Възложителят задържа гаранцията за изпълнение при пълно неизпълнение на поръчката.

(9) Възложителят има право да удържи от стойността на гаранцията за изпълнение, размера на начислените неустойки по чл.13 от този договор.

VII. САНКЦИИ.

Чл.13.(1) Ако Изпълнителят не изпълни доставката в срок, същият дължи неустойка в размер на 0,15 на сто върху стойността на неизпълнената доставка за всеки просрочен ден, но не повече от 10 (десет) на сто от стойността на договора, посочен в чл.8, ал.1.

(2) При частично неизпълнение, Изпълнителят дължи неустойка в размер на 5 % (пет на сто) от стойността на неизпълнената част.

(3) При забава изпълнението на гаранционното обслужване по чл.5, т.1 и т.2, Изпълнителят дължи неустойка в размер на 0,01% /нула цяло, нула едно на сто/ върху стойността на аварираната техника за всеки просрочен час.

(4) При забава на дължимо плащане, Възложителят дължи неустойка в размер законната лихва за забава върху неизплатената в срок сума за всеки просрочен ден;

(5) За неизпълнението на други задължения по договора, различни от тези по алинея 1 и алинея 2, неизправната страна дължи на изправната неустойка в размер до 10 (десет) на сто от стойността на договора. Страната, която е понесла вреди от неизпълнението може да търси обезщетение и за по-големи вреди.

(6) При прекратяване на договора по чл.15, т.1. страните не си дължат неустойки.

VIII. ИЗМЕНЕНИЕ И ПРЕКРАТЯВАНЕ НА ДОГОВОРА.

Чл.14. Изменението на договора се извършва по взаимно съгласие с подписване на двустранен анекс между страните. Изменението на договора не трябва да води до нарушение на разпоредбите в ЗОП, регламентиращи правните основания за изменение на договор за обществена поръчка.

Чл.15. Този договор се прекратява:

1. по взаимно писмено съгласие между страните, чрез подписване на двустранно споразумение;

2. с изпълнение на задълженията на страните по него, включително задълженията на Изпълнителя в рамките на гаранционния срок;

3. едностранно от Възложителя с писмено уведомление до другата страна, когато Изпълнителят бъде обявен в неплатежоспособност или бъде открита процедура за обявяването му в несъстоятелност или ликвидация.

4. едностранно от Възложителя с 10-дневно писмено предизвестие до другата страна, когато Изпълнителят не изпълни задължението си по този договор.

Чл.16. Възложителят има право да развали договора с едностранно 15-дневно писмено предизвестие до другата страна, когато Изпълнителят виновно забави изпълнение на задължение по този договор с повече от 10 (десет) дни.

НЕПРЕОДОЛИМА СИЛА.

Чл.17.(1)Страните не носят отговорност за неизпълнение на задълженията си, ако неизпълнението на задълженията е предизвикано от действието на непредвидимо и непредотвратимо събитие от извънреден характер и извън разумния им контрол, възникнало след сключване на договора, което прави изпълнението невъзможно (форсмажорно обстоятелство, непреодолима сила). Страната, която се позовава на форсмажорно обстоятелство, трябва да докаже причинната връзка между неизпълнението на задълженията си и непреодолимата сила.

(2) Настъпването на форсмажорното обстоятелство по ал.1 се доказва с надлежно оформен документ от компетентен орган и се фиксира със съставяне и подписване на двустранен протокол.

(3) Страната, която се позовава на форсмажорното обстоятелство, трябва в 3 (три) дневен срок от настъпването му, писмено да уведоми за това другата страна. При неизпълнение на това задължение страната няма право да се позовава на форсмажорни обстоятелства.

(4) Неизправната страна, която е била в забава при настъпването на непреодолимата сила, няма право да се позовава на форсмажорно обстоятелство.

(5) Не е налице непреодолима сила, ако съответното обстоятелство се е случило вследствие на неположена дължима грижа от страна по този договор или ако при полагане на дължимата грижа това обстоятелство може да бъде преодоляно.

(6) Докато трае непреодолимата сила, изпълнението на задълженията се спира.

(7) Ако непреодолимата сила продължи повече от 100 (сто) дни и няма признаци за скорошното й преустановяване, Възложителят има право да прекрати договора едностранно като писмено уведоми другата страна. Ако непреодолимата сила трае толкова, че Изпълнителят вече няма интерес от изпълнението той има право да прекрати договора едностранно като писмено уведоми другата страна.

X. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ.

Чл.18.(1) Всички уведомления между страните, които ще бъдат отправяни по този договор са валидни, ако са извършени в писмен вид на български език и са изпратени по факс или с препоръчана поща с обратна разписка на следния адрес:

1.за Възложителя: Министерство на вътрешните работи – гр. София, ул. „Княз Борис I" № 124.

2. за Изпълнителя: „Обединение „С&Т – ОСИ"" – гр. София, бул. „Искърско шосе" № 7, Търговски център „Европа", сграда 6, ет. 3.

(2) Всяка страна по този договор е длъжна в 3-дневен срок от промяна на адреса/ факса по ал.1 да уведоми другата за настъпилата промяна и да посочи новия си адрес/ факс за кореспонденция.

(3) Ако страната по договора не изпълни задълженията си по ал. 2 се счита, че

уведомленията по ал. 1 са връчени редовно.

Чл.19. Всички спорове, породени от този договор или отнасящи се до него, или до допълнителни споразумения към него, включително и споровете, породени от или отнасящи се до тълкуване, недействителност, неизпълнение или прекратяване, ще бъдат решавани по взаимно съгласие с подписване на двустранно споразумение. Ако между страните не бъде постигнато споразумение, спорът се отнася за решаване пред компетентен съд. Когато предметът на спора между страните е за имуществени права, той се отнася за разрешаване пред компетентен съд в град София.

Чл.20. Страните по този договор ще решават споровете, възникнали при и по повод изпълнението му по взаимно съгласие и с писмени споразумения, а при непостигане на съгласие въпросът се отнася за решаване пред компетентния съд на територията на Република България, съгласно разпоредбите на Българското законодателство.

Чл.21. За неуредените по този договор въпроси се прилагат разпоредбите на законодателството на Република България.

Настоящият договор се изготви и подписа в три екземпляра - два за Възложителя и един за Изпълнителя.

Неразделна част от настоящият договор са следните приложения:

Приложение № 1 „Техническа спецификация" - 17 листа;

Приложение №2 „Техническа оферта" - 75 листа на изпълнителя, съгласно която е определен за изпълнител;

Приложение №3 „Ценова оферта" - 2 листа на изпълнителя, съгласно която е определен за изпълнител.

ВЪЗЛОЖИТЕЛ: ..... *(подпис, дата и печат)* ЗАМ. ДИРЕКТОР НА ДУССД /съгл. заповед № 8121з – 200/02.02.2017г./ .....16.03.17г..... ЛИЦЕ, ОТГОВОРНО ЗА СЧЕТОВОДНИТЕ ЗАПИСВАНИЯ: Иванка Червенкова */подпис/* (06.04.2017г.) */дата/*	ИЗПЪЛНИТЕЛ: Злати Петров ..... *(подпис и печат)* „ОБЕДИНЕНИЕ „С&Т – ОСИ"" ЗЛАТИ ПЕТРОВ Представляващ 03.04.2017г. *Дата на подписване:*

Забележка: Проектът на този договор се допълва с всички предложения от офертата на определения изпълнител на обществената поръчка (чл. 41, ал. 2 ЗОП).

Приложение №1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

1. Обща информация:

В съответствие с осъществяваните от МВР дейности по поддържането на инфраструктурата на PKI за издаване на български документи за самоличност и необходимостта за проверка на българските и документите на гражданите на други страни на граничните пунктове при пътуване, този проект трябва да направи разширение на системите за "публичен частен ключ" (PKI) за използването им в АИС "Граничен контрол".

С въвеждането на PKI в документите за пътуване се дава възможност за автоматично, без човешка намеса потвърждение, че лицето, което представя документ за задгранично пътуване, е едно и също лице, показано на страницата с данни, както и върху чипа с уверението, че данните са били поставени там от издаващия орган и че данните не са променени.

При проверка на граничен контрол трябва да може да се провери автентичността, целостта, сигурността и оригиналността на е-документ, т.е. дали:

1.1. Чипът е истински, издаден от оторизиран орган и данните в него, са непроменени;

1.2. Чувствителните данни, записани в чипът са защитени срещу неоторизиран достъп и комуникацията между чипа и устройството за четене са защитени срещу подслушване;

1.3. Чипът е заменен от копие.

2. Използвани термини и съкращения

име	Съкращение	Роля/обяснение
е-документ		документи за пътуване с електронен носител на информация
чип		електронен носител на информация в е-документ
АИС „ГК"		Автоматизирана информационна система „Граничен контрол"
Basic Access Control	**BAC**	Основен контрол за достъп до данни, съхранени в електронния носител на информация (чипа), вграден в документа на национални и чужди документи за пътуване
Brussels Interoperability Group	**BIG**	Брюкселска оперативна група за съвместимост
Federal Office for Information Security in Germany	**BSI**	Германската федерална служба за информационна сигурност
Certificate Authorities	**CA**	Институция, която е упълномощена да издава цифрови сертификати и да ги подписва със своя частен ключ; Осигурява доверие между непознати страни; Наричан още сертифициращ (удостоверяващ) орган
Country Signing Certification Authority Certificate	**CSCAC**	Сертификат издаден от CSCA; Самоподписан, носи Публичния ключ на държавата;
Document Signer Certificate	**DSC**	Сертификат на органа за подпис на документи, издаден от CSCA; Съхранява се в инспек. система и/или в чипа на

		документа
Country Signing Certification Authority	**CSCA**	Сертифициращ орган удостоверяващ цифров подпис на държавата; - Издава и управлява сертификата на органа за подпис на документи (DS)
Country Signing Registration Authority	**CSRA**	Регистриращ орган на държавата за подписване
Certificate Policy	**CP**	Политика за предоставяне на удостоверителни услуги
Certificate Revocation List	**CRL**	Списък с анулирани сертификати
Country Verifying Certificate Authority	**CVCA**	Орган удостоверяващ цифров подпис на държавата за проверка на документи; Издава и управлява сертификата на вътрешните и външни DVCAs
Country Verifying Registration Authority	**CVRA**	Регистриращ орган на държавата за проверка
Document Signer	**DS**	Орган за подписване на документи
Distinguished Name	**DN**	Уникално име
Digital Signature Algorithm	**DSA**	Вид криптографски алгоритъм за създаване на подпис
Document Verifier	**DV**	Верификатор на документи
Document Verifier Certificate Authority	**DVCA**	Издава и управлява сертификатът на Система за проверка – IS
Document Verifier Registration Authority	**DVRA**	За регистрация на свързваните към системата Инспекционни системи (IS) и за обработка на постъпващите от тях заявки за издаване на сертификати
Extended Access Control	**EAC**	Разширен контрол за достъп на Системата за проверка до биометричните данни (изображения на пръстови отпечатъци) съхранени в електронния носител на информация(чипа), вграден в документа на национални и чужди документи за пътуване
Elliptic Curves Digital Signature Algorithm	**ECDSA**	Вид криптографски алгоритъм за създаване на подпис
EUCertificate Policy	**EUCP**	Политика за предоставяне на удостоверителни услуги на ЕС
Hardware Security Modul	**HSM**	Хардуерен криптографски модул за съхранение на частни ключове
International Civil Aviation Organization	**ICAO**	Международна организация за гражданска авиация
ICAO Public Key Directory	**ICAO PKD**	Публичната директория за ключове на ICAO
Inspection system	**IS**	Инспекционна система
Document Signer Public Key	**KPuDS**	Публичен ключ за проверка на автентичността на Document Security Object (SOD)
Lightweight Directory Access Protocol	**LDAP**	Протокол за опростен достъп до регистър
Logical Data Structure	**LDS**	Логическа структура на данните

Machine Readable Travel Documents	**MRTDs**	Машинно читаеми документи за пътуване
Machine Readable Zone	**MRZ**	MRZ се състои от лични данни, отпечатани върху долната част на страницата на данни на Е-паспорта. Информация може да бъде прочетена като се прекара страница на OCR четец (скенер). MRZ се използва за отключване на информацията, съдържаща се във вградения чип.
National Public Key Directory	**NPKD**	Директория, съдържаща български и чужди сертификати, CRL и др.
Optical Character Recognition	**OCR**	Оптично разпознаване на символи
Online Certificate Status Protocol	**OCSP**	Протокол за on-line проверка на статуса на сертификати; За публикуване на издадените сертификати на DS и CRL
Passive Authentication	**PA**	Механизъм за установяване на автентичността на документ чрез проверка на електронния подпис;
Password Authenticated Connection Establishment	**PACE**	Изграждане на връзка с използването на парола
Public Key Cryptography Standards	**PKCS**	Криптографски стандарт за пренос на публичен ключ
Public Key Infrastructure	**PKI**	Инфраструктура на публичния ключ
Registration Authority	**RA**	Регистриращ орган
Radio Frequency Identifcation	**RFID**	Радиочестотната идентификация - метод за автоматично идентифициране на обекти, при който от идентификатори върху обекта се четат или записват данни чрез радиовълни
Secure/Multipurpose Internet Mail Extensions	**S/MIME**	Протокол за сигурно предаване на данни през Интернет
Document Security Object	**SOD**	С RFC3369 CMS Signed Data Structure, подписана от DS; Файл - съхранява хеш стойностите на всички файлове, съхранявани в чипа (снимка, пръстов отпечатък и др.) и цифров подпис на тези хешове; Записва се в чипа на електронния документ
Supplemental Access Control	**SAC**	Допълнителен контрол на достъпа за машинно четене на документи за пътуване.

Secure Socket Layer	**SSL**	Мрежови протокол, който се използва за сигурен пренос на данни по TCP/IP мрежи; Осигурява защитени от подслушване тунели за поточно-ориентиран пренос на информация; Използва криптографски алгоритми, PKI и цифрови сертификати
Single Point of Contact	**SPOC**	Единно звено за контакт - за обмен на български и чужди сертификати и съобщения от и към страните чл. на ЕС, от и към трети страни

3. Обхват на дейностите

3.1. Описание на основните дейности

3.1.1. Изграждане на система за съхранение, използване и предоставяне на български и чужди сертификати за изпълнение на функциите по автентикация на издателя на документите - Passive Authentication (PA).

3.1.2. Изграждане на система, разрешаваща на работните места на АИС "Граничен контрол" достъп до изображения на пръстови отпечатъци, записани в електронния носител на информация на национални и чужди документи за пътуване - Extended Access Control (EAC).

3.2. Описание на съществуващите системи за публичен-частен ключ (PKI) изградени за обслужване процеса на издаване на документи за самоличност с електронен носител

Към момента МВР разполага с изградена инфраструктура за публичен-частен ключ (PKI):

3.2.1. Описание на софтуера:

3.2.1.1. За всички CA, Document Signer, OCSP и DVRA:

3.2.1.1.1. Операционна система Microsoft Windows Server 2008 Standard Edition

3.2.1.1.2. СУБД Microsoft SQL Server 2008 Standard Edition

3.2.1.1.3. JDK version 6 Update 13

3.2.1.1.4. REDHat Jboss Enterprise Application Platform version 4.2.3

3.2.1.1.5. ANT version 1.7.1

3.2.1.2. За всички CA, Document Signer:

3.2.1.2.1. HSM - Utimaco SafeGuard CryptoServer за съхранение на частния ключ.

3.2.1.3. За всички CA и OCSP:

3.2.1.3.1. EJBCA version 3.10.6 за CSCA

3.2.1.3.2. EJBCA version 3.9.0 за всички останали CA и OCSP

3.2.1.4. За всички Document Signer:

3.2.1.4.1. Sign Server version 3.0

3.2.1.5. За OCSP:

3.2.1.5.1. OpenDS version 2.0.0

3.2.2. Описание на средата:

3.2.2.1. CSCA – функционира offline. Типа на ключа е RSA с дължина 4096. Срокът на валидност на сертификата е 15 години и три месеца. Срокът за използване на ключа е 5 години.

3.2.2.2. Има регистрирани два **Document Signer** – съответно за паспорти и разрешения за пребиваване на чужденци. Валидността на сертификата на Document Signer за паспорти е 5 години и 3 месеца, а на сертификата на Document Signer за разрешения за пребиваване е 10 години и 3 месеца. Срокът за използване на ключ за двата Document Signer е три месеца.

3.2.2.3. При подновяване на ключа на двата Document Signer CSCA издава CRL (Certificate Revocation List) със срок на валидност 3 месеца. CSCA сертификата, CRL и издадените сертификати на DS се публикуват в OCSP, който функционира offline на сървъра на CSCA и в online OCSP за обслужване на производството - подписването и проверка на документите при качествен контрол и при връчване на документите. Информацията в online OCSP се актуализира при подновяване на ключа на DS.

3.2.2.4. При издаване на нов CRL, той се публикува, заедно със сертификата на CSCA на Internet страницата на МВР.

3.2.2.5. CVCA – функционира offline. Типа на ключа е ECDSA 256. Срокът на валидност

на сертификата е 3 години.Срокът за използване на ключа е 3 години. При подновяване на сертификата се издава и Linked сертификат, за връзка с предходния. CVCA не издава CRL със сертификатите за DVCA

3.2.2.6. Има регистрирани две **DVCA – DVCA-P** и **DVCA-R**. Типа на ключа за двете DVCA, съобразно изискванията на TR-03110 на BSI съвпада с типа на ключа на CVCA и е ECDSA 256. Срокът на валидност на сертификатите на DVCA с 3 месеца. Срокът на използване на ключа на DVCA е 2 месеца

3.2.2.7. За проверка на документите с електронен носител при призводството – качествен контрол и връчване, се използват инспекционните системи, регистрирани в DVCA-P. За поддържане на инспекционните системи в DVCA-P функционира DVRA-P

3.2.2.8. Срокът на валидност на сертификатите на инспекционните системи в DVCA-P е 1 месец, а техния тип – ECDSA 256. Частният им ключ се съхранява в смарт- карта.

3.2.2.9. В момента в DVCA-R няма регистрирани инспекционни системи.

3.3. Цел на изпълнение на поръчката:

Изграждане на разширение на системите за публичен частен ключ (PKI), изградени за обслужване на процеса на издаване на документи за самоличност с електронен носител, върху системата за Граничен контрол, с чиято помощ да може на граничните пунктове да се проверяват както българските е-документи за пътуване, така и тези на чуждестранните граждани. Разширението на системите за PKI цели да бъдат изпълнени и задълженията, произтичащи от Решения на ЕК С (2009) 7476 от 5 октомври 2009 за обмен на информация на сертификати за паспорти и други документи за пътуване, издавани от държавите - членки и ЕК С (2011) 5478 от 4 август 2011г. за обмен на сертификати за разрешителни за пребиваване за граждани на трети страни.

3.4. Разширение на съществуващите системи на CSCA/CSRA и CVCA/CVRA с цел осигуряване на новата функционалност към системата за Граничен контрол.

3.4.1. CSCA - сертифициращ орган удостоверяващ цифров подпис на държавата, издава и управлява сертификатите на органа за подписване на документи (DS);

3.4.1.1. За издадените **CSCA** сертификати да бъде осигурена функционалност за предоставянето им на:

3.4.1.1.1. NPKD,

3.4.1.1.2. ICAO - PKD

3.4.1.2. При генериране на списък с анулирани сертификати (revocationlist) да бъде осигурена функционалност за предоставянето на този списък на **ICAO - PKD и NPKD** в рамките на 48 часа.

В случай на липса на инциденти горният обмен да се извършва най-малко веднъж на 90 дни.

3.4.2. DS - Орган за подписване на документи

3.4.2.1. За издадените DS сертификати да бъде осигурена функционалност за предоставянето им на **ICAO - PKD** и **NPKD**.

3.4.3. CSRA (Country Signing Registration Authority)

3.4.3.1. Да се осигури функционалност, позволяваща автоматизирано получаване на CSCA, DS сертификати и CRLs от ICAO – PKD в NPKD.

3.4.4. CVCA - Орган удостоверяващ цифровия подпис на държавата за проверка на документи - издава и управлява сертификата на вътрешните и външни DVCAs;

3.4.4.1. Да се осигури функционалност, позволяваща управление на механизмите за обмен на CV сертификати (автоматично и ръчно);

3.4.5. CVRA - национален орган за регистрация на чужда държава в система за валидиране (EAC PKI), за валидиране на е-документи на чужда държава.

3.4.5.1. Действа чрез SPOC за страните от ЕС.

3.4.5.2. Да се осигури функционалност, позволяваща, одобряване на заявка за цифров сертификат за верификация. Тази заявка трябва да бъде заверена от националния CVCA и изпратена през SPOC на държава-членка на ЕС;

3.4.5.3. Да се изгради административен интерфейс, чрез който да се конфигурира SPOC за връзка със SPOC на държава-членка на ЕС ;

3.4.5.4. Инсталирането и последователното подновяване на получените цифрови

сертификати за верификация да се извършва автоматично.

3.5. Разширение на системите за PKI - изграждане на DV, DVRA и IS.

Проверката за автентичност на е-документи с помощта на PKI ще се изпълнява на съществуващите работни места на АИС „Граничен контрол", които да бъдат интегрирани в изградени инспекционни системи от 2 типа:

тип 1 – обслужва множество терминали (работни места), които четат цялата информация от чипа, в т.ч. биометрична (EAC);

тип 2 – чете информация от чипа, без биометрична (изпълнява PA) и обслужва едно работно място;

Разширението на системите за PKI да включва изграждане на DV (Document Verifier) – „Граничен контрол", като част от on-line сертифициращи вериги (със съответни криптиращи алгоритми) CVCA – DV – IS - T(1)… – T(n), както и на прилежащ Document Verifier Registration Authority (DVRA) за регистрация на свързваните към системата Инспекционни системи (IS) и за обработка на постъпващите от тях заявки за издаване на сертификати.

3.5.1. Проектиране на Инспекционни системи от тип 1 с централизиран криптомодул – HSM като част от сертифициращите вериги CVCA-DV-IS–T(1)… – T(n)

3.5.2. DV(Document Verifier)

3.5.2.1. Създаване отношения на доверие с CVCAs на собственото и на другите държави;

3.5.2.2. Заявка за DV сертификати, като процедура за издаване, използвана от CVCAs;

3.5.2.3. Създаване отношения на доверие с IS в държавата;

3.5.2.4. Получаване IS и DV сертификат заявен от IS;

3.5.2.5. Предоставяне на IS и DV сертификати, спазвайки политиката за управление на сертификати;

3.5.3. DVCA - издава и управлява сертификатите на Система за проверка (IS);

3.5.3.1. Сертифициращ орган за проверка на документи (DVCA)

3.5.3.1.1. Заявка за генериране на ключове и сертификати;

3.5.3.1.2. Въвеждане на вече издаден (import) на DV сертификат;

3.5.3.1.3. Интерфейс за издаване на сертификат за IS;

3.5.3.1.4. Интерфейс за отмяна на IS;

3.5.3.1.5. Интерфейс за подновяване на IS.

3.5.3.2. Регистриращ орган - DVRA

3.5.3.2.1. Придобиване на данни за IS;

3.5.3.2.2. Изменение на данните за IS;

3.5.3.2.3. Заявка за сертификат за IS;

3.5.3.2.4. Подновяване на сертификат за IS;

3.5.3.2.5. Списък на DV сертификати.

3.5.4. IS - Инспекционни системи (тип 1)

3.5.4.1. Създаване отношения на доверие с DV в рамките на държавата;

3.5.4.2. Да се осигури интерфейс за връзка между NPKD и системата за проверка IS итерминали на IS на ГКПП:

3.5.4.2.1. Предоставяне сертификатите на DSs и CRLs изтеглени от ICAO на IS и терминали на IS за граничен контрол;

3.5.4.3. Изтегляне на всички DV Сертификати чрез DVRA. Те ще са от взаимен обмен между държави членки през SPOC или да са заредени ръчно за страни извън ЕС;

3.5.4.4. Създаване отношения на доверие с устройствата за четене към работните станции(терминали на IS) (и забрана, ако е необходимо);

3.5.4.5. При издаване на нов DV сертификат, автоматично да се изтрива стария сертификат на DV върху IS.

3.5.4.6. Прилагане на тази информация, при управление работата на устройствата за четене към работните места, свързани с IS;

3.5.5. Упълномощаване на работните места на АИС "Граничен контрол" за достъп до информацията записана в чипа чрез Extended Access Control (EAC)

3.5.5.1. Да се разработи система за упълномощаване на работните места на АИС

"Граничен контрол" за достъп до изображения на пръстови отпечатъци, записани в електронния носител на информация на национални и чужди документи за пътуване, чрез Extended Access Control (EAC).

3.5.5.1.1. Да се предостави програмен интерфейс към разширението на PKI във вид на динамична програмна библиотека за удостоверяване от страна на работното място на АИС „ГК" като терминал на сертифицирана Инспекционна система за нуждите на изпълнение на EAC и пасивна автентикация.

3.5.6. Терминално устройство за четене на документи / работната станция

3.5.6.1. Създава отношения на доверие с IS – тип 1;

3.5.6.2. Четене на предоставени документи, като се прилагат правилните протоколи (PA, EAC) от IS – тип 1;

3.5.6.3. Терминалните устройства са минимум 60 бр. и се обслужват от поне 3 бр. IS от тип 1 (с възможност за увеличаване на броя на инспекционните системи).

3.5.7. Работно място на АИС „ГК" за четене на документи - IS тип 2. Броят на работните места е минимум 600.

Работата на техническото приложение да бъде съобразена с наличната вече в Гранична полиция техника (четци, скенери за пръстови отпечатаци, софтуер, налични компютърни конфигурации, с които работи граничния полицай) а също и автоматичните гейтове на аерогарите за извършване на PA и EAC.

4. Функционалности, които да се предлагат от техническото решение за разширение на изградения PKI

4.1. Изграждане на National Public Key Directory (NPKD)

4.1.1. Изисквания към NPKD

4.1.1.1. Да бъде изградена национална Директория за поддържане на публичните ключове - NPKD, която да съдържа всички български и чужди сертификати, списъците с невалидните сертификати (CRL) и основните списъци (masterlist), използвани при пасивната автентекация както и други списъци при необходимост.

4.1.1.2. Да бъдат използвани директорийни услуги, които предоставят начин за съхранение, обновяване, откриване и защита на информацията в директорията.

4.1.1.3. Да бъде изграден LDAP сървър за съхранение на сертификатите и списъците на анулирани сертификати (CRL). За работа с този сървър да се използва LDAP протокол - Lightweight Directory Access Protocol LDAP - v3 (RFC 2251), предоставящ възможност на директорийните услуги за представяне на данните. Да се изгради NPKD, като се определи подобна на ICAO-PKD спецификация за изпълнение.

Минимумът атрибути, които трябва да се използват са:

4.1.1.3.1. Country (страна) - код на страната с една или две букви; определят държавата, където се намират определени части от организацията;

4.1.1.3.2. Organization (организация);

4.1.1.3.3. Organizational Unit - организационна единица и обекти листа. Обектите листа са физически или логически мрежови ресурси. Поради това, че обектите листа са най-ниската част от йерархичната структура - те не могат да съдържат други обекти. Обекти от тип листа са: cn - за запис на DS и CRL;

4.1.1.3.4. Общо наименование;

4.1.1.3.5. Сериен номер.

Атрибутите са описани и специфицирани в RFC2256.

4.1.1.4. За достъп до директорията да се използва LDAP протокол.

4.1.1.5. За предаване на данни да се използва LDAPS протокол.

4.1.2. Зареждане на NPKD

4.1.2.1. Да се разработят програмни средства за зареждане на NPKD с български и чуждестранни сертификати, CRL и др. списъци, постъпващи от различни източници (от Country Signing Certification Authority - CSCA България, от ICAO Public Key Directory - PKD, от двустранни контакти, от работни групи)

4.1.2.2. Да има възможност ръчно да се създава LDIF файл, използвайки данни от PKI.

4.1.2.3. Да се поддържа синхронизация на данните за DSc и CRL издавани от CA, както и

чуждите сертификати на други държави, изтеглени от ICAO PKD.

4.1.3. Извличане и предоставяне на сертификатите и CRL от NPKD.

4.1.3.1. Да бъде предоставена функционалност за извличане на сертификатите и CRL от NPKD и управление на процеса на предоставянето им за целите на АИС „ГК“. За тази функционалност да се предоставипрограмен интерфейс във вид на динамична програмна библиотека.

4.2. Изграждане на SPOC

4.2.1. Автоматизирано изпращане на заявки за издаване на DV-сертификати през SPOC на държавите-членки на ЕС;

4.2.2. Автоматизирано получаване на заявки за издаване на DV-сертификати от SPOC на държавите-членки на ЕС;

4.2.3. Уведомяване за получени заявки и обслужване на заявките чрез интерфейс за ръчно обслужване (приемане на заявката и връщане на съответния сертификат);

4.2.4. Автоматизирана дистрибуция на DV - сертификати и вериги сертификати през SPOC на държавите-членки на ЕС;

4.2.5. Автоматизирано приемане на DV - сертификати и вериги сертификати от SPOC на държавите - членки на ЕС;

4.2.6. Автоматизирано инсталиране на приетите сертификати на DV;

4.2.7. Автоматизирано приемане на искане за сертификати и вериги сертификати, необходими за EAC от SPOC на държавите-членки на ЕС;

4.2.8. Автоматизирано изпращане на искане за сертификати и вериги сертификати необходими за EAC към SPOC на държавите-членки на ЕС и получаването им;

4.2.9. Автоматизирано инсталиране на получените сертификати и вериги сертификати върху DV;

4.2.10. Автоматизирано получаване на искане за сертификати и вериги сертификати необходими за EAC от SPOC на държавите-членки на ЕС и изпращането им към искащия SPOC. SPOC и SPOC CA да бъдат изпълнени съгласно изискванията на ЕК - Решения на ЕК (С (2006) 2909, (С(2002) 3069) и европейски стандарт CSN 36 9791 и всички техни изменения към датата на подаване на оферта.

4.3. Разработване на програмни средства за транспортиране на заявки за сертификати, получаване, актуализация и съхранение на сертификати за осигуряване на NPKD и SPOC

Да бъдат създадени всички необходими интерфейси за свързване в рамките на PKI, отнасящи се за български и чужди е-документи за пътуване.

4.3.1. Off-line - интерфейс (използва се за ръчна обработка с операторска намеса); Да се използва при генериране на CRL от CSCA, сертификати от CSCA и CVCA и при подписване на заявки на DVCA „ГК” от CVCA;

4.3.2. Външни – интерфейси извън изградената PKI система. Тези интерфейси да бъдат автоматични и да се използват за връзка от и към други държави:

4.3.2.1. NPKD – ICAO - LDAP – on-line, за получаване и изпращане на DSC и CRL през доверителен канал към базата на ICAO LDAP;

4.3.2.2. NPKD – ICAO - LDIF – off-line, за ръчно изтегляне и записване (download/import) на DSC и CRL-(резервен ICAO-интерфейс), от ICAO-уеб страницата;

4.3.2.3. SPOC - on-line, за обмен на DV-заявки за сертификати и DV-сертификати между държавите-членки на ЕС съгласно изискванията на ЕК.

4.3.2.4. SPOC - off-line, за обмен на DV-заявки за сертификати и DV-сертификати между държавите-членки на ЕС съгласно изискванията на ЕК в случаи на технически проблеми за работа на SPOC - on-line.

4.3.3. Интерфейс за връзка с NPKD

4.3.3.1. Да управлява, разпространява и съхранява всички ICAO-PKD данни за страната, както и да ги зарежда в NPKD.

4.3.3.2. Да дава възможност за доверително Trusted управление на сертификатите, идващи от ICAO-PKD и masterlists.

4.3.3.3. Да бъде осигурено всичко необходимо за on-line връзка с ICAO LDAP.

4.3.3.4. Да бъдат осигурени следните функционалности за CS PKI:

4.3.3.4.1. Да се използват автоматизирани процеси за записване на българските DS, CRL в NPKD и в ICAO - PKD чрез ICAO - LDAP;

4.3.3.4.2. За изтегляне на чуждите сертификати на DS, CRL и основните списъци (masterlists) на CSCA от ICAO - LDAP;

4.3.3.4.3. Неавтоматизирани CS процеси (Ръчна намеса от страна на оператор);

4.3.3.4.3.1. Регистриране и импортиране на чуждестранни CSCA-сертификати;

4.3.3.4.3.2. Изтегляне на чуждите DS, CRL, CSCA masterlist (резервно изтегляне чрез ICAO - LDIF от ICAO - PKD);

4.3.3.4.3.3. Обработване на DS-група заявки;

4.3.3.4.3.4. Импортиране на DS-група сертификати;

4.3.4. Интерфейс за връзка със SPOC

4.3.4.1. За пакетна обработка на данни, свързани със заявки за издаване на сертификати и издадени сертификати;

4.3.4.2. Да се получават и обработват заявки за DV сертификати от SPOC;

4.3.4.3. Да събира DV заявки (действие на оператор);

4.3.4.4. Да извършва трансфери (от оператор) DV заявки към CVCA (off-line трансфер);

4.3.4.5. Оператор да извършва процеса по сертифициране от CVCA и да прави експорт на всички получени сертификати;

4.3.4.6. Да извършва трансфер на DV сертификатите обратно към SPOC (off-line трансфер, също действие извършвано от оператор),

4.3.4.7. SPOC автоматично да разпределя обработените заявки за сертификати на съответните заявители (on-line трансфер).

4.3.4.8. Да бъде осигурено всичко необходимо за on-line връзка на SPOC с другите SPOC. Да работи като регистриращ орган за националното CVCA (поддръжане на приложения за всички необходими обработки за първоначалната регистрация на външните CVCA и DV).

4.4. Разработване на програмни средства за транспортиране на заявки за сертификати, получаване, актуализация и съхранение на сертификати за осигуряване на АИС „ГК"

4.4.1. Интерфейс за връзка между NPKD и АИС „ГК":

4.4.1.1. Дистрибутиране сертификатите на CSCA, DSCs, CRLs изтеглени от ICAO до IS за граничен контрол;

4.4.2. Интерфейс за връзка между SPOC и DVCA „ГК"

4.4.2.1. Да бъдат осигурени следните функционалности за CV PKI:

4.4.2.1.1. Автоматизирани CV процеси за IS-тип 1 на ГК. Издаване на CVCA сертификационна верига (заявка и нейната дистрибуция);

4.4.2.1.2. Локални неавтоматизирани CV процеси (чрез ръчна намеса от страна на оператор);

4.4.2.1.2.1. DV / CVCA регистриране;

4.4.2.1.2.2. Заявка и издаване на DV - сертификат, подписан от CVCA;

4.4.2.1.2.3. Изпращане на чуждестранните SPOC;

4.4.2.1.2.4. Генериране на DV-група заявки за сертифициране от CVCA;

4.4.2.1.2.5. Издаване на DV-групата сертификати;

4.4.2.1.2.6. Да има осигурена възможност за изпращане на e-mail за уведомяване за издадените сертификати в отговор на чужди заявки;

4.5. Разработване на програмни средства за работа със сертификати при изпълнение на EAC

4.5.1. Да бъде разработен програмен интерфейс към АИС ГК, осигуряващ механизма за изпълнение на EAC за достъп до пръстовите отпечатъци, записани в чипа;

4.5.1.1. Да бъде разработено приложение, което да не е WEB базирано, да работи с четец „3M", използван в АИС „ГК". Да се предоставят изходните кодове;

4.5.1.2. Приложението да позволява да се изпълнява механизма на EAC и да предоставя прочетените пръстови отпечатъци за верификация във формат, съгласуван с Заявителя;

4.5.1.3. Да се предостави програмен интерфейс във вид на динамична програмна

библиотека за осъществяване на достъп чрез EAC до изображения на пръстови отпечатъци, записани в чипа.

5. Специфициране на техническите средства: комуникационни, сървъри, криптомодули, работни станции и др. с техните роли и функции.

5.1. Централна компонента (сървъри, Hardware Security Modules – HSM и др.)

5.1.1. За гарантиране на режим на работа 24x7 (двадесет и чстири часа, седем дни в седмицата) с минимални прекъсвания (включително планирани) оборудването ще бъде разположено в Основен и Резервен център. Връзката между двата центъра е 100 Mbps TCP/IP.

5.1.2. С цел максималното уплътняване на хардуерните ресурси на разширението и осигуряване на резервираност да бъде използвана система за виртуализация, като софтуерните и хардуерните и компоненти са така подбрани, че да гарантират едновременната работа на цитираните по-долу логически сървъри върху всеки един от физическите сървъри за виртуализация.

5.1.2.1. Да бъде предложена архитектура, която осигурява максимална надеждност в рамките на Основния център, включително автоматично рестартиране на виртуалните машини при спиране на един физически сървър (high availability) и преместването им без спиране върху друг физически сървър, и осигурява автоматизирано прехвърляне на работата в Резервния център за не повече от 30 минути след вземане на решение, включително преконфигуриране на репликацията на данни в правилната посока. Всички основни компоненти в Основния център да бъдат резервирани по начин, който да гарантира, че само фактори извън доставеното оборудване могат до доведат до необходимостта от прехвърляне на работата в Резервния център.

5.1.2.2. Минимално необходими технически и програмни средства и минимални изисквания към тях:

5.1.2.2.1. Шест HSM в Основен (1 - за DVCA, 3 - за инспекционните системи и 2 - за SPOC и SPOC CA) и два HSM в Резервен център (1 - за DVCA, 1 - за инспекционна система);

5.1.2.2.2. Два сървъра за виртуализация в Основен и един сървър за виртуализация в Резервен център;

5.1.2.2.3. Два сървъра за SPOC в Основен център;

5.1.2.2.4. Два LAN/SAN комутатора в Основен и един LAN/SAN комутатор в Резервен център;

5.1.2.2.5. Два LAN комутатора в основен и един LAN комутатор в резервен център;

5.1.2.2.6. По един дисков масив и в двата центъра;

5.1.2.2.7. По едно диск-базирано архивиращо устройство за всеки център;

5.1.2.2.8. Базов и системен софтуер, включително необходимите лицензи;

5.1.2.2.9. HSM устройствата да бъдат сертифицирани съгласно един от следните стандарти за сигурност:

5.1.2.2.9.1. FIPS 140-2 ниво 3 или по-високо;

5.1.2.2.9.2. PP-SSCD;

5.1.2.2.9.3. BSI Cryptographic Modules Security Level "Enhanced".

Производителността на HSM устройствата да удовлетворява изискванията по т. 5.2.

5.1.2.2.10. Виртуализационен клъстер – да осигури възможността за конфигуриране на виртуални машини на всички сървъри, които са минимум следните:

5.1.2.2.10.1. NPKD - 2 сървъра в клъстер (за база данни съдържаща български и чужди сертификати, CRL);

5.1.2.2.10.2. DVRA - 2 сървъра в клъстер (за регистрация на Инспекционни системи (IS от тип 1) и за обработка на постъпващите от тях заявки за издаване на сертификати);

5.1.2.2.10.3. DVCA - 2 сървъра в клъстер (за издаване и управление на сертификатите на инспекционните системи– IS от тип 1);

5.1.2.2.10.4. IS – 3 сървъра (инспекционните системи (тип 1));

5.1.2.3. Тестова среда – 1 виртуализационен сървър;

5.2. Сървърите и дисковите масиви да са включени в листата със съвместими устройства,

публикувана от производителя на софтуера за виртуализация и в листата за съвместимост на Microsoft за Windows Server.

Софтуерните лицензи да бъдат съобразени с техническите характеристики на устройствата в рамките на предложения хардуер и броя на крайните потребители.

При използване на повече от един сървър за приложения, като неразделна част от предложението да бъде включено и решение за разпределение на натоварването (load-balancing) между тях. Хардуерът, който се предлага да е съвместим с наличния - посочен в т.3.2.

Виртуализационните сървъри да са минимум двупроцесорни сървъри с процесори 2 x E5-2650 или по-мощни (според SPECint_rate2006) с 48 GB RAM, или еквивалентни. Да се гарантира отговор в рамките на 1.2 sec при едновременна заявка (заявки, постъпили за период до 5 sec) от 50 крайни устройства, свързани към централната компонента на 256 kbps. Върху всички сървъри за виртуализация в Основен и Резервен център да бъде инсталирано и дисково пространство 6TB след RAID6, за да могат да бъдат използвани и за архивиране, развой и обучение без да се натоварват дисковите системи и мрежата за данни. Всички сървъри да бъдат оборудвани поне с четири Ethernet порта (2 LAN 1 Gbps, 2 LAN/SAN 10 Gbps) и да позволяват teaming/bonding. Всеки един сървър да позволява пълно отдалечено управление, включително графична конзола, медия и захранване. Сървърите да са с резервирани захранвания. Софтуерът за виртуализация да се зарежда от пространство, вътрешно за сървъра, различно от цитираните по-горе 6 TB. Всички дискове, захранвания, вентилатори да са заменяеми без изключване на захранването (hot-swap).

5.2.1. Централните мрежови комутатори (ЦМК) от трето ниво се явяват ключови за производителността на разширението. Предназначението им е да осъществяват връзка между компонентите на разширението в Основния и между компонентите на разширението в Резервния център. Трафика за управление и трафика, генериран от и към крайните потребители, да бъдат изнесени в отделни комутатори. В случай че за срока на договора ЦМК не осигуряват достатъчна производителност и надеждност, Изпълнителят да подмени за своя сметка доставените комутатори с подходящи. За подсигуряване на стабилната работа на iSCSI е необходимо и поддръжка на FlowControl и 9K JumboFrames едновременно, UnicastStormControl, RapidSpanning Tree, VLAN support, Layer 3 dynamic routing, non-blockingdesign, поне 256 KB packet buffer per SAN port. С цел да се редуцират пътищата за многомаршрутност (Multipathing), те да позволяват конфигуриране в стек и bounding/teaming между портове на отделните елементи на стека. Комутаторите да са с резервирани захранвания. Отпадането на един комутатор не трябва да води до нарушаване на функционалността на разширението. Минималната конфигурация на LAN/SAN комутаторите да е 24x10 Gbps Ethernet-порта на комутатор. Комутаторите за управление и достъп да са с поне 24x1 Gbps Ethernet- порта на комутатор и да отговарят на описаните по-горе изисквания. Връзката между LAN/SAN комутаторите и комутаторите за достъп и управление да става по резервирана 10 Gbps линия.

5.2.2. Дисковият масив да е оборудван с не по-малко от 10x300GB, 15 Krpm дискове. За осигуряване на необходимата надеждност, дисковият масив да разполага с поне два контролера, работещи в резервирана двойка и да предоставя поне по две 10Gbps Ethernet връзки на контролер с поддръжка на многомаршрутност (multipathing). Контролерите да поддържат поне RAID10, 5 и 6. Допустимо е дисковия масив да е базиран и на Fibre Channel 8Gbps или 16Gbps front-end връзки към сървърите, като Изпълнителят да осигури цялото необходимо допълнително оборудване. Дисковият масив да е с лицензи за реални и shadow копия на данните, лицензи за репликация, съвместими със софтуера за виртуализация и софтуера за автоматизирано превключване между Основен и Резервен център. Дисковата подсистема да поддържа поне 50 диска. Дисковият масив да е с резервирани захранвания и да гарантира, че при спиране на захранването няма да има загуба на данни, причинена от дисковия масив и че незаписаните данни ще бъдат пазени поне една седмица. Смяна на основни компоненти като захранвания и контролери не трябва да води до необходимост от спиране на системата.

5.2.3. Устройството за архивиране на данните да е базирано на дискове, за да се

осигури необходимата надеждност, както в архивирането, така и във възстановяването. Софтуерът за архивиране да позволява архивиранетона виртуалните машини и информацията в базите данни и приложенията, както и на всички физически сървъри. Устройството, или софтуерът за архивиране да позволява дедубликиране на данните, за да се редуцира необходимия дисков обеми да осигурява архивиране на всички виртуални машини – пълно и частично. Да има възможност за възстановяване на отделни файлове, без пълно възстановяване на системата. Да може виртуална машина да бъде стартирана директно от архива, преди пълното и възстановяване на постоянното и място или в другия център. Да позволява репликиране на виртуална машина в другия център.

5.2.4. SPOC сървърите да са от същия модел като сървърите за виртуализация и да отговарят на същите изисквания, като процесорите да са 2 x Intel Xeon E5-2620, или еквивалент, 16 GB RAM, 4x 1 Gbps Ethernet порта, 1TB вътрешно дисково пространство след RAID.

5.3. В Резервния център архитектурата да е аналогична, Дисковият масив, да е с капацитет не по-малко от 6 x 300 GB, 15 krpm и 6 x 3 TB. Да се осигури време на отговор не повече от 2.5 sec при едновременна заявка (заявки, постъпили за период до 5 sec) на 50 крайни устройства свързани към разширението на 256 kbps.

И в двата центъра е осигурено непрекъснато токозахранване 220V и климатизация. Изискванията за консумирана мощност и климатизация да бъдат описани в техническото предложение.

Цялото оборудване да е инсталирано в шкафове (ракове) с подходящи конзоли и KVM комутатори независимо от наличието на системи за отдалечено управление на сървърите. Всички устройства да са SNMP управляеми. В шкафа да се осигурят две независими вериги на захранване, подходящо защитени и изолирани една от друга, за недопускане разпространението на проблем от едната (например късо съединение) към другата верига.

При конфигурирането на комутаторите да се използват VLANs за изолиране на трафика между SAN, LAN, хостовете и портовете, ангажирани с трафика между хостовете и мрежата за предаване на данни на МВР (МПД).

Да се предложи „План за преминаване от Основен към Резервен център и обратно".

Планът да е поне във варианти за планирано преминаване и преминаване в случай на авария на компонент.

6. Специфициране на необходимите програмни средства: системни, приложни и развойни с всички необходими лицензи.

Софтуерната платформа да е напълно съвместима с посочения в 3.2. софтуер.

Софтуерната платформа да е последна версия към момента на изпълнение на проекта.

Изпълнителят на поръчката следва да достави и инсталира всички софтуерни лицензи според избраната архитектура и платформи, необходими за нормално функциониране и поддръжка на разширението.

Изпълнителят осигурява поддръжка на тези лицензи за минимум 36 месеца.

7. Осигуряване на възможност за развитие на разширението.

Разширението на системите за PKI да бъде изградено така, че в бъдеще да може да се използва и надгражда за:

7.1. Други потребители в МВР;

7.2. Други е-документи (лична карта, свидетелство за управление на моторно превозно средство, др.);

7.3. SAC (Supplemental Access Control) - допълнителен контрол на достъпа за машинно четене на е-документи;

7.4. PACE - (Password Authenticated Connection Establishment) - Изграждане на връзка с използването на парола.

8. Административни процеси и дейности

Да бъдат изготвени документи, описващи следните процеси и дейности в разширението на PKI:

8.1. Администриране на технологичните процеси;

8.2. Конфигуриране на необходимите настройки и непрекъснат контрол за осигуряване работоспособността на всички процеси;

8.3. Дейности и процеси, необходими за осъществяване на контрол за спазване на нормативните изисквания, осигуряващи сигурността на PKI;

8.4. Генериране на ключове, извършване на криптографски операции (от HSMs), издаване на сертификати;

8.5. Контрол за поддържане цялостта на записите на сертификатите в NPKD (осигуряване на консистентност на данните);

8.6. Администриране на данните - архивиране / възстановяване;

8.7. Администриране на ключове - архивиране / възстановяване;

8.8. Контрол за правилното протичане на аварийни и възстановителни процедури;

8.9. Управление на потребителите, които ще работят с разширението;

8.10. Управление на NPKD и SPOC;

8.11. Контрол на извършваните дейности в NPKD и SPOC;

8.12. Процедури за извършване на одит на дейностите.

9. Други

9.1. Общи функционални изисквания

При генерирането, използването, съхранението и защитата на всички частни ключове и мастер списъци с подписи да се използват HSMs.

9.1.1. Подновяване на сертификат преди изтичане на неговата валидност;

9.1.2. Транспортиране на генерираните сертификати

9.1.3. обявяване на сертификат за невалиден - CRL;

9.1.4. Издаване на предупредително съобщение за наближаващо изтичане (конфигурируем параметър) на валидността на сертификата.Срокът за валидност на сертификатите за IS трябва да бъде не повече от 1 месец.

9.1.5. Да няма възможност за продължаване срока на валидност – генерират се нови ключове и нов сетификат (верига от сертификати).

Достъпът на потребителите до HSM да се поддържа от PIN PAD.

9.2. За изпълнение на разширението се допуска използване и адаптиране на готово техническо решение.

10. Фази на изпълнение на разширението:

10.1. Фаза 1 - дейности, осигуряващи изискванията, описани в т.3.4 и функционалностите от т.4.1, т.4.2 и т.4.3

10.2. Фаза 2 - дейности, осигуряващи изискванията, описани в т.3.5 и функционалностите от т.4.4 и т.4.5

11. Етапи на изпълнение на фаза 1

11.1. Етап 1 - Изготвяне на проект на техническо решение, отговарящо на изискванията в настоящата „Техническа спецификация“, описани в т.3.4, т.4.1, т.4.2 и т.4.3

Техническото предложение да съдържа минимум следните документи:

11.1.1. Детайлно описание на функционалните изисквания – само в случай на предложено готово техническо решение;

11.1.2. Детайлно описание на техническите изисквания – само в случай на предложено готово техническо решение;

11.1.3. Детайлен архитектурен модел на разширението;

11.1.4. Техническа документация на програмните интерфейси;

11.1.5. Детайлен план за организиране и осъществяване на обучение, и необходимата за обучението документация;

11.1.6. Детайлен план за провеждане на тестове и детайлни тестови сценарии покриващи всички изисквания към разширението (функционални, интеграционни и тестове за

производителност) в т.ч.:

11.1.6.1. Генериране на ключови двойки;

11.1.6.2. Издаване на сертификати;

11.1.6.3. Записване на сертификати и CRL в NPKD;

11.1.6.4. Трансфер на сертификати и заявки за сертификати от и към SPOC;

11.1.6.5. Тестване на трансфер на сертификати и CRL от и към ICAO-PKD;

11.1.6.6. Транспортиране на заявки за сертификати, получаване, актуализация и съхранение на сертификати.

Изготвеното техническо предложение се съгласува със заявителя.

11.2. Етап 2 - Доставка на необходимите технически и програмни средства и реализиране на включеното във фаза 1 на разширението в тестова среда.

11.2.1. Доставка на техническите и програмните средства, разопаковане, монтаж, инсталация и конфигуриране.

11.2.2. Изпълнение на тестовите сценарии по т. 11.1.6.

11.2.3. Изготвяне на тестове за приемане на включеното във фаза 1 на разширението при внедряването му. Съгласува се със Заявителя.

11.3. Етап 3 - Внедряване на включеното във фаза 1 на разширението и обучение.

11.3.1. Инсталиране и настройка в експлоатационна среда;

11.3.2. Провеждане на тестовете от т. 11.2.2 в експлоатационна среда;

11.3.3. Провеждане на тестовете от т. 11.2.3;

11.3.4. Пускане в редовна експлоатация включеното във фаза 1;

11.3.5. Провеждане на обучение.

Обучението е предназначено за две категории служители - потребители (до 5 служители) и администратори (до 5 служители) Практическите обучения да се извършват на тестова платформа за всички дейности. Тестовата среда да съответства на експлоатационната по отношение на функционалностите на разширението.

11.3.5.1. Обучението да се извърши по предварително съгласувани и утвърдени теми и график;

11.3.5.2. Да бъдат подготвени работни и нагледни материали за обучението;

11.3.5.3. Обучението да включва семинарна и практическа част;

11.3.6. Документация

Да бъдат предоставени следните ръководства и процедури:

11.3.6.1. Ръководства за инсталиране и изграждане на всички компоненти, реализирани на фаза 1 на разширението на PKI;

11.3.6.2. Ръководства и процедури за администриране и експлоатация на NPKD и SPOC;

12. Етапи на изпълнение на фаза 2

12.1. Етап 1 - Изготвяне на проект на техническо решение, отговарящо на изискванията в настоящата „Техническа спецификация“, описани в т.3.5, т.4.4 и т.4.5

Техническото предложение да съдържа минимум следните документи:

12.1.1. Детайлно описание на функционалните изисквания – само в случай на предложено готово техническо решение;

12.1.2. Детайлно описание на техническите изисквания – само в случай на предложено готово техническо решение;

12.1.3. Детайлен архитектурен модел на разширението;

12.1.4. Техническа документация на програмните интерфейси;

12.1.5. Детайлен план за организиране и осъществяване на обучение, и необходимата за обучението документация;

12.1.6. Детайлен план за провеждане на тестове и детайлни тестови сценарии покриващи всички изисквания към разширението (функционални, интеграционни и тестове за производителност) в т.ч.:

12.1.6.1. Генериране на ключови двойки;

12.1.6.2. Издаване на сертификати;

12.1.6.3. Трансфер на сертификати и заявки за сертификати от и към SPOC, DVRA, DV, IS;

12.1.6.4. Транспортиране на заявки за сертификати, получаване, актуализация и съхранение на сертификати.

Изготвеният проект се съгласува със Заявителя.

12.2. Етап 2 - Доставка на необходимите технически и програмни средства и реализиране на включеното във фаза 2 на проекта в тестова среда.

12.2.1. Доставка на техническите и програмните средства, разопаковане, монтаж, инсталация и конфигуриране.

12.2.2. Изпълнение на тестовите сценарии по т. 12.1.6.

12.2.3. Тестване на функционалността за заявяване и получаване на сертификати за изпълнение на пасивна автентикация чрез изпълнение на такава на работно място на АИС „Граничен контрол" – за български е-документи както и такива на поне една държава-членка на ЕС;

12.2.4. Тестване на функционалността за упълномощаване на работните места на АИС "Граничен контрол" за достъп до чувствителната информация на национални и чужди е-документи за пътуване чрез EAC;

12.2.5. Предоставяне на изходни кодове на приложението за прочитане на изображения на пръстови отпечатъци, записани в чипа чрез EAC с описание на програмната среда за генериране на изпълним код. Тестване на интерфейса, осигуряващ средства за изпълнение на Extended Access Control за извличане на пръстови отпечатъци чрез компилация и изпълнение на разработеното приложение, което извлича пръстовите отпечатъци от електронен документ, прочетен с четеца на документи на фирма 3M, използван в АИС „Граничен контрол" с помощта на неговия програмен интерфейс (SDK), за национални и чужди е-документи за пътуване;

12.2.6. Да се осигури техническа възможност за анализ на трафика при работа на разширението с цел доказване на функционалността му;

12.2.7. Провеждане на тестове за натоварване;

12.2.8. Изготвяне на тестове за приемане на разширението при внедряването му. Съгласува се със Заявителя.

12.3. Етап 3 - Внедряване на включеното в Етап 1 и Етап 2 на Фаза 2, обучение и цялостно внедряване на проекта.

12.3.1. Инсталиране и настройка в експлоатационна среда на включеното във фаза 2;

12.3.2. Провеждане на тестовете по т.11.2.2 и от т.12.2.2 до т.12.2.7 включително, в експлоатационна среда;

12.3.3. Провеждане на тестовете по т.11.2.3 и т. 12.2.8;

12.3.4. Провеждане на обучение;

Обучението е предназначено за три категории служители - потребители (до 5 служители) и администратори (до 5 служители) на техническото решение, и програмисти - за използване на програмните интерфейси (до 10 служители). Практическите обучения да се извършват на тестова платформа за всички дейности.

Тестовата среда да съответства на експлоатационната по отношение на функционалностите на разширението.

12.3.4.1. Обучението да се извърши по предварително съгласувани и утвърдени теми и график;

12.3.4.2. Да бъдат подготвени работни и нагледни материали за обучението;

12.3.4.3. Обучението да включва семинарна и практическа част;

12.3.5. Пускане в редовна експлоатация на разширението;

12.3.6. Документация:

Да бъдат предоставени следните ръководства и процедури:

12.3.6.1. Ръководства за инсталиране и изграждане на всички компоненти, включени във фаза 2 на разширението на PKI;

12.3.6.2. Процедура за генериране двойката ключове и сертификати за DVCA Граничен контрол;

12.3.6.3. Процедура за генериране двойката ключове и сертификати за IS;

12.3.6.4. Процедура за упълномощаване на работните места на АИС "Граничен контрол" за достъп до изображения на пръстови отпечатъци, записани в електронния носител на информация на национални и чужди е-документи за пътуване, чрез EAC.

13. Изисквания към предмета на поръчката:

13.1. Изисквания към инсталацията/монтажа и пускането в експлоатация

13.1.1. Изпълнителят по договор е отговорен за цялостната инсталация и пускане в експлоатация на доставеното оборудване;

13.1.2.Изпълнителят по договор е отговорен за осигуряване на успешното взаимно функциониране на всички инсталирани продукти;

13.1.3. Настройките на оборудването като IP адресация, протоколи, VLAN, услуги и др. и цялостното интегриране в комуникационно-информационната среда на МВР да се извършат от изпълнителя съвместно със специалисти на Възложителя;

13.1.4. Представители на възложителя и изпълнителя провеждат съвместни предварителни и приемателни тестове на реализираното техническо решение;

13.1.5. Тестовата среда да отговаря на експлоатационната.

13.2. Изисквания към оборудването:

13.2.1. Цялото оборудване да е ново, да не е използвано преди това и да е в производствената листа на производителя за 2014 година;

13.2.2. Цялото оборудване да работи в диапазон на напрежението от 187 V (220 V - 15%) до 242 V (220 V + 10%), при 50Hz +/ - 0.5 Hz.

13.2.3. Всички технически и програмни средства да бъдат изцяло съвместими с наличните, описани в Приложение 1 – „Техническа спецификация".

13.2.4. Всички изделия да са окомплектовани с всички необходими аксесоари, осигуряващи работата им и свързването им към други системи, като например: токозахранващи кабели, входни устройства, захранващи адаптери, токозахранващи удължители, кабели за вътрешно и междинно свързване, адаптери, монтажни китове и т.н.

13.2.5. За всяка единица доставен артикул Изпълнителят е длъжен да гарантира, че същата е напълно съвместима със спецификациите на другите артикули, включени в Приложение 1 – „ Техническа спецификация";

13.3. Изисквания към гаранционния сервиз

13.3.1. Гаранционният срок да бъде стандартен фирмен гаранционен срок за предлаганите изделия, но не по-малък от 36 месеца;

13.3.2. Гаранционното обслужване на техническото решение да бъде 24 часа, 7 дни в седмицата.

Изпълнителят е отговорен за предоставяне на гаранционно обслужване. За всички технически проблеми да има разкрито помощно бюро (хелп деск) за техническа поддръжка. Достъпът до Помощното бюро да е осигурен чрез телефонен номер, факс и e-mail в България, които да не поставят потребителите пред необходимост да заплащат разговори по международни тарифи или по такива за разговори на големи разстояния. Изпълнителят да предостави информация за сервиз (обслужващ център) в София - адрес и телефонни номера, както и списък на персонала, който ще оказва нужното съдействие и помощ;

– За срока на договора да се осигурят:

• Достъп до сайта на производителя с възможност за изтегляне на обновления за програмните продукти;

• Достъп до сайта на производителя с възможност за изтегляне на нови версии за програмните продукти;

• Възможност за регистриране на проблеми и консултации денонощно директно към производителя - по телефон и електронна поща;

• Консултации и системна помощ на място за програмните продукти;

13.3.3. Максималното време за реакция е до 4 часа от момента, в който потребителят е заявил наличие на проблем. Изпълнителят изпраща квалифициран персонал на място.

13.3.4. Когато отстраняването на проблема или ремонтът изисква повече от 24 часа, Изпълнителят по договор да предостави еквивалентно устройство за временна замяна. В този случай, гаранционният срок на взетото за ремонт устройство се удължава с времето за отстраняване на повредата;

– При подмяна на носител на информация не се допуска неговото изнасяне от МВР;

– Гаранционно обслужване на софтуера включва актуализиране/надстройване на софтуера в отговор на каквито и да са установени несъответствия във функционирането на системното и приложното програмно осигуряване, както и при промени в европейски стандарт CSN 36 9791, Решения на Европейската комисия **C(2008) 8657 от 22.12.2008, C(2009) 7476 от 5.10.2009, C(2002) 3069 , C(2009) 3770 от 20.5.2009, C(2011) 5478 от 4.8.2011**.

14. Доставката се съпровожда с:

14.1. Декларация/сертификат за произход за всяко изделие;

14.2. Декларация, в която се посочва, че в случай на отказ или дефект на оборудването и програмните средства за същите е осигурена поддръжка в границите на територията на Република България;

Приложение №13
Образец!

ДО
МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ
ГР. СОФИЯ,
УЛ.“6-ТИ СЕПТЕМВРИ” № 29

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

Уважаеми Дами и Господа,

След запознаване с документацията за участие в открита процедура за възлагане на обществена поръчка с предмет: *„Разширение на системите за публичен частен ключ (PKI), изградени за обслужване на процеса на издаване на документи за самоличност с електронен носител, включително изграждане на единна точка за контакт (SPOC) и връзка с ICAO – PKD върху системата за граничен контрол”*,

ние сме съгласни валидността на нашето предложение да бъде **90** календарни дни от крайния срок за подаване на оферти и ще остане обвързващо за нас, като може да бъде прието по всяко време преди изтичането на този срок.

До подготвянето на официален договор, това техническо предложение с писменото приемане от Ваша страна и известие за възлагане на договор, ще формират обвързващо споразумение между двете страни.

Ние: **Обединение „C&T-ОСИ”**
/изписва се името на участника/
.....
/БУЛСТАТ или ЕИК/
София, 1528, бул. Искърско шосе № 7 Търговски център Европа, сграда 6, ет.3
/адрес по регистрация/

предлагаме да изпълним поръчката, съгласно изискванията на Възложителя при следните условия:

I. Предлагаме следните срокове:

1. Изпълнението на поръчката се извършва на две фази:

1.1.**Фаза 1**. Дейности, осигуряващи изискванията по т. 3.4 и функционалностите по т. 4.1, т. 4.2 и т. 4.3 от Техническа спецификация.

Етап 1. Изготвяне на проект на техническо решение, отговарящо на изискванията по т. 3.4, т. 4.1, т. 4.2 и т. 4.3 от Техническа спецификация - до **30** календарни дни след подписване на договора.

Етап 2. Доставка на необходимите технически и програмни средства и реализиране на включеното във Фаза 1 на разширението в тестова среда – до **90** календарни дни след приемане на етап 1.

Етап 3. Внедряване на включеното във фаза 1 на разширението и обучение – до **30** календарни дни след приемане на етап 2.

1.2.Фаза 2. Дейности, осигуряващи изискванията по т. 3.5 и функционалностите по т. 4.4 и т. 4.5 от Техническа спецификация.

Етап 1. Изготвяне на проект на техническо решение, отговарящо на изискванията по т. 3.5, т. 4.4 и т. 4.5 от Техническа спецификация – до **30** календарни дни след приемане на Етап 3 от Фаза 1.

Етап 2. Доставка на необходимите технически и програмни средства и реализиране на включеното във фаза 2 на проекта в тестова среда – до **60** календарни дни след приемане на етап 1.

Етап 3. Внедряване на включеното в Етап 1 и Етап 2 на Фаза 2, обучение и цялостно внедряване на проекта – до **60** календарни дни след приемане на етап 2.

2.Гаранционен срок - стандартен фирмен гаранционен срок за доставените изделия -не по-малко от **36** месеца.

3.Гаранционно обслужване - **24** часа, **7** дни в седмицата, като:

3.1.Време за реакция - максимално - до **4** часа от момента, в който потребителят е заявил наличие на технически проблем;

3.2.Време за отстраняване на проблема- до **24** часа.

4.Обучението ще се извършва по предварително съгласувани и утвърдени теми и график.

II. Декларираме, че изпълнението на поръчката ще отговаря изискванията на възложителя при стриктно спазване на техническата спецификация от документацията за участие в процедурата.

III. Прилагаме следните документи, декларации и информация, изисквани съгласно Техническата спецификация от документацията за участие в процедурата, които представляват неразделна част от Техническото ни предложение:

III.1. Декларация приема и предлага сроковете за изпълнение на поръчката

III.2 Декларация по т.13. и т. 14 от Техническата спецификация

.....

Приложение: Описание на видовете изделия и дейности за разширение на системите за публичен частен ключ –PKI, които отговарят на заложените изисквания в техническата спецификация.

Дата 18.05.2015 г. **Подпис и печат: .....**

/Злати Петров, представляващ Обединение „C&T-ОСИ“/

или

Упълномощен да подпише предложението от името на ..... */изписва се името на участника/* ..... */изписва се името на упълномощеното лице и длъжността/.*

Забележка: Предложените от участника срокове за изпълнение на поръчката не могат да бъдат по-големи от посочените в обявлението.

Описание на видовете изделия и дейности за разширение на системите за публичен частен ключ –PKI, които отговарят на заложените изисквания в техническата спецификация.

Консорциум „ C&T – ОСИ“

СЪДЪРЖАНИЕ

СЪДЪРЖАНИЕ НА ТАБЛИЦИТЕ 6
съдържание на фигурите 6
ЗА НАС 7
УВОД 7
ПРЕГЛЕД НА РЕШЕНИЕТО електронни паспорти 8
ИЗГЛЕД НА СТРУКТУРАТА НА ВИСОКОТО НИВО 9
СЕРТИФИЦИРАЩ ОРГАН ЗА СТРАНАТА (Country Signing CA) 9
СЕРТИФИЦИРАЩ ОРГАН ЗА ПРОВЕРКА В СТРАНАТА (Country Verifying CA) 10
СТРУКТУРА ЗА ВАЛИДИРАНЕ НА ОСНОВНИЯ КОНТРОЛ ВЪРХУ ДОСТЪПА В СТРАНАТА (BAC) 12
КОМПОНЕНТИ НА РЕШЕНИЕТО ЗА ПРОВЕРКА НА КОНТРОЛА ВЪРХУ РАЗШИРЕНИЯ ДОСТЪП В СТРАНАТА (EAC) 13
СТРУКТУРА НА РЕШЕНИЕТО 13
КОМПОНЕНТИ НА РЕШЕНИЕТО 13
ПРЕДЛОЖЕНА архитектура 16
СЪЗДАВАНЕ НА НАЦИОНАЛЕН КЛАСИФИКАТОР НА ПУБЛИЧНИТЕ КЛЮЧОВЕ (NPKD) 18
СЪЗДАВАНЕ НА ЕДИННА ТОЧКА ЗА КОНТАКТ (SPOC) 18
РАЗРАБОТВАНЕ НА SW 19
РАЗРАБОТВАНЕ НА СОФТУЕРНИ ПРОДУКТИ ЗА РАБОТА СЪС сертификати ПРИ ИЗВЪРШВАНЕ НА КОНТРОЛ ВЪРХУ РАЗШИРЕНИЯ ДОСТЪП (EAC) 19
СЕГМЕНТИРАНЕ НА МРЕЖАТА 20
ЛОГИЧЕСКО РАЗПРЕДЕЛЕНИЕ 21
ИНДИВИДУАЛНО РАЗПОЛОЖНИЕ 22
ИЗИСКВАНИЯ КЪМ ХАРДУЕРА 23
ЗОНА CA 23
ЗОНА DMZ 23
ЗОНА IS КОНЦЕНТРАТОРИ 23
тестова СРЕДА 24
ХАРДУЕРНИ МОДУЛУ ЗА СИГУРНОСТ 24
ЗОНА CA 24
ЗОНА DMZ 25
ЗОНА IS 25
SafeNet LUNA CONFIGURATION 25
ЗОНА CA 25
ЗОНА DMZ 25
ЗОНА IS 26

КОНФИТУРАЦИ НА Entrust SW 26
Entrust IS Client (600 clients) УСЛУГИ 26
ОБЩ ПОДХОД 26
Описание на ИТ инфраструктура 27
Общо описание 27
Описание на хардуерните устройства 33
Основен и резервен център за данни 33
Основен център за данни – виртуализационнен клъстер с два физически сървъра – Сървър 1 и Сървър 2 33
Основен център за данни – виртуализационен клъстер с два физически сървъра – Сървър SPOC1 и Сървър SPOC2 34
Основен център за данни – един физически сървър – Сървър Тест със следната конфигурация: 35
Резервен център за данни – един физически сървър – Сървър 1 със следната конфигурация: 35
Основен и резервен център за данни – дисков масив – по един брой масив на всяка локация 36
Основен и резервен център за данни – по един брой устройство за архивиране на данните на всяка локация: 38
Основен и резервен център за данни – софтуер за архивиране 38
Основен и резервен център за данни – LAN и LAN/SAN комутатори 38
VCS Fabric 39
Основни характеристики на LAN комутаторите 41
Основни характеристики на LAN/SAN комутаторите 43
LAN/SAN BoM 44
Основен и резервен център за данни – KVM комутатор – по един брой на всяка локация 45
Основен и резервен център за данни – конзола – по един брой за всяка локация 45
Основен и резервен център за данни – сървърен шкаф – по един брой за всяка локация: 46
Информация за планиране на сървърното помещение 49
План за преминаване от Основен към Резервен център и обратно 51
ДОКУМЕНТАЦИЯ 62
ОБУЧЕНИЕ И ПРЕДАВАНЕ НА ЗНАНИЯ 62
РАЗРАБОТКИ СЪОБРАЗНО НУЖДИТЕ НА КЛИЕНТА 63
ФАЗА 1 – РАЗРАБОТВАНЕ НА ИНФРАСТРУКТУРА 63
ФАЗА 2 – ИЗГРАЖДАНЕ НА СИСТЕМАТА 63
ФАЗА 3 - ИЗПИТАНИЯ 64
ФАЗА4 – инсталация и миграция КЪМ ПРОИЗВОДСТВЕНА СИСТЕМА 64
Референции 65
ЕКИП 66

СЪДЪРЖАНИЕ НА ТАБЛИЦИТЕ

Таблица 1 – Предимства на електронните паспорти от първо и второ поколение 8
Таблица 2 – Нови компоненти на решението на CSCA 10
Таблица 3 – Структура за валидиране на контрол на достъпа 12
Таблица 4 – Компоненти на решението CVCA 13
Таблица 5 – Основни технически характеристики ICX7450 42
Таблица 6 – Основни технически характеристики VDX6740 43
Таблица 7 – Окомплектовка на мрежовото оборудване 44
Таблица 8 - Основен център за данни 49
Таблица 9 - Резервен център за данни 50

СЪДЪРЖАНИЕ НА ФИГУРИТЕ

Фигура 1 - Опростена структура на CVCA 13
Фигура 2 - Схематично изображение на предложеното решение 17
Фигура 3 - Логическо сегментиране 21
Фигура 4 - Разпределение на физическите устройства 22
Фигура 5 - Физическа инфраструктура 28
Фигура 6 - VMware vCenter Site Recovery Manager 30
Фигура 7 - Физическа топология на мрежата – основен център за данни 39
Фигура 8 - VCS fabric 40
Фигура 9 – Физическа топология – резервен център за данни 41
Фигура 10 – ICX7450 изглед отпред и отзад 41
Фигура 11 – Разположение на оборудването в комуникационен шкаф – основен център 47
Фигура 12 – Разположение на оборудването в комуникационен шкаф – резервен център 48

ЗА НАС

S&T AG е един от лидерите в сферата на системната интеграция и предоставянето на комплексни ИТ решения в Централна и Източна Европа.

Компанията разполага с около 70 клона в 19 държави. Сферите на компетентност на S&T AG обхващат голямо разнообразие от професионални ИТ услуги, с основен фокус върху планирането, проектирането и експлоатацията на специфични за клиента решения, както и аутсорсинг, интеграция и консултации в ИТ сектора.

C&T България ЕООД е създадена в края на 1993 г. като дъщерна фирма на австрийското акционерно дружество S&T AG. Днес компанията разполага с три търговски и сервизни центъра в страната – София, Пловдив и Варна.

C&T България има доказан опит в проектирането, изграждането и внедряването на цялостни ИТ инфраструктурни решения за нуждите на частния бизнес и държавния сектор. Благодарение на своя дългогодишен опит, стабилна партньорска мрежа и високо квалифициран екип, днес компанията е един от водещите системни интегратори в България.

Нашата експертиза обединява голямо разнообразие от висококачествени, ефективни и гъвкави решения в няколко ключови области:

- Внедряване на цялостни инфраструктурни и хардуерни решения
- Проектиране и интеграция на системни решения
- Софтуерен и хардуерен съпорт
- Консултантски услуги
- ИТ аутсорсинг

OSI.SI е компания ориентирана към своите клиенти, която предлага гъвкави и базирани на стандарти решения в областта на сигурността на информационните технологии и интегриране на системи. От основаването си през 2008 година, OSI.SI се ангажира с проекти свързани с информационните технологии за почти всички най-големи фирми в Словения, разширявайки своите продажби и услуги в други страни. На базата на експертните оценки и опита с местните ресурси, SI.SI е в състояние да предложи пълни решения за управление на информационните технологии във възможно най-кратки срокове. Нашите експертни оценки включват консултации и внедряване на системи за инфраструктура с публични ключове (PKI), сигурност на информационните технологии (IDM, SIEM ...), разработване на софтуер, както и интегриране на системи с фокусиране върху инфраструктурата на Oracle.

УВОД

C&T България ЕООД и ОСИ Систем интегрейшън д.о.о. обединиха усилията и експертизата си с цел да предадат предложение и, при евентуално спечелване на процедурата, да реализират дейностите свързвани с изпълнение на проекта „Разширение на системите за публичен частен ключ (PKI), изградени за обслужване на процеса на издаване на документи за самоличност с електронен носител, включително изграждане на единна точка за контакт (SPOC) и връзка с ICAO – PKD върху системата за граничен контрол"

Консорциум „C&T- ОСИ" има удоволствието да предостави на вниманието на Министерството на вътрешните работи настоящото предложение за издаване и проверка електронни документи за самоличност. Проблемите със сигурността, разработването на технологии и новоразработените стандарти накараха правителствата в целия свят да се насочат към издаване на съвременни документи за пътуване с автоматично, без човешка намеса, разчитане и потвърждение, че лицето, което представя документ за задгранично пътуване, е едно и също лице, показано на страницата с данни, както и върху чипа с уверението, че данните са били поставени там от издаващия орган и че данните не са променени

(MRTD). Общоизвестни като електронни паспорти, тези документи съдържат чип която съхранява информация, която може да се сравни с данни в паспорта.

За да се улесни интероперативноста между отделни страни, международната организация за гражданско въздухоплаване (ICAO) спомогна за въвеждането на световни стандарти за въвеждане на електронните паспорти. Тъй като тези електронни паспорти съдържат лични данни, сигурността и целостта представляват критични изисквания.

Технологията Инфраструктура на публичните ключове (PKI) служи като гръбнак за защита на чувствителната информация в съвременните електронни паспорти. PKI се превърна в интегрална технология за сигурността и инфраструктурата за проверка на електронните паспорти. Сигурността на тези важни и чувствителни документи трябва да бъде защитена с помощта на надеждни и доказани софтуерни решения, свеждащи до минимум измамите чрез проверка на целостта и произхода на личните, и биометрични данни, съдържащи се в чипа, вграден в електронните паспорти. Тези PKI решения, заедно със софтуера на продавача за издаването им и четците и софтуера на граничния контрол, изграждат „рамката на доверие" по цялата верига в електронните паспорти.

ПРЕГЛЕД НА РЕШЕНИЕТО ЕЛЕКТРОННИ ПАСПОРТИ

За да се улесни интероперативноста между отделни страни, международната организация за гражданско въздухоплаване (ICAO) спомогна за въвеждането на световни стандарти за въвеждане на електронните паспорти. Тъй като тези електронни паспорти съдържат лични данни, то сигурността и целостта представляват критични изисквания. В резултат на това бяха разработени два стандарта за електронни паспорти, които да подпомогнат страните в прехода им от традиционните документи за пътуване на хартиен носител.

- **Контрол върху основния достъп (BAC):** изграден с цел да сведе до минимум фалшифицирането на документите за самоличност, електронни паспорти първо поколение използват чип за контрол върху основния достъп RFID или CSC съдържащ прости биометрични данни (обикновена снимка на лицето), заедно с идентификационни данни дублирани на хартиения документ. Дигиталните подписи върху електронните паспорти, подлежащи на контрол върху основния достъп (BAC), спомагат за предотвратяването на клонирането или модифицирането на документите за самоличност при правилната им употреба, при преминаване на границата.
- **Контрол върху разширения достъп (EAC):** Второто поколение електронни паспорти, наречени EAC, позволява на правителствата да използват средство за по-добра биометрия, което е по-трудно за поставяне в RFID/CSC, обикновено пръстов отпечатък или сканиран образ на ириса. Електронните паспорти EAC изискват също така кодиране на съдържанието на чипа, дори ако някой престъпник успее да присвои биометрия, достъпът до съдържанието на чипа се отказва чрез кодирането.

Таблица 1 по-долу предоставя основните предимства на електронните паспорти от първо и второ поколение.

ТАБЛИЦА 1 – ПРЕДИМСТВА НА ЕЛЕКТРОННИТЕ ПАСПОРТИ ОТ ПЪРВО И ВТОРО ПОКОЛЕНИЕ

Основен контрол върху достъпа (BAC)	Разширен контрол върху достъпа (EAC)
Чипът RFID/CSC съдържа електронен вариант на отпечатаното съдържание	Включване на разширени биометрични данни (например пръстови отпечатъци, сканиран образ на ириса) които са устойчиви на присвояване (ниска степен на приемане на фалшиви данни).
Кодиран пренос на данни (30 до 60 бита)	Усилено кодиране на данните при пренасяне

	(128 бита)
Дигитален подпис върху съдържанието на чипа от паспортна служба, невъзможност за фалшифициране на подписа	Съдържанието на чипа не може да бъде дублирано или клонирано.
Граничният контрол не може да сравни отпечатаното съдържание, електронния вариант и външния вид на лицето.	Терминалът за разчитане на електронните паспорти се самоидентифицира с електронните паспорти
Ако образът на лицето запаметен в CSC чипа е с по-добро качество и резолюция от снимката в документа на хартиен носител, съществува по-голяма възможност машината да сравни снимката на лицето	Чипът RFID/CSC ще предостави разширените биометрични данни само на доверени четци.
	Подобрен достъп за международна проверка

Първото поколение електронни паспорти използва основен контрол върху достъпа (BAC), който предполага пасивно и опционално активно идентифициране и се произвежда в много страни по света. Страните-членки на ЕС получиха директива за издаване на електронни паспорти, съдържащи изображения на лицата защитени чрез BAC през август 2006 година. Правителството на САЩ предприе същата мярка за страните обхванати от програмата за отмяна на визите през октомври 2006 година.

Тази функционалност, базирана на инфраструктурата с публичен ключ X.509 PKI, предлага проверка и удостоверяване на това дали документът е подписан от легитимен орган-издател, и данните запаметени в чипа не са променени след издаването.

Понастоящем страните осъвременяват своите програми за електронни паспорти, преминавайки към рамката на второто поколение, която включва възможностите за разширен контрол върху достъпа (EAC). Страните-членки на ЕС ще трябва да добавят матрични данни с цифрови отпечатъци и/или сканиран образ на ириса към MRTD с биометричните данни защитени чрез схемата EAC.

Чрез идентифицирането на терминала и чипа, EAC се стреми да повиши сигурността на MRTD и тази на биометричните данни (например сканираното изображение на ириса и/или пръстовия отпечатък) запаметени в безконтактния чип в електронните паспорти.

ИЗГЛЕД НА СТРУКТУРАТА НА ВИСОКОТО НИВО

Въпреки че и двете използват PKI за изграждане на доверието необходимо за системата за електронните паспорти, решенията базирани на BAC и EAC по принцип имат различна визия за управлението на експлоатационния живот на сертификатите. Тези различия се отнасят до начина на обмен и отхвърляне на сертификатите (при наличие на такива) и дори до бинарната структура на самите сертификати.

Сертифициращият орган (CA), който поддържа BAC е известен като Органът на страната подписващ сертификата CA (CSCA) и CA, който упражнява разширения контрол върху достъпа, е известен като сертифициращ орган извършващ проверка в страната (CVCA).

СЕРТИФИЦИРАЩ ОРГАН ЗА СТРАНАТА (COUNTRY SIGNING CA)

CSCA има следните характеристики:

- Издава цифрови сертификати X.509 съгласно RFC 2459/RFC 3280
- Издава списъци на отменени сертификати X.509 (CRL) съгласно RFC 2459/RFC 3280

- Осигурява администриране на политиките и привеждане в действие на функциите свързани с издаването и използването на сертификатите на подписващите документи (DS)

СЕРТИФИЦИРАЩ ОРГАН ЗА ПРОВЕРКА В СТРАНАТА (COUNTRY VERIFYING CA)

CVCA има следните характеристики:

- Издава цифрови сертификати с възможност за проверка с карта по ISO 7816
- Осигурява администриране на политиките и въвеждане на функциите свързани със структурата, издаването и използването сертификати на сертифициращите органи за проверка CA (DV), които включват използването на идентификатор, който контролира наличните биометрични данни към заинтересованите страни при използването им в схемата за разширен контрол върху достъпа до електронните паспорти (EAC)
- Издаването на Linked сертификати асоциирани с предходни такива (или първоначален сертификат със самостоятелен подпис от CVCA) в случай на обръщение на ключ в CVCA

Ролята на CVCA е да издава сертификати за един или повече компоненти на DV, които от своя страна използват тези сертификати за издаване на сертификати за инспекционните системи (IS). Схемата за разширен контрол върху достъпа EAC не разчита на списъците с отхвърлени сертификати CRL, за да отмени активния статус на потенциално нередовни сертификати. В действителност, EAC разчита на краткия експлоатационен живот на сертификатите, за да предотврати продължителното използване на нередовните сертификати. От тази гледна точка експлоатационният живот на сертификатите издадени от инспекционните системи (IS) се измерва в дни, този на издадените от органите за проверка на документите (DV) се измерва в седмици или месеци. Планирането на сертификатите съответства на компонентите използващи сертификата. DV например ще управлява валидността на своя собствен сертификат на базата на валидността определена от висшестоящия орган CVCA. Инспекционната система ще има подобна връзка с висшестоящата инстанция DV, а DV към CVCA.

Съгласно "BSI – Профил на общите критерии – съвременни документи за пътуване с автоматично разчитане с "Приложение на ICAO" Механизъм за разширен контрол върху достъпа" версия 1.1 (от 7 септември 2007 година), и "BSI – Технически насоки – Напреднал защитен механизъм при съвременни документи за пътуване с автоматично разчитане – Механизъм за разширен контрол върху достъпа (EAC), версия 1.11RC2 – TR-03110". Сертификатът CVCA следва да бъде свързващ сертификат или сертификат със самостоятелно подписване, издаден от CVCA". "BSI – Технически насоки – Напреднал защитен механизъм при съвременни документи за пътуване с автоматично разчитане.

– Механизъм за разширен контрол върху достъпа (EAC), версия 1.11RC2 – TR-03110" – Разширен контрол върху достъпа (EAC), Версия 1.11 – TR-03110" определя че CVCA и CSCA могат да бъдат управлявани от една и съща структура, въпреки че всяка от тях изисква своя собствена уникална двойка ключове.

Таблица 2 по-долу са показани в детайли компонентите на решението CSCA.

ТАБЛИЦА 2 – НОВИ КОМПОНЕНТИ НА РЕШЕНИЕТО НА CSCA

Document Signer	
Това е DS компонента на e-Passport решението. Неговите сертификати се издават от CSCA. Компонентите за отпечатване и персонализация отправят Web Services (WS) заявки към DS с цел DSO подписване и връщане. DS подписва DSO с частния ключ, асоцииран с неговия сертификат (издаден от CSCA).	
Вторичен компонент	**Предназначение**

Сървър за проверка	Действа като заверка на DS и подписва DSO при поискване, през SDS, чрез компонентите за отпечатване и персонализиране.
Услуга доставка на подписа	Услугата доставка на подписа (SDS) действа като интерфейс между компонентите за външно отпечатване и персонализиране, и сървъра за проверка. Приема входящите обаждания за подпис на DSO, трансформира и нормализира същите (създава неподписани DSO) и ги прехвърля към сървъра за проверка. SDS е отговорна и за прехвърлянето на отговорите от страна на сървъра за проверка на компонентите-заявители.
Помощна програма за създаване на вътрешен код офлайн	Дава възможност на оператора да поиска и внесе лични документи в сървъра за проверка когато същите трябва да се запазят в HSM и когато CSCA работи офлайн.

СТРУКТУРА ЗА ВАЛИДИРАНЕ НА ОСНОВНИЯ КОНТРОЛ ВЪРХУ ДОСТЪПА В СТРАНАТА (BAC)

ТАБЛИЦА 3 – СТРУКТУРА ЗА ВАЛИДИРАНЕ НА КОНТРОЛ НА ДОСТЪПА

Валидиране на документа – Структура за многостранно разпределение на материалите (BAC)	
Поверява осигуряването на структурата за валидиране на документите с помощта на управляемите характеристики на X509 за осигуряване на идентифицирани SSL линкове между различните компоненти. Нормалната структура на публичния ключ X.509 PKI може да се; може да бъде CSCA, самостоятелни гранични сертификационни органи CA, или при структура за разширен контрол върху достъпа EAC да бъде управлявана от CA за издаване на документи за самоличност в единна точка за контакт. Структурата за валидиране е интегрирана с ICAO PKD в търговски продукт за разчитане и писане в PKD включително изписване на Digital Signer и списъци на отменените сертификати, както и качване на основния списък. Чете също така от PKD, за да получи чужди основни списъци както и за достъп до сертификатите на подписващия документа, и списъците на отменените сертификати (CRL). Материалите за валидиране се разпространяват автоматично към станциите със системи за проверка на границите през защитен канал за валидиране, така че могат да валидират всички вътрешни и чужди документи.	
Четящо/пишещо устройство за PKD	
Това е компонент от решението за електронните паспорти служещ за откриване на материали за многостранно валидиране. Неговият сертификат се издава от ICAO PKD.	
Подписващ основния списък	
Това е компонентът от решението за електронните паспорти, служещ за публикуване на подписания списък със сертификати на CSCA, за укрепване на доверието в другите страни. Служи също така за определяне на местен основен списък с проверени и одобрени, издадени от CSCA, който ще бъде издаден от IS за валидиране на чуждестранни паспорти .	
DVWS	
Компонентът Административни услуги публикува WSDL за защитена връзка от структурата на IS, така че Концентратора на системата за проверка на електронните паспорти (IS) и тази на клиента да могат автоматично да актуализират материалите за валидиране и в рамките на структурата на разширения контрол върху достъпа за актуализиране на CV сертификатите за идентифициране от терминалите.	
Системи за проверка (IS)	
IS представлява система за проверка, обикновено експлоатирана от митническите служби или от служба граничен контрол. IS е отговорна за разчитането на електронните данни от MRTD, проверката на подписа върху DSO, самоидентифицирането пред MRTD и показването на различни изходящи данни и съобщения на оператора.	
Вторичен компонент	**Предназначение**
Клиент на системата за проверка (IS)	Клиентът на системата за проверка (IS) за удостоверяване на доверието е доверителен компонент разположен в системата за проверка (IS). Действа като интерфейс между софтуера IS и инфраструктурата на PKI. Клиентът на системата за проверка (IS) за удостоверяване на доверието ще приеме заявки от софтуера на IS за валидиране на обекта с подписаните данни в електронните паспорти (пасивно удостоверяване).

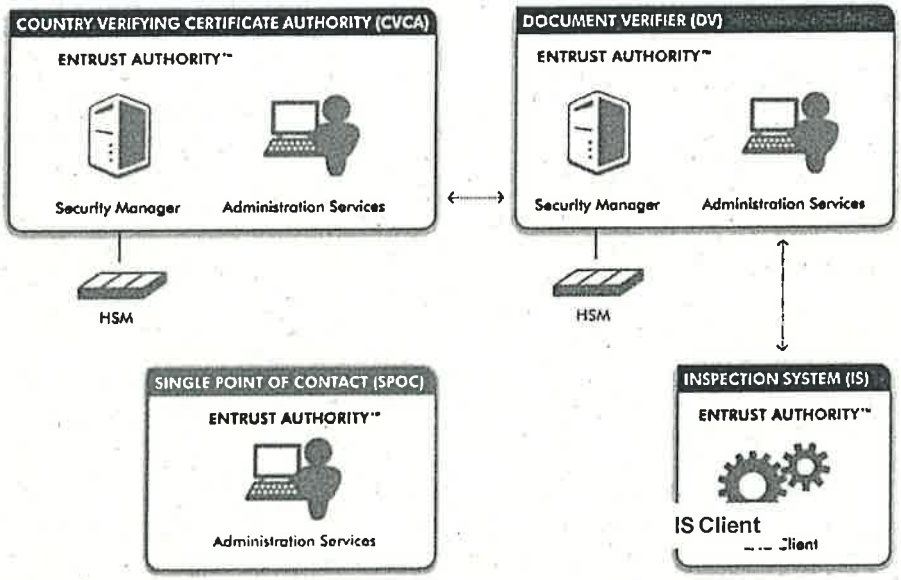
	Клиентът на системата за проверка (IS) за удостоверяване на доверието ще изпълни тези заявки локално на базата на материалите за валидиране получени през защитения канал. Клиентът на системата за проверка (IS) за удостоверяване на доверието влиза в DVWS директно или през концентратора на системата за проверка на електронните паспорти (IS), за да получи местните материали за валидиране.

КОМПОНЕНТИ НА РЕШЕНИЕТО ЗА ПРОВЕРКА НА КОНТРОЛА ВЪРХУ РАЗШИРЕНИЯ ДОСТЪП В СТРАНАТА (EAC)

Този раздел разглежда детайлно всеки от компонентите на решението CVCA.

СТРУКТУРА НА РЕШЕНИЕТО

На *Error! Reference source not found.1* по-долу е показана структурата на решението CVCA с Entrust.



ФИГУРА 1 - ОПРОСТЕНА СТРУКТУРА НА CVCA

КОМПОНЕНТИ НА РЕШЕНИЕТО

Таблица 4 по-долу предлага подробно описание на всеки от компонентите на решението CVCA.

ТАБЛИЦА 4 – КОМПОНЕНТИ НА РЕШЕНИЕТО CVCA

Сертификационен орган за проверка в страната (Country Verifying Certificate Authority)
CVCA представлява PKI, който издава ISO 7816 CV сертификати за DV. Първичният сертификат на CVCA трябва да бъде самоподписан.
Сертифициращ орган за проверка на документи
DV представлява PKI, който издава сертификати по ISO 7816 за CV за системите за проверка (IS-es). Всяка DV може да има един или повече първични сертификата, всеки от тях издаден от различен орган CVCA.

Вторичен компонент	Предназначение
Ръководител по сигурността	Изисква и поддържа сертифицирането от една или повече CVCA и издава CV сертификати по ISO 7816 за оторизиране на IS. Издава също така ограничен брой сертификати X.509 с административно предназначение.
Администрация на Ръководителя по сигурността	Администрира политиката свързана с CA. може да се използва и за администриране на юридически лица-крайни потребители, но това нормално се оставя на Административните услуги.
Административни услуги	Администрира юридически лица-крайни потребители на PKI. Осигуряват мрежов интерфейс който позволява на оторизираните администратори да администрират дистанционно юридическите лица-крайни потребители на PKI. При DV, AS използва мрежов интерфейс за да позволи на IS да управляват свои собствени сертификати автоматично, както и да откриват вериги от сертификати и Linked сертификати от висшестоящи CVCAs през DV.

Система за проверка (IS)

IS представлява система за проверка, обикновено експлоатирана от митническите служби или от служба граничен контрол. IS е отговорна за разчитането на електронните данни от MRTD, проверката на подписа върху DSO, самоидентифицирането пред MRTD и показването на различни изходящи данни и съобщения на оператора.

Вторичен компонент	Предназначение
Клиент на системата за проверка (IS)	Клиентът на системата за проверка на доверителния орган представлява доверителен компонент разположен в системата за проверка (IS). Действа като интерфейс между софтуера на IS и инфраструктурата на PKI. Клиент на системата за проверка (IS) приема заявки от софтуера на IS за дигитални подписи в рамките на EAC и заявки за Linked сертификати или вериги от сертификати. Клиент на системата за проверка (IS) ще изпълни тези заявки локално или ще осигури достъп до тези услуги през идентифициран канал до концентратора за изпълнение. Клиентът на системата за проверка (IS) действа като крайна точка за IS. Клиентът на системата за проверка (IS) ще поиска личните данни от DV и ще ги управлява след това автоматично. Клиентът на системата за проверка (IS) може да работи като крайна точка за личните данни в IS, или като интерфейс между софтуера на IS и концентратора на системата за проверка.

Единна точка за контакт (SPOC)

Непоказана в предходната схема на структурата, но представляваща важен компонент от електронните паспорти в рамките на контрола върху разширени достъп EAC, представлява въведената единна точка за контакт (SPOC). Моделът единна точка за контакт е предназначен да опрости и стандартизира поискването на чуждестранни DVCA сертификати. Всяка изнася единичен SPOC интерфейс и въвежда същия SPOC интерфейс, абстрахирайки се от тези на отделните продавачи на CVCA.

Моделът единна точка за контакт и протоколът за управление на сертификата са

определени от Групата за интероперативност в Брюксел (BIG), работеща под ръководството на комисията към ЕС по Член 6. Спецификацията е одобрена от комисията към ЕС по Член 6 през юни 2009 г.

Вторичен компонент	Предназначение

Единна точка за контакт	Въвеждането на доверителна единна точка за контакт SPOC представлява комплект от услуги в рамките на Административните услуги на Доверителния орган. Същото е разпределено между три интерфейса:
	• Мрежовата услуга единна точка за контакт позволява следната размяна на ключове, сертификати и информация:
	  • Заявка от DVCA за сертификат от чуждестранна CVCA
	  • Изпращане от CVCA на сертификат до чуждестранна DVCA
	  • Заявка за списък на валидни CVCA сертификати от страната домакин с цер изграждане на вериги от сертификати за идентифициране на MRTD
	  • Общи съобщения – текстови в свободна форма
	Заявките от чуждестранна единна точка за контакт ще бъдат пренасочени към местна CVCA, или ако са офлайн – за ръчна обработка.
	• Мрежовата услуга на местната CVCA е предназначена за автоматична обработка на заявките за сертификати проверка на документи без намесата на DV администратор. Услугата се поисква от DV CKM и позволява:
	  • Поискване на CV сертификати
	  • Поискване и получаване на нов DV сертификат
	Заявките от DVCA ще бъдат пренасочени към местна CVCA или подходяща регистрирана чуждестранна единна точка за контакт или за ръчна обработка.
	• GUI Интерфейсът за администриране на единна точка за контакт, който позволява на администратора да:
	  • Преглежда и обработва заявки от единна точка за контакт
	  • Създава, преглежда и обработва изходящи заявки от единна точка за контакт
	  • Преглежда и регистрира чуждестранна единна точка за контакт

Структурата на CVCA е по-сложна от тази на CSCA.

ПРЕДЛОЖЕНА АРХИТЕКТУРА

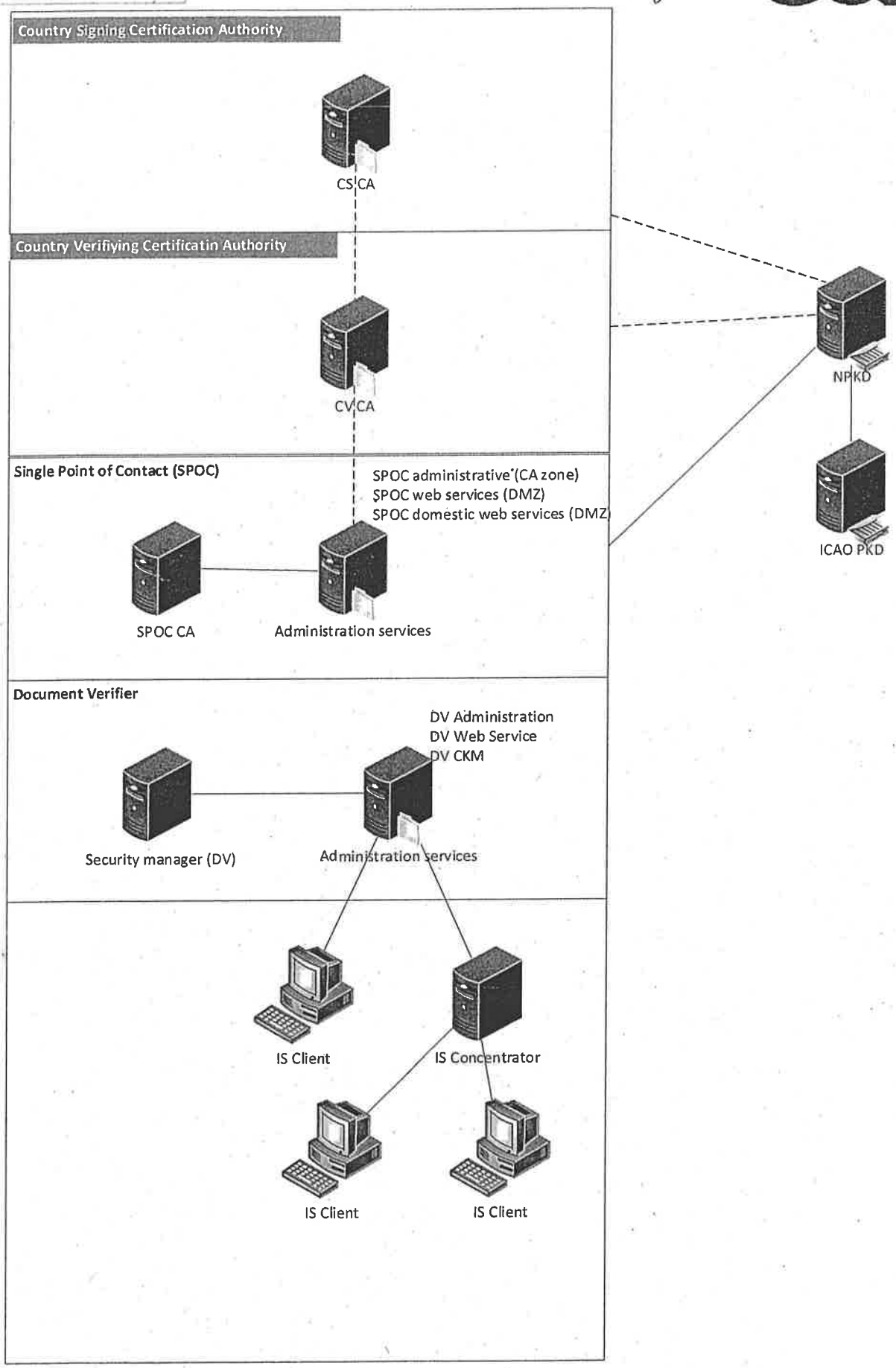
Текущата версия на EJBCA 3.10 и 3.9 е доста стара. Функциите на EAC не се поддържат в тази версия и изискват доразработване. Актуализирането с версия Enterprise означава съвършено нова инсталация. Обновяване до нова версия на EJBCA е възможно, обаче с новата версия на EJBCA решението с отворен код EAC не се поддържа.

Следователно, единствената възможност с EJBCA е да се премине към Enterprise версия, която не е съвместима с предишната версия. Обновяване до Enterprise версия би означавало всъщност изцяло нова инсталация.

В нашето предложение ние решихме да разширим текущата EJBCA реализация с Entrust инфраструктура. Entrust инфраструктурата ще предложи оптимален път за разширение на функционалностите на текущата реализация чрез добавяне на изискваните функционалности.

Предлаганото решение се основава на изпитаната продуктова гама на Entrust e-passport PKI и на клиентско доработване

На ***Error! Reference source not found.2*** по-долу е илюстрирана очакваната опростена логическа структура като част от решението.



ФИГУРА 2 - СХЕМАТИЧНО ИЗОБРАЖЕНИЕ НА ПРЕДЛОЖЕНОТО РЕШЕНИЕ

Решението Entrust e-Passport покрива цялата необходима функционалност

- Модул PKD/NPKD за публикуване на сертификати и CLR в ICAO PKI, разчитане на сертификати и CRL от ICAO PKD и публикуване в NPKD
- DVCA за издаване на сертификати съгласно EU EAC за системи за проверка (IS)
- DVCA RA (DV администриране) за регистрация и управление на системи за проверка
- IS Концентратор като централна система за проверка (тип 1 IS е определена в техническите изисквания)
- IS Client като самостоятелен клиент на IS client или клиент на IS Концентратор
- Единна точка за контакт-CA с поддръжка за издаване на сертификати за обслужване на единна точка за контакт в съответствие със спецификацията на ЕС
- SPOC сървър за изграждане на управление на EAC сертификати с други страни-членки на ЕС, включително мрежови услуги със спецификациите на EU единна точка за контакт и функционалността на единна точка за контакт RA за регистриране и управление, изпращане/получаване на услуги на/от чуждестранна единна точка за контакт, управление, поддръжка на офлайн режим (ръчна обработка на заявки) и поддръжка на онлайн режим (автоматична обработка на заявки).

Функционалното описание на продуктите на Entrust e-Passport е дадено в предходната глава.

СЪЗДАВАНЕ НА НАЦИОНАЛЕН КЛАСИФИКАТОР НА ПУБЛИЧНИТЕ КЛЮЧОВЕ (NPKD)

NPKD ще бъде изграден на сървър съвместим с LDAP v3 на базата на софтуер с отворен източник OpenLDAP. Сървърът на NPKD ще използва стандартна LDAP схема, разширена със схемата ICAO PKD LDAP.

Синхронизирането на NPKD и PKD ще се осъществи чрез Entrust PKD Writer Service и Entrust PKD Reader service. PKD Writer Web service записва главни списъци, CRL и Document Signer сертификати към ICAO PKD. PKD Writer Web service записва също така и поддържа архив с материалите които са качени. PKD Reader service контактува периодично с ICAO PKD или националната PKD, сваля чуждестранни главни списъци, Document Signer сертификати и CRL и ги копира на съответните места в DV Web Service за разпределение или в системите за проверка.

С това предложение се изпълняват всички изисквания посочени в т. 4.1 **Изграждане на National Public Key Directory (NPKD)** от Техническата спецификация.

СЪЗДАВАНЕ НА ЕДИННА ТОЧКА ЗА КОНТАКТ (SPOC)

Във връзка с техническите изисквания посочени 4.2 .

Функционалността единна точка за контакт ще бъде въведена с помощта на сървъра Entrust SPOC. Сървърът Entrust SPOC осигурява:

- Администриране на единна точка за контакт – Администрирането на ЕДИННА ТОЧКА ЗА КОНТАКТ (SPOC) е базиран в мрежата интерфейс за администриране на единна точка за контакт. SPOC администраторите използват SPOC Administration за управление на заявките за сертификати от чуждестранни единни точки за контакт и местни проверители на документи.
- SPOC Web Service – мрежова услуга предназначена за автоматично изпращане и получаване на заявки за сертификати от чуждестранни единни точки за контакт.
- SPOC Domestic Web Service - SPOC Domestic Web Service е мрежова услуга за представяне на заявки за сертификати от местни проверители на документи към местна CVCA, или към чуждестранни единни точки за контакт за обработка от чуждестранни CVCA.

РАЗРАБОТВАНЕ НА SW

Раздел 4.3 **„Разработване на програмни средства за транспортиране на заявки за сертификати, получаване, актуализация и съхранение на сертификати за осигуряване на NPKD и SPOC“** от техническата спецификация разглежда софтуерните продукти за транспортиране на заявки за сертифициране, получаване, актуализиране и съхранение на сертификати за осигуряване на NPKD и единна точка за контакт. Тази функционалност е действително въведена в пакета Entrust ePass. За да осигурим функционалността описана в раздел 4.3, ние планираме инсталирането на:

- Entrust DVCA RA (Администриране на DV) - DV Administration е базиран в мрежата интерфейс за администриране на проверител на документи. DV администраторите използват DV Administration за управление на DV сертификати и заявки за сертификати, системи за проверка и сертификати издадени от тях и заявки за сертификати.
- Entrust PKD Writer Service и Entrust PKD Reader service
- SPOC Administration - SPOC Administration е базиран в мрежата интерфейс за администриране на единна точка за контакт. SPOC използват SPOC Administration за управление на заявки за сертификати и единни точки за контакт и местни проверители на документи.
- SPOC Web Service - SPOC Web Service е мрежова услуга предназначена за автоматизирано изпращане и получаване на заявки за сертификати към/от единна точка за контакт.
- SPOC Domestic Web Service - SPOC Domestic Web Service е мрежова услуга предназначена за автоматизирано представяне на заявки за сертификати от местни проверители на документи към местни CVCA, или към единна точка за контакт за обработка от чуждестранна CVCA.

В Раздел 4.4 **„Разработване на програмни средства за транспортиране на заявки за сертификати, получаване, актуализация и съхранение на сертификати за осигуряване на АИС „ГК“** се изисква също така разработване на софтуер – “Разработване на софтуерни продукти за транспортиране на заявки за сертификати, получаване, актуализиране и съхранение на сертификати предназначени за "BC" AIS”. Както по-горе, тези функционалности са покрити от пакета Entrust suite.

- Entrust PKD Writer Service и Entrust PKD Reader service
- DV Web Service - в EAC системата, the DV Web Service е мрежова услуга преназначена за автоматизирана обработка на заявки за сертификати към системата за проверка без намесата на администратор. DV Web Service трябва да комуникира с IS Концентратор или IS Клиент. В BAC системата, DV Web Service може да осигури CSCA сертификати, основни списъци и CRL, както и Document Signer сертификати за системите за проверка.
- SPOC Administration - SPOC Administration е базиран в мрежата интерфейс за администриране на единична точка за контакт. SPOC администраторите използват SPOC Administration за управление на заявки за сертификати от чуждестранна единна точка за контакт и местни проверители на документи.
- SPOC Web Service - SPOC Web Service е мрежова услуга предназначена за автоматизираното изпращане и получаване на заявки за сертификати към/от чуждестранна единна точка за контакт.
- SPOC Domestic Web Service - SPOC Domestic Web Service е мрежова услуга предназначена за автоматизирано представяне на заявки за сертификати от местни проверители на документи към местни CVCA, или към чуждестранна точка за контакт, за обработка от чуждестранна CVCA.

РАЗРАБОТВАНЕ НА СОФТУЕРНИ ПРОДУКТИ ЗА РАБОТА СЪС СЕРТИФИКАТИ ПРИ ИЗВЪРШВАНЕ НА КОНТРОЛ ВЪРХУ РАЗШИРЕНИЯ ДОСТЪП (EAC)

Раздел 4.5 разглежда разработването на софтуерни продукти за работа със сертификати при извършване на EAC. Планираме покриването на тези функционалности по следния начин.

Entrust Authority IS Concentrator - Entrust Authority IS Concentrator е компонент от Entrust BAC (PA) и/или системата EAC. В системата BAC (PA), IS Concentrator получава материалите от CSCA (CSCA сертификати, главни списъци, CRL и Document Signer сертификати) от DV Web Service и ги предоставя на присъединените IS клиенти. В системата EAC, IS Concentrator управлява EAC сертификатите за една или повече системи за проверка и предоставя сертификатите на присъединените клиенти.

Entrust Authority IS Client - Entrust Authority IS Client е компонент от системата Entrust BAC и/или EAC. В системата BAC, IS клиентът събира материалите от CSCA (CSCA сертификати, главни списъци, CRL и Document Signer сертификати) и ги използва за да извършва пасивно идентифициране на BAC с чиповете за разчитане на пътни документи с машина (MRTD). IS Client може да работи в присъединен, или самостоятелен режим. В присъединен режим IS Concentrator предоставя CSCA материалите на IS клиента. В самостоятелен режим IS клиентът получава CSCA материалите директно от DV Web Service. В системата EAC, IS клиентът управлява EAC сертификатите за една или повече системи за проверка, включително пълното управление на валидността на сертификатите на системата за проверка.

DV Web Service – В системата EAC, DV Web Service е мрежова услуга предназначена за автоматизирана обработка на заявки да сертификати от системата за проверка без намесата на администратор. The DV Web Service трябва да комуникира с IS Concentrator или IS Client. В Системата BAC, DV Web Service може да осигури CSCA сертификати, главни списъци, CRL и Document Signer сертификати за системите за проверка.

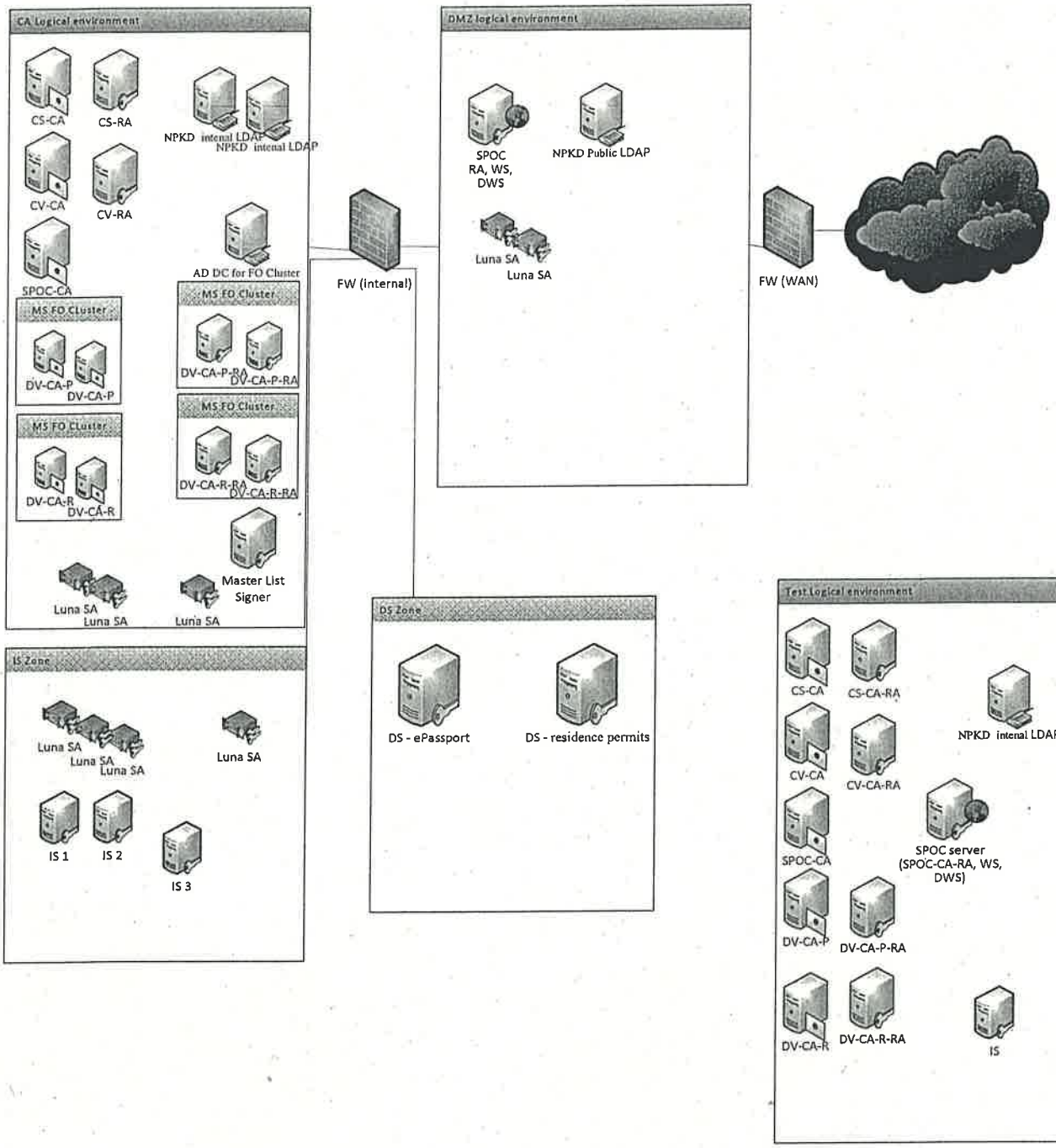
Разработки по поръчка – разработване на приложение за десктоп (извън мрежата) с поддръжка на 3M четящи устройства и дисплей на данните от ICAO LDS, интегриране с Entrust IS Client, осигурявайки функционалност на електронната проверка на MRTD документи (ICAO PA, EU EAC), разчитане на пръстови отпечатъци от чип.

СЕГМЕНТИРАНЕ НА МРЕЖАТА

На *Фигура 3* е представена структурата на сегментиране на мрежата. Съществуват няколко различни логически среди:

- **Зона CA,** в която ще се инсталира инфраструктурата на Сертифициращия орган (CA). Ще има също така вътрешна NPKD директория, RA приложения с изключение на единна точка за контакт.
- **Зона DMZ,** в която ще се предлагат външни услуги, като: единна точка за контакт (RA, мрежови услуги, местни мрежови услуги,) и NPKD публичен LDAP.
- **Зона DS (подписващ документа) –** със съществуващи сървъри на подписващи документи. Съществуващите сървъри ще бъдат интегрирани в новата инфраструктура чрез издаване нов сертификат.
- **Зона IS (системи за проверка) –** ще има 3 IS концентратора (виж 3.5.6.3)
- **Зона за тестова среда –** тестване на всички CA, RA, единна точка за контакт и директорията NPKD.

ЛОГИЧЕСКО РАЗПРЕДЕЛЕНИЕ

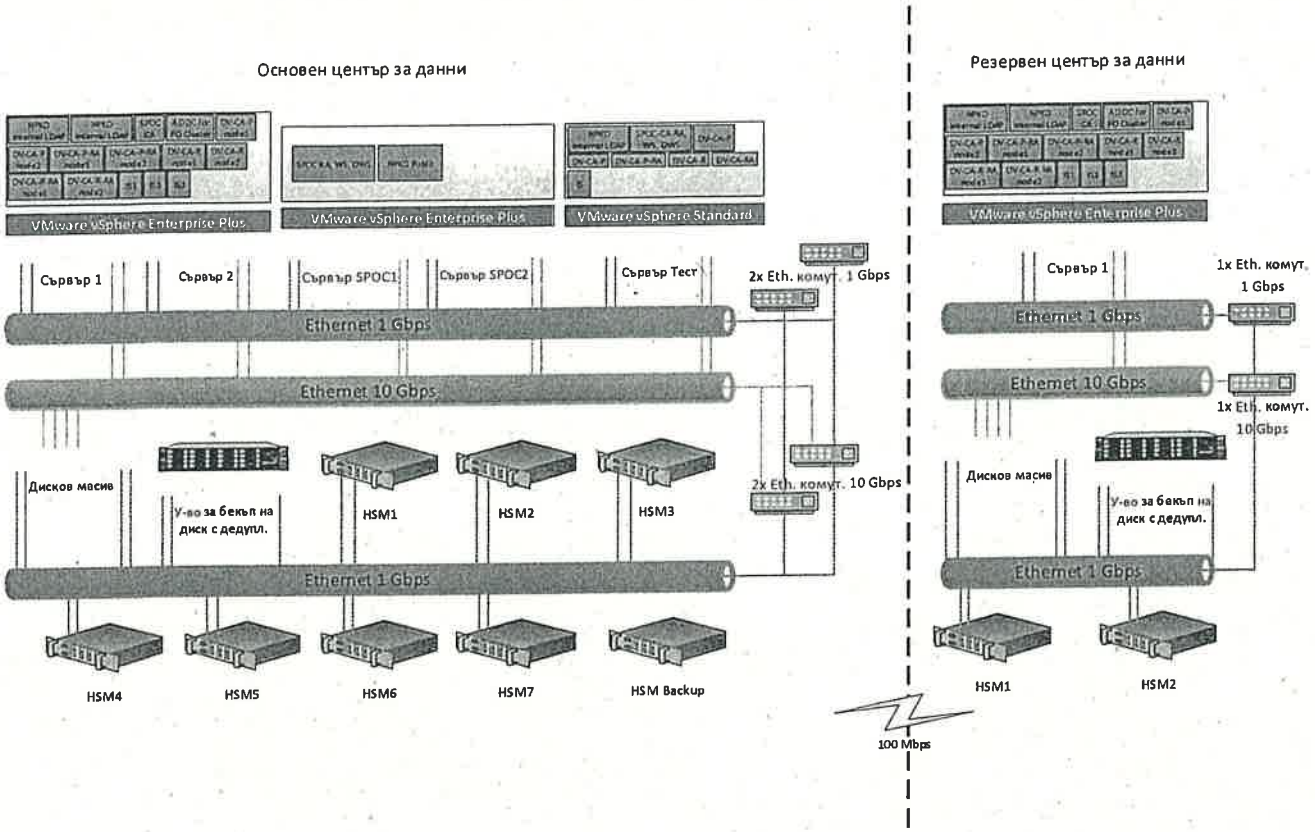


ФИГУРА 3 - ЛОГИЧЕСКО СЕГМЕНТИРАНЕ

Зелен цвят – съществуващи сървъри.

ИНДИВИДУАЛНО РАЗПОЛОЖНИЕ

Разположение на хардуерните устройства и виртуалните машини



ФИГУРА 4 - РАЗПРЕДЕЛЕНИЕ НА ФИЗИЧЕСКИТЕ УСТРОЙСТВА

ИЗИСКВАНИЯ КЪМ ХАРДУЕРА

ЗОНА CA

В зоната CA ще бъде монтирано следното оборудване.

Зона CA :

- 3 x VMware vSphere сървъра – съгласно подробното описание по-долу.
- 3 x Safenet Luna SA 1700 (10 cl, 10 partitions /HSM)
- 1 x Safenet Backup HSM (2 partitions)

Списък на виртуалните машини с активни услуги:

- NPKD1 LDAP internal (Windows 2012 R2 Standard/OpenLDAP)
- NPKD2 LDAP internal (Windows 2012 R2 Standard/OpenLDAP)
- SPOC-CA (Windows 2008 R2 Standard /Entrust SM 8.1 sp1)
- AD DC (Windows 2012 R2 Standard / for MS Fail Over clusters Clusters)
- DV-CA-P node 1 (Windows 2008 R2 Enterprise/Entrust SM 8.1 sp1)
- DV-CA-P node 2 (Windows 2008 R2 Enterprise/Entrust SM 8.1 sp1)
- DV-CA-P-RA Administration node 1 (Windows 2008 R2 Enterprise /Entrust Admin Services 8.3)
- DV-CA-P-RA Administration node 2 (Windows 2008 R2 Enterprise /Entrust Admin Services 8.3)
- 8.3)
- DV-CA-R node 1 (Windows 2008 R2 Enterprise /Entrust SM 8.1 sp1)
- DV-CA-R node 2 (Windows 2008 R2 Enterprise /Entrust SM 8.1 sp1)
- DV-CA-R-RA Administration node 1 (Windows 2008 R2 Enterprise /Entrust Admin Services 8.3)
- DV-CA-R-RA Administration node 2 (Windows 2008 R2 Enterprise /Entrust Admin Services 8.3)

ЗОНА DMZ

- 2 x VMware vSphere сървъра – съгласно подробното описание по-долу.
- 2 x Safenet Luna SA 1700 (1 cl, 1 partitions /HSM)

Списък на виртуалните машини с активни услуги:

- NPKD LDAP public (Windows 2012 R2 Standard/OpenLDAP)
- SPOC (RA/Web Service/Domestic Web Service) (Windows 2008 R2 Standard/Entrust Admin Services 8.3)

ЗОНА IS КОНЦЕНТРАТОРИ

В зоната IS ще бъдат инсталирани 3 сървъра. Предвидени са в допълнение

- 4x Safenet Luna SA 1700 (3cl, 3 partitions)

Инсталираният на сървъра софтуер ще бъде:

- 3 x IS Concentrator (60 клиенти) (Windows 2008 R2 Standard)
- IS Client SW

ТЕСТОВА СРЕДА

В изпитателната среда ще има само един инсталиран vSphere с виртуални машини, като всички услуги ще бъдат като тези в производствената среда.

Виртуални сървъри на сървъра vSphere:

- NPKD LDAP internal (Windows 2012 R2 Standard/OpenLDAP)
- SPOC-CA (Windows 2008 R2 Standard /Entrust SM 8.1 sp1)
- SPOC server (SPOC-CA-RA, WS, WDS) (Windows 2008 R2 Standard /Entrust SM 8.1 sp1)
- DV-CA-P (Windows 2008 R2 Standard /Entrust SM 8.1 sp1)
- DV-CA-P-RA Administration (Windows 2008 R2 Standard/Entrust Admin Services 8.3)
- DV-CA-R (Windows 2008 R2 Standard /Entrust SM 8.1 sp1)
- DV-CA-R-RA Administration (Windows 2008 R2 Standard/Entrust Admin Services 8.3)
- IS server (Windows 2008 R2 Standard /Entrust IS Concentrator)

ХАРДУЕРНИ МОДУЛУ ЗА СИГУРНОСТ

Предложените хардуерни модули за сигурност са SafeNet Luna SA с ниво 3 на сертифициране на FIPS 140-2. Luna SA представляват HSM модули, които поддържат въвеждането на електронните паспорти, като интегрирането със софтуера Entrust е одобрено. Всички HSM ще бъдат еднотипни с известни разлики по отношение на предназначението и мястото на употреба.

Основните характеристики на LUNA SA са:

Сертификати:

- FIPS 140-2 ниво 3
- Общи критерии EAL4+
- Поддръжка на BAC & EAC електронните паспорти

Криптография

- Пълна поддръжка на Suite B
- Асиметрични: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) с означени, определени от потребителя и криви на Brainpool curves
- Симетрични: AES, RC2, RC4, RC5, CAST, DES, Triple DES, ARIA, SEED
- Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512), SSL3-MD5-MAC, SSL3-SHA-1-MAC
- Генериране на номер на произволен принцип: одобрени съгласно FIPS 140-2 DRBG (SP 800-90 CTR режим)

Криптографски API

- PKCS#11, Java (JCA/JCE), Microsoft CAPI и CNG, OpenSSL
- Подробности за продукта са дадени в предложените допълнителни материали и брошури.

С SafeNet LUNA SA всички изисквания заложени в 5.1.2.2.9 са изпълнени.

ЗОНА СА

- 2x Luna SA 1700 (FIPS 140-2 L3, PIN PAD) в режим висока наличност на първичното местоположение
- 1x Luna SA 1700 (FIPS 140-2 L3, PIN PAD) лиценз за 10 дяла на DR
- Лиценз за 10 клиенти да всеки HSM
- Лиценз за 10 дяла (услуги) за всеки HSM

За три услуги ще има активирана защита. За да постигнем това, ние предложихме лиценз за дяловете за защита, както и HSM за защита.

- Лиценз за бекъп за 2 дяла
- HSM за защита (да се използва само Luna G5 с модифициран фърмуер за защита)

ЗОНА DMZ

В DMZ планираме инсталирането на 2 HSM. HSM ще бъде приспособен с 2 дяла, тъй като сървърът за единна точка за контакт генерира два ключа, които изискват собствен дял.

- 2x Luna SA 1700 (FIPS 140-2 L3, PIN PAD) в режим висока наличност
- Лиценз за 2 дяла (за единна точка за контакт са необходими 2 дяла)
- Лиценз за 1 клиент

ЗОНА IS

В ЗОНАТА IS ще има 4 HSM. 3 от HSM ще бъдат на първичното местоположение и един на вторичното. Всички HSM ще бъдат в HA клъстер и всеки клиент ще използва свои собствен дял.

- 4x Luna SA 1700 (FIPS 140-2 L3, PIN PAD)
- лиценз за 3 дяла за всеки HSM
- лиценз за един клиент

SAFENET LUNA CONFIGURATION

ЗОНА CA

SKU	Описание на продукта	количество
908-000162-003-000	Luna SA 1700,Local PED Bundle (2 HSMP,CL,SW 5.2.3,FW 6.2.1/6.10.2,Local PED,20 PED KEYS, Backup HSM)	1
908-000157-003-000	Luna SA 1700,PED-Auth,2 HSMP,CL,SW V5.2.3,FW6.2.1/6.10.2	2
908-000198-001-000	Ъпгрейд на 10 дяла, заводски монтаж, Luna SA	3
908-50000-910-000	Лиценз за всеки допълнителен компютър в мрежата за свързване към HSM	12
908-000067-001	Лиценз Luna HSM отдалечен бекъп (2 дяла)	1
020-160001-001	Удължена едногодишна поддръжка	3

ЗОНА DMZ

SKU	Описание на продукта	количество
908-000157-003-000	Luna SA 1700,PED-Auth,2 HSMP,CL,SW V5.2.3,FW6.2.1/6.10.2	2
908-000197-001-000	Ъпгрейд на 5 дяла, заводски монтаж, Luna SA	2
020-160001-001	Удължена едногодишна поддръжка	3

ЗОНА IS

SKU	Описание на продукта	количество
908-000157-003-000	Luna SA 1700,PED-Auth,2 HSMP,CL,SW V5.2.3,FW6.2.1/6.10.2	4
908-000197-001-000	Ъпгрейд на 5 дяла, заводски монтаж, Luna SA	4
908-50000-910-000	Лиценз за всеки допълнителен компютър в мрежата за свързване към HSM	1
020-160001-001	Удължена едногодишна поддръжка	3

КОНФИТУРАЦИ НА ENTRUST SW

Entrust лицензите се предлагат по следния начин:

- Entrust SPOC software
- Entrust DVCA software
- Entrust IS concentrator (3 servers)
- Entrust IS Client (600 clients)

ENTRUST IS CLIENT (600 CLIENTS) УСЛУГИ

ОБЩ ПОДХОД

Във връзка с въвеждането на новите функционалности консорциумът "C&T – ОСИ" ще следва стандартната методология за проекта. По принцип услугите са разделени на няколко части.

Изисквания: осигурява пълно разбиране на дейността и техническите изисквания за текущия проект, както и бъдещите фази на развитие.

Анализ и структура: планиране и изследване на всички аспекти на проекта включително подходите с всички временни цели и източници, външни и вътрешни изисквания на дейността за временни одобрения, разпределение на задачите между членовете на персонала във връзка с проекта и операциите, осигуряване и подготовка на инфраструктурата

Монтаж и конфигурация: монтаж и конфигурация на Entrust SW and Safenet HSMs интеграционни в съответствие с анализа и проекта

- Изграждане на инфраструктурата (Фаза 1 от изграждането)
- Изграждане на системата (Фаза 2)

Фаза изпитания: провеждане на изпитания за осигуряване на качеството на всички новоразработени компоненти и точки за интегриране с външните системи. (Фаза 3)

Прехвърляне и операции: осигурява поддръжка на прехвърлянето както и тестване на системата преди пуск в действие, обучение на новите администратори и тактическа оперативна. (Фаза 4)

ОПИСАНИЕ НА ИТ ИНФРАСТРУКТУРА

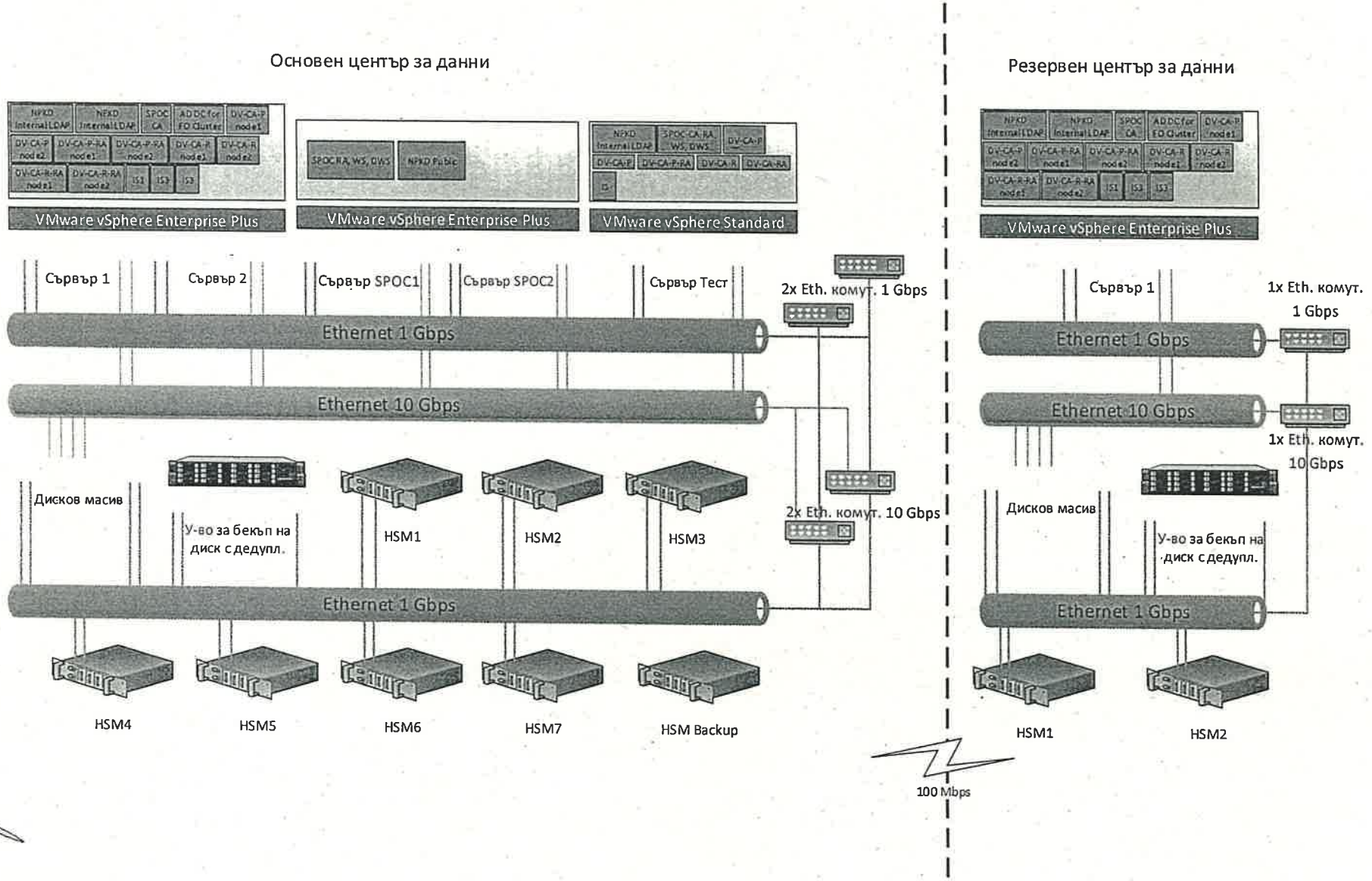
ОБЩО ОПИСАНИЕ

Хардуерната и софтуерната инфраструктура е проектирана да удовлетвори изцяло и едновременно всички изисквания на:

- техническата спецификация на обществената поръчка;
- отговорите на зададените въпроси, които са неизменна част от техническата спецификация;
- спецификата на предложеното от нас цялостно решение.

Разположението на хардуерните устройства е показано на следната диаграма.

Разположение на хардуерните устройства и виртуалните машини



ФИГУРА 5 - ФИЗИЧЕСКА ИНФРАСТРУКТУРА

Една от основните цели на предложената ИТ инфраструктурата е осигуряване на висока наличност на ИТ услугите чрез:

- резервираност на всички критични устройства;
- резервираност на критичните компоненти вътре в самите устройства;
- резервираност на 1 Gbps и 10 Gbps мрежата;
- резервираност на електрозахранването;
- използване на технически средства за бекъп и възстановяване, гарантиращи бързо възстановяване на информацията и работните процеси;
- репликация на критичните данни на резервния център за данни по начин, който (при необходимост) да позволи бързо стартиране на ИТ услугите от резервния център;
- използване на изцяло виртуализирана сървърна среда – както в основния център за данни, така и в резервния. Както е описано по-долу, предложението ни за сървърна виртуализация е реализирано с продукти компанията VMware. С цел използване на всички функционалности на VMware vSphere за продукционните машини, сме включили най-високия клас на продукта – Enterprise Plus. С това постигаме високо ниво на непрекъснатост и поставяме стабилна основа за надграждане на инфраструктурата в бъдеще съгласно последните тенденции в ИТ технологиите;
- осигуряване на всички необходими хардуерни и софтуерни средства за прехвърляне на всички критични процеси на резервния център за данни в случай на срив на основния, както и на връщане на ИТ процесите в основния център за данни, след неговото възстановяване;
- осигуряване на желаното ниво на техническо обслужване и сервизна поддръжка.

Както вече споменахме, всяка сървърна машина в нашето предложение е виртуална (с изключение на HSM, които по задание трябва да са хардуерни устройства). Сървърната виртуализация е реализирана с VMware vSphere Enterprise Plus и VMware vSphere Standard (само за Тест сървъра).

На основния център за данни сме предвидили два виртуализационни клъстера като всеки клъстер се състои от 2 физически сървъра (нода).

Виртуализационен клъстер 1 – Сървър 1 и Сървър 2.

Виртуализационен клъстер 2 – Сървър SPOC1 и Сървър SPOC2.

Сървър Тест е самостоятелен физически сървър, тъй като той ще се ползва за непродукционни цели.

На резервния център за данни сме предвидили 1 сървър, който в случай на някакъв срив на основния център за данни може да стартира която и да е критична продукционна виртуална машина от основния център за данни.

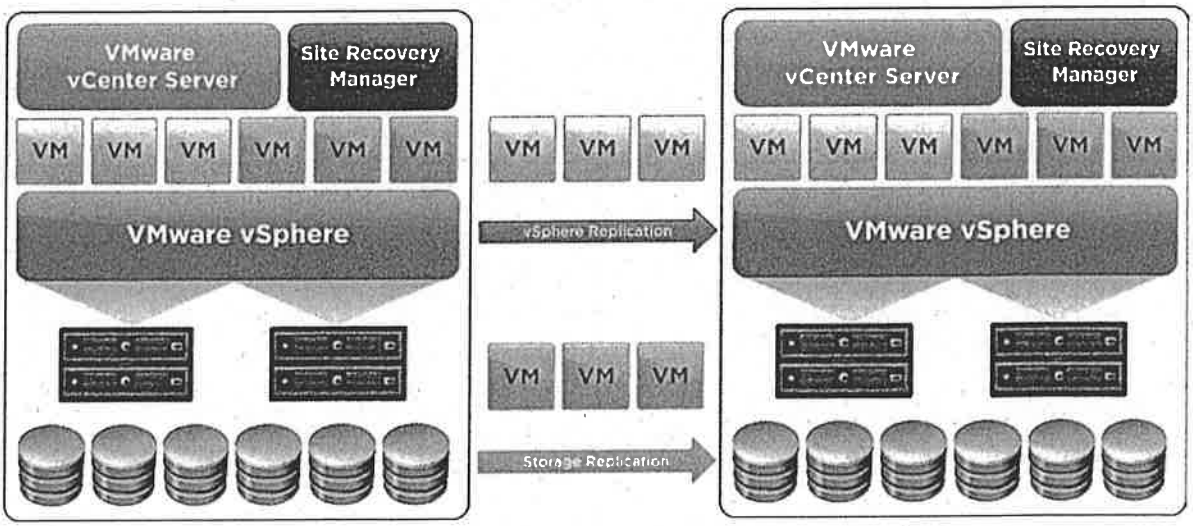
Между двата центъра за данни се осъществява репликация на виртуалните машини с използване на VMware vCenter Site Recovery Manager (SRM) и софтуера за репликация на предложените дискови масиви Fujitsu ETERNUS DX100 S3, който софтуер се нарича Advanced Copy Manager Remote (ACM R).

VMware vCenter Site Recovery Manager (SRM) е водещ софтуерен продукт на пазара за възстановяване от срив на виртуализирани среди. Той допълва VMware vSphere, осигурявайки

най-лесната и най-надеждната защита от срив за всички виртуализирани приложения. SRM осигурява ценово ефективна репликация на vSphere и поддържа голям брой високопроизводителни продукти за сторидж базирана репликация, които репликират виртуалните машини на резервния център. SRM осигурява лесен интерфейс за настройване на планове за възстановяване, които са координирани на всички инфраструктурни нива, заменяйки водещите до грешки наръчници за възстановяване. Плановете за възстановяване могат да бъдат тествани безопасно и неограничен брой пъти, за да се гарантира постигане на желаното ниво. В момент на срив на едната локация или миграция, SRM автоматизира прехвърлянето на услугите от основния на резервния център (failover) и връщането им от резервния на основния център, когато основният център е възстановен (failback). По този начин се осигуряват тествани и предвидими RPO и RTO.

SRM изисква продукт за репликация, който работи „под" SRM. SRM дефакто поддържа всички масово използвани решения за сторидж репликация на повечето производители на сторидж продукти. Потребителят избира сам дали да ползва vSphere Replication (малки организации с неголяма критичност) или решение за сторидж базирана репликация за бизнес критични приложения. Ние ви предлагаме втория вариант.

Традиционните планове за възстановяване са сложни за реализация. Обикновено те са описани в ръководства, в които са възможни грешки и които бързо започват да се разминават с реалността при промени в конфигурацията. Със SRM настройването на план за възстановяване е лесно и може да стане за минути, вместо седмици с традиционните ръководства. Чрез интерфейс, който е тясно интегриран с VMware vCenter Server, потребителят просто избира кои виртуални машини да защити, локира необходимите за тези машини ресурси на резервния център и определя ред на включване на тези вече репликирани виртуални машини в резервния център.



Фигура 6 - VMware vCenter Site Recovery Manager

SRM значително улеснява плановете за възстановяване като автоматично координира повечето ръчни стъпки от традиционните планове.

Със SRM плановете може да се тестват неограничен брой пъти, без да се прекъсват нормалните работни системи. SRM генерира подробен рапорт за резултатите от теста, включително постигнатото RTO. С тази информация, организациите придобиват увереност, че тяхната защита от срив действително отговаря на нуждите. Резултатите от тестовете може да бъдат записани и използвани за доказване на съответствие с изисквания за устойчивост на сривове.

SRM автоматизира целия процес на възстановяване и миграция. След иницииране на failover, услугите автоматично се възстановяват без ръчна намеса. Тъй като автоматизацията елиминира рискът на ръчните процеси, failover може да се изпълни много по-бързо и с високо предвидимо RPO. Типичното време за възстановяване е около 30 минути.

В допълнение към възстановяването от срив, SRM често се ползва да улесни и автоматизира планирани миграции и предпазващи прехвърляния към втория център. Автоматичното обратно връщане към основния център позволява бързо и лесно връщане на приложенията от втория сайт към основния, използвайки оригиналните планове за възстановяване.

Както казахме, SRM се интегрира тясно с „лежащия" под него продукт за репликация, с vSphere и vCenter Server. SRM стъпва на следните компоненти:

Репликация на виртуални машини на резервния център за данни. SRM изисква продукт, който да копира данните на виртуалната машина (дефакто файл) на резервния център за данни. Този продукт

може да е vSphere Replication (част от SRM) или решения за репликация, обикновено предоставяно от доставчика на външния сторидж, върху който се съхраняват виртуалните машини (нашето предложение).

SRM се интегрира с продукта за репликация чрез адаптер за репликация на сториджа – Storage Replication Adapter (SRA). Това е помощен софтуер, написан от производителя на решението за репликация, позволяващ SRM да „види" кои виртуални машини се репликират и да координира изпълнението на плановете за възстановяване със слоя за репликация.

Интеграция с vCenter Server. SRM изисква отделни vCenter инстанции и на основния, и на резервния център за данни. SRM се инсталира на двете локации и се интегрира директно със съответните локални vCenter инстанции.

Настройка на плановете за възстановяване. SRM осигурява лесен интерфейс за създаване на планове за различни сценарии. Потребителите могат да асоциират ресурси на основния и резервния център, задавайки кои виртуални машини да бъдат защитени, техния ред на стартиране, както и временно спиране на машините с нисък приоритет. Потребителите също могат да включват собствени скриптове и автоматично да реконфигурират IP адресите на техните виртуални машини.

SRM е съвместим ACM R (софтуера за отдалечена репликация на предложените от нас дискови масиви Fujitsu ETERNUS DX100 S3). Поради това, SRM комуникира с ACM R и съответно изчислителните ресурси, необходими за репликация на виртуалните машини са пренасочени към дисковите масиви. По този начин сървърите за виртуализация са облекчени при изчисление на задачите, свързани с репликация на виртуалните машини.

Чрез VMware vSphereEnterprise Plus в основния център за данни, при срив на физически сървър всяка продукционна виртуална машина е може да бъде автоматично рестартирана върху другия работещ физически сървър от виртуализационния клъстер – функционалност VMware vSphere High Availability, която е налична в предложения от нас лиценз VMware vSphere Enterprise Plus.

В основния център за данни сървърна виртуална машина може да бъде преместена на другия физически сървър от виртуализационния клъстер без това да води до прекъсване на услугите, предоставяни от тази виртуална машина – функционалност VMware vSphere vMotion, която е налична в предложения от нас лиценз VMware vSphere Enterprise Plus.

Изискването за автоматизирано прехвърляне на работата в резервния център за данни за не повече от 30 минути след взимане на решение, включително преконфигуриране на репликацията на данни в правилната посока е постигнато в нашето предложение чрез използване на VMware vCenter Site Recovery Manager (SRM).

Предложеният от нас бекъп софтуер Veeam Backup and Replication Standard текущо е едно от водещите решение за защита на виртуални среди.

Продуктът позволява бекъп на виртуални машини с възможност за пълното им възстановяване или възстановяване на избрани файлове, директории или обекти на приложения.

Възстановяването е изключително бързо като може да се случи за 2-15 минути.

Софтуерът поддържа дедупликация на данните в самия сървър, подлежащ на бекъп или може да ползва вградената дедупликация на предложеното от нас устройство за бекъп на диск.

Veaam Backup включва възможност за криптиране на данните, които се бекъпират.

В допълнение към репликацията на виртуалните машини, реализирана с VMware SRM и Advanced Copy Manager Remote, предложеният от нас продукт Veeam Backup позволява самостоятелна репликация на виртуална машина на другия център за данни и репликация на бекъп информацията на резервния център за данни.

Veeam поддържа функционалност за проверка на бекъп данните, с което гарантира, че резервното копие е годно за възстановяване. Същата проверка се прави и за репликираните данни, с което потребителят може да е сигурен, че каквото и да е бекъпирал и/или репликирал, то възстановяването ще е коректно.

Поради специфичната функционалност на Veeam Backup да стартира виртуална машина директно от бекъп копието, бекъпираните данни може да се използват за тестови цели. По този начин Veeam бекъп добавя стойност към терабайтите бекъп информация, които иначе просто биха стояли, изчаквайки случай на нужда от възстановяване.

Veeam Backup and Replication се интегрира отлично с VMware vSpherem вкл. и в т. нар. vSphere Web клиент. Това позволява да се наблюдава бекъп инфраструктурата директно от интерфейса на vSphere Web клиента.

Чрез описаната по-горе концепция всички основни компоненти в основния център за данни са резервирани по начин, който гарантира, че само фактори извън доставеното оборудване могат да доведат до необходимостта от прехвърляне на работата в резервния център за данни.

ОПИСАНИЕ НА ХАРДУЕРНИТЕ УСТРОЙСТВА

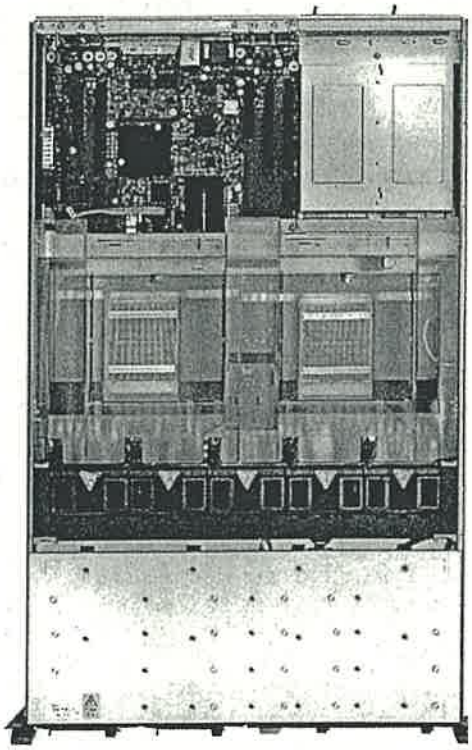
Предложението ни за ИТ инфраструктура включва следните устройства и инфраструктурни софтуерни лицензи.

ОСНОВЕН И РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ

ОСНОВЕН ЦЕНТЪР ЗА ДАННИ – ВИРТУАЛИЗАЦИОННЕН КЛЪСТЕР С ДВА ФИЗИЧЕСКИ СЪРВЪРА – СЪРВЪР 1 И СЪРВЪР 2

Всеки един от тези сървъри има следната конфигурация:

- Марка – Fujitsu;
- Модел – PRIMERGY RX2540 M1;
- Инсталирани два броя процесори Intel Xeon E5-2650 v3 като всеки процесор е с номинална честота 2.3 GHz, 10 физически ядра, 20 логически нишки, 25 MB L3 кеш, QPI 9.6 GTps, DDR4 контролер за памет с 4 канала на 2133 MHz;
- 96 GB DDR4 2133 MHz RAM, регистрова, ECC, организирана като 4x 8 GB + 4x 16 GB, т. е. общо 8 модула;
- Производителност съгласно теста SPECint_rate2006 – 850 точки. Производителността на сървър с два броя процесори от специфицирания в заданието тип Intel Xeon E5-2650 на същия тест е около 540 точки.
- Инсталирано дисково пространство 6 TB след RAID 6 и отделно 1 TB след RAID 1 (за зареждане на софтуера за виртуализация).



Пространството от 6 TB след RAID 6 е постигнато е с използване на 5 броя твърди дискове като всеки диск е SAS 6 Gbps, 2 TB, hot-plug за критични бизнес приложения.

Пространството от 1 TB след RAID 1 е постигнато с използване на 2 броя твърди дискове като всеки диск е SAS 6 Gbps, 1 TB, hot-plug за критични бизнес приложения.

Всички дискове са свързани към хардуерен RAID контролер Fujitsu EP420i, който присъства в списъка на съвместими RAID контролери на VMware за продукта vSphere. EP420i поддържа твърди дискове и SSD устройства със SATA интерфейс с максимална скорост 6 Gbps, както и със SAS интерфейс със скорости 6 Gbps и 12 Gbps. Поддържаните и включени в предложението ни RAID нива са 0, 1, 1+0, 5, 5+0, 6 6+0. Контролерът има 2 GB кеш памет. Нашето предложение включва и опцията за защита на кеш паметта с кондензатор и енергонезависима флаш памет.

- Ethernet 1 Gbps портове – 2 броя чрез вградения LoM (LAN on module);
- Ethernet 10 Gbps порта – 2 броя чрез включения в нашето предложение конвергиран мрежов контролер Fujitsu FUJITSU Converged Network Adapter (CNA) Emulex OCe14102;
- Мрежовите портове позволяват teaming/bonding.
- Контролер за отдалечено управление iRMC S4 с интегриран графичен контролер със собствена видео памет 256 MB и собствен порт за управление 1 Gbps. Предложението ни включва iRMC S4 Advanced опцията, с която постигаме пълно отдалечено управление, включително графична конзола, медия и захранване.
- Вентилатори – 5 броя, 4+1 резервирани и hot-plug.
- Два резервирани захранващи модула, всеки по 800 W с ефективност Platinum;
- Всички дискове, захранвания и вентилатори са заменяеми без изключване на захранването (hot-swap).

Предложената конфигурация на сървър гарантира отговор в рамките на 1.2 sec при едновременна заявка (заявки, постъпили за период до 5 sec) от 50 крайни устройства, свързани към централната компонента на 256 kbps.

ОСНОВЕН ЦЕНТЪР ЗА ДАННИ – ВИРТУАЛИЗАЦИОНЕН КЛЪСТЕР С ДВА ФИЗИЧЕСКИ СЪРВЪРА – СЪРВЪР SPOC1 И СЪРВЪР SPOC2

Всеки един от тези сървъри има следната конфигурация:

- Марка – Fujitsu;
- Модел – PRIMERGY RX2540 M1;
- Инсталирани два броя процесори Intel Xeon E5-2620 v3 като всеки процесор е с номинална честота 2.4 GHz, 6 физически ядра, 12 логически нишки, 15 MB L3 кеш, QPI 8 GTps, DDR4 контролер за памет с 4 канала на 1866 MHz;
- 32 GB DDR4 2133 MHz RAM, регистрова, ECC, организирана като 4x 8 GB;
- Инсталирано дисково пространство 1 TB след RAID 1, постигнато с използване на 2 броя твърди дискове като всеки диск е SAS 6 Gbps, 1 TB, hot-plug за критични бизнес приложения. Дисковете са свързани към хардуерен RAID контролер Fujitsu CP400i, който присъства в списъка на съвместими RAID контролери на VMware за продукта vSphere. CP400i поддържа твърди дискове и SSD устройства със SATA интерфейс с максимална скорост 6 Gbps, както и със SAS интерфейс със скорости 6 Gbps и 12 Gbps. Поддържаните и включени в предложението ни RAID нива са 0, 1, 1+0, 5, 5+0;
- Ethernet 1 Gbps портове – 2 броя чрез вградения LoM (LAN on module);
- Ethernet 10 Gbps порта – 2 броя чрез включения в нашето предложение конвергиран мрежов контролер Fujitsu FUJITSU Converged Network Adapter (CNA) Emulex OCe14102;
- Контролер за отдалечено управление iRMC S4 с интегриран графичен контролер със собствена видео памет 256 MB и собствен порт за управление 1 Gbps. Предложението ни включва iRMC S4 Advanced опцията, с която постигаме пълно отдалечено управление, включително графична конзола, медия и захранване.

- Вентилатори – 5 броя, 4+1 резервирани и hot-plug.
- Два резервирани захранващи модула, всеки по 800 W с ефективност Platinum;
- Всички дискове, захранвания и вентилатори са заменяеми без изключване на захранването (hot-swap).

ОСНОВЕН ЦЕНТЪР ЗА ДАННИ – ЕДИН ФИЗИЧЕСКИ СЪРВЪР – СЪРВЪР ТЕСТ СЪС СЛЕДНАТА КОНФИГУРАЦИЯ:

- Марка – Fujitsu;
- Модел – PRIMERGY RX2540 M1;
- Инсталиран един брой процесор Intel Xeon E5-2620 v3 с номинална честота 2.4 GHz, 6 физически ядра, 12 логически нишки, 15 MB L3 кеш, QPI 8 GTps, DDR4 контролер за памет с 4 канала на 1866 MHz;
- 32 GB DDR4 2133 MHz RAM, регистрова, ECC, организирана като 4x 8 GB;
- Инсталирано дисково пространство 1 TB след RAID 1, постигнато с използване на 2 броя твърди дискове като всеки диск е SAS 6 Gbps, 1 TB, hot-plug за критични бизнес приложения. Дисковете са свързани към хардуерен RAID контролер Fujitsu CP400i, който присъства в списъка на съвместими RAID контролери на VMware за продукта vSphere. CP400i поддържа твърди дискове и SSD устройства със SATA интерфейс с максимална скорост 6 Gbps, както и със SAS интерфейс със скорости 6 Gbps и 12 Gbps. Поддържаните и включени в предложението ни RAID нива са 0, 1, 1+0, 5, 5+0;
- Ethernet 1 Gbps портове – 2 броя чрез вградения LoM (LAN on module);
- Ethernet 10 Gbps порта – 2 броя чрез включения в нашето предложение конвергиран мрежов контролер Fujitsu FUJITSU Converged Network Adapter (CNA) Emulex OCe14102;
- Контролер за отдалечено управление iRMC S4 с интегриран графичен контролер със собствена видео памет 256 MB и собствен порт за управление 1 Gbps. Предложението ни включва iRMC S4 Advanced опцията, с която постигаме пълно отдалечено управление, включително графична конзола, медия и захранване.
- Вентилатори – 5 броя, 4+1 резервирани и hot-plug.
- Два резервирани захранващи модула, всеки по 800 W с ефективност Platinum;
- Всички дискове, захранвания и вентилатори са заменяеми без изключване на захранването (hot-swap).

РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ – ЕДИН ФИЗИЧЕСКИ СЪРВЪР – СЪРВЪР 1 СЪС СЛЕДНАТА КОНФИГУРАЦИЯ:

- Марка – Fujitsu;
- Модел – PRIMERGY RX2540 M1;
- Инсталирани два броя процесори Intel Xeon E5-2650 v3 като всеки процесор е с номинална честота 2.3 GHz, 10 физически ядра, 20 логически нишки, 25 MB L3 кеш, QPI 9.6 GTps, DDR4 контролер за памет с 4 канала на 2133 MHz;
- 128 GB DDR4 2133 MHz RAM, регистрова, ECC, организирана като 8x 16 GB;

- Производителност съгласно теста SPECint_rate2006 – 850 точки. Производителността на сървър с два броя процесори от специфицирания в заданието тип Intel Xeon E5-2650 на същия тест е около 540 точки.
- Инсталирано дисково пространство 6 TB след RAID 6 и отделно 1 TB след RAID 1 (за зареждане на софтуера за виртуализация).

  Пространството от 6 TB след RAID 6 е постигнато е с използване на 5 броя твърди дискове като всеки диск е SAS 6 Gbps, 2 TB, hot-plug за критични бизнес приложения.

  Пространството от 1 TB след RAID 1 е постигнато с използване на 2 броя твърди дискове като всеки диск е SAS 6 Gbps, 1 TB, hot-plug за критични бизнес приложения.

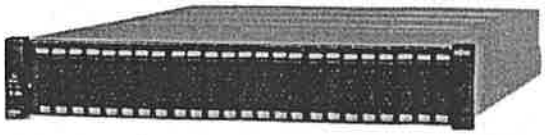
  Всички дискове са свързани към хардуерен RAID контролер Fujitsu EP420i, който присъства в списъка на съвместими RAID контролери на VMware за продукта vSphere. EP420i поддържа твърди дискове и SSD устройства със SATA интерфейс с максимална скорост 6 Gbps, както и със SAS интерфейс със скорости 6 Gbps и 12 Gbps. Поддържаните и включени в предложението ни RAID нива са 0, 1, 1+0, 5, 5+0, 6 6+0. Контролерът има 2 GB кеш памет. Нашето предложение включва и опцията за защита на кеш паметта с кондензатор и енергонезависима флаш памет.

- Ethernet 1 Gbps портове – 2 броя чрез вградения LoM (LAN on module);
- Ethernet 10 Gbps порта – 2 броя чрез включения в нашето предложение конвергиран мрежов контролер Fujitsu FUJITSU Converged Network Adapter (CNA) Emulex OCe14102;
- Мрежовите портове позволяват teaming/bonding.
- Контролер за отдалечено управление iRMC S4 с интегриран графичен контролер със собствена видео памет 256 MB и собствен порт за управление 1 Gbps. Предложението ни включва iRMC S4 Advanced опцията, с която постигаме пълно отдалечено управление, включително графична конзола, медия и захранване.
- Вентилатори – 5 броя, 4+1 резервирани и hot-plug.
- Два резервирани захранващи модула, всеки по 800 W с ефективност Platinum;
- Всички дискове, захранвания и вентилатори са заменяеми без изключване на захранването (hot-swap).

ОСНОВЕН И РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ – ДИСКОВ МАСИВ – ПО ЕДИН БРОЙ МАСИВ НА ВСЯКА ЛОКАЦИЯ

Конфигурациите на тези два дискови масива са еднакви с изключение на конфигурацията на дисковете:

- Марка – Fujitsu;
- Модел – ETERNUS DX100 S3;

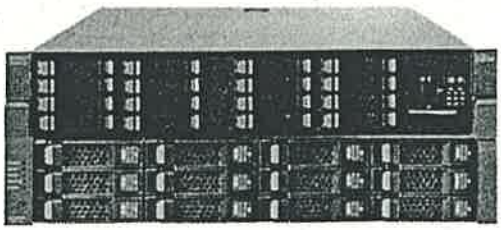


- Инсталирани дискове
  - в основен център:
    - 10x 300 GB, SAS 6 Gbps, 15 000 rpm, hot-plug, осигуряващи 1.33 TiB използваемо пространство след RAID 1+0 в конфигурация 1x (5D+5D);
    - 10x 900 GB, SAS 6 Gbps, 15 000 rpm, hot-plug, осигуряващи 6.4 TiB използваемо пространство след RAID 5 в конфигурация 2x (4D+1P);
    - 1x 300 GB, SAS 6 Gbps, 15 000 rpm, hot-spare;
    - 1x 900 GB, SAS 6 Gbps, 15 000 rpm, hot-spare;
    - Общо 22 диска, поместени в 2U шаси, което също така съдържа двата контролера на дисковия масив;
  - Инсталирани дискове в резервен център:
    - 6x 300 GB, SAS 6 Gbps, 15 000 rpm, hot-plug, осигуряващи 0.79 TiB използваемо пространство след RAID 1+0 в конфигурация 1x (3D+3D);
    - 6x 3 TB, NL-SAS 6 Gbps, 7 200 rpm, hot-plug, осигуряващи 10.68 TiB използваемо пространство след RAID 6 в конфигурация 1x (4D+2P);
    - 1x 300 GB, SAS 6 Gbps, 15 000 rpm, hot-spare;
    - 1x 3 TB, NL-SAS 6 Gbps, 7 200 rpm, hot-spare;
    - Общо 14 диска, поместени в 2 броя 2U шасита (за 2.5" и 3.5" дискове) като шасито за 2.5" дискове съдържа двата контролера на дисковия масив;
- Два броя инсталирани и активирани контролера, работещи в режим на резервирана двойка;
- 2x 10 Gbps Ethernet порта на всеки един контролер – за връзка със сървърите;
- 2x 1 Gbps Ethernet порта на всеки един контролер – за репликация между основния и резервния център за данни;
- Многомаршрутност (Multipathing) е включена. Поддържат се от една страна инструментите за Multipathing на хипервайзора и използваните операционни системи. В допълнение към тези инструменти, производителят на дисковия масив Fujitsu предлага свой софтуер за Multipathing, който е наличен за безплатно изтегляне на интернет страницата на Fujitsu;
- Контролерите поддържат RAID нива 0, 1, 1+0, 5, 5+0, 6;
- Включени лицензи:
  - за моментни копия (snapshots) – стандартно включен;
  - лиценз за thin provisioning – стандартно включен;
  - качество на услугите – QoS;
  - пълни локални копия – включен лиценз за софтуерен продукт Advanced Copy Manager Local;
  - отдалечена синхронна и асинхронна репликация – включен лиценз за софтуерен продукт Advanced Copy Manager Remote.
- Предложените лицензи, както и всички други възможни лицензи за предложения модел дисков масив Fujitsu ETERNUS DX100 S3, се купуват веднъж за дадената машина. Функционалностите им не зависят от броя дискове или дисковото пространство. В бъдеще, при необходимост от повече дисково

пространство следва да се закупят само дискове и шасита, т. е. няма лицензиране на терабайт или брой дискове. Политиката за лицензиране на функционалностите на масива е прозрачна и гарантира предвидима ниска обща цена на притежание;

- Лицензите за репликация (Advanced Copy Manager Local и Remote) са съвместими със софтуера за виртуализация VMware vSphere и със софтуера за автоматизирано превключване между основния и резервния център за данни VMware vCenter Site Recovery Manager;
- Дисковата подсистема поддържа разширение до 144 диска;
- Дисковият масив е с резервирани захранващи модули;
- При спиране на захранването чрез енергията на кондензатор, незаписаните на дискове данни в кеша се записват на енергонезависима флаш памет, където могат да останат неограничено дълго време;
- Смяна на основни компоненти може да се извършва без спиране на системата;
- Обновяване на фърмуеър може да се извършва без прекъсване на достъпа до информацията, съхраняване в дисковия масив.

ОСНОВЕН И РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ – ПО ЕДИН БРОЙ УСТРОЙСТВО ЗА АРХИВИРАНЕ НА ДАННИТЕ НА ВСЯКА ЛОКАЦИЯ:



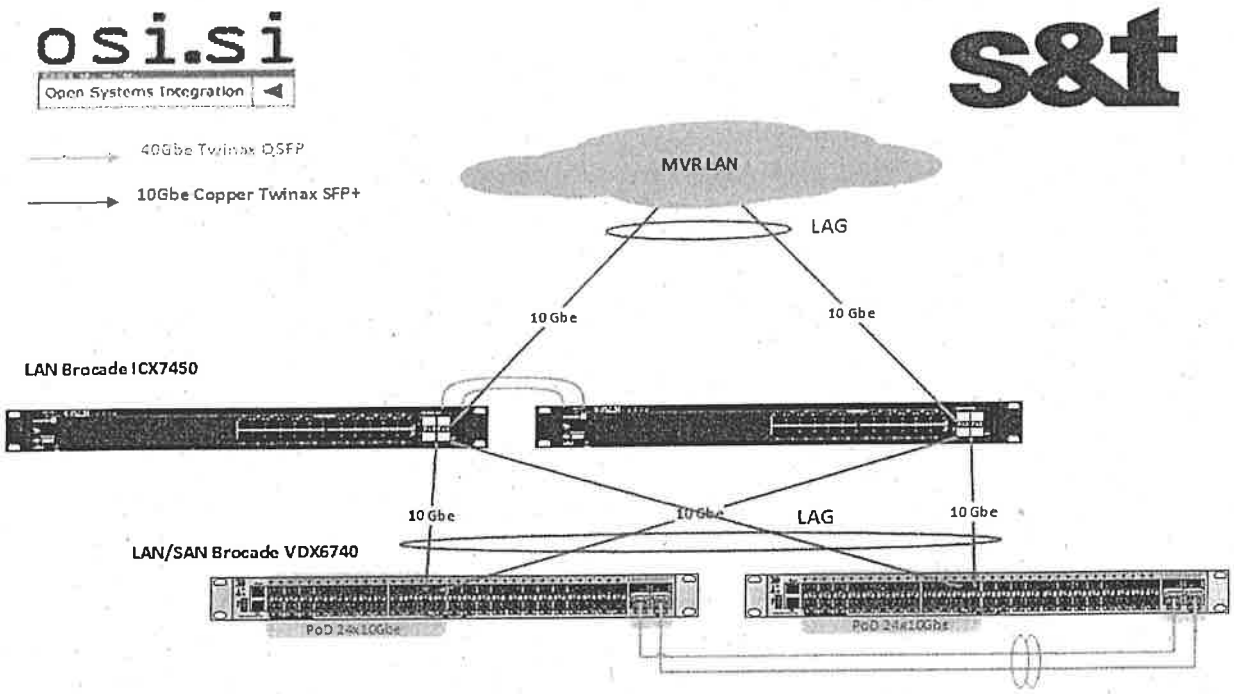
- Марка – Fujitsu;
- Модел – ETERNUS CS800 S5 Scale;
- Устройството е базирано на дискове като осигурява надеждност, както в архивирането, така и във възстановяването.
- Конфигурацията включва:
  - 16 TB пространство след RAID 6 и броено преди дедупликация;
  - 3x 1 Gbps Ethernet порта;
  - CS800 S5 притежава функционалност за дедупликация на данните преди да бъдат записани на дисковете (inline deduplication);

ОСНОВЕН И РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ – СОФТУЕР ЗА АРХИВИРАНЕ

- Veeam Backup and Replication Standard Edition. Позволява архивиране на всички виртуални машини - пълно и частично. Има възможност за възстановяване на отделни файлове без пълно възстановяване на системата. Позволява виртуална машина да бъде стартирана директно от архива, преди пълното и възстановяване на постоянното и място или в другия център. Позволява репликиране на виртуална машина в другия център.

ОСНОВЕН И РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ – LAN И LAN/SAN КОМУТАТОРИ

За осъществяване на връзка между компонентите на разширението в Основния и между компонентите в Резервния център предлагаме използването на високо-надеждни двойно резервирани комутатори на фирмата Brocade. Двойката LAN комутатори конфигурирани в „stack" се свързват с двойката LAN/SAN комутатори конфигурирани в „VCS fabric". На *Фигура 7* е показана LAN/SAN топологията на свързване на комутаторите в Основен център:



ФИГУРА 7 - ФИЗИЧЕСКА ТОПОЛОГИЯ НА МРЕЖАТА – ОСНОВЕН ЦЕНТЪР ЗА ДАННИ

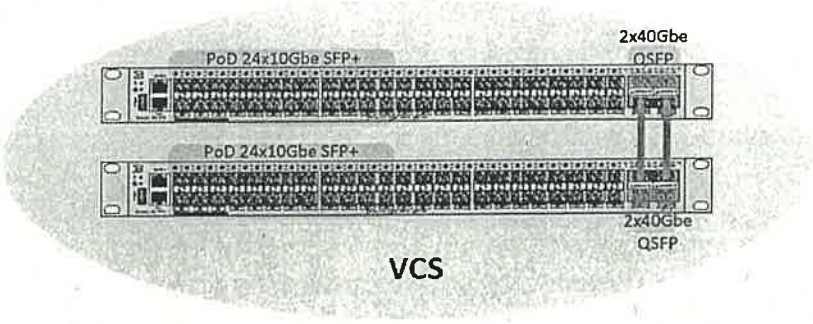
Топологията се състои от 2x ICX7450, 24 портов гигабитов комутатор, конфигуриран в стек. Стекът е конфигуриран с добавянето на стакващи модули от по 40Gbps. Всеки комутатор разполага с по два такива модула за резервираност като общият „stack bandwidth" възлиза на 160Gbps full duplex. В комутаторите за добавени също така и модули с по 4x10GbE SFP+ модули за връзка с LAN/SAN комутаторите като ще се конфигурира LAG от 4 отделни порта с обща честотна лента от 80Gbps между двете логически шасита – LAN stack и VCS fabric. Към конфигурацията на LAN комутаторите е добавен лиценз за отключване на пълната Layer 3 функционалност (Dynamic routing protocols – OSPF, BGPv4 и др.).

Дойката LAN/SAN комутатори се състои от 2x VDX6740, с активирани 24 порта 1/10GbE SFP+ и 2x 40GbE QSFP порта. Предложеният модел може при нужда да се ъпгрейдне до 48x 1/10GbE SFP+ и 4x 40GbE QSFP порта с добавянето на PoD (Port on Demand) лиценз. Платформата позволява и добавянето на FCoE лиценз, с който се отключва FCoE и FC функционалност при нужда. Двойката LAN/SAN комутатори е конфигурирана в VCS фабрика, като е свързана помежду си с 2x 40Gbps twinax кабели.

VCS FABRIC

„VCS fabric" технологията на Brocade елиминира много от недостатъците на класическите етернет мрежи, използвани в центровете за данни. Заедно с подобренията, добавени към стандартната етернет фабрика като логически плоски мрежи без нужда от имплементиране на Spanning Tree Protocol (STP), се добавя и разширена автоматизация с централизирано управление. „VCS fabric" включва уникални функционалности улесняващи цялостното управлението на трафика в центровете за данни, като предоставя мащабируема LAN мрежа, автоматизирана VM свързаност, цялостна прозрачност и високо-ефективен Equal-Cost Multipathing от 1-3 OSI слой с множество Layer 3 шлюзове. VCS предлага автоматично формиране на фабриката и самолекуване. При свързването на два комутатора, поддържащи VCS fabric, те автоматично сформират фабрика и се самоконфигурират. В случай, че предоставяния Bandwidth се окаже недостатъчен, от администраторите се изисква само да добавят нов кабел между комутаторите във фабриката и те се самоконфигурират и новия кабел вече е част от фабриката.

Натоварването се разпределя абсолютно по равно (в ASICs) между всички налични конекции, като осигурява устойчивост и непрекъсваемост на потока от данни.



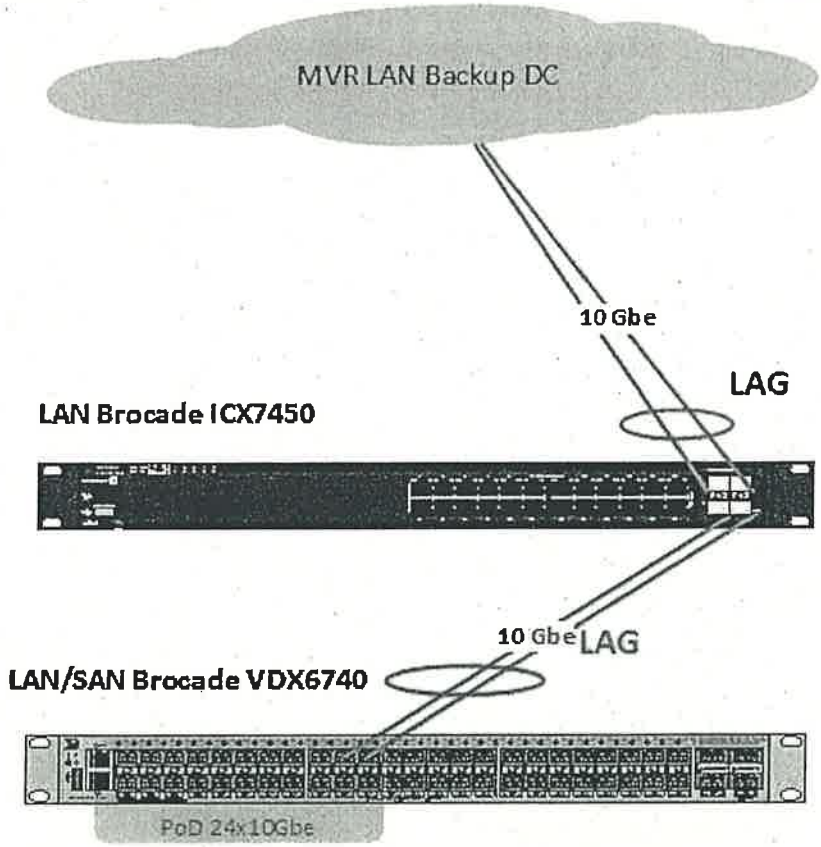
ФИГУРА 8 - VCS FABRIC

На *Фигура 8* е дадена схема на централните комутатори, които ще бъдат с активирани 24x10 Gbps SFP+ порта, но благодарение на наличните физически 48 порта, броят на активните портове може лесно да се увеличи само с допълнителен лиценз. Също с допълнителен лиценз могат да се отключат още 2x40Gbps QSFP порта при нужда.

Повече информация, касаеща „VCS fabric" технологията е дадена в допълнителните материали.

На *Фигура 9* е дадена топологията на свързване на LAN и LAN/SAN комутаторите в Резервния център. Резервният център ще се използва само в случаите ако Основният е напълно недостъпен и затова в него не се предвижда резервираност на оборудването. За постигане на хомогенност са избрани същите модели на комутаторите (ICX7450-24 и VDX6740), но по един брой.

Също като при комутаторите в Основен център, допълнителни портове могат да се активират само с закупуването на лиценз.



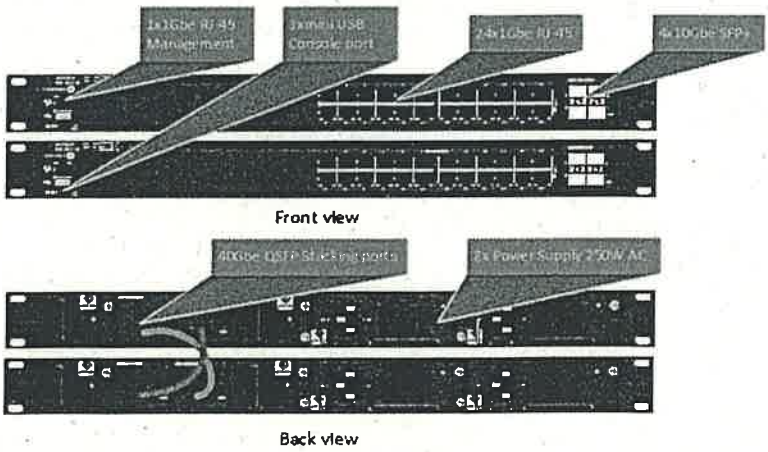
ФИГУРА 9 – ФИЗИЧЕСКА ТОПОЛОГИЯ – РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ

ОСНОВНИ ХАРАКТЕРИСТИКИ НА LAN КОМУТАТОРИТЕ

За LAN комутатори са избрани модели на водещия производител Brocade. Избраният модел е в ценовата листа на производителя от 2015 година и отговаря на съвременните стандарти за изграждане на LAN инфраструктура.

Комутаторът е конфигуриран с резервирани AC захранвания и дублирани вентилатори. Шасито има три слота за вграждане на допълнителни мрежови модули. В настоящата конфигурация те за запълнени с модули за стакване (2x40Gbps) и uplink модул с 4x10Gbps SFP+.

ICX7450 поддържат стакване на до 12 броя комутатора със "stacking bandwidth" от 160 Gbps и поддръжка на bounding/teaming между портове от различни елементи от



ФИГУРА 10 – ICX7450 ИЗГЛЕД ОТПРЕД И ОТЗАД

стека. Комутаторите за конфигурирани потока за въздух да минава с посока отзад напред т.е. всмуква се през вентилаторите на захранванията и излиза от страната на портовете. Така комутаторите ще бъдат ориентирани с портовете, сочещи към гърба на шкафа за да се оптимизира дължината и разпределението на мрежовите кабели. Комутаторите ще бъдат предоставени с активирани Premium Layer 3 функционалности – обобщени в таблицата с техническите характеристики.

В *Таблица 5* са дадени основните характеристики на LAN комутаторите:

ТАБЛИЦА 5 – ОСНОВНИ ТЕХНИЧЕСКИ ХАРАКТЕРИСТИКИ ICX7450

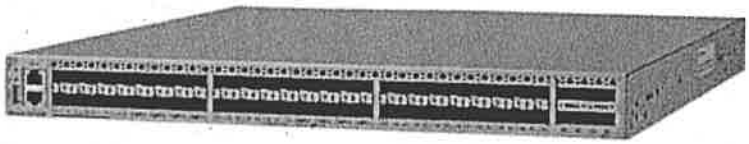
Техническа характеристика	Стойност
Капацитет на комутиращата матрица	288 Gbps – line rate (non-blocking)
Stacking bandwidth	160 Gbps
Jumbo Frames	9216 bytes
Max MAC адреси	32000
Maximum router in hardware	16000 (IPv4), 3000 (Ipv6)
Max VLANs	4096
Брой устройства в стак	12
Advanced IPv4/v6 L3 routing	С Premium license - включен
Макс. разстояние между суичовете в стак	10 км
Входящо напрежение / честота	AC: 100 to 240 VAC @ 50 to 60 Hz
Switch power utilization† (25°C)	
Idle (no PoE load)	63 W
10% traffic	64 W
100% traffic	69 W
Switch heat dissipation†, § (25°C)	
Idle (no PoE load)	215 BTU/hr
10% traffic	218 BTU/hr
100% traffic	235 BTU/hr
MTBF† (25°C)	399 973 часа

Пълната техническа спецификация може да се намери в брошурите дадени като допълнителни материали.

ОСНОВНИ ХАРАКТЕРИСТИКИ НА LAN/SAN КОМУТАТОРИТЕ

За LAN/SAN комутатори са избрани модели на водещия производител Brocade. Избраният модел е в ценовата листа на производителя от 2014 година и отговаря на съвременните стандарти за изграждане на LAN/SAN инфраструктура.

Brocade VDX6740 предлага до 48x 10 GbE SFP+ порта и до 4x 40 GbE порта, които при нужда могат да се разделят на 4x10 GbE SFP+. В допълнение комутаторът е един от най-икономичните на пазара, като консумира максимум по 2W на 10GbE port. Комутаторите са конфигурирани с резервирани захранвания и вентилаторни модули. За оптимизиране на дължината на мрежовите кабели е избрана посока на охлаждащия въздух да бъде back-to-front (топлия въздух излиза от страната на портовете).



Някои от отличителните характеристики на предложените комутатори са ниска латентност (850 ns), 24 MB packet buffers (по подразбиране са конфигурирани packet buffer 280 KB на порт), DCB Priority Flow Control (PFC) classes 8, Maximum jumbo frame size 9216 bytes, UnicastStormControl, Rapid Spanning Tree, VLAN support, Layer 3 dynamic routing, non-blocking design. Маршрутизаторите се конфигурират във VCS фабрика, която се управлява като едно логическо устройство и ефективно балансира мрежовия трафик по множество пътища (до 16) без блокиране на портове.

Brocade VCS fabrics рационализира внедряването и нормалните мрежови операции с вградените си функции, които дават възможност за автоматично конфигуриране и управление. Тези характеристики включват:

- Brocade VCS Logical chassis – единна точка за управление и наблюдение.
- Self-forming и self-healing fabric – конфигурирането е опростено дотолкова, доколкото физическо свързване на елементите на фабриката. При повреда на член на фабриката, той може да се извади и да се замени също без прекъсване.
- Zero-touch provisioning и Zero-touch scale-out - При вече работеща фабрика, добавянето на нов комутатор се изчерпва с физическото му свързване. Фабриката се разширява без прекъсване на трафика.
- In-Service Software Upgrades – Обновяването на софтуера се извършва без прекъсване на Layer 2 и 3 трафик, FC и FCoE.

ТАБЛИЦА 6 – ОСНОВНИ ТЕХНИЧЕСКИ ХАРАКТЕРИСТИКИ VDX6740

Техническа характеристика	Стойност
Капацитет на комутиращата матрица	1.28 Tbps
Port-to-port latency	850 ns
1/10 GbE SFP+ ports	до 64
40 GbE QSFP+ (10 GbE breakout cable)	4

2/4/8/16 Gb Fibre Channel Flex Ports	до 32
10 GbE Ports on Demand (PoD)	24, 32, 40, 48, 56, 64
Jumbo Frames	9216 bytes
Max MAC адреси	160000
Maximum router in hardware	12000
Max VLANs	4096
Advanced IPv4/v6 L3 routing	Yes
Queues per port	8
Maximum switches in a VCS fabric	48
Maximum ECMP paths in a VCS fabric	16
Maximum switches across which a vLAG can span	8
Cooling fans	N+1 redundant, integrated into power supplies
Power supplies	Two internal, redundant, field-replaceable, load-sharing AC power supplies
Maximum power consumption	Brocade VDX 6740: 110 W
Heat dissipation	375.1 BTU/hr

Пълната техническа спецификация може да се намери в брошурите дадени като допълнителни материали.

В конфигурацията са включени всички необходими кабели и аксесоари за монтажа на оборудването в комуникационен шкаф.

LAN/SAN BOM

В *Таблица 7* са дадени Bill of Materials (BoM), които ще бъдат доставени, инсталирани и конфигурирани за нуждите на цялостното решени.

ТАБЛИЦА 7 – ОКОМПЛЕКТОВКА НА МРЕЖОВОТО ОБОРУДВАНЕ

№	Описание на продукта	Партиден номер	К-во
LAN комутатори			
1	24-port 1 GbE switch, 3 modular slots for optional uplinks/stacking. Power supply, fan & modules need to be ordered separately	ICX7450-24	3
1.1	ICX7450/6610/6650 NONPOE 250W AC PSU, intake airflow, back to front airflow	RPS15-I	6
1.2	ICX 7450 intake airflow fan, back to front airflow	ICX-FAN10-I	6

1.3	Power Cord for RPS2/3/5/9, European version	PCEURO	6
1.4	40GE Direct Attached QSFP+ to QSFP+ Active Copper cable, 1m, 1-pack	40G-QSFPQSFP-C-0101	2
1.5	ICX 7450 4-port 1/10GbE SFP+ Module	ICX7400-4X10GF	3
1.6	ICX 7450 1-port 40GbE QSFP+ Module	ICX7400-1X40GQ	4
1.7	ICX 7450 LAYER 3 PREMIUM SOFTWARE LICENSE	ICX7450-PREM-LIC	3
1.8	DIRECT ATTACHED SFPP ACTIVE COPPER, 3M,1-PACK	10G-SFPPTWX-0301	6
1.9	ESSENTIAL PARTS ONLY SUPPORT - ICX7450-24 (3 yr)	ICX7450-SVLNDP-3	3
LAN/SAN комутатори			
	VDX 6740, 24P SFP+ PORTS ONLY - NO OPTICS, AC, PORT SIDE EXHAUST AIRFLOW	BRVDX6740-24-R	3
	2-PORT 40G Ports on Demand(POD) LICENSE FOR VDX6740 AND VDX6740T	BR-VDX6740-2X40G-POD	2
	FRU, 6510/6505/6710/6740 FIXED RACK MOUNT KIT for 4 post racks	XBR-R000291	3
	40GE Direct Attached QSFP+ to QSFP+ Active Copper cable, 1m, 1-pack	40G-QSFP-QSFP-C-0101	2
	Power Cord for RPS2/3/5/9, European version	PCEURO	6
	ESSENTIAL PARTS ONLY SUPPORT - BR-VDX6740-24-R (3 yr)	6740-24-SVLNDP-3	3
Twinax кабели			
	DIRECT ATTACHED SFPP COPPER,3M,8-PACK	10G-SFPPTWX-0308	9

ОСНОВЕН И РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ – KVM КОМУТАТОР – ПО ЕДИН БРОЙ НА ВСЯКА ЛОКАЦИЯ

- Марка – Fujitsu;
- Модел – S4-0812 – IP KVM модел с включени всички кабели и аксесоари за коректно свързване на всички сървъри и конзолата RC25;

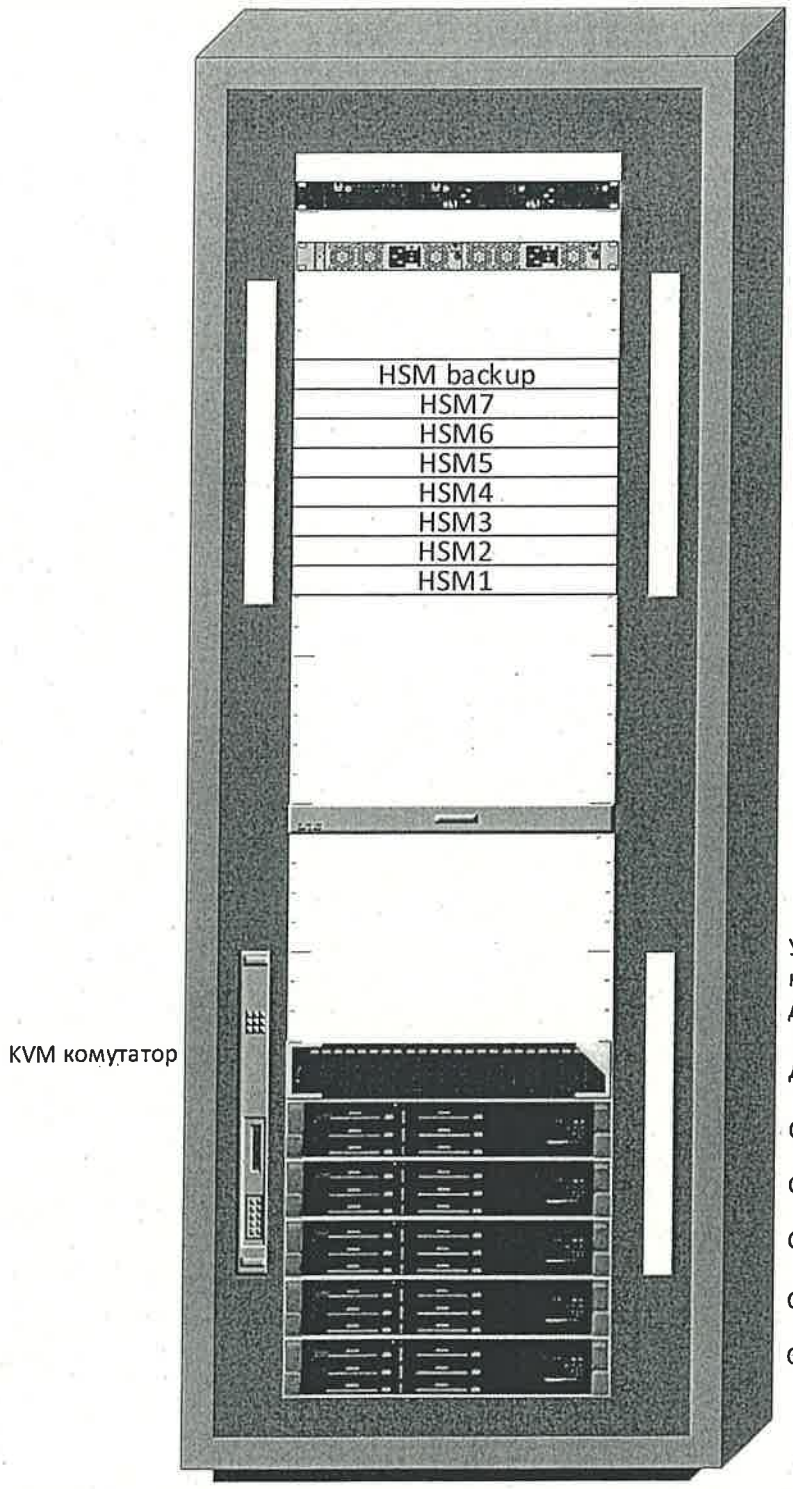
ОСНОВЕН И РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ – КОНЗОЛА – ПО ЕДИН БРОЙ ЗА ВСЯКА ЛОКАЦИЯ

- Марка – Fujitsu;
- Модел – RC25, 17", 1280x1024.

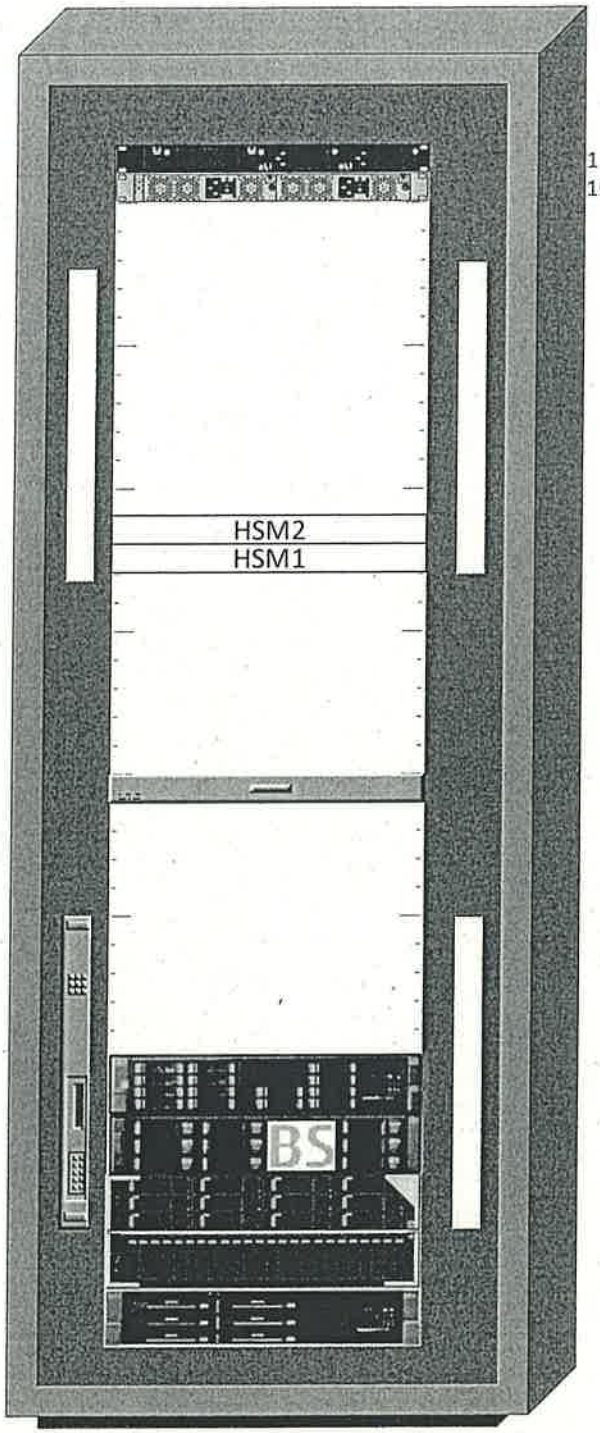
ОСНОВЕН И РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ – СЪРВЪРЕН ШКАФ – ПО ЕДИН БРОЙ ЗА ВСЯКА ЛОКАЦИЯ:

- Марка – Fujitsu;
- Модел – RC25, 17", 1280x1024.
- PRIMECENTER M1 Rack 742S – 42U, 700 mm широчина. В шкафа са предвидени всички компоненти и аксесоари за коректно монтиране и окабеляване на предложените устройства, интерфейсни и захранващи кабели. Електрозахранването е по две независими вериги. Всички устройства с изкл. на KVM комутатора и конзолата разполагат с два захранващи модула, които ще се свържат съответно към различна захранваща верига. Захранващите елементи в шкафа за едната верига са напълно изолирани от другата.

Подреждането на устройствата в шкафа за основния център за данни е показано на *Фигура 11* по-долу. Изгледа на устройствата, подредени в шкафа в резервния център е показано на*Фигура 12*.



ФИГУРА 11 – РАЗПОЛОЖЕНИЕ НА ОБОРУДВАНЕТО В КОМУНИКАЦИОНЕН ШКАФ – ОСНОВЕН ЦЕНТЪР



Резервен център за данни

ФИГУРА 12 – РАЗПОЛОЖЕНИЕ НА ОБОРУДВАНЕТО В КОМУНИКАЦИОНЕН ШКАФ – РЕЗЕРВЕН ЦЕНТЪР

osi.si
Open Systems Integration

s&t

ИНФОРМАЦИЯ ЗА ПЛАНИРАНЕ НА СЪРВЪРНОТО ПОМЕЩЕНИЕ

За коректно електрозахранване от 2 независими линии, в сървърното помещение за всеки център за данни трябва да бъдат осигурени 4 броя захранващи конектори от тип IEC 310, 16 A. Шкафът ще има 4 броя IEC 309 16 A конектора, показани на снимката.

Таблица 8 - Основен център за данни

Център за данни	Тип	Име	Марка	Модел	Активна мощност на 100% товар, W	Отд. топлина при 100% товар, BTU/h	Вис., U	Тегло, kg
1	Сървър	Сървър 1	Fujitsu	RX2540 M1	441.84	1507.620659	2	25
1	Сървър	Сървър 2	Fujitsu	RX2540 M1	441.84	1507.620659	2	25
1	Сървър	SPOC1	Fujitsu	RX2540 M1	274.99	938.3048277	2	25
1	Сървър	SPOC2	Fujitsu	RX2540 M1	274.99	938.3048277	2	25
1	Сървър	Тест	Fujitsu	RX2540 M1	204.99	699.4549133	2	25
1	Дисков масив	Дисков масив	Fujitsu	DX100 S3	556.01	1897.184869	2	25
1	Бекъп на диск	Бекъп на диск	Fujitsu	CS800 S5	685	2337.317019	4	55
1	HSM1	HSM1	SafeNet	Luna 1700	180	614.1854939	1	15
1	HSM2	HSM2	SafeNet	Luna 1700	180	614.1854939	1	15
1	HSM3	HSM3	SafeNet	Luna 1700	180	614.1854939	1	15
1	HSM4	HSM4	SafeNet	Luna 1700	180	614.1854939	1	15
1	HSM5	HSM5	SafeNet	Luna 1700	180	614.1854939	1	15
1	HSM6	HSM6	SafeNet	Luna 1700	180	614.1854939	1	15
1	HSM6	HSM7	SafeNet	Luna 1700	180	614.1854939	1	15
1	HSM6	HSM8	SafeNet	Luna 1700	180	614.1854939	1	15

1	IP KVM комутатор	IP KVM комут.	Fujitsu	S4-0812	25	85.30354083	0	4
1	Rack Console	Конзола 17"	Fujitsu	RC25	25	85.30354083	1	11
1	Ethernet Switch 1 10 Gbps	Комут.	Brocade	VDX6740	110	375.3355796	1	8.66
1	Ethernet Switch 2 10 Gbps	Комут.	Brocade	VDX6740	110	375.3355796	1	8.66
1	Ethernet Switch 3 1 Gbps	Комут.	Brocade	ICX7450	69	235.4377727	1	7
1	Ethernet Switch 4 1 Gbps	Комут.	Brocade	ICX7450	69	235.4377727	1	7
					4727.66	**16131.45**	**29**	**371.32**

ТАБЛИЦА 9 - РЕЗЕРВЕН ЦЕНТЪР ЗА ДАННИ

Център за данни	Тип	Име	Марка	Модел	Активна мощност на 100% товар, W	Отд. топлина при 100% товар, BTU/h	Вис., U	Тегло, kg
1	Сървър	Сървър 1	Fujitsu	RX2540 M1	454.43	1550.579522	2	25
1	Дисков масив	Дисков масив	Fujitsu	DX100 S3	573.45	1956.692619	4	70
1	Бекъп на диск	Бекъп на диск	Fujitsu	CS800 S5	685	2337.317019	4	55
1	HSM1	HSM1	SafeNet	Luna 1700	180	614.1854939	1	15
1	HSM2	HSM2	SafeNet	Luna 1700	180	614.1854939	1	15
1	IP KVM комутатор	IP KVM комут.	Fujitsu	S4-0812	25	85.30354083	0	4
1	Rack Console	Конзола 17"	Fujitsu	RC25	25	85.30354083	1	11
1	Ethernet Switch 2 10 Gbps	Комут.	Brocade	VDX6740	110	375.3355796	1	8.66
1	Ethernet Switch 3 1 Gbps	Комут.	Brocade	ICX7450	69	235.4377727	1	7
					2301.88	**7854.34**	**15**	**210.66**

Предложението ни включва следните лицензи за инфраструктурен софтуер за основния и резервния център за данни:

- VMware vSphere Enterprise Plus – 10 броя. Лицензирането е за всеки инсталиран процесор в сървър, който ще бъде виртуализационен хост:
  - Основен център – Сървър 1, Сървър 2, Сървър SPOC1, Сървър SPOC2;
  - Резервен център – Сървър 1;
- Поддръжка 24x7 за 3 години на VMware vSphere Enterprise Plus – 10 броя;
- VMware vSphere Standard – 1 брой. За Сървър Тест основен център;
- Поддръжка 24x7 за 3 години на VMware vSphere Standard – 1 брой;
- VMware vCenter Server Standard – 2 броя – по един брой за всеки център за данни;
- Поддръжка 24x7 за 3 години на VMware vCenter Server Standard Edition – 2 броя;
- VMware vCenter Site Recovery Manager Standard, пакет за репликация на 25 виртуални машини с включена поддръжка 24x7 за 3 години – 4 броя такива пакети – по 2 пакета за всеки център за данни;
- Microsoft Windows Server 2012 R2 Datacenter Edition – 4 броя. Позволява работа с неограничен брой виртуални машини на дадения физически сървър с инсталирана в тях операционна система Windows Server 2008 R2 / 2012 R2. За:
  - Основен център за данни – Сървър 1, Сървър 2, Сървър Тест;
  - Резервен център за данни – Сървър 1;
- Microsoft Windows Server 2012 R2 Standard Edition – 2 броя – Сървър SPOC1, Сървър SPOC2 основен център за данни. Позволява работа с до 2 броя виртуални машини на дадения физически сървър с инсталирана в тях операционна система Windows Server 2008 R2 / 2012 R2, което е достатъчно за нашето решение;
- Microsoft Server 2012 CAL per user – 660 броя.
- Veeam Backup and Replication Standard – 11 броя – за всички сървъри, лицензиране на процесор.

ПЛАН ЗА ПРЕМИНАВАНЕ ОТ ОСНОВЕН КЪМ РЕЗЕРВЕН ЦЕНТЪР И ОБРАТНО

1. Общи понятия

VMware SRM предлага възможност за планирано мигриране (failover) на виртуалните машини от основния център **(Protected Site)** в резервния център **(Recovery Site)** и съответно планирано мигриране обратно (failback) от резервния център в основния център.

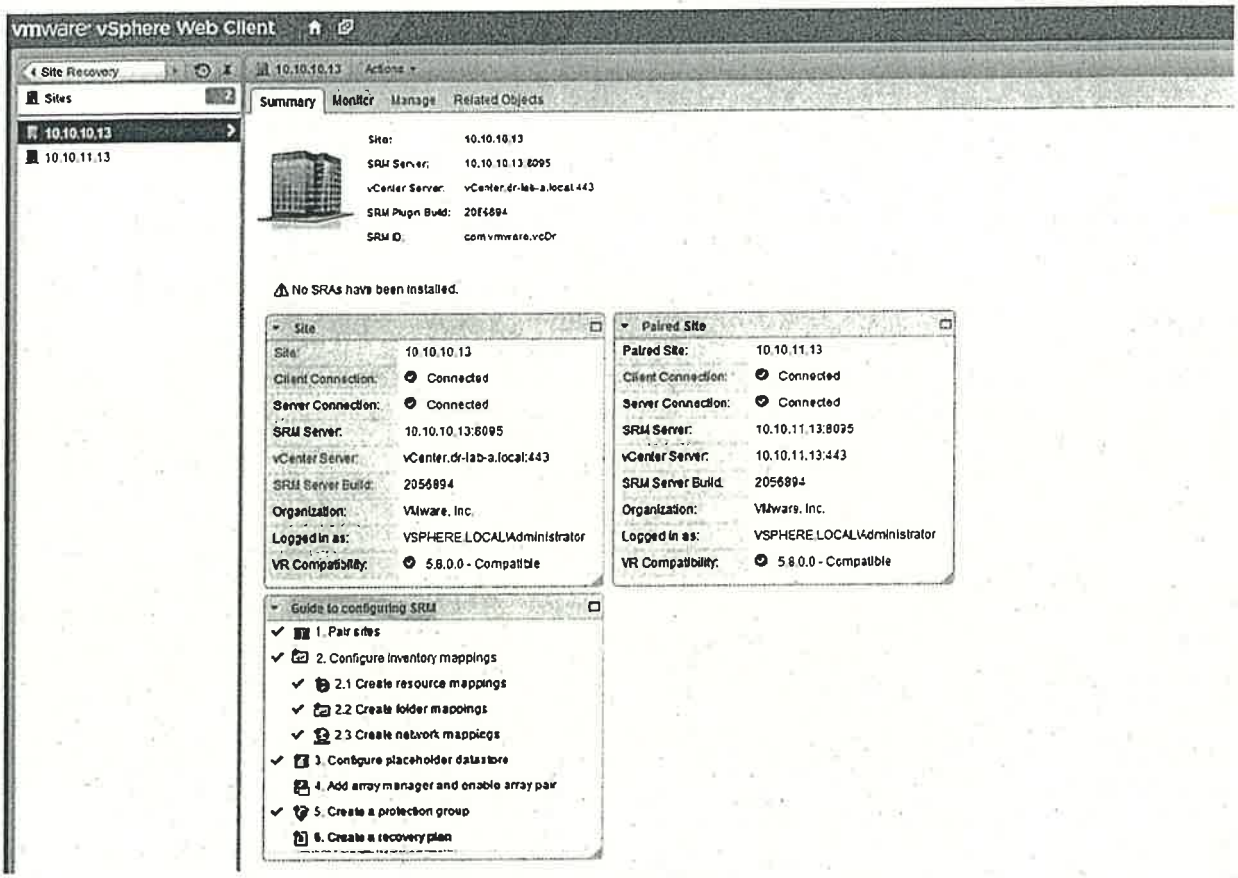
Също така SRM предлага възможност за аварийно възстановяване на виртуалните машини в резервния център, при ситуация на аварийно отпадане на основния център. Също така съществува възможност за миграция на виртуалните машини обратно в основния център, след възстановяване на функционалността му.

Планираната Миграция (Planned migration) позволява преместване на виртуалните машини от защитения център към резервния, като преместването става с Минимален Риск от загуба на данни. При наличие на някакъв проблем по време на миграцията, процеса спира и се дава възможност за отстраняване то му, след което се осъществява успешно миграцията.

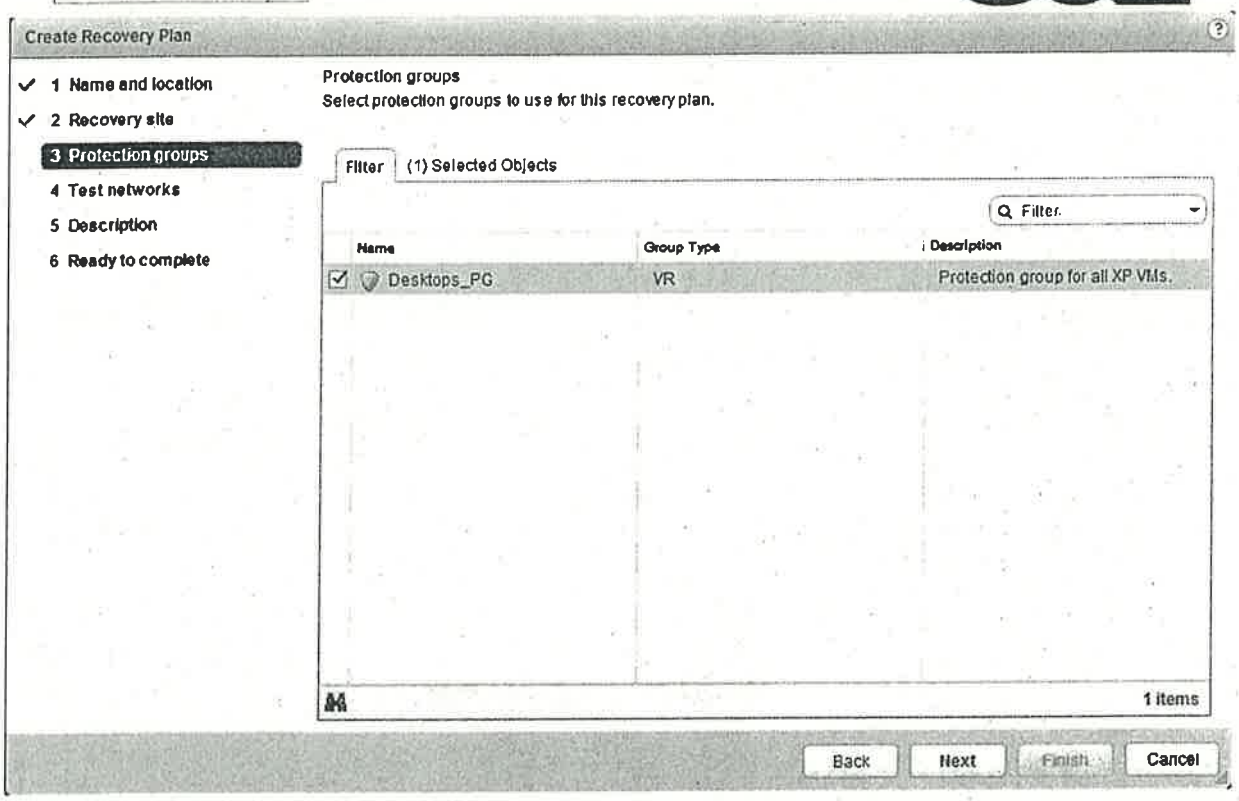
Събитие на аварийна ситуация (Disaster recovery event) е събитие на непланирана миграция на виртуалните машини в резервния център в ситуация на прекъсната връзка между двата центъра (основния център се предполага, че е с нарушена функционалност или липса на

функционалност). Непланирания failover не спира при поява на грешка по време на миграцията. Това позволява бързо възстановяване при наличие на аварийно събитие.

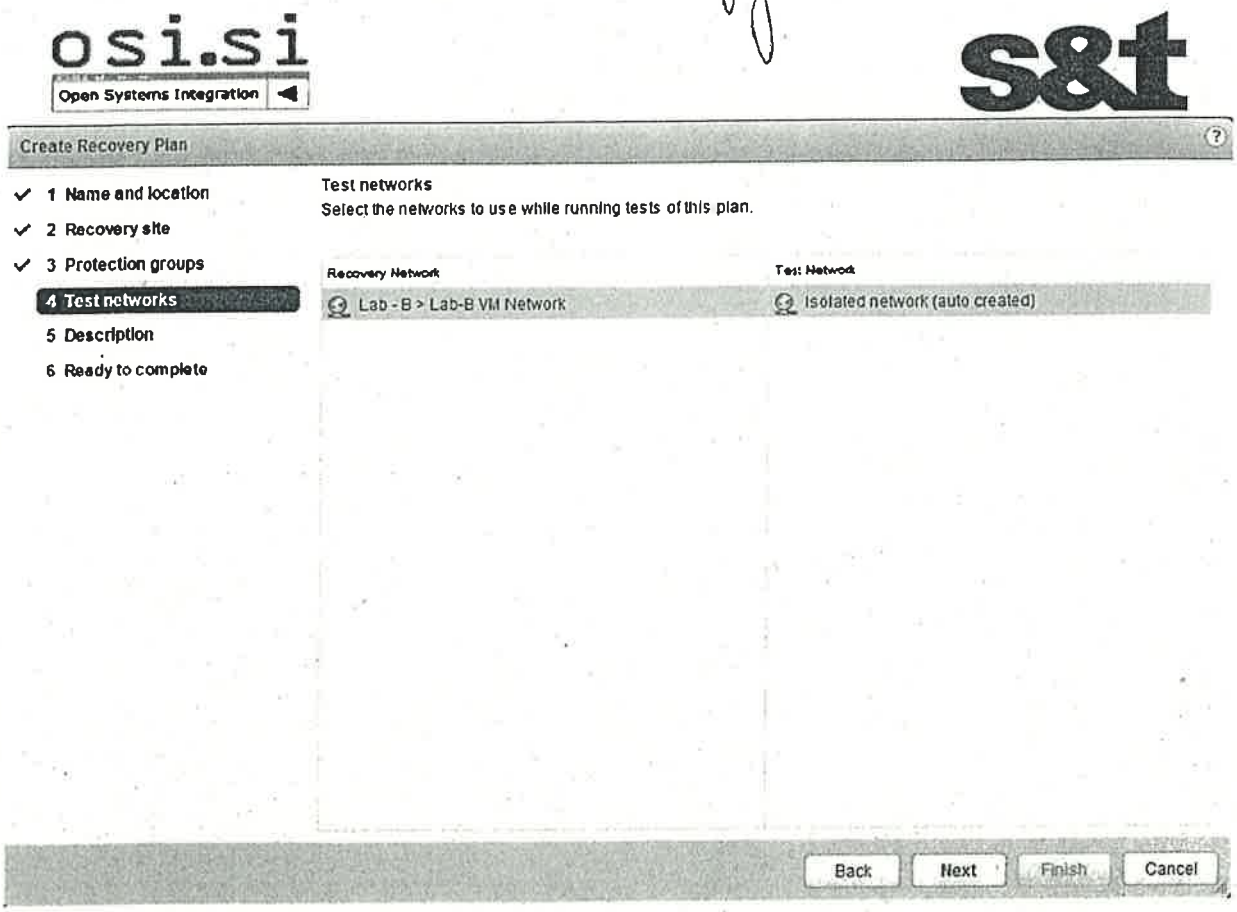
2. Създаване на план за аварийна ситуация - Recovery Plan
   - Всички действия се извършват от SRM
   - На защитения център се отваря vSphere Web Client и се извършва логване с administrator акаунт.
   - На левия панел, „**Home**“, „**Site Recovery**“.
   - Избиране на“ **Sites**“.
   - Избиране на „**Protected Site**“ и се предоставят administrator логон криденшъли за „**Recovery Site**“.
   - Избиране на „**Related Objects**“ , „**Recovery Plans**“.



   - Следва „**Create Recovery Plan**“ wizard, въвеждат се данните за плана
   - Извършва се избор на защитена група, която ще се използва за този план



- Избиране на тестова мрежа. Тази мрежа ще се използва по време на тестване на плана на резервния център



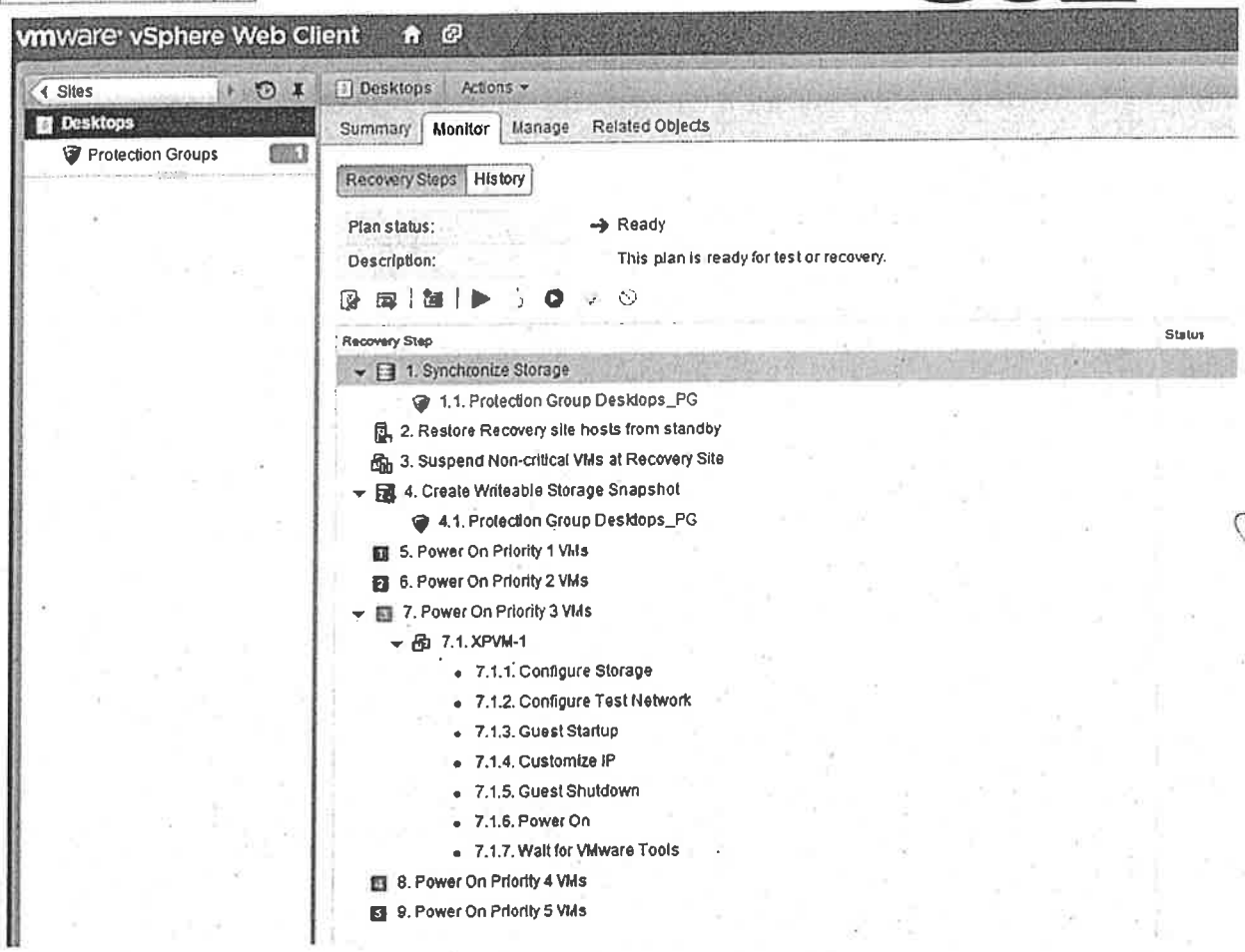
Преглеждане на настройките, следва бутон финиш „**Finish**“ за създаване на recovery plan.

На този етап плана вече е създаден.

3. Тестване на план за аварийни ситуации – Recovery Plan

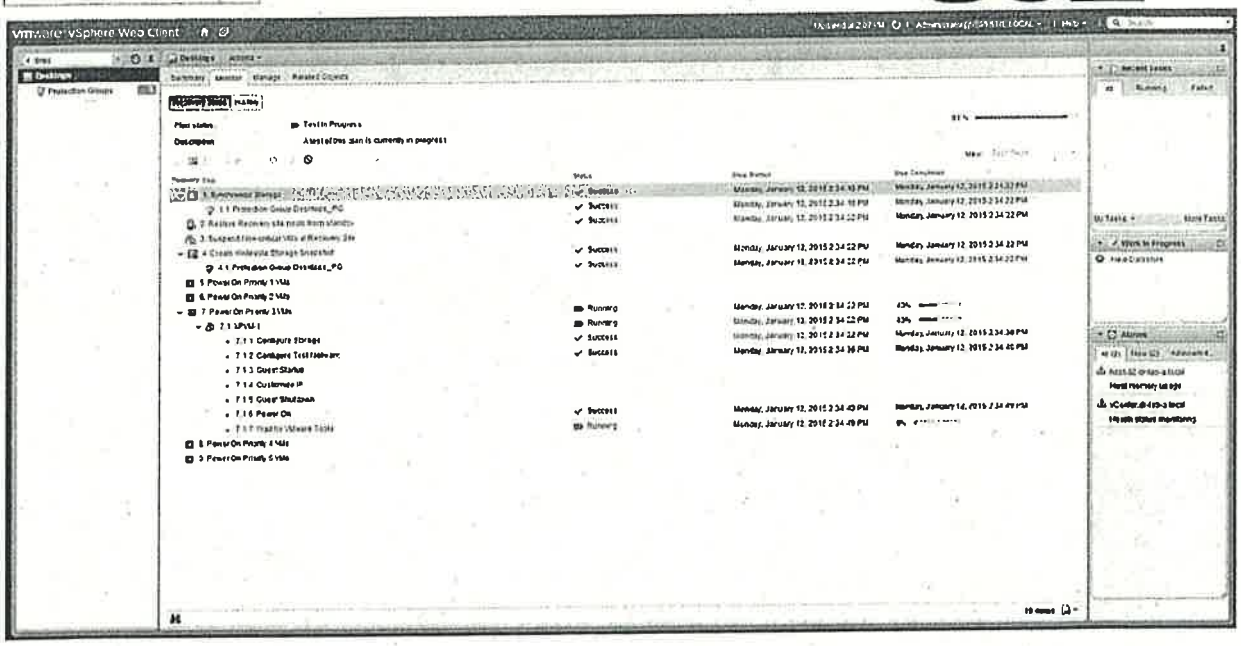
Финалната част от създаването на плана е неговото тестване.

- Така, както е отворен прозореца за стъпки по възстановяване, се кликва върху зеления бутон-стрелка за стартиране на теста на recovery plan.

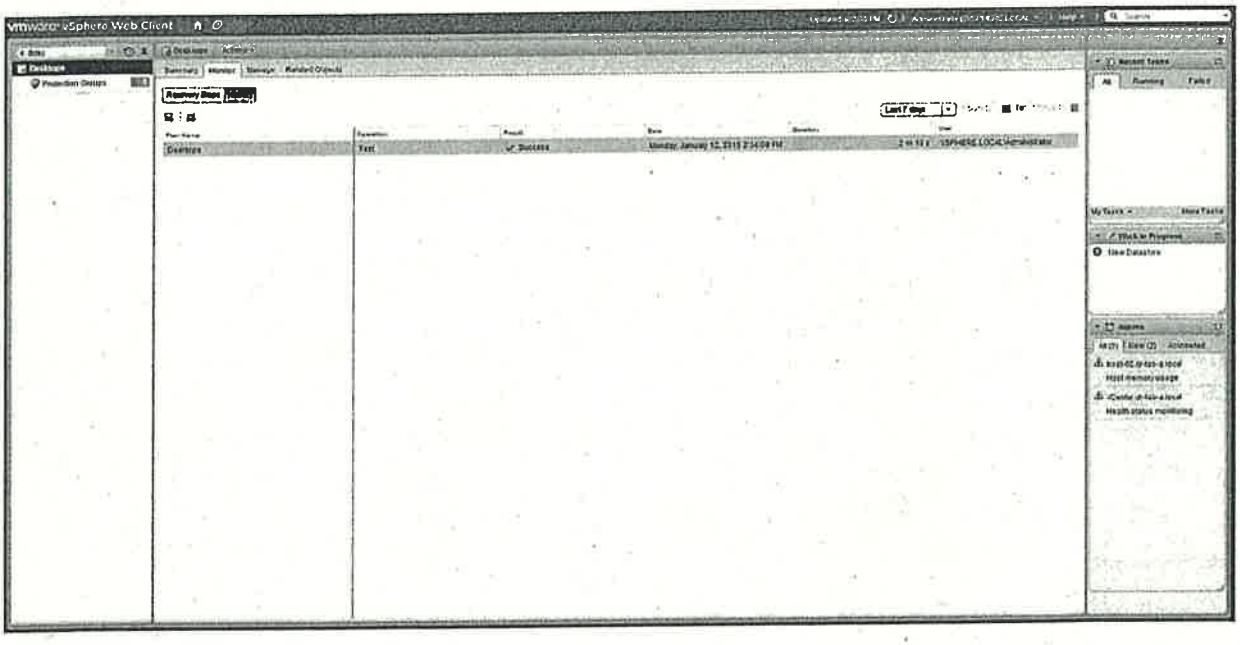


Потвърждаване чрез бутона „**Next**“.

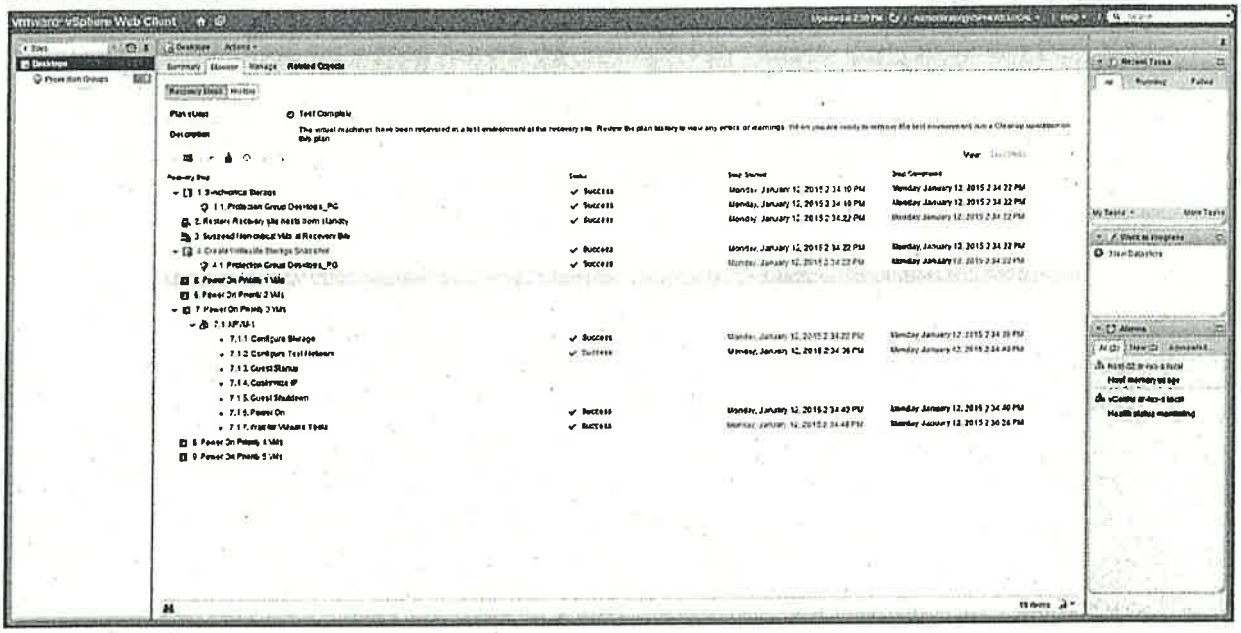
- Кликване на „**Finish**“ то за стартиране на тестовата процедура.
- Може да се наблюдава степента на завършване на процедурата по тестване



- Когато завърши процедурата, избира се „**History**“ бутон за да се визуализира резултата от теста и евентуално за наличието на грешки.



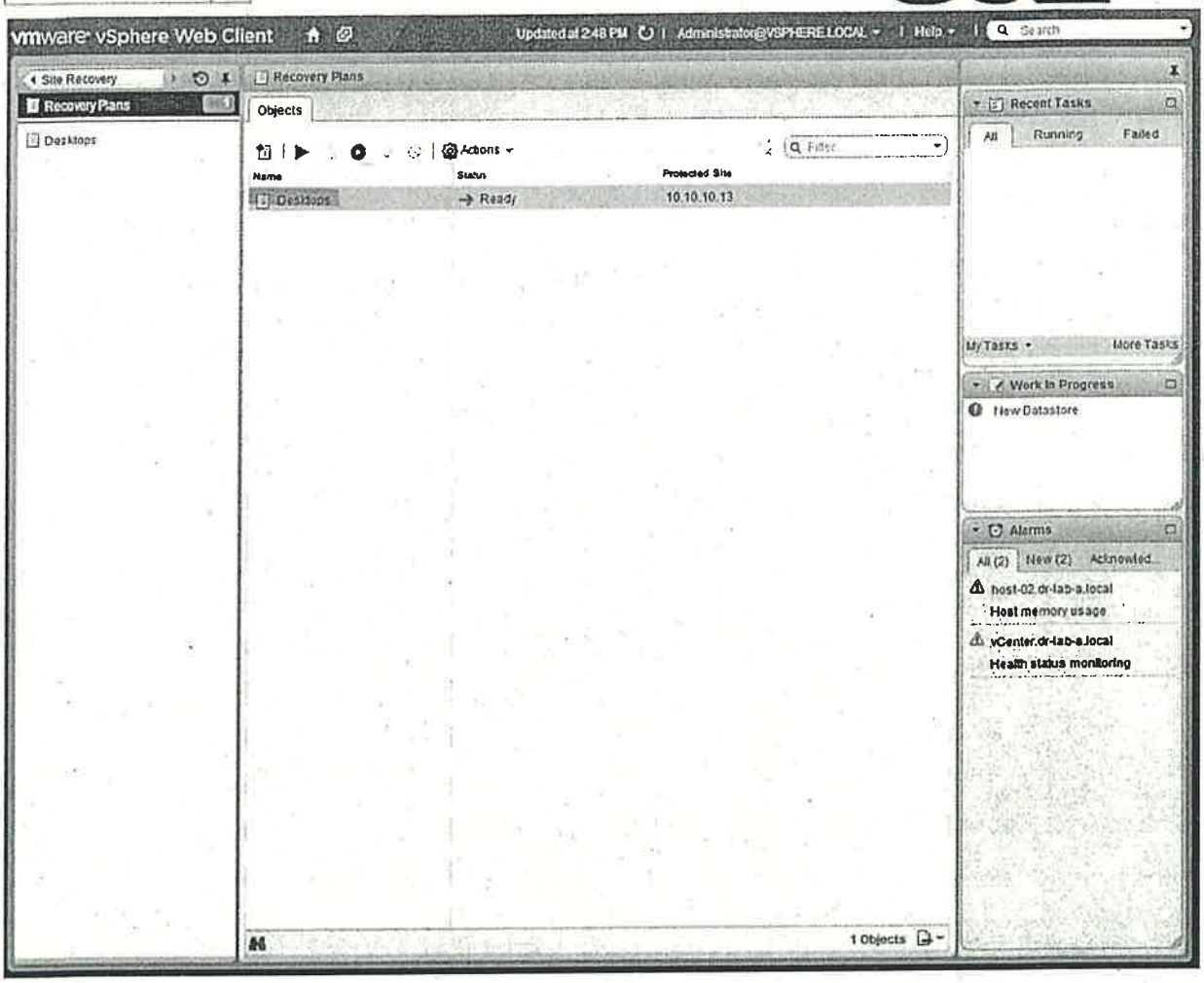
- След успешното завършване на тест процедурата се избира „**Cleanup Recovery Plan**“.



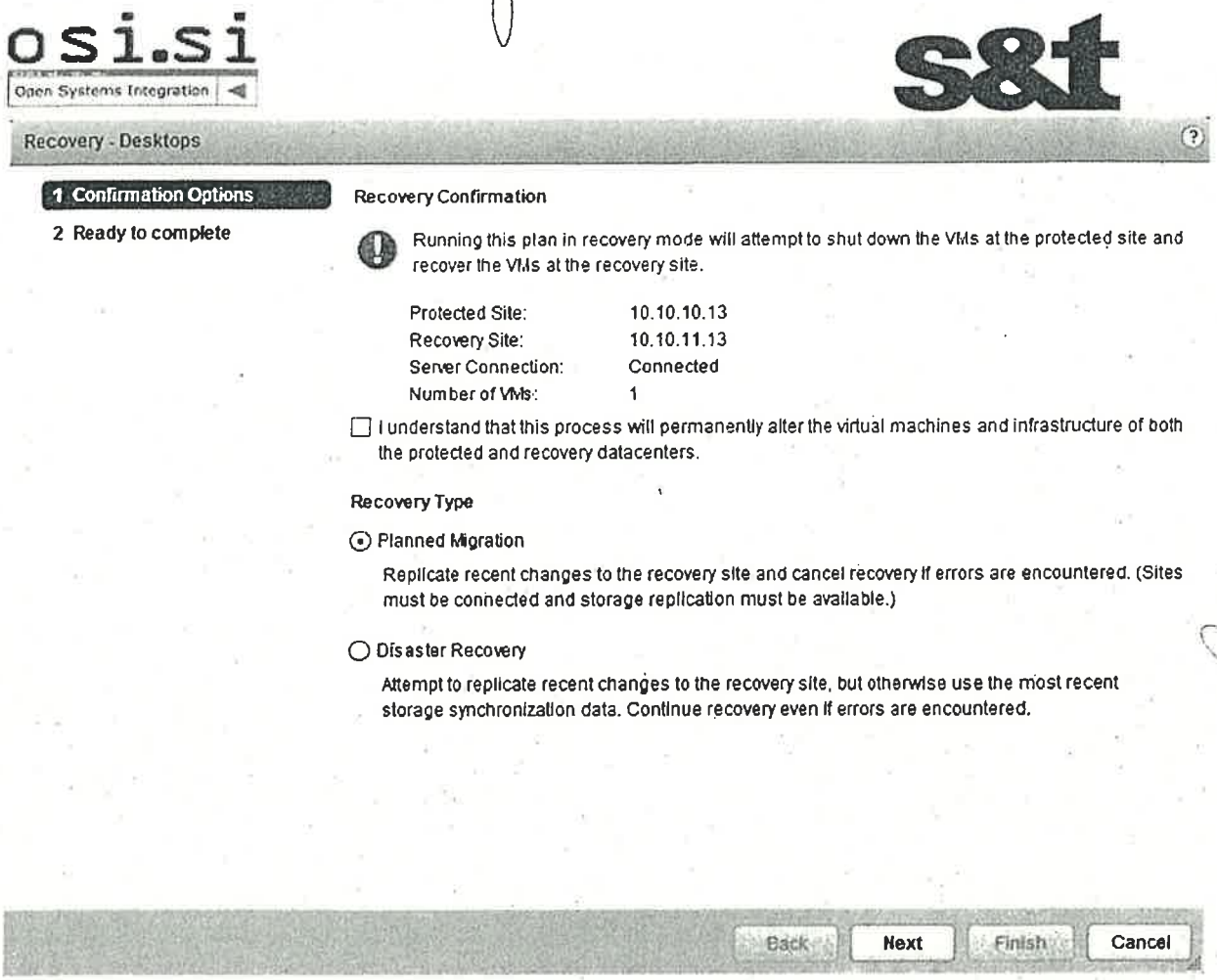
- Следва преглед на cleanup информацията и кликване на“ **Next“**.
- кликване „**Finish“** за стартиране cleanup процеса.
- С това приключва конфигурацията на плана в SRM

4. Планирана миграция – Planed Failover

- В основния център (**Protected Site)**, се отваря vSphere Web Client и се извършва логване с administrator акаунт.
- На левия панел, се избира „**Home“**, след това „**Site Recovery“**.
- Следва на „**Recovery Plans“** конфигуриране recovery plans.
- Избор на вашия recovery plan, кликване на „**Run recovery plan“.**



- В прозореца за потвърждение на процедурата по възстановяване се избира "I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters" check-box. Прави се проверка, че е избран" **Planned Migration**" като тип за възстановяване. Кликване на „**Next**" за продължаване.



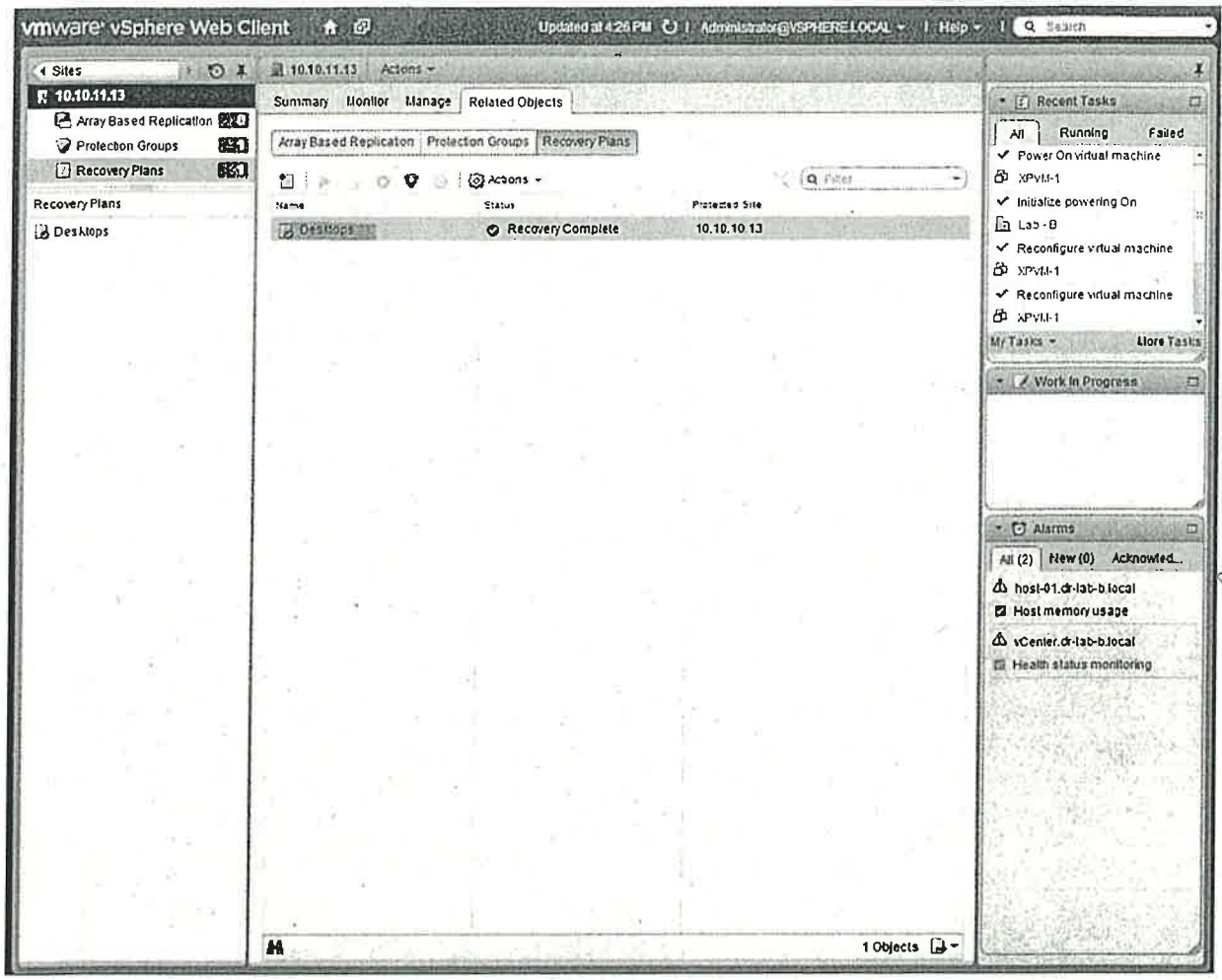
- Преглед на настройките, следва **„Finish“** за стартиране на процеса за планирана миграция.

В зависимост от броя на виртуалните машини, отнема известно време за финализиране на процеса по миграция. Когато процеса приключи, виртуалните машини трябва д бъдат стартирани на сървърите в резервния център.

5. Планирана миграция обратно в основния център – Planed Failback

За извършване на Планирана миграция обратно в основния център, трябва да се извърши процедурата **„Reprotect recovery plan“,** при която двата центъра си разменят ролите – основния става резервен, а резервния основен:

- Избира се съответния recovery plan, след което се кликва на **„Reprotect recovery plan“.**



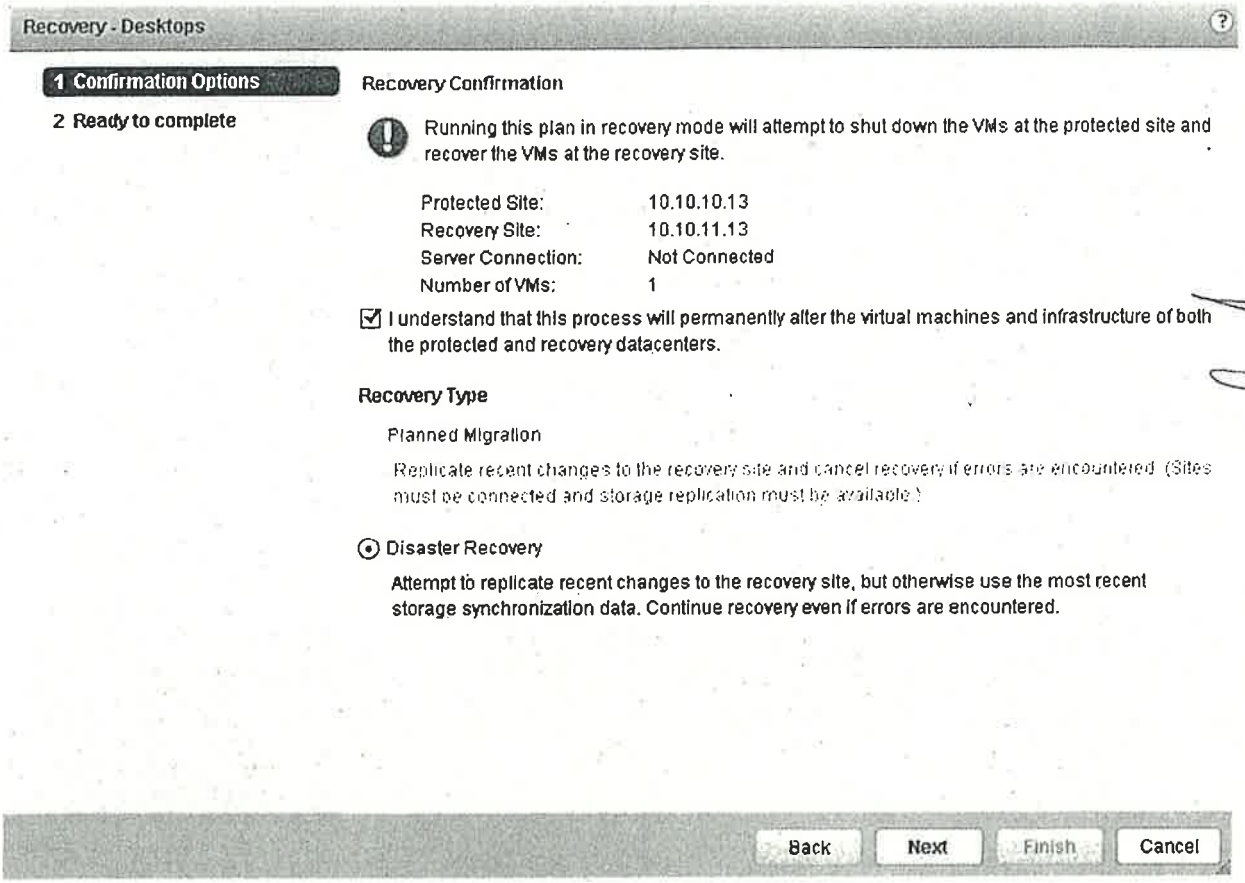
- Избира се "I understand that this operation cannot be undone" check-box и се кликва **„Next"**.
- Избира се **„Finish"** за стартиране reprotection процеса.
- След завършване на процеса reprotection, двата основни центъра са с разменени роли. За миграция на виртуалните машини в основния център се изпълнява процедурата от предишната точка – **„Планирана миграция"**, след което и двата центъра са отново с разменени роли, т.е в нормалното им състояние.

6. Непланирана миграция – Disaster Recovery

Този процедура е подобна на процедурата „Планирана Миграция", но в този случай Основния център не е наличен, отпаднал е.

- В **„Recovery Site"**, избира се **„Site Recovery"** , след това **„Recovery Plans"**.
- Избира се съответния recovery plan, след което се кликва червения бутон **„Run recovery plan"**.

- Следва да се отбележи че опцията Planned Migration не е налична поради отпадането на основния център. Следва избор на "I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters" checkbox и кликване на „**Next**".



- Преглед на настройките и кликване на „**Finish**" то за стартиране на процеса по възстановяване. След завършване на процеса по възстановяване, виртуалните машини трябва да бъдат стартирани на сървърите в резервния център

7. Миграция обратно в основния център след аварийна ситуация – Failback

След възстановяване функционалността на основния център и възстановяване на връзката между двата центъра, се изпълнява процедурата „**Планирана миграция обратно в основния център**"

ДОКУМЕНТАЦИЯ

В края на проекта консорциумът "C&T – ОСИ" ще предостави на клиента:
Техническа документация, която ще покрива инсталираната структура и спецификацията на доставеното решение. Техническата документация ще включва:

- Ръководства за монтаж и въвеждане в експлоатация, описващи структурата, компонентите и процедурите за защита/възстановяване, на процедурите за администриране на данни.

Документация свързана с PKI, която ще описва всички процеси и процедури свързани с PKI (заявка 12.3.6 в техническата документация)

- Процедура за генериране на двойка ключове и сертификати за DVCA на Служба Граничен контрол;
- Процедура за генериране на двойка ключове и сертификати за IS;
- Процедура за оторизиране на работните места на AIS на Служба Граничен контрол за достъп до пръстовите отпечатъци запаметени на електронен информационен носител за национални и чуждестранни документи за пътуване чрез EAC.
- Процедури за генериране на ключове на SM

Всички дейности и процеси ще съответстват на изискванията на българските CSCA и EAC CPS (Декларация за сертификационни практики) и ще бъдат документирани съгласно изискванията на раздел 8.3 от техническата документация.

Други документи отнасящи се до Entrust и Safenet, като ръководство за монтаж, ръководство за потребителя.

ОБУЧЕНИЕ И ПРЕДАВАНЕ НА ЗНАНИЯ

В края на проекта ще осигурим официално обучение на администраторите, потребителите и другите IT специалисти. Обучението ще обхване три категории служители

- Потребители – потребители на системата, които ще работят с PKI. Обучението ще бъде насочено към решението за внедряване на системата и процесите. Приблизителна продължителност на обучението – 5 дни.
- Администраторите на решението ще се фокусират върху администрирането на системата и нейната специфика (процедури за защита/възстановяване, поддръжка на системата)
- Програмист – предаване на знания на разработчици на приложения и представители на МВР.

Освен официалното обучение, в края на проекта ще се проведе предаване на знания на персонала на клиента по време на изпълнението на проекта.

РАЗРАБОТКИ СЪОБРАЗНО НУЖДИТЕ НА КЛИЕНТА

Съществена част от проекта ще бъдат разработките съобразени с потребностите на клиента, съгласно раздел 4.5. Ще се използват стандартни методологии за разработване на софтуерни продукти.

Разработки съобразени с потребностите на клиента – разработване на приложение за десктоп (извънмрежово) с поддръжка на 3M четящи устройства и дисплей на данни за ICAO LDS, интегриране с Entrust IS Client, осигуряване на функционалност за електронна проверка на MRTD документи (ICAO PA, EU EAC), разчитане на пръстови отпечатъци от чип.

ФАЗА 1 – РАЗРАБОТВАНЕ НА ИНФРАСТРУКТУРА

Фаза 1 съдържа следните задачи

- Прецизиране на разположението на устройствата в сървърния шкаф – ако са необходими промени спрямо описанието по-горе;
- Прецизиране на изискванията за захранваща мощност – ако са необходими промени спрямо описанието по-горе;
- Доставка на хардуерните устройства и системния софтуер;
- Физически монтаж на хардуерните устройва;
- Мрежови комутатори и мрежово окабеляване;
- Конфигуриране на VLAN
- Инсталиране на системната инфраструктура – конфигурация на хардуерните устройства, виртуална среда, операционни системи, инсталиране на виртуални сървъри\VM
- Определяне на онлайн политиката на SPOC\DVCA

ФАЗА 2 – ИЗГРАЖДАНЕ НА СИСТЕМАТА

Във втората фаза ще се изгради PKI системата с всички съответни компоненти. Първоначалното изграждане на CA (CVCA, DVCA, CSCA, ...) ще се извърши в производствена среда. Задачите в тази фаза са:

- Встъпителна среща
- Изграждане на LDAP
  - Инсталиране на Master
  - Създаване и обмен на LDAP база данни
- Инсталиране на мрежата
  - Подготовка и монтаж на конфигурацията за VLAN и конфигурацията за превключване
- Монтаж на CA
  - Монтаж на Entrust DVCA
  - Монтаж на Entrust SPOC CA
  - Интеграция между CSCA/CVSA и SPOC
  - Създаване на снапшоти и бекъпи
- Първоначално тестване на CA
  - Първоначално тестване на CSCA
  - Първоначално тестване на CVCA

- Първоначално тестване на DVCA
- Първоначално тестване на SPOC CA

- Document Signers
  - Издаване на сертификати за съществуващия Document Signer.
- PKI Административни услуги
  - Административни услуги за DVCA RA
- Master List Signer

- Издаване на сертификат за съществуващия Master List Signer

ФАЗА 3 - ИЗПИТАНИЯ

Една от най-важните и интензивни задачи. В тази фаза системата ще се тества съгласно проекта и спецификациите.

Изпитателна фаза

- Тестване на инфраструктурата – хардуерни устройства, системен софтуер – среда за виртуализация, операционни системи, бекъп среда.
- Интегриране и функционални изпитания на PKI
  - Изпитания за общо интегриране
  - Тестване на PKI системата (генериране на двойки ключове, издаване на сертификати)
  - Съхранение на сертификатите и CRL в NPKD;
  - Прехвърляне на сертификати и заявки за сертификати за и от SPOC;
  - Тестване на прехвърлянето на сертификати и CRL от и до ICAO-PKD;
  - Транспортиране на заявки за сертификати, получаване, актуализиране и съхранение на сертификати.

ФАЗА4 – ИНСТАЛАЦИЯ И МИГРАЦИЯ КЪМ ПРОИЗВОДСТВЕНА СИСТЕМА

Последната фаза за миграция към производството и приемателни изпитания. Предвиждат се следните задачи:

Движение и монтаж към производствената система

- Миграция на LDAP данни
- Инсталиране и инициализация на всички HSM
- Процедура за първичен ключ за нова CSCA
- Процедура за първичен ключ за нова CVCA
- Процедура за първичен ключ за нова DVCA
- Процедура за първичен ключ за SPOC CA
- Административни услуги за четящо и пишещо устройство за PKD
- Административни услуги за CVCA
- Административни услуги за DVCA
- Инсталиране на SPOC в работна среда
- Инсталиране на IS концентратори в работна среда
- Изграждане на клъстери в конфигурацията за всички PKI сървъри

Приемане

- Приемателни изпитания
- Приемане на одиторската проверка
- Окончателна документация на конфигурацията на системата.

РЕФЕРЕНЦИИ

OSI Slovenia разполага с голяма по обем референтна литература в областта на PKI:

- **Министерство на публичната администрация на Словения:**
  - Изграждане и поддържане на национална агенция сертифициране за правителството (SI-GOV CA) и гражданите (SI-GEN CA)
  - Изграждане и поддържане на Служба TimeStamping (CA)
  - Изграждане и поддържане на решение за национален контрол върху основния достъп до електронните паспорти (ePass BAC)
  - Изграждане на система от единни точки за контакт
- **Министерство на отбраната на Словения:**
  - Изграждане и поддържане на вътрешна PKI система (Entrust, nCipher HSM, смарткарти за идентифициране)
- **Министерство на вътрешните работи на Словения:**
  - Изграждане и поддържане на вътрешна PKI система (Entrust, смарткарти за идентифициране)
- **Cetis, Словения**
  - Изграждане на PKI система за национални карти за здравно осигуряване на базата на EJBCA
  - Изграждане и развитие на PKI система за тахографи.
- **Словенски пощи**
  - Изграждане и поддържане на CA за Словенските пощи (Entrust, Thales HSM, ...)
- **Agencija za komercijalnu djelatnost d.o.o., Хърватия**
  - Консултантски услуги с изграждане и въвеждане на PKI система за национални електронни лични карти.
  - Изграждане и развитие на PKI система за тахографи
- **Agencija za komercijalnu djelatnost d.o.o., Босна**
  - Изграждане и развитие на PKI система за тахографи
- **Министерство на съобщенията и информационните технологии (MCIT) на Афганистан**
  - Изграждане на PKI система за поддържане на национални електронни лични карти (e-ID)
  - Разработване и въвеждане на CMS система за персонализиране на електронни лични карти (все още не е в производство).

ЕКИП

Rudi Ponikvar, водещ архитект с основни компетенции в областта на PKI инфраструктурата. Работи с PKI инфраструктурата в продължение на повече от 20 години.

Tomaž Grenko, системен инженер с основни компетенции в областта на PKI инфраструктурата и HSM. Участие в много PKI проекти в Словения с над десет години опит в областта.

Ivan Bolčina, водещ разработчик на SW, с дългогодишен опит в поддържането и разработването на решения в областта на PKI инфраструктурата.

Jure Žvikart, разработчик на Java SW

Marko Šmid, консултант в областта на мрежовата инфраструктура с основни компетенции в областта на сигурността на мрежите

Miha Poberaj, консултант в областта на IT инфраструктурата и информационни технологии с основни компетенции в сферата на DB, интегриране на системи, сървъри за приложения.

Тошо Янков – ръководител отдел Внедряване и поддръжка

Владимир Димитров – сервизен инженер с компетенции в областта на база данни и виртуализация с опит над 15 години

Цветелин Симеонов – инженер с компетенции в областта на компютърни мрежи, информационна сигурност и защита на информацията, с опит повече от 10 години

Димитър Георгиев – сервизен инженер с компетенции в областта на дискови масиви и бекъп

Ангел Матов – сервизен инженер с компетенции в областта на хардуер – сървъри и сториджи

Ангел Генчев – сервизен инженер с компетенции в областта на дискови масиви и сървъри

Георги Попов – сервизен инженер с компетенции и областта на сървъри

Дата: 18.05.2015 г.

Подпис:

/ Злати Петров – Представляващ консорциума/

Приложение №2
Образец!

ДЕКЛАРАЦИЯ
ЗА
ЗАПОЗНАВАНЕ С УСЛОВИЯТА НА ПОРЪЧКАТА

Долуподписаният Злати Стойчев Петров,
в качеството ми на Представляващ (*посочва се длъжността и качеството, в което лицето има право да представлява и управлява - напр. изпълнителен директор, управител и др.*) на Обединение „С&Т-ОСИ",
ЕИК:....., със седалище и адрес на управление гр. София, България, п. код. 1528, бул. Искърско шосе №7, Търговски център „Европа", сграда 6, ет.3 – участник в открита процедура за възлагане на обществена поръчка с предмет:
„Разширение на системите за публичен частен ключ (PKI), изградени за обслужване на процеса на издаване на документи за самоличност с електронен носител, включително изграждане на единна точка за контакт (SPOC) и връзка с ICAO – PKD върху системата за граничен контрол"

ДЕКЛАРИРАМ, ЧЕ:

приемам и предлагам срок за изпълнение на поръчката 300 дни , включително съгласно раздел III.1.4.) от обявлението:

1. Изпълнението на поръчката се извършва на две фази:

1.1.Фаза 1. Дейности, осигуряващи изискванията по т. 3.4 и функционалностите по т. 4.1, т. 4.2 и т. 4.3 от Приложение 1 – Техническа спецификация.

Етап 1. Изготвяне на проект на техническо решение, отговарящо на изискванията по т. 3.4, т. 4.1, т. 4.2 и т. 4.3 от Приложение 1 – Техническа спецификация - до **30 календарни дни** след подписване на договора.

Етап 2. Доставка на необходимите технически и програмни средства и реализиране на включеното във Фаза 1 на разширението в тестова среда – до **90 календарни дни** след приемане на етап 1.

Етап 3. Внедряване на включеното във фаза 1 на разширението и обучение – до **30 календарни дни** след приемане на етап 2.

1.2.Фаза 2. Дейности, осигуряващи изискванията по т. 3.5 и функционалностите по т. 4.4 и т. 4.5 от Приложение 1 – Техническа спецификация.

Етап 1. Изготвяне на проект на техническо решение, отговарящо на изискванията по т. 3.5, т. 4.4 и т. 4.5 от Приложение 1 – Техническа спецификация – до **30 календарни дни** след приемане на Етап 3 от Фаза 1.

Етап 2. Доставка на необходимите технически и програмни средства и реализиране на включеното във фаза 2 на проекта в тестова среда – до **60 календарни дни** след приемане на етап 1.

Етап 3. Внедряване на включеното в Етап 1 и Етап 2 на Фаза 2, обучение и цялостно внедряване на проекта – до **60 календарни дни** след приемане на етап 2.

2. Гаранционен срок - стандартен фирмен гаранционен срок за доставените изделия - 36 месеца.

3. Гаранционно обслужване - **24 часа, 7 дни** в седмицата, като:

3.1. Време за реакция - максимално - до **4 часа** от момента, в който потребителят е заявил наличие на технически проблем;

3.2. Време за отстраняване на проблема- до **24 часа**.

4. Обучение ще извършим по предварително съгласувани и утвърдени теми и график.

5. Когато Изпълнителят е сключил договор / договори/ за под изпълнение, Възложителят извършва окончателно плащане към него, след като бъдат представени доказателства, че Изпълнителят е заплатил на подизпълнителя / подизпълнителите за изпълнените от тях работи – **неприложимо**.

18.05.2015 г.
дата (дд/мм/гггг)

Декларатор: .....

гр./с./ София
/подпис и печат/

/ Златин Петров – Представляващ консорциума/

Приложение №2
Образец!

ДЕКЛАРАЦИЯ
По т.13 и т.14 от Техническата спецификация

Долуподписаният Злати Стойчев Петров,
в качеството ми на Представляващ (*посочва се длъжността и качеството, в което лицето има право да представлява и управлява - напр. изпълнителен директор, управител и др.*) на Обединение „С&Т-ОСИ",
ЕИК:....., със седалище и адрес на управление гр. София, България, п. код. 1528, бул. Искърско шосе №7, Търговски център „Европа", сграда 6, ет.3 – участник в открита процедура за възлагане на обществена поръчка с предмет:
„*Разширение на системите за публичен частен ключ (PKI), изградени за обслужване на процеса на издаване на документи за самоличност с електронен носител, включително изграждане на единна точка за контакт (SPOC) и връзка с ICAO – PKD върху системата за граничен контрол*"

ДЕКЛАРИРАМ, ЧЕ:

Ако спечелим поръчката при изпълнението на проекта ще бъдат изпълнени следните изисквания"

13.1. Инсталация/монтаж и пускане в експлоатация

13.1.1. Консорциумът С&Т-ОСИ ще извърши цялостната инсталация и пускане в експлоатация на доставеното оборудване;

13.1.2.Ще осигурим успешното взаимно функциониране на всички инсталирани продукти;

13.1.3. Настройките на оборудването като IP адресация, протоколи, VLAN, услуги и др. и цялостното интегриране в комуникационно-информационната среда на МВР ще бъдат извършени от нас съвместно със специалисти на Възложителя;

13.1.4. Представители на възложителя и на Консорциума ще проведат съвместни предварителни и приемателни тестове на реализираното техническо решение;

13.1.5. Тестовата среда ще отговаря на експлоатационната.

13.2. Оборудване:

13.2.1. Цялото оборудване ще е ново, неизползвано преди това и ще е е в производствената листа на производителя за 2014 година;

13.2.2. Цялото оборудване ще работи в диапазон на напрежението от 187 V (220 V - 15%) до 242 V (220 V + 10%), при 50Hz +/ - 0.5 Hz.

13.2.3. Всички технически и програмни средства ще бъдат изцяло съвместими с наличните, описани в Приложение 1 – „Техническа спецификация".

13.2.4. Всички изделия ще са окомплектовани с всички необходими аксесоари, осигуряващи работата им и свързването им към други системи, като например: токозахранващи кабели, входни устройства, захранващи адаптери, токозахранващи удължители, кабели за вътрешно и междинно свързване, адаптери, монтажни китове и т.н.

13.2.5. За всяка единица доставен артикул Консорциумът гарантира, че същата е напълно съвместима със спецификациите на другите артикули, включени в Приложение 1 – „ Техническа спецификация";

13.3. Гаранционен сервиз

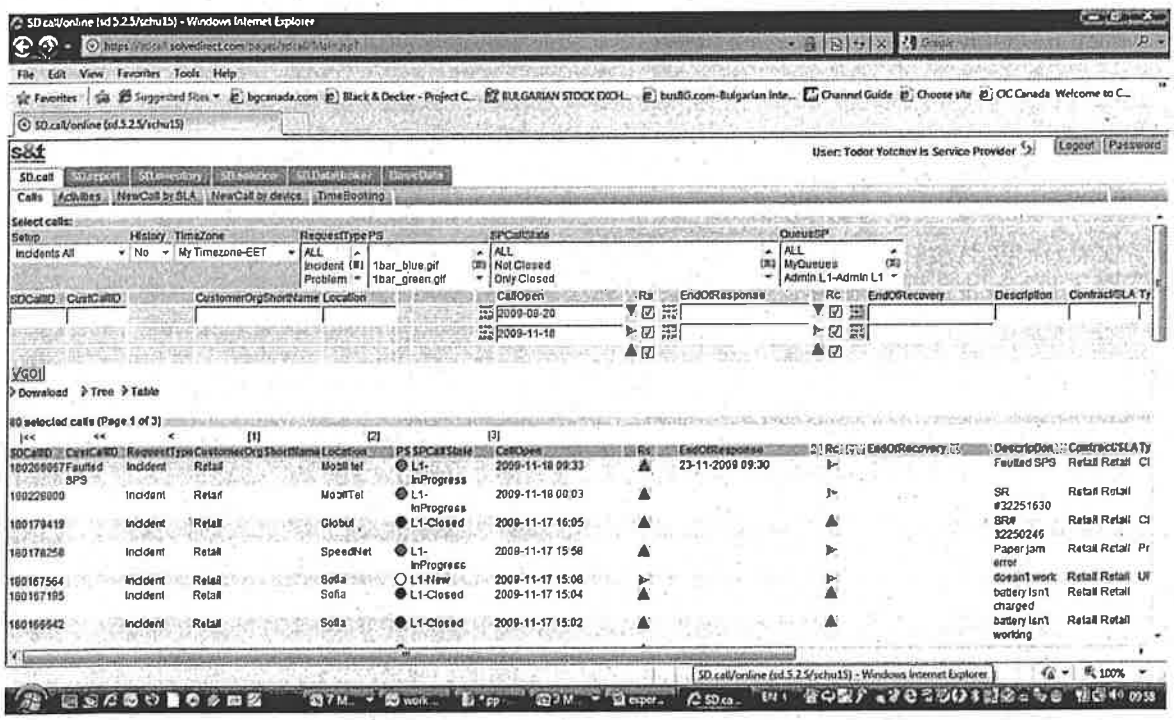
13.3.1. Гаранционният срок ще бъде стандартен фирмен гаранционен срок за предлаганите изделия от 36 месеца. За начало на гаранционния срок на техниката се счита датата, която е посочена в Приемателно-предавателния протокол.

При доставка се проверяват комплектността и работоспособността на оборудването. Подписва се приемателно-предавателен протокол и се издава гаранционна карта за всяка единица комплектно изделие. В гаранционната карта се описват серийните номера както на комплектното изделие, така и отделните компоненти, вложени в него.

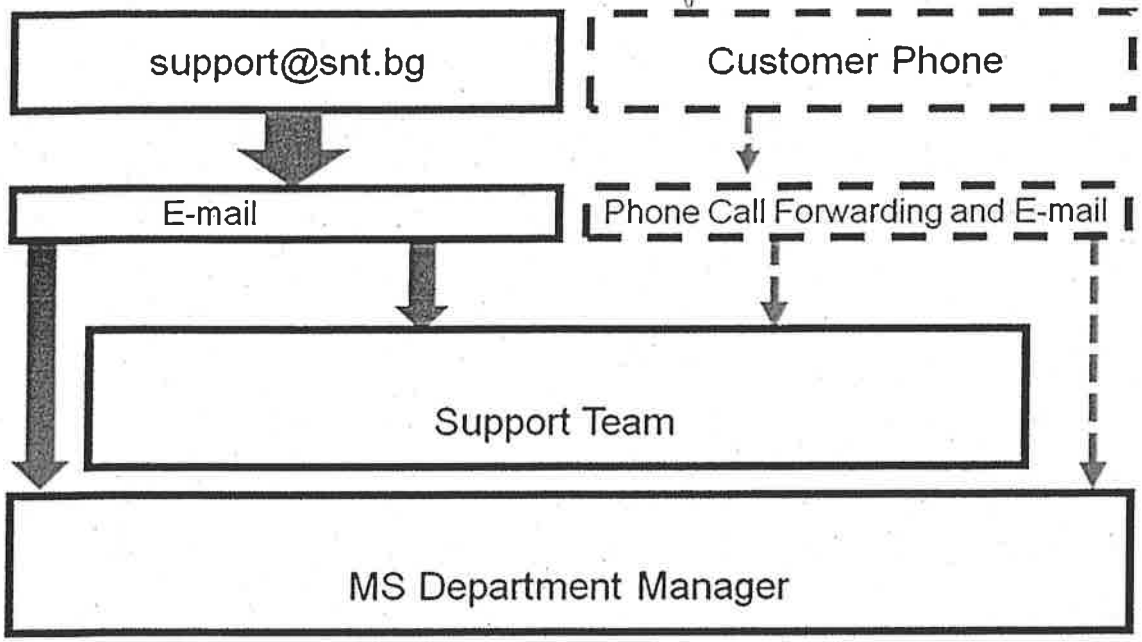
13.3.2. Гаранционното обслужване на техническото решение ще бъде 24 часа, 7 дни в седмицата.

Консорциумът ще бъде отговорен за предоставяне на гаранционно обслужванс. За всички технически проблеми ще има разкрито помощно бюро (хелп деск) за техническа поддръжка. Достъпът до Помощното бюро е осигурен чрез телефонен номер, факс и e-mail в България, които няма да поставят потребителите пред необходимост да заплащат разговори по международни тарифи или по такива за разговори на големи разстояния.

13.3.2.1.Автоматизираната „Help desk" система за сервизни договори за незабавно уведомяване на дежурните сервизни инженери за възникнали дефекти на обслужваните системи е изградена на базата на продуктите Solve Direct Solutions https://sdcall.solvedirect.com. В системата on-line се документират стриктно и се проследяват заявките на клиентите и свързаните с тях сервизни дейности. Всички ремонти се регистрират в детайли, като се пази информация за повредата, серийния номер на устройството, дата и час на регистриране на проблем, описание на извършената сервизна дейност и резултатът от нея, изразходваното време, продуктовият номер на подменената част и т.н.



Изготвят се ежемесечни отчети за, необходимите часове за поправка, средно време за отговор при даване на заявка, средно време за сервизна дейност, продуктова ефективност и т.н.
На база на вградените възможности HELPDESK системата е изградена също „Автоматизирана известяваща система за сервизни договори със специално ниво на обслужване" за незабавно уведомяване (чрез е-майл и SMS) на дежурните сервизни инженери за възникнали проблеми на обслужваните системи.



Примерен формуляр за регистриране на проблем.

	• **Customer Service Order** • **Creation Report**	**S&T Bulgaria EOOD** ***7 Iskarsko shosse blvd, 1528 Sofia Europa Park, Building 6, 3d floor phone +359 2 96517 90 fax +359 2 97516 00***

Date received:	
Customer : **Full address of installation:**	Warranty and after Warranty repairs
Local customer site contact name:	Vasil Arabadjiiski
Local customer site phone number:	00359878398503
Local customer email address:	vasil.arabadzhiyski@btc.bg
Customer call reference (Ticket #)	Faulted disk drive
Local System handle:	180692282
Model number:	DMX2000
Serial number:	CK287751207
Problem description:	

Faulted disk drive	
Call Receipt handler:	Dimitar Georgiev
Call Receipt handler e-mail address:	support@snt.bg
Support level:	Warranty and after Warranty repairs

13.3.2.2. Понастоящем „C&T България" разполага с 3 централни сервизни офиси в София, Пловдив, и Варна и локални партньорски офиси, което дава възможност максималното разстояние между сервизния офис и крайния клиент да не бъде по-голямо от 50 км.

Списък на основните сервизни центрова на C&T България ЕООД

Основен диспечерски сервизен център:
София 1528
Бул. "Искърско шосе " 7, Бизнес парк Европа, сграда 6, ет.3
тел.: 965 17 84, 965 17 10
факс: 975 16 00
e-mail: snt@snt.bg
http://www.snt.bg

Активно работно време на сервиза: от 9:00 до 18:00 часа за дните от понеделник до петък

Лица за контакт:

1. Тошо Янков – Директор на сервиза - за връзка и препращане на повикванията към сервизните центрове в страната;

2. **Пловдив 4000**
   Ангел Матов
   0888958452

3. **Варна**
   Явор Иванов
   0888723834

13.3.2.3.Списък на персонала, който ще оказва нужното съдействие и помощ;

Rudi Ponikvar, водещ архитект с основни компетенции в областта на PKI инфраструктурата. Работи с PKI инфраструктурата в продължение на повече от 20 години.

Tomaž Grenko, системен инженер с основни компетенции в областта на PKI инфраструктурата и HSM. Участие в много PKI проекти в Словения с над десет години опит в областта.

Ivan Bolčina, водещ разработчик на SW, с дългогодишен опит в поддържането и разработването на решения в областта на PKI инфраструктурата.

Jure Žvikart, разработчик на Java SW

Marko Šmid, консултант в областта на мрежовата инфраструктура с основни компетенции в областта на сигурността на мрежите

Miha Poberaj, консултант в областта на IT инфраструктурата и информационни технологии с основни компетенции в сферата на DB, интегриране на системи, сървъри за приложения.

Тошо Янков – ръководител отдел "Внедряване и поддръжка"

Владимир Димитров – сервизен инженер с компетенции в областта на база данни и виртуализация с опит над 15 години

Цветелин Симеонов – инженер с компетенции в областта на компютърни мрежи, информационна сигурност и защита на информацията, с опит повече от 10 години

Димитър Георгиев – сервизен инженер с компетенции в областта на дискови масиви и бекъп

Ангел Матов – сервизен инженер с компетенции в областта на хардуер – сървъри и сториджи

Ангел Генчев – сервизен инженер с компетенции в областта на дискови масиви и сървъри

Георги Попов – сервизен инженер с компетенции и областта на сървъри

– За срока на договора ще бъдат осигурени:

• Достъп до сайта на производителя с възможност за изтегляне на обновления за програмните продукти;

• Достъп до сайта на производителя с възможност за изтегляне на нови версии за програмните продукти;

• Възможност за регистриране на проблеми и консултации денонощно директно към производителя - по телефон и електронна поща;

• Консултации и системна помощ на място за програмните продукти;

13.3.3. Максималното време за реакция е до 4 часа от момента, в който потребителят е заявил наличие на проблем. Изпълнителят изпраща квалифициран персонал на място.

13.3.4. Когато отстраняването на проблема или ремонтът изисква повече от 24 часа, Консорциумът С&Т-ОСИ по договор ще предостави еквивалентно устройство за временна замяна. В този случай, гаранционният срок на взетото за ремонт устройство се удължава с времето за отстраняване на повредата;

– При подмяна на носител на информация не ще се допуска неговото изнасяне от МВР;

– Гаранционно обслужване на софтуера ще включва актуализиране/надстройване на софтуера в отговор на каквито и да са установени несъответствия във функционирането на системното и приложното програмно осигуряване, както и при промени в европейски стандарт CSN 36 9791, Решения на Европейската комисия **С(2008) 8657 от 22.12.2008, С(2009) 7476 от 5.10.2009, С(2002) 3069 , С(2009) 3770 от 20.5.2009, С(2011) 5478 от 4.8.2011.**

13.4. Обща информация за възможностите и услугите на сервизния център на "С&Т България" ЕООД.

Обслужване на клиенти

С&Т България ЕООД разполага с скип от висококвалифицирани сервизни инженери, оборудвани с най-съвременна измервателна и сервизна апаратура.

Добре поддържаната складова наличност на резервни части и специалната "гореща" връзка са гаранция за бързо доставяне на нужните за ремонта части. Всички представителства на C&T са способни да предложат богата гама от услуги, договори и условия на предложени от клиентите проблеми за решаване.

Краткото време за реакция, от 0-24 часа и опцията за удължаване на гаранцията са ключови услуги, които предлагаме на нашите клиенти от телекомуникациите, банковия сектор, държавния сектор, здравеопазването, транспорта и промишлеността.

13.4.1. C&T България ЕООД – Сервизен център на Hitachi Data Systems, Fujitsu, CISCO, Oracle SUN и EMC за България

C&T България ЕООД предлага гаранционна и извънгаранционна хардуерна и софтуерна поддръжка за всички продукти, производство на HDS, Fujitsu, CISCO, Oracle SUN и EMC за страната, в съответствие със стандартите на HDS, CISCO, EMC, Oracle SUN и Fujitsu. Фирмата е оторизиран сервизен център от началото на 1994 година и понастоящем разполага централни сервизни офиси в София, Пловдив и Варна и локални партньорски офиси, което дава възможност максималното разстояние между сервизния офис и крайния клиент да не бъде по-голямо от 50 км.

C&T България предлага пълна хардуерна и софтуерна поддръжка, включваща следните дейности:

- Възможност за извършване на инсталация и обучение на клиента, което значително води до намаляване вероятността от повреда;
- Възможност за извършване профилактика, съобразена със спецификата на продукта и изискванията за неговата надеждност;
- Предоставяне на оборотна техника, в случай че ремонтът отнема повече време;
- Съхраняване на потребителската информация в случай че се налага подмяна на твърдия диск на персоналния компютър.
- Консултации на място и по телефона за хардуерни и системни софтуерни проблеми;
- Безплатен труд и части (включени в гаранцията и сервизните договори);
- Посещение на място в рамките на един работен ден;
- Възможност за 4 часа време за реакция и 24 часа за приключване на ремонт за цялата страна;
- Възможност за извършване непрекъсната поддръжка (24x7);
- Възможност за извършване дистанционна диагностика на софтуерни и хардуерни дефекти, която свежда времето за реакция до минимум;
- Възможност за извършване хардуерно надграждане (hardware upgrade) и софтуерна актуализация на системния и приложен софтуер на (SW Updates);
- Предлагане на допълнителна гаранция за хардуер и софтуер;
- Предлагане на различни видове договори за сервиз, с цел задоволяване на специфичните нужди на клиента за поддръжка, профилактика и актуализиране на системите.

За изпълнение на тези функции „C& T България" ЕООД разполага с:

- Висококвалифицирани сервизни специалисти, обучавани в учебните центрове на

партньорите и оборудвани със сервизни коли, инструменти и комуникационни средства.

- Сервизните ни инженери имат сертификати за цялата гама комуникационни устройства на Cisco Systems. Специализацията в UNIX и Windows базираните системи, в персоналните компютри и периферия на сервизните инженери, добрата квалификация и богатият опит, им позволяват да са взаимозаменяеми. Специалистите постоянно преминават различни обучения върху новите продукти в съответствие с учебните програми.
- Добре поддържана складова база за резервни части.

- Извършва се всекидневна актуализация и анализ на складовата наличност. Ефективна стокова наличност се поддържа, чрез изготвяне на поръчки, въз основа на количеството повредени части, гаранционни и договорни нужди и необходими части за сервизни нужди.
- Изградена система за стриктно документиране и проследяване на заявките на клиентите, ремонтите и движението на складовите наличности. Всички ремонти се регистрират в детайли в присъствието на клиента, като се описва видът на повредата, серийният номер, датата на приемане и датата на започване на работата, гаранционна карта, описание на извършената сервизна дейност и резултатът от нея, изразходваното време, продуктовият номер на подменената част и кодът на повредата, номерът на поръчката, ако частта е поръчвана и т.н.
- Изготвят се ежемесечни отчети, базирани на гореспоменатите документи, чрез анализиране на съответните продукти, необходимите часове за поправка, средно време за отговор при даване на заявка, средно време за сервизна дейност, време за доставка на поръчаните части, продуктова ефективност и печалба.

14. Доставката ще бъде съпроводена с:

14.1. Декларация/сертификат за произход за всяко изделие;

14.2. Декларация, в която ще бъде посочено, че в случай на отказ или дефект на оборудването и програмните средства за същите е осигурена поддръжка в границите на територията на Република България;

18.05.2015 г.
дата (дд/мм/гггг)

гр./с./ София

Декларатор:.....
/подпис и печат/

Приложение №14
Образец!

ЦЕНОВА ОФЕРТА

От: Консорциум „С&Т-ОСИ"
/наименование на участника/

Във връзка с обявена открита процедура за възлагане на обществена поръчка, с предмет: *„Разширение на системите за публичен частен ключ (PKI), изградени за обслужване на процеса на издаване на документи за самоличност с електронен носител, включително изграждане на единна точка за контакт (SPOC) и връзка с ICAO – PKD върху системата за граничен контрол"*, Ви представяме нашата ценова оферта:

Изделие	К-во (брой)	Ед. цена в лева без ДДС	Ед. цена в лева с вкл. ДДС	Обща цена в лева без ДДС	Обща цена в лева с вкл. ДДС
1. HSM	9	62 171,00	74 605,20	559 539,00	671 446,80
2. Сървъри	6	11 016,00	13 219,20	66 096,00	79 315,20
3. LAN комутатори	3	6 405,00	7 686,00	19 215,00	23 058,00
4. SAN комутатори	3	17 707,00	21 248,40	53 121,00	63 745,20
5. Дисков масив	2	64 603,00	77 523,60	129 206,00	155 047,20
6.Диск-базирано архивиращо устройство	2	37 742,00	45 290,40	75 484,00	90 580,80
Общо цена за доставка на техническите средства от т.1 до т.6 включително в лева без и с ДДС				**902 661,00**	**1 083 193,20**
Софтуер и лицензи, разработка	1	1 594 456,00	1 913 347,20	1 594 456,00	1 913 347,20
Общо цена за софтуер, лицензи и разработка в лева без и с ДДС				**1 594 456,00**	**1 913 347,20**
В посочените цени са включени и всички разходи по гаранционното обслужване за срок от 36 месеца.					

ОБЩА ЦЕНА ЗА ПРЕДМЕТА НА ПОРЪЧКАТА **2 497 117.00** /словом: **Два милиона четиристотин деветдесет и седем хиляди сто и седемнадесет** / в лева без ДДС

ОБЩА ЦЕНА ЗА ПРЕДМЕТА НА ПОРЪЧКАТА **2 996 540,40**./словом: **Два милиона деветстоти деветдесет и шест хилади петстотин и четиридесет и 0,40**./ в лева с ДДС

Посочените цени са определени при пълно съответствие с условията на образуването им, посочени в документацията за участие в процедурата.

ДЕКЛАРИРАМ, ЧЕ:

1. Гаранцията обхваща всички разходи, свързани с пътуване, пощенски услуги, комуникации и замяна на повредените компоненти без допълнително заплащане;

2. Разходите за доставка на технически и програмни средства, разопаковане, монтаж, инсталация, конфигуриране, тестване, внедряване, обучение, актуализиране на софтуера и гаранционно обслужване са за сметка на изпълнителя.

Дата: 18.05.2015 г. ПОДПИС и ПЕЧАТ: .....

Златн Петров

Представляващ консорциума

/длъжност на представляващия участника/

Забележка: **Ако участникът не е данъчно регистрирано по ЗДДС лице, той отбелязва това обстоятелство в забележка към офертата.**