33-00-133/03.04.2024

Приложение 2а

ЗАЯВКА по Договор № 40-00-138 от 13.12.2022 г.	☑
ЗАЯВКА по Договор № 40-00-138 от 13.12.2022 г. **(актуализирана)**	☐ [1]

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*14*
Описание на дейност/проект съгласно ПГ:	*Изграждане на „Система за генериране на видими цифрови печати (vds) за документи за виза чрез системата за издаване на визи“*	
CPV код	*72262000-9*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ* *(При изпълнение на дейностите не се предвижда достъп до класифицирана информация, включително и класифицирана информация на Европейския съюз)*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**		*1 600 000 лв.*
Срок за плащане: *(еднократно, на части, периодично или др.)*		*Еднократно след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка и фактура*
Плащане с акредитив / Авансово плащане (условия) ДА/НЕ		*НЕ*
Документи за плащане с акредитив		*НЕ Е ПРИЛОЖИМО*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**		*До 9 месеца от подписване на заявката*
Гаранционен срок:		
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*		*Еднократно с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка*
Приложения: (*напр: технически параметри,образци на отчетни документи*)		*Техническа спецификация*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		
Ръководител на проект/дейност по заявката (напр: представител на дирекцията – Заявител):		

[1] Отбелязва се в случай че заявката е актуализирана

ЗАЯВКАТА е ОДОБРЕНА ОТ:	
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:	

Съгласувано с:

, директор на дирекция „Бюджет и финанси“

, главен счетоводител

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

ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	
Ръководител на проект/дейност по заявката	
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	

Приложение № 1 към чл. 38, ал. 3

[*Възложител*]

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

за

ИЗГРАЖДАНЕ НА „СИСТЕМА ЗА ГЕНЕРИРАНЕ НА ВИДИМИ ЦИФРОВИ ПЕЧАТИ (VDS) ЗА ДОКУМЕНТИ ЗА ВИЗА ЧРЕЗ СИСТЕМАТА ЗА ИЗДАВАНЕ НА ВИЗИ“

СЪДЪРЖАНИЕ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

1.1. Използвани акроними

Акроним	Описание
АИС	Автоматизирана информационна система
АМС	Администрация на Министерския съвет
АОП	Агенция по обществени поръчки
АПК	Административнопроцесуален кодекс
БУЛСТАТ	Регистър Булстат
МЕУ	Министерство на електронното управление
ЗДОИ	Закон за достъп до обществена информация
ЗЕДЕП	Закон за електронния документ и електронния подпис
ЗЕУ	Закон за електронното управление
ИТ	Информационни технологии
КАО	Комплексно административно обслужване
ТР	Търговски регистър
ДХЧО	Държавен хибриден частен облак
ЦАИС	Централизирана автоматизирана информационна система
SDK	Software development kit
API	Application programming interface/Приложно програмен интерфейс
PKI	Инфраструктура с публични ключове за обслужване на процеса на издаване на БЛД с ЕНИ и проверката им, включваща PKI (PKI за PA) за гарантиране целостта и автентичността на цифровите данни, съхранявани в ЕНИ и PKI (PKI за EAC) за предоставяне на достъп на оторизирани системи за проверка до цифровите данни, съхранявани в ЕНИ
БЛД	Български лични документи
ЕНИ	Електронен носител на информация в БЛД

BSI	Германската федерална служба за информационна сигурност
CA	Certificate Authorities. 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
CSCA	Country Signing Certification Authority. Сертифициращ орган, удостоверяващ цифров подпис на държавата. Издава и управлява сертификата на органа за подпис на документи (DSC)
DS	Document Signer. Орган за подписване на документи
DS-V	Орган за подписване на документи виза, чийто сертификат се издава от CSCA. Цифрово подписва данните, кодирани в баркода, персонализиран върху визовия стикер.
ECDSA	Elliptic Curves Digital Signature. Вид криптографски алгоритъм за създаване на цифров подпис
MRZ	Machine Readable Zone. Машинно-четима зона съдържаща информация за самоличността на лицето (например имена, дата на раждане, ЕГН, пол, номер на личната карта и т.н)

1.2. Технологични дефиниции

Термин	Описание
Виртуална комуникационна инфраструктура	Инфраструктура, която на база съществуваща физическа свързаност, предоставена от МЕУ, предоставя възможност за изграждане на отделни и защитени виртуални мрежи за всяка една от структурите в сектора, при гарантиране на сигурен и защитен обмен на информация в тях.
Държавен хибриден частен облак	Централизирана на ниво държава информационна инфраструктура (сървъри, средства за съхранение на информация, комуникационно оборудване, съпътстващо оборудване, разпределени в няколко локации, в помещения отговарящи на критериите за изграждане на защитени центрове за данни), която предоставя физически и виртуални ресурси за ползване и администриране от секторите и структурите, които имат достъп до тях, в зависимост от нуждите им, при гарантиране на високо ниво на сигурност, надеждност, изолация на отделните ползватели и невъзможност от намеса в работоспособността на информационните им системи или неоторизиран достъп до информационните им ресурси. Изолацията на ресурсите и мрежите на отделните секторни ползватели (е-Общини, е-Правосъдие, е-Здравеопазване, е-Полиция) се гарантира с подходящи мерки на логическо ниво (формиране на отделни

	клъстери, виртуални информационни центрове и мрежи) и на физическо ниво (клетки и шкафове с контрол на достъпа).
Софтуер с отворен код	Компютърна програма, която се разпространява при условия, които осигуряват безплатен достъп до програмния код и позволяват: Използването на програмата и производните на нея компютърни програми, без ограничения в целта; Промени в програмния код и адаптирането на компютърната програма за нуждите на нейните ползватели; Разпространението на производните компютърни програми при същите условия. Списък на стандартни лицензионни споразумения, които предоставят тези възможности, който може да бъде намерен в подзаконовата нормативна уредба към Закона за електронно управление или на: http://opensource.org/licenses.
Машинночетим формат	Формат на данни, който е структуриран по начин, по който, без да се преобразува в друг формат позволява софтуерни приложения да идентифицират, разпознават и извличат специфични данни, включително отделни факти и тяхната вътрешна структура.
Отворен формат	Означава формат на данни, който не налага употребата на специфична платформа или специфичен софтуер за повторната употреба на съдържанието и е предоставен на обществеността без ограничения, които биха възпрепятствали повторното използване на информация.
Метаданни	Данни, описващи структурата на информацията, предмет на повторно използване.
Официален отворен стандарт	Стандарт, който е установен в писмена форма и описва спецификациите за изискванията как да се осигури софтуерна оперативна съвместимост.

Система за контрол на версиите	Технология, с която се създава специално място, наречено "хранилище", където е възможно да се следят и описват промените по дадено съдържание (текст, програмен код, двоични файлове). Една система за контрол на версиите трябва да може: • Да съхранява пълна история - кой, какво и кога е променил по съдържанието в хранилището, както и защо се прави промяната; • Да позволява преглеждане разликите между всеки две съхранени версии в хранилището; • Да позволява при необходимост съдържанието в хранилището да може да се върне към предишна съхранена версия; • Да позволява наличието на множество копия на хранилището и синхронизация между тях. Цялата информация, налична в системата за контрол на версиите за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, трябва да може да бъде достъпна публично, онлайн, в реално време.
Първичен регистър	Регистър, който се поддържа от първичен администратор на данни - административен орган, който по силата на закон събира или създава данни за субекти (граждани или организации) или за обекти (движими и недвижими) за първи път и изменя или заличава тези данни. Например Търговският регистър е първичен регистър за юридическите лица със стопанска цел, Имотният регистър е първичен регистър за недвижима собственост.

1.3. Дефиниции за нива на електронизация на услугите

Термин	Описание
Ниво 1	Информация - предоставяне на информация за административни услуги по електронен път, включително за начини и места за заявяване на услугите, срокове и такси.
Ниво 2	Едностранна комуникация - информация съгласно дефиницията за Ниво 1 и осигурен публичен онлайн достъп до шаблони на електронни формуляри.
Ниво 3	Двустранна комуникация - заявяване и получаване на услуги изцяло по електронен път, включително електронно подаване на

	данни и документи, електронна обработка на формуляри и електронна персонална идентификация на потребителите.
Ниво 4	Извършване на сделки или транзакции по услуги от Ниво 3, включващи онлайн разплащане или доставка.

2. ВЪВЕДЕНИЕ

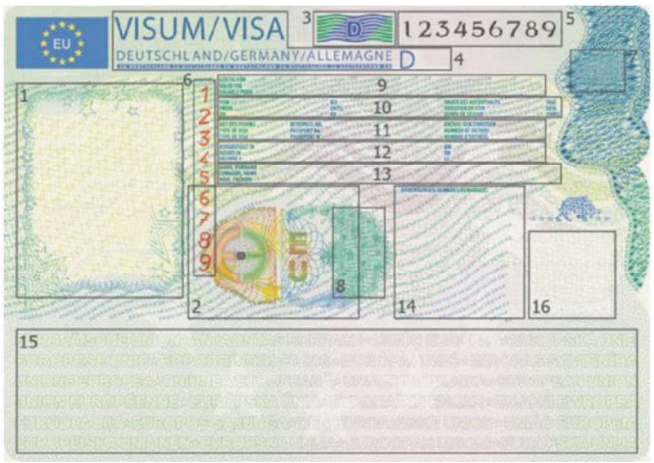
2.1. Цел на документа

Целта на настоящия документ е да опише софтуерните изисквания към изпълнението на проект с наименование: „*Система за генериране на видими цифрови печати (VDS) за документи за виза чрез системата за издаване на визи*“.

В настоящото техническо задание са описани и изискванията към проектната организация, документацията и отчетността.

Регламент (ЕО) № 1683/95 на Съвета от 29 май 1995 г. установява единен формат за визи. С цел предотвратяване на подправянето и фалшифицирането на визи ЕК приема Решение за изпълнение C(2018) 674 на Комисията от 12 февруари 2018 г. за определяне на технически спецификации за единния формат за визи. Определят се допълнителни правила за подобряване на сигурността на визовия стикер и за предотвратяване на по-нататъшно фалшифициране.

С Решение за изпълнение на Комисията C(2020) 2672 от 30 април 2020 г Комисията на ЕС и държавите-членки актуализират Виза стикера с добавяне на видим цифров печат (VDS) в шенгенските визи, с цел допълнителна защита при издаването на документа. Допълнителният слой с криптографска сигурност към физически документ предотвратява използването на откраднати Виза бланки. Видимият цифрово-подписан печат е криптографски подписана структура от данни, съдържаща характеристики на документа, кодирана като двуизмерен (2D) баркод, отпечатан върху хартиен документ. Кодът съдържа съществената информация за съответния документ, както и цифров подпис, който предпазва от манипулиране на данни. Цифровият печат е съгласно техническите указания на ICAO (Doc 9303 - part 13) и BSI TR-03137. Добавянето на цифров печат с криптографски подпис, който включва данните, отпечатани върху визовия стикер, позволява на контролните органи да проверяват автентичността на визите чрез сравняване на отпечатаните данни и тези, включени в цифровия печат. Това е особено важно, когато достъпът до визовата информационна система не е възможен. Република България е задължена да прилага тези изисквания и да издава шенгенски визи с цифров печат в клетка 16 на визовия стикер.



Фиг.1 Бланка на виза

Цифровите печати са двуизмерен баркод, който съдържа подмножество от информацията, отпечатана върху стикера за виза. Тази подгрупа информация, представена като 2D баркод е цифрово подписана от „подписващ баркод“, упълномощен от Сертифициращ орган, удостоверяващ цифров подпис на държавата – CSCA (сертифициращ орган на изградената PKI инфраструктура за БЛД с ЕНИ – единствен за издаващата държава).

Настоящият проект включва доставка, инсталиране и въвеждане в експлоатация на необходимия хардуер и софтуер за генериране на видими цифрови печати (VDS), който ще бъде използван от компетентните органи на МВнР при издаване на визи.

2.2. За възложителя – функции и структура

Министерството на външните работи ръководи, координира и контролира осъществяването на държавната политика на Република България в отношенията й с други държави, като осигурява поддържането и развитието на външнополитическия диалог, политиката на сигурност и двустранното, регионалното и многостранното сътрудничеството. Осъществява общата координация в областта на външната политика и международната дейност на Република България.

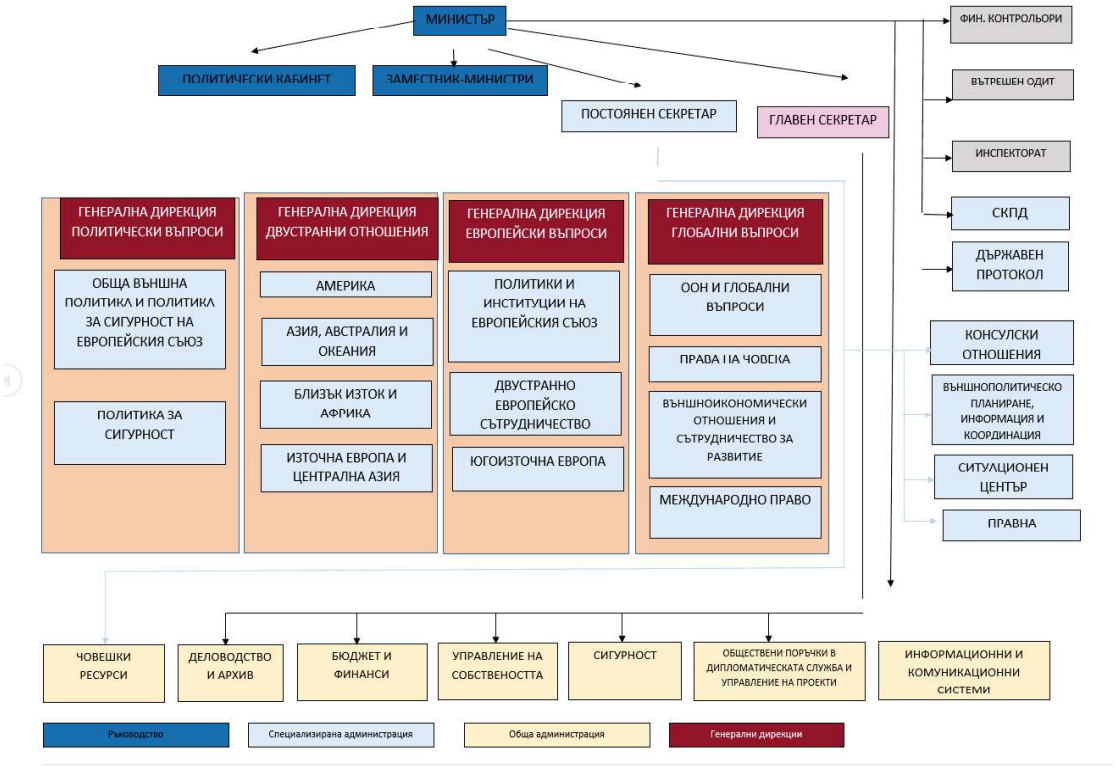
Взаимодейства с висшите органи на държавната власт при осъществяването на правомощията им в областта на външната политика и международната им дейност, координира и участва в подготовката и провеждането на посещенията на държавни и правителствени делегации на най-високо и високо равнище в Република България и в чужбина;

Поддържа и развива дипломатическите и консулските отношения на Република България с други държави, както и отношения с акредитираните в Република България чуждестранни представителства и мисии на международните организации и контролира изпълнението на международноправните задължения на Република България към тях като приемаща страна.

Координира международното сътрудничество, осъществявано от другите министри и ръководители на ведомства, координира и участва в подготовката, сключването и изпълнението на международните договори на Република България;

Защитава правата и интересите на българската държава и на българските граждани и юридически лица в чужбина в рамките на международноправните норми и установената практика, предприема дипломатически действия за опазване на българското културно-историческо наследство и паметници в чужбина.

Структурата на Министерство на Външните Работи е представена във Фигура 1:



Фигура 1. Структура на МВнР

2.3. За проекта

Основната цел на проекта се състои в изграждане на „Система за генериране на видими цифрови печати (vds) за документи за виза чрез системата за издаване на визи“.

Настоящият проект включва доставка, инсталиране и въвеждане в експлоатация на необходимия хардуер и софтуер за генериране на видими цифрови печати (VDS), който ще бъде използван от компетентните органи на МВнР при издаване на визи.

2.4. Нормативна рамка

Проектът се осъществява в съответствие с изискванията, регламентирани със следните нормативни актове и стратегически документи:

- COMMISSION IMPLEMENTING DECISION C(2020) 2672 of 30.4.2020;
- ICAO specifications [ICAO-VDS-TR], [ICAO-9303-7], [ICAO-9303-12], [ICAO-9303-13].

3. Цели, обхват и очаквани резултати от изпълнение на проекта

3.1. Общи и специфични цели на проекта

Настоящият проект включва доставка, инсталиране и въвеждане в експлоатация на необходимия хардуер и софтуер за генериране на видими цифрови печати (VDS), който ще бъде използван от компетентните органи на МВнР при издаване на визи.

Постигането на общата цел ще бъде реализирано чрез следните специфични цели, съответстващи на планираните по проекта дейности:

- Доставка, монтаж, инсталация, конфигурация, провеждане на обучение за служители на МВнР и гаранционна поддръжка на хардуерен модул за сигурност HSM – 2 бр., сървър за софтуер за генериране на видим цифрово подписан печат - 2 бр., специализиран софтуер за генериране на видим цифрово подписан печат - 2 бр., работна станция за наблюдение и управление на системата – 1 бр.

3.2. Разработка на функционалностите на системата и реализиране на интеграции с вътрешни за МВнР системи

3.3. Обхват на проекта

Описаните в т. 3.1 цели се осъществяват с изпълнението на следните основни дейности, които формират обхвата на проекта:

• Дейност 1 Доставка, монтаж, инсталация, конфигурация, провеждане на обучение за служители на МВнР и гаранционна поддръжка на хардуерен модул за сигурност HSM – 2 бр., сървър за софтуер за генериране на видим цифрово подписан печат - 2 бр., специализиран софтуер за генериране на видим цифрово подписан печат - 2 бр., работна станция за наблюдение и управление на системата – 1 бр

• Дейност 2 Разработка на функционалностите на системата и реализиране на интеграции с вътрешни за МВнР системи

Подробна информация за конкретните дейности по проекта ще бъде публично достъпна на адрес: https://projectregister.egov.bg/, след одобрение на ТС от МЕУ.

3.4. Целеви групи

Целевите групи, към които е насочен проектът, обхващат:

• служители на Министерството на външните работи;

• длъжностни лица от задграничните представителства на Република България;

• оправомощени служители на други институции съобразно компетентността им съгласно Наредбата за реда за достъп до Националната визова информационна система на Република България и до Визовата информационна система на Европейския съюз.

3.5. Очаквани резултати

Очакваните резултати от изпълнението на настоящата поръчка са:

В резултат на изпълнението на настоящия проект ще бъдат закупени:

- сървър за софтуер за генериране на видим цифрово подписан печат – 2 бр.
- Хардуерен модул за сигурност HSM – 2 бр.

- Специализиран софтуер за генериране на видим цифрово подписан печат – 2 бр.
- Ще бъде разработена допълнителна функционалност към консулската система eConsulate (КБДИ)
- Ще бъде проведено обучение за служители на МВнР
- Ще бъде предвидена гаранционна поддръжка на хардуерен модул за сигурност
- Ще бъде осигурена работна станция за наблюдение и управление на системата – 1 бр

3.6. Период и място на изпълнение

1. Срокът за изпълнение на дейност 1 доставка, монтаж, инсталация, конфигурация, въвеждане в експлоатация на решението и провеждане на обучение и дейност 2 е до 4 (четири) месеца от влизане в сила на договора.

2. Срокът на гаранция и поддръжка на оборудването (хардуер и софтуер) е предложеният от Изпълнителя срок за съответното оборудване при спазване на минималните изисквания, посочени в таблицата от раздел IV на настоящата техническа спецификация.

Мястото на изпълнение е Министерство на външните работи, гр. София. .

4. ТЕКУЩО СЪСТОЯНИЕ

Министерството на външните работи поддържа и развива дипломатическите и консулските отношения на Република България с други държави, както и отношения с акредитираните в Република България чуждестранни представителства и мисии на международните организации и контролира изпълнението на международноправните задължения на Република България към тях като приемаща страна.

Основните цели на визовата политика са свързани с изграждането и поддържането на необходимата инфраструктура и материална среда и изготвяне на съответните нормативни и административни документи, които да съответстват на изискванията за присъединяване към Шенген с оглед ефективното прилагане на правото и практиката на Шенген. Жизненоважна част от тази инфраструктура е поддържането и развитието на Националната визова информационна система (НВИС) в съответствие с изискванията на ЕС и шенгенските изисквания и свързването ѝ с Визовата информационна система на Европейския съюз (ВИС на ЕС). Редът за достъп до НВИС е уреден Наредбата за реда за достъп до Националната визова информационна система на Република България и до Визовата информационна система на Европейския съюз, приета с ПМС № 129 от 12.05.2011 г.

Националната визова информационна система (НВИС) е изградена в съответствие с изискванията на регламент 767/2008 на Европейския парламент и на Съвета (Регламент за ВИС) за централизиране на информацията, обработвана в дипломатическите и консулски представителства на Република България и за изграждане и поддържане на национален регистър на заявленията за български визи, на издадените визи, както и на биометричните

данни, снемани от кандидатите за визи. НВИС е система с национално значение и гарантира непрекъснат, целогодишен и денонощен (24х7) достъп до ВИС на ЕС не само на МВнР, но и на всички национални органи, имащи съответните права - Главна дирекция “Гранична Полиция” на МВР, Дирекция „Миграция” на МВР, звената „Миграция” при ОДМВР и СДВР, Държавната агенция за бежанците при Министерския съвет, службите за опазване на вътрешния ред и националната сигурност, службите за борба с тероризма и организираната престъпност.

Системата се експлоатира в дипломатическите и консулски представителства (ДКП) на Република България зад граница и в Националния визов център (НВЦ) на дирекция "Консулски отношения" на МВнР. Достъп до системата и съхраняваните данни имат и служители на ДАНС, Главна дирекция „Гранична полиция“- МВР, Дирекция „Миграция“- МВР и Дирекция „Български документи за самоличност“.

НВИС е основен компонент на Националната интегрирана консулска система и е основно средство, подпомагащо работата на дирекция "Консулски отношения” като автоматизира голяма част от дейностите на дирекцията, включително обработка на заявления за визи и издаване на визи, обработка на заявления за български документи за самоличност, издаване на временни паспорти, извършване на консулска регистрация на български граждани, извършване на нотариални заверки, легализации и регистрация на исканията за административни и други консулски услуги.

НВИС е изградена на две нива. Първото ниво е реализирано като самостоятелни информационни системи, разположени в консулските представителства на България зад граница, а второто - като централна информационна система, разположена в Националния визов център в дирекция "Консулски отношения" на МВнР. Основни функции на Н.ВИС са приемане и обработка на заявления за издаване на визи и приемане на заявления за български документи за самоличност и за продължаване срока на валидност на паспорти на български граждани зад граница.

Компонентите на централната система на Националната визова информационна система (VC2011) включва:

1. Система за консултация на визи чрез Шенгенската мрежа за консултация на визи VIS Mail;

2. Система за проверка на кандидатите за визи и техните документи за пътуване в Шенгенската информационна система (ШИС);

3. Национален интерфейс за връзка с Визовата информационна система на ЕС (НИ.ВИС);

4. Комуникационна система за обмен на електронна поща VIS Mail;

5. Комуникационна система за предаване на информацията от постъпващи заявления за български документи за самоличност към АИС "Български документи за самоличност" на МВР.

НВИС е изградена като група тясно интегрирани информационни системи и компоненти:

- информационна система, която централизира информацията, обработвана в задграничните консулски представителства и поддържа национален регистър на заявленията за български визи, на издадените визи, както и на биометричните данни, снемани от кандидатите за визи;

- система за обмен на информация за консулско сътрудничество и консултация на визи VIS Mail;

- национален интерфейс за връзка с Визовата информационна система на ЕС;

- система за проверка на кандидатите за визи и техните документи за пътуване в базата данни на Шенгенската информационна система;

- система за съгласуване издаването на български и шенгенски визи с компетентните национални органи (ДАНС, Дирекция „Миграция" на МВР) – „национално консултиране";

- система за обработка на подадени в дипломатическите и консулски представителства заявления за български документи за самоличност – лични карти, паспорти и СУМПС и за предаване на информацията, към Националния регистър на българските лични документи на МВР;

- система за обмен на информация с АИС "Граничен контрол" на МВР;

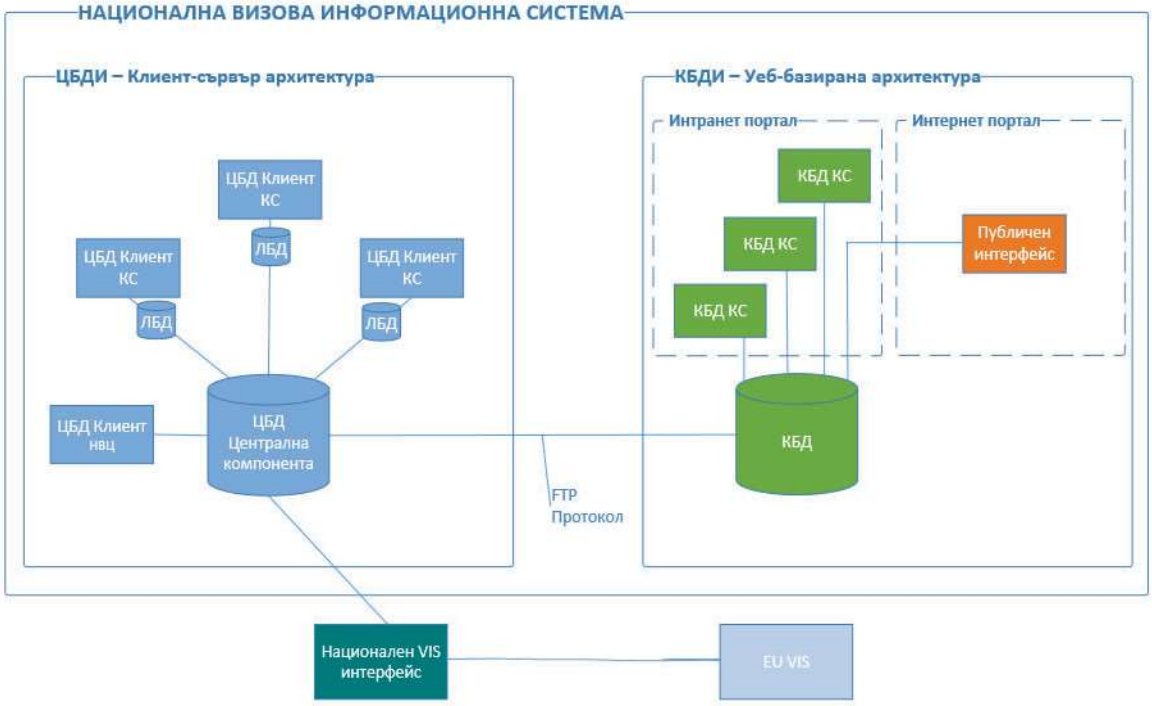
- система за извършване на нотариални заверки, легализации и регистриране на други консулски услуги в ДКП. Поддържане на централизиран регистър на извършените в ДКП консулски услуги, заверки и легализации;

- система за консулска регистрация на български граждани, живеещи зад граница;

- система за идентификация на български и чужди граждани;

- комуникационна система за обмен на информацията между ДКП и НВЦ, система за централизирано администриране на общосистемна и управляваща информация – въвеждане и актуализация на номенклатури, цени на извършваните в КС услуги по тарифи 1,3 и 4, визов режим, разпределение и отчет на бланки (визови стикери, тела и стикери за временни паспорти и удостоверения за завръщане на чужди граждани), условия за национално и шенгенско консултиране, списъци с валидни документи за пътуване и др.

На схемата са представени отделните компоненти (ЦБДИ и КБДИ), които заедно съставят Националната визова информационна система:



Фиг. Обща архитектура на НВИС

Легенда:1. ЦДБ – Централна база данни; 2. КБД – Клиентска база данни; 3. ЛБД – Локална база данни

В ДКП зад граница от м. април 2018 г. е въведена в експлоатация информационна система, която е уеб-базирана и съдържа следните функционално обособени модули:

- Приложение, обслужващо клиентска база данни, което осъществява връзката с централния компонент на НВИС, работещо успоредно и съвместно със съществуващия компонент на НВИС в НВЦ;

- Външен портал, достъпен през Интернет, за подаване на електронни заявления и необходимите документи и атрибути за предоставяне на визови и консулски услуги, заплащане на услуги и резервиране на час за прием. Външният портал поддържа собствен изглед на данните от клиентската база данни, като достъпа до клиентската база данни става през интерфейс с вътрешния портал, който единствено има достъп до тези данни;

- Вътрешен портал, използван от служители на консулските служби, предназначен за обработка на получените заявления за консулски услуги и въвеждането им в клиентската база данни.

Компонентите на КБД са разработени на JAVA и работят върху следните платформи и технологии:

- Виртуална машина – VMWare vSphere ESXi и Microsoft Hyper-V;
- Сървърна ОС – Linux Debian и Linux Ubuntu;

- Приложни сървъри – Apache, Apache ACE, Apache Tomcat, JBoss EAP, Alfresco;
- Сървър бази данни – PostgreSQL;
- Обмен на файлове между ЦБДИ и КБДИ – XML файлове по FTP протокол;
- Достъп до справочни услуги – OpenLDAP;
- Услуги за сигурност – Secure Token Service;

Външни за КБД приложения, интегрирани за работа с нея са:

- Приложение за биометрия – Biometrix;
- Приложение за сканиране - Scan Server.

В Националния визов център работи централна компонента на информационна система, която има клиент-сървър архитектура и изпълнява следните основни функции:

- Поддържане на регистър на заявленията за визи и български документи за самоличност вкл. с биометрични данни на притежателите им, както и на извършените консулски услуги, нотариални заверки и легализации;
- Обмен на информация между ДКП и НВЦ;
- Вземане на решения по заявленията за визи на определени категории лица;
- Национално съгласуване на заявленията за визи на определени категории лица;
- Проверка на кандидатите за визи и предоставените от тях документи за пътуване в Шенгенската информационна система;
- Подпомагане на локалното консулско сътрудничество чрез системата за обмен на информация за консулско сътрудничество VIS Mail;
- Предоставяне на информация за постъпващите заявления за визи, взетите решения и издадени визи към Визовата информационна система на ЕС (ВИС на ЕС);
- Осигуряване извършването на справки във ВИС на ЕС за постъпили заявления и издадени визи от други държави-членки на Шенген;
- Поддръжка на национална база с обработените заявления за визи и издадени визи, заявления за български документи за самоличност, нотариални и други консулски услуги и др.;
- Предоставяне на информацията от постъпващите заявления за издаване на български документи за самоличност към АИС Български документи за самоличност на МВР.

Системата се експлоатира в средата на Microsoft Windows Server 2012, Windows 8/10, използва СУБД IBM Informix Dynamic Server и е разработено чрез SAP Sybase PowerBuilder 11.5. Националният интерфейс за връзка с Визовата информационна система на ЕС е реализиран като J2EE приложение в средата на Oracle WebLogic.

Системата е разработена от Института по компютърни технологии при Министерството на вътрешните работи и е въведена в експлоатация от 1995 г., като непрекъснато е била надграждана и обновявана до закриването на Института с Постановление № 11 на МС от 30.01.2014 г. От 2016 г. поддръжката на системата се извършва по договор № 56-ОП-И/25.08.2016 г. с предмет: "Поддръжка и обновяване на програмното и техническо осигуряване на националната визова информационна система (НВИС) и на визовата дейност в консулските служби на Р България", по Обособена позиция 1: „Поддръжка и осъвременяване на техническото осигуряване и инфраструктурата на НВИС", финансиран по договор за безвъзмездна финансова помощ с рег. № 812108-116, екз. 3/13.10.2015 г. по линия на фонд „Вътрешна сигурност" 2014-2020, в рамките на инструмента за външните граници, съфинансиран от Европейския съюз,.

НВИС е инсталирана в НВЦ и в РВЦ, намиращи се на следните адреси:

Национален визов център - гр. София, ул. „Ал. Жендов"№ 2

Резервен визов център - гр. София, ул. „Витошко лале"№ 16.

5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

5.1. Общи изисквания към изпълнението на проекта

Обществената поръчка се изпълнява в рамките на проект с наименование изграждане на „Система за генериране на видими цифрови печати (VDS) за документи за виза чрез системата за издаване на визи" финансиран от МВнР. Изпълнителят следва да спазва всички нормативни изисквания по отношение на дейността на МВнР и електронното управление в Република България.

5.2. Общи организационни принципи

Задължително изискване е да се спазят утвърдените хоризонтални и вертикални принципи на организация на изпълнението на предмета на обществената поръчка за гарантирано постигане на желаните резултати от проекта, така че да се покрие пълният набор от компетенции и ноу-хау, необходими за изпълнение на предмета на поръчката, а също така да се гарантира и достатъчно ниво на ангажираност с изпълнението и проблемите на проекта:

- Хоризонталният принцип предполага ангажиране на специалисти от различни звена, така че да се покрие пълният набор от компетенции и ноу-хау по предмета на проекта и същевременно екипът да усвои новите разработки на достатъчно ранен етап, така че да е в състояние пълноценно да ги използва и развива и след приключване на проекта;

- Вертикалният принцип включва участие на експерти и представители на различните управленски нива, така че управленският екип да покрива както експертните области, необходими за правилното и качествено изпълнение на проекта, така и управленски и организационни умения и възможности за осъществяване на политиката във връзка с изпълнението на проекта. Чрез участие на ръководители на звената – ползватели на резултата от проекта, ще се гарантира достатъчно ниво на ангажираност на институцията с проблемите на проекта.

5.3. Управление на проекта[2]

Участниците трябва да предложат методология за управление на проекта, която смятат да приложат, като се изтъкнат ползите й за успешното изпълнение на проекта. Предложената методология трябва да съответства на най-добрите световни практики и препоръки (например Project Management Body of Knowledge (PMBOK) Guide, PRINCE2, Agile/SCRUM/Kanban, RUP и др. еквивалентни).

Възложителят изисква методология за управление на проекта, която участниците трябва да приложат и която съответства на най-добрите практики и препоръки..

Дейностите по управление на проекта трябва да включват като минимум управление на реализацията на всички дейности, посочени в настоящия проект, и постигане на очакваните резултати, както и разпределението на предложените участници в екипа за управление на поръчката по роли, график и дейности при изпълнение на настоящия проект.

Доброто управление на проекта трябва да осигури:

- координиране на усилията на експертите от страна на Изпълнителя и Възложителя и осигуряване на висока степен на взаимодействие между членовете на проектния екип;
- оптимално използване на ресурсите;
- текущ контрол по изпълнението на проектните дейности;
- разпространяване навреме на необходимата информация до всички участници в проекта;
- идентифициране на промени и осигуряване на техните анализ и координация;
- осигуряване на качеството и полагане на усилия за непрекъснато подобряване на работата за удовлетворяване на изискванията на участниците в проекта.

Методологията трябва да включва подробно описание на:

- фазите на проекта;
- организация на изпълнение:
    - структура на екипа на Изпълнителя;
    - начин на взаимодействие между членовете на екипа на Изпълнителя;
    - връзки за взаимодействие с екипа на Възложителя;
- проектна документация:
    - видове доклади;
    - техническа и експлоатационна документация;
    - време на предаване;
    - съдържание на документите;
    - управление на версиите;
- управление на качеството;
- график за изпълнение на проекта.

В графика участниците трябва да опишат дейностите и стъпките за тяхното изпълнение максимално детайлно, като покажат логическата връзка между тях. В графика трябва да са посочени датите за предаване на всеки от документите, изготвени в изпълнение на обществената поръчка.

5.4. Управление на риска

В техническото си предложение участниците трябва да опишат подхода за управление на риска, който ще прилагат при изпълнението на поръчката.

Участниците трябва да представят и списък с идентифицираните от Възложителя рискове с оценка на вероятност, въздействие и мерки за реакция.

През времето за изпълнение на проекта Изпълнителят трябва да следи рисковете, да оценява тяхното влияние, да анализира ситуацията и да идентифицира (евентуално) нови рискове.

В хода на изпълнение на поръчката Изпълнителят следва да поддържа актуален списък с рисковете и да докладва състоянието на рисковете най-малко с месечните отчети за напредъка.

При изготвянето на списъка с рискове Участниците следва да вземат предвид следните идентифицирани от Възложителя рискове:

- Промяна в нормативната уредба, водеща до промяна на ключови компоненти на решението – предмет на разработка на настоящия проект;
- Недобра комуникация между екипите на Възложителя и Изпълнителя по време на аналитичните етапи на проекта;
- Ненавременно изпълнение на всяко от задълженията от страна на Изпълнителя;
- Неправилно и неефективно разпределяне на ресурсите и отговорностите при изпълнението на договора;
- Забавяне при изпълнение на проектните дейности, опасност от неспазване на срока за изпълнение на настоящата поръчка;
- Грешки при разработване на функционалностите на системата;
- Недостатъчна яснота по правната рамка и/или променяща се правна рамка по време на изпълнение на проекта;
- Липса на задълбоченост при изследването и описанието на бизнес процесите и данните;
- Неинформиране на Възложителя за всички потенциални проблеми, които биха могли да възникнат в хода на изпълнение на дейностите;
- Риск за администриране на системата след изтичане на периода на гаранционна поддръжка.

6. ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА

В техническото си предложение участниците трябва да предложат подход за изпълнение на проекта, като включат минимум следните етапи:

6.1. Анализ на данните и изискванията

Функционален обхват на проекта

Разработка на функционалностите на системата и реализиране на интеграции с вътрешни за МВнР системи с цел отпечатване на визов стикер, върху който да се отпечатва криптографски подписан цифров печат (2d баркод), който да съдържа определена част от данните на визовия стикер.

Независимо от източника на финансиране са приложими и предварителните условия за допустимост (Приложение №1 от Пътната карта за електронно управление 2016-2020) за финансиране на проекти по ОП "Добро управление", в т.ч.:

▪ Предвидените за разработка и внедряване услуги трябва да бъдат регистрирани предварително в Регистъра на услугите към Административния регистър (съгласно чл. 61 от Закона за администрацията) и да бъдат въведени и валидирани данни за броя на транзакциите по предоставяне на тези услуги в Модула „Самооценка на административното обслужване“ в Интегрираната информационна система на държавната администрация (ИИСДА). Услугите, които ще бъдат надградени, и новоразработените услуги трябва да отговарят на изискванията за електронни услуги с минимално Ниво 4, където е приложимо (т.е. услугата изисква заплащане на такса), или Ниво 3, в случаите, в които за предоставяне на услугата не се изисква заплащане на такса; Дефинициите за нивата на електронизация на административните услуги са регламентирани в Наредбата за административния регистър към Закона за администрацията;

▪ В процеса на бизнес анализ да бъдат изследвана съвместимостта на бизнес процесите на Възложителя с вече одобрени оптимизирани референтни модели за предоставяне на услуги и нормативни изисквания на Базисен модел за Комплексно административно обслужване в държавната администрация. При наличие на разработени модели за предоставяне на услуги по „Епизоди от живота“ и „Събития от бизнеса“, които включват услуги, предоставяни от Възложителя, да бъдат съобразени нуждите от модификации в референтните модели, за да се постигне подобряване на времето и намаляване на административната тежест при комплексно обслужване, спрямо предоставянето на отделните услуги поединично;

▪ В случай че се касае за административни услуги, те трябва да бъдат разграничени на базата на разлики в бизнес процесите и да не бъдат генерализирани и/или обобщавани на базата на типа на действие (например ако Системата издава няколко различни вида удостоверения, с които се удостоверяват различни обстоятелства, административните услуги трябва да бъдат регистрирани отделно);

▪ Удостоверителните административни услуги трябва да бъдат регистрирани и като вътрешни административни услуги и да бъде реализирана възможност за предоставянето на

тези услуги като електронни вътрешно- административни услуги за нуждите на комплексното административно обслужване чрез служебен онлайн интерфейс.

1.1.1. Специфични изисквания към етапите на бизнес анализа и разработка

В настоящия проект не се предвижда разработка или надграждане на публични електронни административни услуги

- [не приложимо] Изпълнителят трябва да следва Методологията за усъвършенстване на работните процеси за предоставяне на административни услуги и Наръчника за прилагане на методологията, приета с Решение № 578 на Министерския съвет от 30 септември 2013 г.;

- Трябва да бъде предвидена фаза на проучване, по време на която да се дефинират потребителските нужди, да се проведат предварителни тестове с потребители и да се изработи план, по който да се адресират идентифицираните нужди;

- Трябва да бъдат предвидени периодични продуктови тествания по време на разработката и внедряването на Системата, с извадка (фокус-група) от бъдещите потребители на електронната услуга (служители в администрацията, граждани, доставчици на обществени услуги), чрез които да се изпита и оцени използваемостта на услугите и потребителските интерфейси, както и за да бъдат отстранени затруднения и несъответствия със заданието;

- Трябва да се спазват нормативните изисквания за еднократно събиране и повторна употреба на данни в държавната администрация (съгласно АПК и ЗЕУ) и в разработените бизнес процеси да не се изискват данни за заявителя и/или за получателя на услугата, които могат да се извлекат автоматично в процеса на електронна идентификация чрез Центъра за електронна идентификация или на база на ЕГН от КЕП. При необходимост изпълнителят трябва да предложи на Възложителя адекватни промени в нормативната уредба, които да хармонизират съответните секторни нормативни изисквания с общите разпоредби на Административнопроцесуалния кодекс, Закона за електронно управление, Закона за електронния документ и електронния подпис и приложимите подзаконови актове, ако действащата нормативна уредба изисква:

  - изрично попълване на типов хартиен формуляр, върху който потребителите трябва да се подпишат собственоръчно и/или който да приложат като изискуем документ при заявяването на електронна административна услуга;
  - изрично деклариране или обявяване на обстоятелства или данни, които се администрират и/или удостоверяват от други държавни органи и могат да

бъдат получени по служебен път, включително и автоматизирано през съответни интеграционни интерфейси;

- други нормативни изисквания, които водят до неоптимални или ненужно бюрократични процеси, които биха могли да бъдат оптимизирани при заявяване и предоставяне на електронни административни услуги;

▪ [не приложимо] Трябва да се разработят информативни текстове за всяка електронна административна услуга, които включват като минимум:

- Условия за предоставяне на услугата;
- Срокове за предоставяне на услугата;
- Такси за заявяване и съответно предоставяне на услугата;
- Начини за получаване на услугата;
- Резултат от предоставяне на услугата;
- Отказ от предоставяне на услугата;

▪ Информативните текстове за всяка електронна административна услуга трябва да бъдат достъпни за потребителите още като първа стъпка от заявяването на услуга;

▪ Тарифирането на услугите трябва да бъде реализирано така, че Системата да съхранява всички версии на тарифите за услуги (от дата до дата) и да прилага съответната тарифа, в зависимост от момента, в който е заявена дадена услуга;

▪ Трябва да бъде оптимизиран потребителският път от влизане на сайта до заявяване и получаване на услуга и пътят от регистрация на нов потребител до заявяване и получаване на услуга;

▪ При оптимизацията на потребителския път трябва да се отчита всяко действие от страна на потребителя (натискане на бутон, въвеждане на данни, прочитане на текст и пр.), което може да се спести.

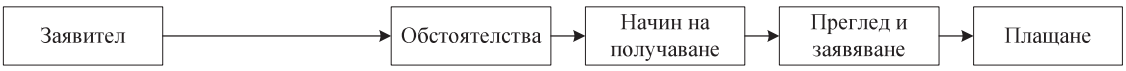
1.1.2. [не приложимо] Специфични изисквания при оптимизиране на процесите по заявяване на електронни административни услуги в зависимост от заявителя

В настоящия проект не се предвижда разработка или надграждане на публични електронни административни услуги.

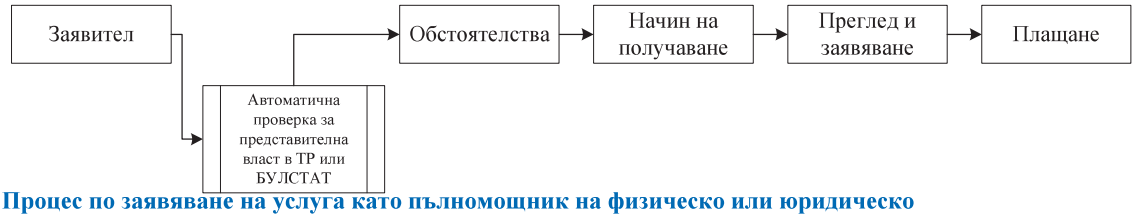
Съгласно действащата нормативна уредба допустимите заявители на електронни административни услуги могат да бъдат разделени в няколко групи, като процесите по заявяване на ЕАУ и необходимите процеси по установяване на допустимостта на заявлението зависят от множество фактори. Трябва да бъде обърнато специално внимание на спецификите в процесите в зависимост от качеството, в което действа заявителят, за да се постигне максимална оптимизация на процеса, като същевременно се защити сигурността на търговския и гражданския оборот.

В приложената диаграма са показани възможни разлики в бизнес процесите в зависимост от качеството, в което действа заявител на ЕАУ:

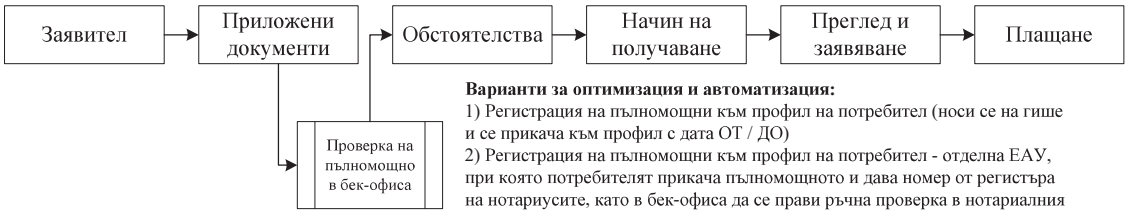
Процес по заявяване „в лично качество“:



Процес по заявяване на услуга като законен представител на юридическо лице:

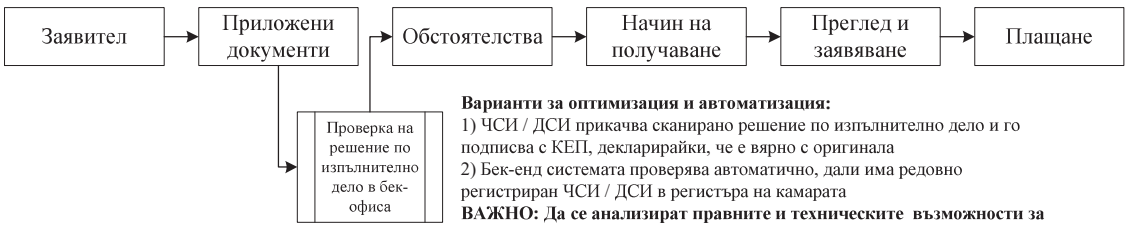


Процес по заявяване на услуга като пълномощник на физическо или юридическо лице:



Варианти за оптимизация и автоматизация:
1) Регистрация на пълномощни към профил на потребител (носи се на гише и се прикача към профил с дата ОТ / ДО)
2) Регистрация на пълномощни към профил на потребител - отделна ЕАУ, при която потребителят прикача пълномощното и дава номер от регистъра на нотариусите, като в бек-офиса да се прави ръчна проверка в нотариалния регистър на пълномощните „Единство“, преди да се активира)
ВАЖНО: Да се анализират правните и техническите възможности за осигуряване на служебен достъп до регистъра на пълномощните, воден от нотариалната камара!

Процес по заявяване на услуга като длъжностно лице:



Варианти за оптимизация и автоматизация:
1) ЧСИ / ДСИ прикачва сканирано решение по изпълнително дело и го подписва с КЕП, декларирайки, че е вярно с оригинала
2) Бек-енд системата проверява автоматично, дали има редовно регистриран ЧСИ / ДСИ в регистъра на камарата
ВАЖНО: Да се анализират правните и техническите възможности за осигуряване на служебен достъп до регистъра на пълномощните, воден от нотариалната камара!

В приложената таблица са представени спецификите и разликите в бизнес процесите в зависимост от качеството, в което действа заявител на ЕАУ, които трябва да бъдат отразени при реализацията на Системата:

Вид заявител	Особености	Специфични процеси
Физическо лице за собствени нужди	Заявява ЕАУ за лични нужди от свое име. Това е най-простият за реализиране случай	Услугата може да бъде предоставена, след като са изпълнени нуждите за идентификация, ако има такива - електронна идентификация по смисъла на ЗЕИ или ЕГН, извлечено от КЕП в преходния период, както и три имена или анонимно.
Законен представител на юридическо лице	Заявява ЕАУ, за да обслужи нужди на юридическо лице, на което е законен представител (т.е. заявителят е вписан като представляващ юридическото лице в съответен регистър)	Услугата може да бъде предоставена, след като са изпълнени нуждите за идентификация - електронна идентификация по смисъла на ЗЕИ или ЕГН, извлечено от КЕП в преходния период, както и автоматична проверка за представителна власт в ТР/БУЛСТАТ/ЦРЮЛНЦ.
Пълномощник на ФЛ или ЮЛ	Заявява ЕАУ, за да обслужи нужди на физическо или юридическо лице, което го е упълномощило (т.е. заявителят трябва да разполага с пълномощно, което му дава необходимия обем и обхват на представителна власт, за заявяване и/или получаване на съответната услуга)	Услугата може да бъде предоставена само след проверка на представителната власт в Регистъра с пълномощни на Нотариалната камара, чрез проверка в Регистъра на овластяванията по смисъла на ЗЕИ или при създадена възможност за регистриране на пълномощни към профила на потребителя или за заявяване на услугата. Пълномощник може да бъде и посредник за предоставяне на ЕАУ по реда на ЗЕУ, в т.ч. Центрове за комплексно административно обслужване.

Длъжностно лице (ЧСИ / ДСИ)	Заявява ЕАУ, за да изпълни определени свои задължения като длъжностно лице спрямо друго физическо или юридическо лице, за което следва да има съответен правен интерес – напр. решение по изпълнително дело.	Услугата може да бъде предоставена само след проверка на длъжностното лице в съответния регистър (ЧСИ/ДСИ) и на правния интерес чрез изискване за декларирането му чрез изрична декларация, подписана с КЕП, и прилагане на копие от решение по изпълнително дело.

1.1.3. [не приложимо] Изисквания за оптимизиране на процесите по подаване на декларации, изискуеми в съответствие с нормативната уредба и вътрешните правила

В настоящия проект не се предвижда разработка или надграждане на публични електронни административни услуги.

- Системата трябва да поддържа номенклатура с редактируеми шаблони на декларации, които да бъдат достъпни за актуализация за администраторите на Системата; Трябва да се поддържа история на версиите на шаблоните и да няма възможност за перманентно премахване/изтриване на шаблони, а само смяна на статуса им и публикуване на нова версия;
- Ако даден бизнес процес изисква подаване на декларация от страна на заявител на услуга, при достигане на съответната стъпка от процеса Системата трябва:
  - да попълва автоматично всички персонални данни на заявителя в електронна форма, генерирана на база на съответния шаблон на декларация
  - да дава възможност на потребителя за избор на съответните обстоятелства, които може да декларира (ако шаблонът на декларацията предвижда възможност за деклариране на опционален набор от предефинирани обстоятелства)
  - да изисква потвърждение на обстоятелствата от страна на потребителя
  - в случай че декларацията трябва да се попълни от лице, различно от заявителя, тя да може да се прикачи като електронно подписан документ или по електронен път да бъде отправяна покана към декларатора за електронно подписване.
- Всяка попълнена електронна декларация трябва да се прикачи автоматично от Системата към заявлението и да бъде подписана заедно с него от потребителя с електронен подпис, освен в случаите, когато заявителят и декларатorът са различни лица и декларацията е подписана отделно от декларатора.

1.1.4. [не приложимо] Изисквания към регистрите и предоставянето на административните услуги

В настоящия проект не се предвижда разработка или надграждане на публични електронни административни услуги.

- Всяка удостоверителна административна услуга в обхвата на Системата трябва да бъде достъпна като вътрешноадминистративна електронна услуга чрез уеб-услуга, като комуникацията се подписва с електронен печат на институцията и с електронен времеви печат по смисъла на Регламент (ЕС) 910/2014;
- Всяка услуга, за която се допуска представителна власт, трябва да бъде интегрирана с Регистъра на овластяванията по смисъла на Закона за електронната идентификация;
- Системата не трябва да съхранява данни, на които възложителят не е първичен администратор, в случай че данните могат да бъдат извличани в реално време от регистър на съответния първичен администратор.
- Всички електронни административни услуги, предоставяни от административните органи на гражданите и бизнеса трябва да се заявяват през Единният портал за достъп до електронни административни услуги и чрез хоризонталната система за е-форми, както и да се прилага Единния модел за заявяване, заплащане и предоставяне на електронни административни услуги.

6.2. Изготвяне на системен проект

Изпълнителят трябва да изготви системен проект, който подлежи на одобрение от Възложителя. В системния проект трябва да са описани всички изисквания за реализирането на Системата. Изготвянето на системния проект включва следните основни задачи:

- Определяне на концепция на информационната система на базата на техническото задание;
- Дефиниране на детайлни изисквания и бизнес процеси, които трябва да се реализират в Системата;
- Дизайн на информационната система, хардуерната и комуникационната инфраструктура;
- Изготвяне на план за техническа реализация;
- Определяне на потребителския интерфейс.

Изпълнението на задачите изисква дефиниране на модели на бизнес процеси, модели на стандартни справки и анализи, модели на печатни бланки, политика за сигурност и защита на данните, основни изграждащи блокове, транзакции, технология на взаимодействие, мониторинг на системата, спецификация на номенклатурите, роли в системата и други. При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, е необходимо да се използва стандартен език за описание на бизнес процеси – BPMN.

Системният проект подлежи на одобрение от Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят е длъжен да ги отрази в системния проект в срок не по-късно от *10* работни дни.

6.3. Разработване на софтуерното решение

Етапът на разработка включва изпълнението на следните задачи:

- Разработка на прототип, който трябва да бъде одобрен от Възложителя и въз основа на който трябва да се разработи цялата система;
- Разработка на модулите на информационната система съгласно изискванията на настоящото техническо задание и системния проект;
- Провеждане на вътрешни тестове на Системата (в среда на разработчика);
- Изготвяне на детайлни сценарии за провеждане на приемателните тестове за етапи „Тестване“ и „Внедряване“ на проекта.

За изпълнение на дейностите по разработка на системата участниците в настоящия проект трябва да опишат в своите технически предложения приложим подход (методология) за софтуерна разработка, която ще използват, както и инструментите за разработка и средата за провеждане на вътрешните тестове. Участниците трябва да опишат как предложеният от тях подход ще бъде адаптиран за успешната реализация на Системата.

6.4. Тестване

Изпълнителят трябва да проведе тестване на софтуерното решение в създадена за целта тестова среда, за да демонстрира, че изискванията са изпълнени. Изпълнителят трябва да предложи и опише методология за тестване, която ще използва в план за тестване с описание на обхвата на тестването, вид и спецификация на тестовете, управление на дефектите, регресионна политика, инструменти, логистично осигуряване и други параметри на процеса.

6.5. Внедряване

Изпълнителят трябва да внедри софтуерното решение в информационната и комуникационна среда на Министерство на Външните Работи Това включва инсталиране, конфигуриране и настройка на програмните компоненти на системата в условията на експлоатационната среда на МВнР.

6.6. Обучение

Изпълнителят трябва да организира и да проведе обучения за следните групи и ползватели на софтуерното решение:

- *Служители в ЦУ на МВнР;*
- *Служители в ЗП на МВнР;*

За провеждането на обученията Изпълнителят е длъжен да осигури за своя сметка *[включват се само тези точки, за които Възложителят няма възможност да осигури изброените ресурси]*:

- Учебни материали;
- Лектори.

6.7. Гаранционна поддръжка

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за период от минимум 24 месеца след приемане в експлоатация на системата.

При необходимост, по време на гаранционния период трябва да бъдат осъществявани дейности по осигуряване на експлоатационната годност на софтуера и ефективното му използване от Възложителя, в случай че настъпят явни отклонения от нормалните експлоатационни характеристики, заложени в системния проект.

Изпълнителят следва да предоставя услугите по гаранционна поддръжка, като предоставя за своя сметка единна точка за достъп за приемане на телефонни и e-mail съобщения.

Приоритетите на проблемите се определят от Възложителя в зависимост от влиянието им върху работата на администрацията. Редът на отстраняване на проблемите се определя в зависимост от техния приоритет.

Минималният обхват на поддръжката трябва да включва:

▪ Извършване на диагностика на докладван проблем с цел осигуряване на правилното функциониране на системите и модулите;

▪ Отстраняване на дефектите, открити в софтуерните модули, които са модифицирани или разработени в обхвата на проекта;

▪ Консултации за разрешаване на проблеми по предложената от Изпълнителя конфигурация на средата (операционна система, база данни, middleware, хардуер и мрежи), използвана от приложението, включително промени в конфигурацията на софтуерната инфраструктура на мястото на инсталация;

▪ Възстановяването на системата и данните при евентуален срив на системата, както и коригирането им в следствие на грешки в системата;

▪ Експертни консултации по телефон и електронна поща за системните администратори на Възложителя за идентифициране на дефекти или грешки в софтуера;

▪ Актуализация и предаване на нова версия на документацията на системата при установени явни несъответствия с фактически реализираните функционалности, както и в случаите, в които са извършени действия по отстраняване на дефекти и грешки, в рамките на гаранционната поддръжка.

7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

7.1. Функционални изисквания към информационната система

Съгласно стандартите на ICAO Doc 9303 за генериране на подписа/сертификата на цифровия печат да се използва съществуващия в момента CSCA за биометрични паспорти и разрешения за пребиваване.

Да бъде изграден подписващ орган Document Signer for VISA (за цифрово подписване на 2D баркода, отпечатан върху единния формат на документа виза.

Да бъдат осигурени следните функционалности:

- Генериране на съвместими с ICAO цифрови печати за визи;
- Генериране на заявка за сертификат към съществуващия в момента CSCA;
- Импорт на издаден сертификат от CSCA;
- Подписване на данните за визата чрез използване на частния ключ, кодирани в баркода;

- Автентикация - възможност за валидиране на данните кодирани в баркода.

Да се осигурява надеждна защита за генериране и съхранение на всички двойки ключове (частен и публичен) за подпис. За генериране, работа и защита на всички частни ключове за подпис на DS-V да се използват хардуерни модули за сигурност (HSM) и криптографски механизми за защита на данните по стандарта FIPS 140-3 Level 3.

Да се гарантира пълно наличие и надеждност на услугите, да е осигурена резервираност, позволяваща непрекъсната работа на сървърите за цифров подпис и хардуерните модули за сигурност (HSM) 24 часа в денонощието.

Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.

2. Във връзка с мрежовата и информационната сигурност на Възложителя/ МВнР и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

(а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Възложителя/МВнР ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Възложителя/МВнР. За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Възложителя/ МВнР, подписват декларации по образец на Възложителя за опазване на информацията, които се предават на Възложителя. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до 2 (два) работни дни от промяната.

3. Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на договора на трети страни без изричното писмено съгласие на Възложителя/ МВнР.

4. При неспазване на изискванията за сигурност на информацията Изпълнителят дължи неустойка съгласно уговореното в договора.

5. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

(а) При изпълнението на задълженията си, осъществяват комуникация с лицата,

които ще имат достъп до системите на МВнР;

(б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на

Изпълнителя (и на подизпълнителите, когато е приложимо);

(в) При получена информация, лицата по чл. 10, ал. 2 от НМИМИС осъществяват

незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Възложителя/ МВнР;

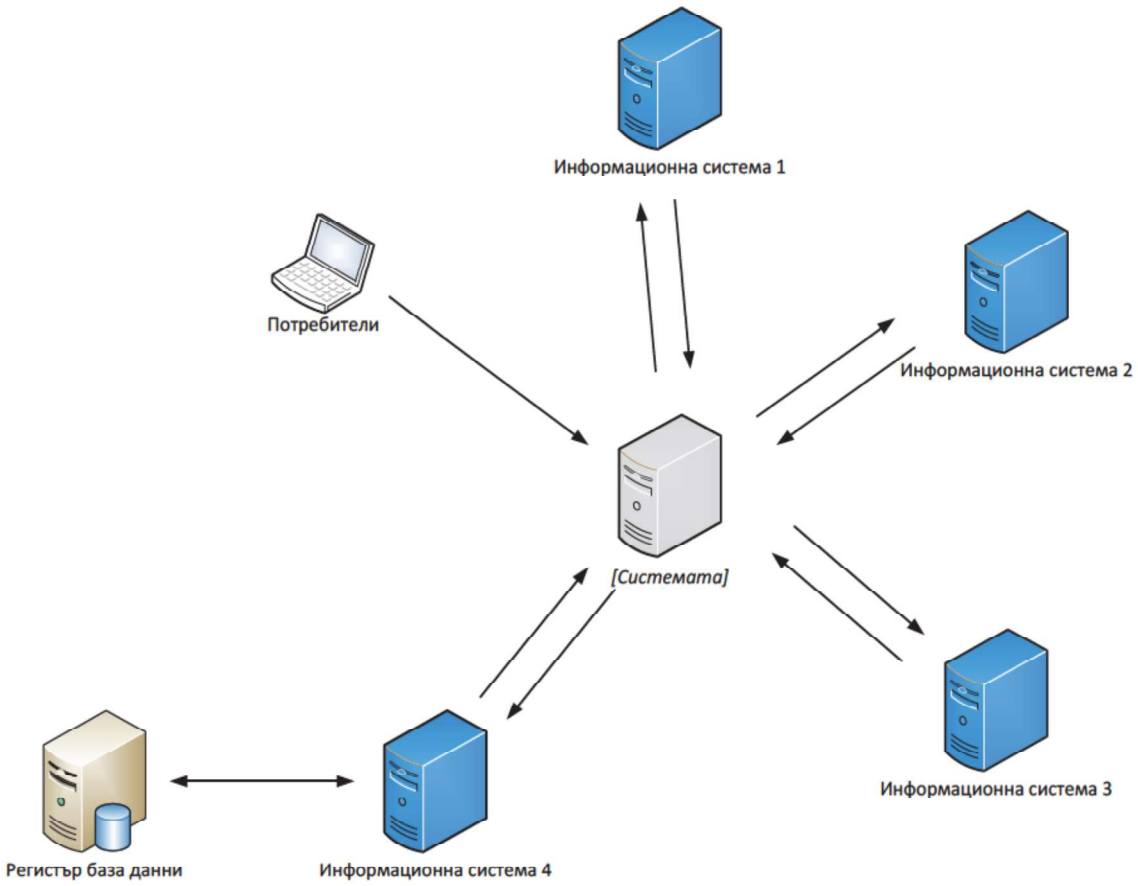
(г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Възложителя/ МВнР, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на МВнР от страна на Възложителя и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.

1.1.5. Интеграция с външни информационни системи

За реализиране на основни бизнес процеси Системата трябва да поддържа интеграция в реално време с информационни системи на други администрации:

Системата е вътрешна за МВнР и връзката с други системи е чрез интерфейси, които са част от нея.

- Интегрираната информационна система на държавната администрация (ИИСДА), в частност Регистъра на услугите, в който се вписват допустимите заявители и получатели на административни услуги - например: проверка на достъпа до съответните обстоятелства; посочване на идентификатор на конкретна административна услуга, за която е нужно извличането на съответните обстоятелства от регистрите;
- Интеграциите с външни информационни системи и регистри трябва да се реализира чрез стандартен интеграционен слой.



1.1.6. Интеграционен слой

▪ [не приложимо] Трябва да бъде разработен и внедрен служебен онлайн интерфейс за машинен обмен на данни и предоставяне на вътрешноадминистративни електронни услуги към информационни системи и регистри на други администрации, публични институции и доставчици на обществени услуги, съгласно действащите изисквания за оперативна съвместимост. Трябва да бъде предвидена интеграция с първични регистри чрез стандартен междинен слой или чрез националната схема за електронна идентификация – конкретната реализация трябва да бъде одобрена от Възложителя след приключване на етапа на бизнес-анализ;

▪ [не приложимо] Трябва да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано машинно поискване и предаване на история на изпълнените транзакции по машинен обмен на данни, предоставените електронни услуги и начислени такси, към информационни системи на други публични институции и доставчици на обществени услуги, с оглед предоставяне на КАО, съгласно действащите изисквания за оперативна съвместимост;

▪ [не приложимо] Трябва да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на документи и нотификации чрез електронна препоръчана поща към подсистемата за сигурно връчване, част от Националната система за електронна идентификация, съгласно действащите изисквания за оперативна съвместимост;

▪ [не приложимо] Трябва да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на транзакционна история към системата за електронна идентификация, съгласно действащите изисквания за оперативна съвместимост;

▪ [не приложимо] Трябва да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на ценни електронни документи към Централизираната система за е-Архивиране, ако е приложимо и съответната система или регистър оперират с такива документи, съгласно действащите изисквания за оперативна съвместимост;

▪ [не приложимо] Трябва да бъде разработен и внедрен служебен онлайн интерфейс за електронни разплащания и интеграция с виртуални POS терминали, позволяващ директно плащане с дебитна или кредитна карта без необходимост от регистрация на отделен потребителски акаунт в система на платежен оператор.

1.1.7. Технически изисквания към интерфейсите

Приложните програмни интерфейси трябва да отговарят на следните архитектурни, функционални и технологични изисквания:

▪ Служебните онлайн интерфейси трябва да се предоставят като уеб-услуги (web-services) и да осигуряват достатъчна мащабируемост и производителност за обслужване на синхронни заявки (sync pull) в реално време, с максимално време за отговор на заявки под 1 секунда за 95% от заявките, които не включват запитвания до регистри и външни системи. Изпълнителят трябва да обоснове прогнозирано натоварване на Системата и да предложи критерии за оценка на максимално допустимото време за отговор на машинна заявка. Критерият за оценка следва да се основава на анализ на прогнозираното натоварване и на наличния хардуер, който ще се използва. Изпълнителят трябва да представи обосновано предложение за минималното време за отговор на заявка на базата на посочените по-горе критерии и да осигури нужните условия за спазването му;

▪ Всички публични и служебни онлайн интерфейси трябва да бъдат реализирани с поддръжка на режими “push” и „pull”, в асинхронен и синхронен вариант – практическото прилагане на всяка от комбинациите трябва да бъде определено на етап бизнес-анализ и да бъдат съобразени реалните казуси (use cases), които всеки интерфейс обслужва;

▪ Трябва да се реализира интегриране на модул за разпределен кохерентен кеш (Distributed Caching) на „горещите данни“, които Системата получава и/или които се обменят през служебните онлайн интерфейси, като логиката на Системата трябва гарантира кохерентност (Cache Coherency) между кешираните данни и данните, съхранявани в базите данни;

▪ Да бъде предвидено създаването и поддържането на тестова среда, достъпна за използване и извършване на интеграционни тестове от разработчици на информационни системи, включително такива, изпълняващи дейности за други администрации или за бизнеса, с цел по-лесно и устойчиво интегриране на съществуващите и бъдещи информационни системи.

1.1.8. [не приложимо] Електронна идентификация на потребителите

В настоящия проект не се предвижда разработка или надграждане на публични електронни административни услуги.

▪ Електронната идентификация на всички потребители трябва да бъде реализирана в съответствие с изискванията на Регламент ЕС 910/2014 и Закона за електронната идентификация;

▪ Трябва да бъде реализирана интеграция с националната схема за електронна идентификация съгласно изискванията на Закона за електронната идентификация и действащите нормативни правила за оперативна съвместимост. За целта подсистемата за автентикация и оторизация на потребителите трябва да поддържа интеграция с външен доставчик на идентичност - в случая с Центъра за електронна идентификация към Държавна агенция „Електронно управление”. Реализацията на интеграцията трябва да бъде осъществена по стандартни протоколи SAML 2.0 и/или OpenID Connect;

▪ Процесът по регистрация на потребители трябва да бъде максимално опростен и бърз, но трябва да включва следните специфични стъпки:

- Визуализиране на информация относно стъпките по регистрация и информация във връзка с процеса за потвърждаване на регистрацията и активиране на потребителския профил. Съвети към потребителите за проверка

на настройките на имейл клиентите, свързани с блокиране на спам, и съвети за включване на домейна на Възложителя в "бял списък";

- Избор на потребителско име с контекстна валидация на полетата (in-line validation), включително и за избраното потребителско име;
- Избор на парола с контекстна валидация на полето (in-line validation) и визуализиране на сложността на паролата като "слаба", "нормална" и "силна";
- Реализиране на функционалност за потвърждение и активиране на регистрацията чрез изпращане на съобщение до регистрирания имейл адрес на потребителя с хипер-линк, с еднократно генериран токън с ограничена времева валидност за потвърждение на регистрацията. Възможност за последващо препращане на имейла за потвърждение, в случай че е бил блокиран от системата на потребителя.

▪ При реализиране на вход в Системата с удостоверение за електронна идентичност, по Националната схема за електронна идентификация, Системата трябва да използва потребителския профил, създаден в Системата за електронна идентификация, чрез интерфейси и по протоколи съгласно подзаконовата нормативна уредба към Закона за електронната идентификация. В случай че даден потребител има регистриран потребителски профил в Системата, който е създаден преди въвеждането на Националната схема за електронна идентификация, Системата трябва да предлага на потребителя възможност за "сливане" на профилите и асоцииране на локалния профил с този от Националната система за електронна идентификация. Допустимо е Системата да поддържа и допълнителни данни и метаданни за потребителите, но само такива, които не са включени като реквизити в централизирания профил на потребителя в Системата за електронна идентификация.

▪ Системата трябва да се съобразява с предпочитанията на потребителите, дефинирани в потребителските им профили в Системата за електронна идентификация, по отношение на предпочитаните комуникационни канали и канали за получаване на нотификации.

1.1.9. [не приложимо] Отворени данни

Проектът е насочен към конкретна дейност и в обхвата му не попада изискване свързано с публикуване на данни по реда на ЗДОИ. В случай че по време на изпълнение на проекта (до етап разработка) бъдат определени данни по реда на ЗДОИ, които да се публикуват в машинно четим отворен формат долните изисквания са приложими:

▪ Трябва да бъде разработен и внедрен онлайн интерфейс за свободен публичен автоматизиран достъп до документите, информацията и данните в Системата (наричани заедно „данните”). Интерфейсът трябва да осигурява достъп до данните в машиночетим,

отворен формат, съгласно всички изисквания на Директива 2013/37/ЕС за повторна употреба на информацията в обществения сектор и на Закона за достъп до обществена информация;

- Трябва да бъде разработен и внедрен онлайн интерфейс за предоставяне на пространствени данни, в машинночетим, отворен формат и интеграция с Националния портал за достъп до пространствени данни, съгласно всички изисквания на Директива 2007/2/ЕО и Закона за достъп до пространствени данни. Трябва да се поддържат всички набори от данни, които са изискуеми по Директива 2007/2/ЕО и за които Възложителят се явява първичен администратор на данните;

- Да бъде предвидена разработката и внедряването на отворени онлайн интерфейси и практически механизми, които да улеснят търсенето и достъпа до данни, които са на разположение за повторна употреба, като например списъци с основни документи и съответните метаданни, достъпни онлайн и в машинночетим формат, както и интеграция с Портала за отворени данни https://data.egov.bg/, който съдържа връзки и метаданни за списъците с материали, съгласно изискванията на Закона за достъп до обществена информация (ЗДОИ);

- Трябва да се разработи и да се поддържа актуално публично описание на всички служебни и отворени интерфейси, отворените формати за данни, заедно с историята на промените в тях, в структуриран машинночетим формат;

- Трябва да се разработят процеси по предоставяне на данни в отворен, машинночетим формат заедно със съответните метаданни. Форматите и метаданните следва да съответстват на официалните отворени стандарти.

1.1.10. Формиране на изгледи

Потребителите на Системата трябва да получават разрези на информацията чрез филтриране, пренареждане и агрегиране на данните. Резултатът се представя чрез:

- Визуализиране на таблици;
- Графична визуализация на екран;
- Разпечатване на хартиен носител;
- Експорт на данни в един или в няколко от изброените формати – ODF, Excel, PDF, HTML, TXT, XML, CSV.

1.1.11. Администриране на Системата

Системата трябва да осигурява администриране на потребителите и правата за достъп чрез административен панел, с който администраторите на системата да създават профили, управляват, назначават, отнемат роли и права на потребителите

7.2. Нефункционални изисквания към информационната система

7.2.1. Авторски права и изходен код

▪ Всички компютърни програми, които се разработват за реализиране на Системата, трябва да отговарят на критериите и изискванията за софтуер с отворен код;

▪ Всички авторски и сродни права върху произведения, обект на закрила на Закона за авторското право и сродните му права, включително, но не само, компютърните програми, техният изходен програмен код, структурата и дизайнът на интерфейсите и базите данни, чието разработване е включено в предмета на поръчката, възникват за Възложителя в пълен обем без ограничения в използването, изменението и разпространението им и представляват произведения, създадени по поръчка на Възложителя съгласно чл. 42, ал. 1 от Закона за авторското право и сродните му права;

▪ Приложимите и допустими лицензи за софтуер с отворен код са:

- GPL (General Public License) 3.0
- LGPL (Lesser General Public License)
- AGPL (Affero General Public License)
- Apache License 2.0
- New BSD license
- MIT License
- Mozilla Public License 2.0
- EUPL (European Union Public License)

▪ Изходният код (Source Code), разработван по проекта, както и цялата техническа документация трябва да бъде бъдат публично достъпни онлайн като софтуер с отворен код от първия ден на разработка чрез използване на система за контрол на версиите и хранилището по глава шеста, раздел IV „Хранилище за изходен код“ от НОИИСРЕАУ;

▪ Да се изследва възможността резултатният продукт (Системата) да се изгради частично (библиотеки, пакети, модули) или изцяло на базата на съществуващи софтуерни решения, които са софтуер с отворен код. Когато е финансово оправдано, да се предпочита този подход пред изграждането на собствено софтуерно решение в цялост, от нулата. Избраният подход трябва да бъде детайлно описан в техническото предложение на участниците;

▪ Да бъде предвидено използването на Система за контрол на версиите и цялата информация за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, да бъде достъпна публично, онлайн, в реално време.

7.2.2. Системна и приложна архитектура

▪ Системата трябва да бъде реализирана като разпределена модулна информационна система. Системата трябва да бъде реализирана със стандартни технологии и да поддържа общоприети комуникационни стандарти, които ще гарантират съвместимост на Системата с бъдещи разработки. Съществуващите модули функционалности трябва да бъдат рефакторирани и/или надградени по начин, който да осигури изпълнението на настоящето изискване;

▪ Бизнес процесите и услугите трябва да бъдат проектирани колкото се може по-независимо с цел по-лесно надграждане, разширяване и обслужване. Системата трябва да е максимално параметризирана и да позволява настройка и промяна на параметрите през служебен (администраторски) потребителски интерфейс;

▪ Трябва да бъде реализирана функционалност за текущ мониторинг, анализ и контрол на изпълнението на бизнес процесите в Системата;

▪ При разработката, тестването и внедряването на Системата Изпълнителят трябва да прилага наложили се архитектурни (SOA, MVC или еквивалентни) модели и дизайн-шаблони, както и принципите на обектно ориентирания подход за разработка на софтуерни приложения;

▪ Системата трябва да бъде реализирана със софтуерна архитектура, ориентирана към услуги - Service Oriented Architecture (SOA);

▪ Взаимодействията между отделните модули в Системата и интеграциите с външни информационни системи трябва да се реализират и опишат под формата на уеб-услуги (Web Services), които да са достъпни за ползване от други системи в държавната администрация, а за определени услуги – и за гражданите и бизнеса; За всеки от отделните модули/функционалности на Системата следва да се реализират и опишат приложни програмни интерфейси – Application Programming Interfaces (API). Приложните програмни интерфейси трябва да са достъпни и за интеграция на нови модули и други вътрешни или външни системи;

▪ Приложните програмни интерфейси и информационните обекти задължително да поддържат атрибут за версия;

▪ Задължително наличие и използване на програмни интерфейси, изискуемите метаданни и атрибути за версия, достъпност за стари версии - минимум 24 месеца след публикуване на нова версия, съгласно изискването по чл. 14 и чл. 41 от НОИИСРЕАУ

- Версията на програмните интерфейси, представени чрез уеб-услуги, трябва да поддържа версията по един или няколко от следните начини:
    - Като част от URL-а
    - Като GET параметър
    - Като HTTP header (Accept или друг)
- За всеки отделен приложен програмен интерфейс трябва да бъде разработен софтуерен комплект за интеграция (SDK) на поне две от популярните развойни платформи (.NET, Java, PHP);
- Системата трябва да осигурява възможности за разширяване, резервиране и балансиране на натоварването между множество инстанции на сървъри с еднаква роля;
- При разработването на Системата трябва да се предвидят възможни промени, продиктувани от непрекъснато променящата се нормативна, бизнес и технологична среда. Основно изискване се явява необходимостта информационната система да бъде разработена като гъвкава и лесно адаптивна, като отчита законодателни, административни, структурни или организационни промени, водещи до промени в работните процеси;
- Изпълнителят трябва да осигури механизми за реализиране на бъдещи промени в Системата без промяна на съществуващия програмен код. Когато това не е възможно, времето за промяна, компилиране и пускане в експлоатация трябва да е сведено до минимум. Бъдещото развитие на Системата ще се налага във връзка с промени в правната рамка, промени в модела на работа на потребителите, промени във външни системи, интегрирани със Системата, отстраняване на констатирани проблеми, промени в модела на обслужване и др. Такива промени ще се извършват през целия период на експлоатация на Системата, включително и по време на гаранционния период;
- Архитектурата на Системата и всички софтуерни компоненти (системни и приложни) трябва да бъдат така подбрани и/или разработени, че да осигуряват работоспособност и отказоустойчивост на Системата, както и недискриминационно инсталиране (без различни условия за инсталиране върху физическа и виртуална среда) и опериране в продуктивен режим, върху виртуална инфраструктура, съответно върху Държавния хибриден частен облак (ДХЧО);
- [не приложимо] Част или всички компоненти на Системата ще бъдат разположени върху Държавния хибриден частен облак като среда за функциониране на информационната система;
- Изпълнителят трябва да проектира, подготви, инсталира и конфигурира като минимум следните среди за Системата: тестова, стейджинг, продуктивна;
- Системата трябва да бъде разгърната върху съответните среди (тестова за вътрешни нужди, тестова за външни нужди, стейджинг и продуктивна);

- Тестовата среда за външни нужди трябва да бъде създадена и поддържана като "Sandbox", така че да е достъпна за използване и извършване на интеграционни тестове от разработчици на информационни системи, включително такива, изпълняващи дейности за други администрации или бизнеса, с цел по-лесно и устойчиво интегриране на съществуващи и бъдещи информационни системи. Тестовата среда за външни нужди трябва да е напълно отделна от останалите среди и нейното използване не трябва да влияе по никакъв начин на нормалната работа на останалите среди или да създава каквито и да било рискове за информационната сигурност и защитата на личните данни;

- Мрежата на държавната администрация (EECM) ще бъде използвана като основна комуникационна среда и като основен доставчик на защитен Интернет капацитет (Clean Pipe) – изискванията на софтуерните компоненти по отношение на използвани комуникационни протоколи, TCP портове и пр. трябва да бъдат детайлно документирани от Изпълнителя, за да се осигури максимална защита от хакерски атаки и външни проникванията чрез прилагане на подходящи политики за мрежова и информационна сигурност от Възложителя в инфраструктурата на Държавния хибриден частен облак и EECM;

- В Техническото си предложение участникът трябва да опише добрите практики, които ще прилага по отношение на всеки аспект от системната и приложната архитектура на Системата;

- За търсене трябва да се използват системи за пълнотекстово търсене (например Solr, Elastic Search). Не се допуска използването на индекси за пълнотекстово търсене в СУБД;

- [не приложимо] Системата трябва да бъде разработена така, че да позволява използването ѝ от много различни институции (т.нар. multitenancy).

- Трябва да бъде създаден административен интерфейс, чрез който може да бъде извършвана конфигурацията на софтуера;

- Всеки обект в системата трябва да има уникален идентификатор;

- Записите в регистрите не трябва да подлежат на изтриване или на промяна, а всяко изтриване или промяна трябва да представлява нов запис.

7.2.3. Повторно използване (преизползване) на ресурси и готови разработки

Проектът следва максимално да преизползва налични публично достъпни инструменти, библиотеки и платформи с отворен код.

За реализацията на Системата следва да се използват в максимална степен софтуерни библиотеки и продукти с отворен код.

Подход за избор на отворени имплементации и продукти

За реализацията на дадена техническа функционалност обикновено съществуват множество отворени алтернативни проекти, които могат да се използват в настоящата Система. Участникът следва да представи базов списък със свободните компоненти и средства, които възнамерява да използва. Отворените проекти трябва да отговарят на следните критерии:

- За разработката им да се използва система за управление на версиите на кода и да е наличен механизъм за съобщаване на несъответствия и приемане на допълнения;
- Да имат разработена техническа документация за актуалната стабилна версия;
- Да имат повече от един активен програмист, работещ по развитието им;
- Да имат възможност за предоставяне на комерсиална поддръжка;
- Да нямат намаляваща от година на година активност;
- По възможност проектите да са подкрепени от организации с идеална цел, държавни или комерсиални организации;
- По възможност проектите да имат разработени unit tests с code coverage над 50%, а проектът да използва Continuous Integration (CI) подходи – build bots, unit tests run, регулярно използване на статични/динамични анализатори на кода и др.

Препоръчително е преизползването на проекти, финансирани със средства на Европейския съюз, както и на такива, в които Участникът има активни разработчици. Използването на closed source и на инструменти, библиотеки, продукти и системи с платен лиценз става за сметка на Изпълнителя, като е допустимо в случаите, когато липсва подходяща свободна алтернатива с необходимата функционалност или тя не отговаря на горните условия.

Изпълнителят трябва да осигури поддръжка от комерсиална организация, развиваща основните отворени продукти, които ще бъдат използвани като минимум за операционните системи и софтуерните продукти за управление на базите данни.

Подход за работа с външните софтуерни ресурси

При използването на свободни имплементации на софтуерни библиотеки е необходимо да се организира копие (fork) на съответното хранилище в общото хранилище за проекти с отворен код, финансирани с публични средства в България (https://git.egov.bg/explore/projects). Използващите свободните библиотеки компоненти задават за "upstream repo" хранилищата в областта governmentbg, като задължително се реферира използваната версия/commit identificator.

Когато се налага промяна в изходния код на използван софтуерен компонент, промените трябва да се извършват във fork хранилището на governmentbg в съответствие с изискванията на основния проект. Изпълнителят трябва да извърши необходимите действия за включване на направените промени в основния проект чрез "pull requests" и извършване на необходимите изисквани от разработчиците на основния проект промени до приемането им. Тези дейности трябва да бъдат извършвани по време на целия проект.

При установяване на наличие на нови версии на използваните проекти се извършва анализ на влиянието върху настоящата система. В случаите, при които се оптимизира използвана

функционалност, отстраняват се пропуски в сигурността, стабилността или бързодействието, новата версия се извлича и използва след успешното изпълнение на интеграционните тестове.

7.2.4. Изграждане и поддръжка на множество среди

Изпълнителят трябва да изгради и да поддържа минимум следните логически разделени среди:

Среда	Описание
Development	Чрез Development средата се осигурява работата по разработката, усъвършенстването и развитието на Системата. В тази среда са налични и допълнителните софтуерни системи и инсталации, необходими за управление на разработката – continuous integration средства, системи за автоматизирано тестване и др.
Staging	Чрез Staging средата се извършват тестове преди разгръщане на нова версия от Development средата върху Production средата. В нея се извършват всички интеграционни тестове, както и тестовете за натоварване.
Sandbox Testing	Чрез Sandbox средата всички, които трябва да се интегрират към Системата, могат да тестват интеграцията си, без да застрашават работата на продукционната среда.
Production	Това е средата, която е публично достъпна за реална експлоатация и интеграция със съответните външни системи и услуги.

Управлението на средите трябва да става чрез автоматизирана система за провизиране и разгръщане на системните компоненти. При необходимост от страна на Възложителя Изпълнителят трябва да съдейства за изграждането на нови системни среди.
Участникът може да предложи изграждането на допълнителни среди според спецификите на предложеното решение.

7.2.5. Процес на разработка, тестване и разгръщане

Процесите, свързани с развитието на Системата, трябва да гарантират висока прозрачност и възможност за обществен контрол над всички разработки по проекта. Изграждането на доверие в гражданите и в бизнеса налага радикално по-висока публичност и прозрачност чрез отворена разработка и публикуването на системите компоненти под отворен лиценз от самото начало на разработката. По този начин гражданите биха могли да съдействат в процесите по развитие и тестване на разработките през целия им жизнен цикъл.

Всички софтуерни приложения, системи, подсистеми, библиотеки и компоненти, които са необходими за реализацията на Системата, трябва да бъдат разработвани като софтуер с отворен код и да бъдат достъпни в публично хранилище. Към настоящия момент следва да се използва общото хранилище за проекти с отворен код, финансирани с публични средства в България (https://git.egov.bg/explore/projects).

В случай че върху част от компонентите, нужни за компилация, има авторски права, те могат да бъдат или в отделно хранилище с подходящия за това лиценз или за тях трябва да бъде предоставен заместващ „mock up“ компонент, така че да не се нарушава компилацията на проекта.

Трябва да се анализират възможностите за включване на граждани в процесите по разработка, тестване и идентифициране на пропуски на софтуера. Участникът трябва да предложи механизъм и процедури за реализирането на такива процеси.

За всеки един разработван компонент Изпълнителят трябва да покрие следните изисквания за гарантиране на качеството на извършваната разработка и на крайния продукт:

- Документиране на Системата в изходния код, минимум на ниво процедура/функция/клас;
- Покритие на минимум 50% от изходния код с функционални тестове *[в случай на надграждане на съществуваща система – 50% от новата функционалност и 20% от съществуващата]*;
- Използване на continuous integration практики;
- Използване на dependency management.

Участникът трябва да опише детайлно подхода си за покриване на изискванията.

Във всеки един компонент на Системата, който се build-ва и подготвя за инсталация (deployment), е необходимо да присъстват следните реквизити:

- Дата и час на build;
- Място/среда на build;
- Потребител извършил/стартирал build процеса;
- Идентификатор на ревизията от кодовото хранилище на компонента, срещу която се извършва build-ът.

7.2.6. Бързодействие и мащабируемост

7.2.6.1 Контрол на натоварването и защита от DoS/DDoS атаки

▪ Системата трябва да поддържа на приложно ниво "Rate Limiting" и/или "Throttling" на заявки от един и същ клиентски адрес както към страниците с уеб-съдържание, така и по отношение на заявките към приложните програмни интерфейси, достъпни публично или служебно като уеб-услуги (Web Services) и служебни интерфейси.

▪ Системата трябва да позволява конфигуриране от страна на администраторите на лимитите за отделни страници, уеб-услуги и ресурси, които се достъпват с отделен URL/URI.

▪ Системата трябва да поддържа възможност за конфигуриране на различни лимити за конкретни автентикирани потребители (напр. системи на други администрации) и трябва да предоставя възможност за генериране на справки и статистики за броя заявки по ресурси и услуги.

7.2.6.2 Кохерентно кеширане на данни и заявки

▪ Отделните информационни системи, подсистеми и интерфейси трябва да бъдат проектирани и да използват системи за разпределен кохерентен кеш в случаите, в които това би довело до подобряване на производителността и мащабируемостта, чрез спестяване на заявки към СУБД или файловите системи на сървърите.

▪ Изпълнителят трябва да опише детайлно подхода и използваните механизми и технологии за реализация на разпределения кохерентен кеш, както и системните компоненти, които ще използват разпределения кеш;

▪ Разпределеният кохерентен кеш трябва да поддържа възможност за компресия на подходящите за това данни – например тези от текстов тип; компресирането на данни може да бъде реализирано и на приложно ниво;

▪ Използваният алгоритъм за създаване на ключове за съхранение/намиране на данни в кеша не трябва да допуска колизии и трябва оптимално да използва процесорните ресурси за генериране на хешове;

▪ Изпълнителят трябва да подбере подходящи софтуерни решения с отворен код за реализиране на буфериране и кеширане на данните в оперативната памет на сървърите. В зависимост от конкретните приложни случаи (Use Cases) е допустимо да се използват и внедрят различни технологии, които покриват по-добре конкретните нужди – например решения като Memcached или Redis в комбинация с Redis GeoAPI могат да осигурят порядъци по-висока мащабируемост и производителност за често достъпвани оперативни данни, номенклатурни данни или документи;

Като минимум разпределен кохерентен кеш трябва да се предвиди при:

▪ Извличане на информация от номенклатури и атомични данни за статус и актуално състояние на партиди от регистри в информационните системи;

▪ Извличане на информация от предефинирани периодични справки;

▪ Информация от лога на транзакциите при достъп с електронно-ИД до дадена услуга;

▪ Информация за извършените плащания;

▪ Други, които са идентифицирани на етап бизнес и системен анализ.

От кеша следва да бъдат изключени прикачени файлове и големи по обем резултати от справки.

7.2.6.3 Бързодействие

▪ При визуализация на уеб-страници системите трябва да осигуряват висока производителност и минимално време за отговор на заявки - средното време за заявка трябва да бъде по-малко от 1 секунда, с максимум 1 секунда стандартно отклонение за 95% от заявките, без да се включва мрежовото времезакъснение (Network Latency) при транспорт на пакети между клиента и сървъра.

▪ Трябва да бъдат създадени тестове за натоварване.

7.2.6.4 Използване на HTTP/2

С оглед намаляване на служебния трафик, времената за отговор и натоварването на сървърите следва да се използва HTTP/2 протокол при предоставяне на публични потребителски интерфейси с включени като минимум следните възможности:

▪ Включена header compression;

▪ Използване на brotli алгоритъм за компресия;

▪ Включен HTTP pipelining;

▪ HTTP/2 Server push, приоритизиращ специфични компоненти, изграждащи страниците (CSS, JavaScript файлове и др.);

▪ Публичните потребителски интерфейси трябва да поддържат адаптивен избор на TLS cipher suites според вида на процесорната архитектура на клиентското устройство - AES-GCM за x86 работни станции и преносими компютри (с налични AES-NI CPU разширения), и ChaCha20/Poly1305
за мобилни устройства (основно базирани на ARM процесори);

▪ Ако клиентският браузър/клиент не поддържа HTTP/2, трябва да бъде предвиден fall-back механизъм към HTTP/1.1. Тази възможност трябва да може лесно да се реконфигурира в бъдеще и да отпадне, когато браузърите/клиентите, неподдържащи HTTP/2, станат незначителен процент.

7.2.6.5 Подписване на документи

▪ При реализацията на електронно подписване с всички видове електронен подпис трябва да се подписва сигурен хеш-ключ, генериран на базата на образа/съдържанието, а не да се подписва цялото съдържание.

▪ Минимално допустимият алгоритъм за хеширане, който трябва да се използва при електронно подписване, е SHA-256. В случаите, в които не се подписва уеб съдържание (например документи, файлове и др.), е необходимо да се реализира поточно хеширане, като се избягва зареждането на цялото съдържание в оперативната памет.

▪ Системата трябва да поддържа подписване на електронни изявления и електронни документи и с електронни подписи, издадени от Доставчици на доверителни услуги в ЕС,

които отговарят на изискванията за унифициран профил на електронните подписи, съгласно подзаконовите правила към Регламент ЕС 910/2014, които влизат в сила и са задължителни от 1 януари 2017 г.;

▪ Трябва да бъдат анализирани техническите възможности за реализиране на подписване на електронни изявления и документи без използване на Java аплет и без да се изисква от потребителите да инсталират Java Runtime, като по този начин се осигури максимална съвместимост на процеса на подписване с всички съвременни браузъри. Такава реализация може да бъде осъществена чрез:

▪ използване на стандартни компоненти с отворен код, отговарящи на горните условия, които са разработени по други проекти на държавната администрация и са достъпни в хранилището, поддържано от Министерство на електронното управление – при наличие на такива компоненти в хранилището те трябва да се преизползват и само да бъдат интегрирани в Системата;

▪ използване на плъгин-модули с отворен код, достъпни за най-разпространените браузъри (Browser Plug-ins), които са адаптирани и поддържат унифицираните профили на електронните подписи, издавани от ДДУ в ЕС, и съответните драйвери за крайни устройства за четене на сигурни носители или по стандартизиран в националната нормативна уредба протокол за подписване извън браузъра;

▪ чрез интеграция с услуги за отдалечено подписване, предлагани от доставчици на доверителни услуги в ЕС.

7.2.6.6 Качество и сигурност на програмните продукти и приложенията

▪ Да бъде предвидено спазването на добри практики на софтуерната разработка – покритие на изходния код с тестове – над 60%, документиране на изходния код, използване на среда за непрекъсната интеграция (Continuous Integration), възможност за компилиране и пакетиране на продукта с една команда, възможност за инсталиране на нова версия на сървъра с една команда, система за управление на зависимостите (Dependency Management);

▪ Публичните модули, които ще предоставят информация и електронни услуги в Интернет, трябва да отговарят на актуалните уебстандарти за визуализиране на съдържание.

7.2.7. Информационна сигурност и интегритет на данните

▪ Не се допуска съхранението на пароли на администратори, на вътрешни и външни потребители и на акаунти за достъп на системи (ако такива се използват) в явен вид. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми (напр. BCrypt, PBKDF2,

scrypt (RFC 7914) за съхранение на пароли и където е възможно, да се използва и прозрачно криптиране на данните в СУБД със сертификати (transparent data-at-rest encryption);

▪ Да бъде предвидена система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата;

▪ Не се допуска използването на Self-Signed сертификати за публични услуги;

▪ Всички уебстраници (вътрешни и публично достъпни в Интернет) трябва да бъдат достъпни единствено и само през протокол HTTPS. Криптирането трябва да се базира на сигурен сертификат с валидирана идентичност (Verified Identity), позволяващ задължително прилагане на TLS 1.2, който е издаден от удостоверителен орган, разпознаван от най-често използваните браузъри (Microsoft Internet Explorer, Google Chorme, Mozilla Firefox). Ежегодното преиздаване и подновяване на сертификата трябва да бъде включено като разходи и дейности в гаранционната поддръжка за целия срок на поддръжката;

▪ Трябва да бъдат извършени тестове за сигурност на всички уебстраници, като минимум чрез автоматизираните средства на SSL Labs за изпитване на сървърна сигурност (https://www.ssllabs.com/ssltest/). За нуждите на автентикация с КЕП трябва да се предвиди имплементирането на обратен прокси сървър (Reverse Proxy) с балансиране на натоварването, който да препраща клиентските сертификати към вътрешните приложни сървъри с нестандартно поле (дефинирано в процеса на разработка на Системата) в HTTP Header-а. Схемата за проксиране на заявките трябва да бъде защитена от Spoofing;

▪ Като временна мярка за съвместимост настройките на уебсървърите и Reverse Proxy сървърите трябва да бъдат балансирани така, че Системата да позволява използване и на клиентски браузъри, поддържащи по-стария протокол TLS 1.1. Това изключение от общите изисквания за информационна сигурност не се прилага за достъпа на служебни потребители от държавната администрация и доставчици на обществени услуги, които имат служебен достъп до ресурси на Системата;

▪ При разгръщането на всички уебуслуги (Web Services) трябва да се използва единствено протокол HTTPS със задължително прилагане на минимум TLS 1.2;

▪ Програмният код трябва да включва методи за автоматична санитизация на въвежданите данни и потребителски действия за защита от злонамерени атаки, като минимум SQL инжекции, XSS атаки и други познати методи за атаки, и да отговаря, където е необходимо, на Наредбата за минималните изисквания за мрежова и информационна сигурност;

▪ При проектирането и разработката на компонентите на Системата и при подготовката и разгръщането на средите трябва да се спазват последните актуални препоръки на OWASP (Open Web Application Security Project);

▪ Трябва да бъде изграден модул за проследимост на действия и събития в Системата. За всяко действие (добавяне, изтриване, модификация, четене) трябва да съдържа следните атрибути:

- Уникален номер;
- Точно време на възникване на събитието;
- Вид (номенклатура от идентификатори за вид събитие);
- Данни за информационна система, където е възникнало събитието;
- Име или идентификатор на компонент в информационната система, регистрирал събитието;
- Приоритет;
- Описание на събитието;
- Данни за събитието.

▪ Астрономическото време за удостоверяване настъпването на факти с правно или техническо значение се отчита с точност до година, дата, час, минута, секунда и при технологична необходимост - милисекунда, изписани в съответствие със стандарта БДС ISO 8601:2006;

▪ Астрономическото време за удостоверяване настъпването на факти с правно значение и на такива, за които се изисква противопоставимост, трябва да бъде удостоверявано с електронен времеви печат по смисъла на Глава III, Раздел 6 от Регламент ЕС 910/2014. Трябва да бъде реализирана функционалност за получаване на точно астрономическо време, отговарящо на горните условия, и от доставчик на доверителни услуги или от държавен орган, осигуряващ такава услуга, отговаряща на изискванията на RFC 3161;

▪ Трябва да бъдат проведени тестове за проникване (penetration tests), с които да се идентифицират и коригират слаби места в сигурността на Системата.

7.2.8. Използваемост

7.2.8.1 Общи изисквания за използваемост и достъпност

▪ При проектирането и разработката на софтуерните компоненти и потребителските интерфейси трябва да се спазват стандартите за достъпност на потребителския интерфейс за хора с увреждания WCAG 2.0, съответстващ на ISO/IEC 40500:2012;

▪ Спецификацията да отговаря на изискванията за достъпността на Интернет страници и мобилни приложения, съгласно хармонизирания стандарт EN 301 549 V2.1.2 (2018-08) - касаещ достъпността на продукти и услуги в сферата на ИКТ, освен в случаите по чл. 58в, ал. 2 или 3 от ЗЕУ

▪ Всички ресурси трябва да са достъпни чрез GET заявка на уникален адрес (URL). Не се допуска използване на POST за достигане до формуляр за подаване не заявление, за генериране на справка и други;

▪ Функционалностите на потребителския интерфейс на Системата трябва да бъдат независими от използваните от потребителите интернет браузъри и устройства, при условие че последните са версии в период на поддръжка от съответните производители. Трябва да бъде осигурена възможност за ползване на публичните модули на приложимите услуги през мобилни устройства – таблети и смарт-телефони, чрез оптимизация на потребителските интерфейси за мобилни устройства (Responsive Design);

▪ Не се допуска използване на Капча (Captcha) като механизъм за ограничаване на достъпа до документи и/или услуги. Алтернативно, Системата трябва да поддържа "Rate Limiting" и/или "Throttling" съгласно изискванията в т. ***7.1.1.*** от настоящите изисквания. Допуска се използването на Captcha единствено при иденетифицирани много последователни опити от предполагаем „бот“;

▪ Трябва да бъде осигурен бърз и лесен достъп до електронните услуги и те да бъдат промотирани с подходящи навигационни елементи на публичната интернет страница – банери, елементи от главното меню и др.;

▪ Публичните уеб страници на Системата трябва да бъдат проектирани и оптимизирани за ефективно и бързо индексиране от търсещи машини с цел популяризиране сред потребителите и по-добра откриваемост при търсене по ключови думи и фрази. При разработката на страниците и при изготвяне на автоматизираните процедури за разгръщане на нова версия на Системата трябва да се използват инструменти за минимизиране и оптимизация на размера на изходния код (HTML, JavaScript и пр.) с оглед намаляване обема на файловете и по-бързо зареждане на страниците;

▪ Не се допуска използването на HTML Frames, за да не се пречи на оптимизациите за търсещи машини;

▪ При разработката на публични уеббазирани страници трябва да се използват и да се реализира поддръжка на:

- Стандартните семантични елементи на HTML5 (HTML Semantic Elements);
- JSON-LD 1.0 (http://www.w3.org/TR/json-ld/);
- Open Graph Protocol (http://ogp.me) за осигуряване на поддръжка за качествено споделяне на ресурси в социални мрежи и мобилни приложения;

▪ В екранните форми на Системата трябва да се използват потребителски бутони с унифициран размер и лесни за разбиране текстове в еднакъв стил.

- Всички текстови елементи от потребителския интерфейс трябва да бъдат визуализирани с шрифтове, които са подходящи за изобразяване на екран и които осигуряват максимална съвместимост и еднакво възпроизвеждане под различни клиентски операционни системи и браузъри. Не се допуска използването на серифни шрифтове (Serif).

- Полета, опции от менюта и командни бутони, които не са разрешени конкретно за ролята на влезлия в системата потребител, не трябва да са достъпни за този потребител. Това не отменя необходимостта от ограничаване на достъпа до бизнес логиката на приложението чрез декларативен или програмен подход.

- Всяка екранна форма трябва да има наименование, което да се изписва в горната част на екранната форма. Наименованията трябва да подсказват на потребителя какво е предназначението на формата.

- Всички търсения трябва да са нечувствителни към малки и главни букви.

- Полетата за пароли трябва задължително да различават малки и главни букви.

- Полетата за потребителски имена трябва да позволяват използване на имейл адреси като потребителско име, включително да допускат всички символи, регламентирани в RFC 1123, за наименуването на хостове;

- Главните и малките букви на въвежданите данни се запазват непроменени, не се допуска Системата да променя капитализацията на данните, въвеждани от потребителите.

- Системата трябва да позволява въвеждане на данни, съдържащи както български, така и символи на официалните езици на ЕС.

- Наименованията на полетата следва да са достатъчно описателни, като максимално се доближават до характера на съдържащите се в тях данни.

- Системата трябва да поддържа прекъсване на потребителски сесии при липса на активност. Времето трябва да може да се променя от администратора на системата без промяна в изходния код. Настройките за време за прекъсване на неактивни сесии трябва да включват и възможността администраторите да дефинират стилизирана страница с информативно съобщение, към която Системата да пренасочва автоматично браузърите на потребителите в случай на прекъсната сесия;

- Дългите списъци с резултати трябва да се разделят на номерирани страници с подходящи навигационни елементи за преминаване към предишна, следваща, първа и последна страница, към конкретна страница. Навигационните елементи трябва да са логически обособени и свързани със съответния списък и да се визуализират в началото и в края на HTML контейнера, съдържащ списъка;

- За големите йерархически категоризации трябва да се предвиди възможност за навигация по нива или чрез отложено зареждане (lazy load).

7.2.8.2 Интернационализация

▪ Системата трябва да може да съхранява и едновременно да визуализира данни и съдържание, което е въведено/генерирано на различни езици;

▪ Всички софтуерни компоненти на Системата, използваните софтуерни библиотеки и развойни комплекти, приложните сървъри и сървърите за управление на бази данни, елементите от потребителския интерфейс, програмно-приложните интерфейси, уебуслугите и др. трябва да поддържат стандартно и да са конфигурирани изрично за спазване на минимум Unicode 5.2 стандарт при съхранението и обработката на текстови данни, съответно трябва да се използва само UTF-8 кодиране на текстовите данни.

▪ Всички публично достъпни потребителски интерфейси следва да поддържат многоезичност, като минимум български и английски език.

▪ Публичната част на Системата трябва да бъде разработена и да включва набори с текстове на минимум два официални езика в ЕС, а именно български и английски език. Преводите на английски език трябва да бъдат осъществени професионално, като не се допуска използването на средства за машинен превод без ръчна проверка и корекции от професионални преводачи.

▪ Версиите на съдържанието на съответните езици трябва да включват всички текстове, които се визуализират във всички елементи на потребителския интерфейс, справките, генерираните от системата електронни документи, съобщения, нотификации, имейл съобщения, номенклатурите и таксономиите и др. Данните, които се съхраняват в Системата само на български език, се изписват/визуализират на български език;

▪ Системата трябва да позволява превод на всички многоезични текстове с подходящ потребителски интерфейс, достъпен за администратори на Системата, без промени в изходния код. Модулът за превод на текстове, използвани в Системата, трябва да поддържа и контекстни референции, които да позволяват на администраторите да тестват и да проверяват бързо и лесно направените преводи и тяхната съгласуваност в реалните екрани, страници и документи;

▪ Публичната част на Системата трябва да позволява превключване между работните езици на потребителския интерфейс в реално време от профила на потребителя и от подходящ, видим и лесно достъпен навигационен елемент в горната част на всяка страница, който включва не само текст, но и подходяща интернационална икона за съответния език;

▪ При визуализация на числа трябва да се използва разделител за хиляди (интервал).

▪ При визуализация на дати и точно време в елементи от потребителския интерфейс в генерирани справки или в електронни документи всички формати за дата и час трябва да са съобразени с избрания от потребителя език/локация в настройките на неговия профил:

- За България стандартният формат е „DD.MM.YYYY HH:MM:SS”, като наличието на време към датата е в зависимост от вида на визуализираната информация и бизнес-смисъла от показването на точно време;
- Системата трябва да поддържа и всички формати съгласно ISO БДС 8601:2006;

7.2.8.3 Изисквания за използваемост на потребителския интерфейс

▪ Електронните форми за подаване на заявления и за обявяване на обстоятелства трябва да бъдат реализирани с AJAX или с аналогична технология, като по този начин се гарантират следните функционалности:

- Контекстна валидация на въвежданите данни на ниво "поле" от форма и контекстни съобщения за грешка/невалидни данни в реално време;
- Възможност за избор на стойности от номенклатури чрез търсене в списък по част от дума (autocomplete) и визуализиране на записи, отговарящи на въведеното до момента, без да е необходимо пълните номенклатури да са заредени в браузъра на клиента и потребителят да скорлира дълги списъци с повече от 10 стойности;

▪ В електронните форми трябва да бъде реализирана валидация на въвежданите от потребителите данни на ниво "поле" (in-line validation). Валидацията трябва да се извършва в реално време на сървъра, като при успешна валидация данните от съответното поле следва да бъдат запазени от сървъра;

▪ Системата трябва да гарантира, че въведените, валидираните и запазените от сървъра данни остават достъпни за потребителите дори за процеси, които не са приключили, така че при волно, неволно или автоматично прекъсване на потребителската сесия поради изтичане на периода за допустима липса на активност потребителят да може да продължи съответния процес след повторно влизане в системата, без да загуби въведените до момента данни и прикачените до момента електронни документи;

▪ Трябва да бъде реализирана възможност за добавяне и редактиране от страна на администраторите на Системата, без да са необходими промени в изходния код, на контекстна помощна информация за:

- всяка електронна форма или стъпка от процес, за която има отделен екран/форма;
- всяка група полета за въвеждане на данни (в случаите, в които определени полета от формата са групирани тематично);
- всяко отделно поле за въвеждане на данни;

▪ Трябва да бъде разработена контекстна помощна информация за всички процеси, екрани и електронни форми, включително ясни указания за попълване и разяснения за особеностите при попълване на различните групи полета или на отделни полета;

▪ Контекстната помощна информация, указанията към потребителите и информативните текстове за всяка електронна административна услуга не трябва да съдържат акроними, имена и референции към нормативни документи, които са въведени като обикновен текст (plain-text). Всички акроними, референции към нормативни документи, формуляри, изисквания и др. трябва да бъдат разработени като хипервръзки към съответните актуални версии на нормативни документи и/или към съответния речник/списък с акроними и термини;

▪ Достъпът на потребителя до контекстната помощна информация трябва да бъде реализиран по унифициран и консистентен начин чрез подходящи навигационни елементи, като например чрез подходящо разположени микро-бутони с икони, разположени до/пред/след етикета на съответния елемент, за който се отнася контекстната помощ, или чрез обработка на "Mouse Hover/Mouse Over" събития;

▪ При проектирането и реализацията на потребителския интерфейс трябва да се отчете, че той трябва да бъде еднакво използваем и от мобилни устройства (напр. таблети), които не разполагат с мишка, но имат чувствителни на допир екрани.

▪ Потребителският интерфейс следва да бъде достъпен за хора с увреждания съгласно изискванията на чл. 48, ал. 5 от ЗОП.

7.2.8.4 Изисквания за използваемост в случаи на прекъснати бизнес процеси

▪ Системата трябва да съхранява перманентно всеки започнал процес/процедура по подаване на заявление или обявяване на обстоятелства, текущия му статус и всички въведени данни и прикачени документи дори ако потребителят е прекъснал волно или неволно потребителската си сесия;

▪ При вход в системата потребителят трябва да получава прегледна и ясна нотификация, че има започнати, но недовършени/неизпратени/неподписани заявления, и да бъде подканен да отвори модула за преглед на историята на транзакциите;

▪ Модулът за преглед на историята на транзакциите трябва да поддържа следните функционалности:

- Да визуализира списък с историята на подадените заявления, като минимум със следните колони – дата, входящ номер, код на тупа формуляр, подател (име на потребител и имена на физическото лице - подател), статус на заявлението;
- Да предлага видни и лесни за използване от потребителите контроли/инструменти:

- за филтриране на списъка (от дата до дата, за предефинирани периоди, като "последния един месец", "последната една година";
- сортиране на списъка по всяка от колоните, без това да премахва текущия филтър;
- свободно търсене по ключови думи по всички колони в списъка и метаданните на прикачените/свързаните документи със заявленията, което да води до динамично филтриране на списъка.

7.2.8.5 Изисквания за проактивно информиране на потребителите

▪ За всички публични интернет страници трябва да бъде реализирана функционалност за публикуване на всяко периодично обновявано съдържание (новини, обявления, обществени поръчки, отворени работни позиции, нормативни документи, отговори по ЗДОИ и др.) в стандартен формат (RSS 2.x, Atom или еквивалент), както и поддържането на публично достъпни статистики за посещаемостта на страницата;

▪ Системата трябва да поддържа възможност за автоматично генериране на електронни бюлетини, които да се разпращат периодично или при настъпване на събития по електронна поща до регистрираните в Системата потребители, които са заявили или са се съгласили да получават такива бюлетини; Потребителите трябва да имат възможност да настройват предпочитанията през потребителския си профил в Системата.

7.2.9. Системен журнал

Изграждането решение задължително трябва да осигурява проследимост на действията на всеки потребител (одит), както и версия на предишното състояние на данните, които той е променил в резултат на своите действия (системен журнал).

Атрибутите, които трябва да се запазват при всеки запис, трябва да включват като минимум следните данни:

- дата/час на действието;
- модул на системата, в който се извършва действието;
- действие;
- обект, над който е извършено действието;
- допълнителна информация;
- IP адрес и браузър на потребителя.

Размерът на журнала на потребителските действия нараства по време на работа на всяка система, което налага по-различното му третиране от гледна точка на организация на базата данни:

- по време на работа на Системата потребителският журнал трябва да се записва в специализиран компонент, който поддържа много бързо добавяне на записи; този подход се налага, за да не се забавя излишно работата на Системата;

- специална фонова задача трябва да акумулира записаните данни и да ги организира в отделна специално предвидена за целта база данни, отделна от работната база данни на Системата;

- данните в специализираната база данни трябва да се архивират и изчистват, като в специализираната база данни трябва да бъде достъпна информация за не повече от 2 месеца назад; при необходимост от информация за предишен период администраторът на Системата трябва първо да възстанови архивните данни;

- трябва да бъде предоставен достъп до системния журнал на органите на реда чрез потребителски или програмен интерфейс; за достъпа трябва да се изисква електронна идентификация.

7.2.10. Дизайн на бази данни и взаимодействие с тях

При използване на база данни (релационна или нерелационна(NoSQL) следва да бъдат следвани добрите практики за дизайн и взаимоедйствие с базата данни, в т.ч.:

- дизайнът на схемата на базата данни (ако има такава) трябва да бъде с максимално ниво на нормализация, освен ако това не би навредило сериозно на производителността;

- базата данни трябва да може да оперира в клъстър; в определени случаи следва да бъде използван т.нар. sharding;

- имената на таблиците и колоните трябва да следват унифицирана конвенция;

- трябва да бъдат създадени индекси по определени колони, така че да се оптимизират най-често използваните заявки; създаването на индекс трябва да е мотивирано и подкрепено със замервания;

- връзките между таблици трябва да са дефинирани чрез foreign key;

- периодично трябва да бъде правен анализ на заявките, включително чрез EXPLAIN (при SQL бази данни), и да бъдат предприети мерки за оптимизиране на бавните такива;

- задължително трябва да се използват транзакции, като нивото на изолация трябва да бъде мотивирано в предадената документация;

- при операции върху много записи (batch) следва да се избягват дългопродължаващи транзакции;

- заявките трябва да бъдат ограничени в броя записи, които връщат;

- при използване на ORM или на друг слой на абстракция между приложението и базата данни, трябва да се минимизира броят на излишните заявки (т.нар. n+1 selects проблем);

▪ при използване на нерелационна база данни трябва да се използват по-бързи и компактни протоколи за комуникация, ако такива са достъпни.

7.2.11. Изисквания по отношение на киберсигурност в съответствие с чл. 12, ал. 1 от НМИМИС

С цел достигане на изискваното ниво на сигурност на информацията, в мрежите и информационните системи следва да се предвидят следните изисквания:

▪ Да бъдат включени адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване.

▪ Да се представят анализ и оценка на риска, които да послужат като основа за включването на адекватни и комплексни изисквания за мрежова и информационна сигурност?

▪ Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика.

▪ Да се използва отделна, изолирана от другите информационни и комуникационни системи и от интернет, подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуникационните системи и техните компоненти. Тази среда трябва да не се използва за други цели.

▪ Да се валидират всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на браузъра, като headers на препращащия и потребителски агент;

▪ Всички данни да бъдат кодирани с HTML, изпращани от клиента и показвани в уеб страница;

▪ Да се ограничават заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по URL;

▪ Да се конфигурира типът и размерът на headers, които уеб сървърът ще приеме;

▪ Да се ограничава времетраенето на връзката (connection Timeout) - времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, както и минималният брой байтове в секунда при изпращане на отговор на заявка:

▪ Да се въведе ограничение на броя неуспешни опити за влизане в системата;

▪ Да не се допуска извеждането на списък на уеб директориите;

▪ Бисквитките (cookies) задължително да имат:

▪ флаг за защита (security flag), който инструктира браузъра, че „бисквитката“ може да бъде достъпна само чрез защитени SSL канали;

▪ флаг HTTP only, който инструктира браузъра, че „бисквитката“ може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента;

▪ Да се предвидят и предприемат мерки за защита на DNS, като задължително се прилага DNSSEC (Domain Name System Security Extensions); - не е приложимо – това е вътрешна система, а не публична.

▪ По отношение на системните записи (Logs) да бъдат предвидени следните възможности:

▪ в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;

▪ за всяко от тези събития в записите се отбелязва с астрономическото време, когато е настъпило събитието;

▪ да бъде предвидена възможност за синхронизиране на часовниците на компоненти на информационните и комуникационните системи, като се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен;

▪ да се предвиди как информацията ще бъде архивирана за срок не по-кратък от дванадесет месеца.

- Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.
- Във връзка с мрежовата и информационната сигурност на Възложителя/ МВнР и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

(а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Възложителя/МВнР ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Възложителя/МВнР. За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Възложителя/ МВнР, подписват декларации по образец на Възложителя за опазване на информацията, които се предават на Възложителя. При

промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до 2 (два) работни дни от промяната.

- Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на договора на трети страни без изричното писмено съгласие на Възложителя/ МВнР.
- При неспазване на изискванията за сигурност на информацията Изпълнителят дължи неустойка съгласно уговореното в договора.
- Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

(а) При изпълнението на задълженията си, осъществяват комуникация с лицата,

които ще имат достъп до системите на МВнР;

(б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на

Изпълнителя (и на подизпълнителите, когато е приложимо);

(в) При получена информация, лицата по чл. 10, ал. 2 от НМИМИС осъществяват

незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Възложителя/ МВнР;

(г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Възложителя/ МВнР, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на МВнР от страна на Възложителя и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.

8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА

8.1. Дейност Доставка, монтаж, инсталация, конфигурация, провеждане на обучение за служители на МВнР и гаранционна поддръжка на хардуерен модул за сигурност HSM – 2 бр., сървър за софтуер за генериране на видим цифрово подписан печат - 2 бр., специализиран софтуер за генериране на видим цифрово подписан печат - 2 бр., работна станция за наблюдение и управление на системата – 1 бр.

8.1.1. Описание на дейността

Дейността включва закупуване на следното:

- сървър за софтуер за генериране на видим цифрово подписан печат – 2 бр.
- Хардуерен модул за сигурност HSM – 2 бр.
- Специализиран софтуер за генериране на видим цифрово подписан печат – 2 бр.

8.1.2. Изисквания към изпълнение на дейността

МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

Сървър за софтуер за генериране на видим цифрово подписан печат – 2 бр.

Процесор: минимум 2 броя Intel® Xeon® Scalable, минимум 8 ядра на процесор, минимум 2.6 GHz, минимум 22.5 MB Cache или еквивалентен последна генерация.

Оперативна памет: поддръжка на 32 DDR5 DIMM слота, поддръжка на RDIMM /LRDIMM модули памет, разширяемост до минимум 8TB.

Системата да бъде доставена с 64GB RAM /5600 MT/s.

Дискова подсистема: сървърното шаси да има налични минимум 8 свободни слота за инсталиране да SAS/SATA/NVMe с форм фактор 2.5“. Да поддържа SAS/SATA/E3.S NVME Gen5. Да има възможност за надграждане с още 18 слота за SAS/SATA/NVMe с форм фактор 2.5“. Да има възможност за поставяне на специализиран модул, служещ за инсталиране на OS. Медиите на специализирания модул да поддържат хардуерен RAID и да не заемат от слотовете за SAS/SATA/E3.S NVME Gen5, както и да поддържат замяна при възникнал дефект без това да нарушава работата на сървъра. Да се достави с минимум 2 броя дискови устройства на специализираният модул с общо използваемо дисково пространство след RAID1 минимум 480GB.

Оптично устройство: вътрешно DVD±RW.

Разширяемост на системата: да разполага с 2 бр. OCP слота, 3 x PCIe Gen 5.0. Да се разширява общо до 8 бр. PCIe Gen 5.0.

Минимална свързаност:

• 4 x 1GbE BaseT порта;

• 1 x 10/100/1000Mbit/s за вграден IPMI контролер за отдалечено управление.

Вградени USB портове: минимум 5 USB порта.

Сървърното шаси да е с размер 2U и да се достави с необходимите компоненти и крепежни елементи за монтаж в стандартен 19” шкаф за сървърно оборудване, както и с телескопичен държач за кабели. Да бъде окомплектовано с всички необходими интерфейсни, мрежови и захранващи кабели за нормална експлоатация.

Захранване:

• Резервирано AC захранване;

• Заменяеми захранващи блокове по време на работа (hot-swap);

• Инсталирани минимум 2 (два) броя захранващи блокове с мощност минимум 1000W с 96% ефективност.

Функционални възможности на вградения IPMI контролер:

• HTML 5 отдалечена конзола;

• Agentless управление;

• Управление, верификация и възстановяване на Firmware;

• Прикачване на виртуална медия;

• Федерирано управление на множество IPMI контролери;

• Deployment and provisioning;

• Поддръжка на Redfish API, JSON, XML, PERL Scripting;

• Сигурност: RBAC, SSO, 2FA.

Да се достави със софтуер за управление, предоставящ следните възможности:

• Да поддържа над 10 000 сървъра;

• HTML 5 базиран интерфейс;

• Предупреждения за статуса на сървърния хардуер, базирани на Redfish събития;

• Поддръжка на REST API;

• Надстройки на Firmware/BIOS спрямо политики за съответствие;

• Профили и съвместимост на сървърни конфигурации;

• Bare-metal инсталации;

• Agent-free управление;

• Поддръжка на Single-sign-on (SSO) автентикация към IPMI контролерите за управление в сървърите и интеграция с LDAP/AD;

• Персонализирани отчети и информация за гаранционния статус на сървърите;

• Интеграция с VMware vCenter с поддръжка на актуализации на ОС, драйвери и фърмуер с VMware vSphere Lifecycle Manager (vLCM);

• Интеграция с Microsoft System Center и възможност за регистриране на липсващи предупреждения;

• Автоматично зониране/управление на SAN комутатори Cisco и Brocade.

Сигурност:

• TPM 2.0;

• Secure Boot;

• Secure erase;

• Immutable silicon root of trust;

• Runtime firmware validation;

• Encrypted virtual media.

Да бъде сертифициран за работа с минимум следните операционни системи:

• VMware ESXi;

• Microsoft Windows Server 2022;

• Canonical Ubuntu;

• Suse Linux Enterprise Server (SLES);

• RedHat Enterprise Linux (RHEL).

Да се достави с инсталирана операционна система Microsoft Windows Server 2019/2022 Standard, с лиценз за всички физически ядра на инсталираните процесори.

Гаранция и поддръжка от производителя на оборудването:

• Минимум 36 месеца от производителя, покритие 24x7;

• Време за реакция: до 4 часа.

Хардуерен модул за сигурност HSM – 2 бр.

Да поддържа и осигурява минимум следните програмируеми API интерфейси: PKCS#11, Java Cryptography Extension (JCE), Microsoft Crypto API (CSP), Microsoft

Cryptography Next Generation (CNG), Microsoft SQL Extensible Key Management (SQLEKM), OpenSSL, Cryptographic eXtended services Interface (CXI).

Да е сертифициран по следните стандарти: IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B, RoHS II, REACH .

Да поддържа като минимум следни криптографски алгоритми:

• RSA, DSA, ECDSA with NIST, Brainpool and FRP256v1 curves, EdDSA;

• DH, ECDH with NIST, Brainpool, FRP256v1 and Montgomery curves;

• AES, Triple-DES, DES;

• MAC, CMAC, HMAC;

• SHA-1, SHA-2, SHA-3, RIPEMD;

• Hash-based deterministic random number generator (DRG.4 acc. AIS 31/

NIST SP800-90B);

• True random number generator (PTG.2 acc. AIS 31).

Да разполага с минимум 2 (два) броя резервирани захранващи блока.

Да поддържа минимум 2 порта RJ45 по 1 Gb/s и възможност за разширение с 2 SFP+ порта по 10Gb/s или 2 порта RJ45 по 1Gb/s.

Да съхранява и защитава от фалшифициране секретните ключове.

Двата HSM да синхронизират секретните ключове по време на създаване.

Да осигурява поддръжка на следните операционни системи:

• Windows;

• Linux.

Да бъде окомплектован с всички необходими интерфейсни, мрежови и захранващи кабели за нормална експлоатация.

Да се достави с необходимите средства за инсталиране в стандартен 19” шкаф за сървърно оборудване.

Гаранция и поддръжка от производителя на оборудването:

• Минимум 36 месеца от производителя, покритие 24x7;

• Време за реакция: до 4 часа.

Специализиран софтуер за генериране на видим цифрово подписан печат – 2 бр.

Да е в архитектура „High availability“ (висока наличност) с 2 независими инстанции със синхронизиране на данните по между им и да е съобразен с предложения сървър по т. 1.

Да поддържа и осигурява минимум следните бази от данни:

• PostgreSQL;

• Oracle.

Да се интегрира с предложените HSM устройства по т. 2.

Да се интегрира с визовата система при използване на Web Service интерфейс (SOAP / REST).

Да приема заявка от визовата система за създаване на видим цифров печат (VDS) с данните за визата (например MRZ на пътника и валидност на визата).

Да кодира необходимите данни за визата и да подписва печата със съответния цифров сертификат от съхраняваните в HSM с последващо кодиране в 2D баркод DataMatrix.

Да бъде интегриран към системата за печатане на Виза бланката за изпращане на 2D баркода.

Да позволява проверка на цялостната коректност на локално генерираните баркодове.

Гаранция и поддръжка от производителя на оборудването:

• Минимум 36 месеца от производителя, покритие 24x7;

• Време за реакция: до 4 часа.

Изпълнителят следва да извърши доставка, монтаж, инсталиране и конфигуриране на предложеното оборудване и софтуер, както и да извърши онлайн обучение за работа с устройствата в рамките на 1 работен ден до 10 потребителя.

Оборудването, предмет на доставката, трябва да бъде фабрично ново и неупотребявано.

8.1.3. Очаквани резултати

Закупени:

- сървър за софтуер за генериране на видим цифрово подписан печат – 2 бр.
- Хардуерен модул за сигурност HSM – 2 бр.
- Специализиран софтуер за генериране на видим цифрово подписан печат – 2 бр.

8.2. Дейност 2 Разработка на функционалностите на системата и реализиране на интеграции с вътрешни за МВнР системи

8.2.1. Описание на дейността

Целта на настоящата дейност е да се разработи допълнителна функционалност към консулската система eConsulate (КБДИ), с която при отпечатване на визов стикер, върху него да се отпечатва криптографски подписан цифров печат (2d баркод), който да съдържа определена част от данните на визовия стикер.

8.2.2. Изисквания към изпълнение на дейността

Криптографски подписаният цифров печат трябва да се изпечатва в клетка 16 от унифицирания формат за визи, установен с Регламент (ЕО) № 1683/95.

Криптографски подписаният цифров печат трябва да отговаря на спецификациите на „ ICAO Technical Report Visible Digital Seals for Non-Electronic Documents v.1.7, 2018“. Всички данни, изисквани от тези спецификации да бъдат кодирани в цифровия печат. Данните, означени като незадължителни в тези спецификации на ICAO не се включват в цифровия печат.

За генериране на цифровия печат ще се използва описанието, посочено в „ISO/IEC 16022: Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification“.

Реализацията на допълнителната функционалност за генериране и отпечатване на 2d баркод върху визовия стикер трябва да следва следните основни стъпки:

- На стъпка отпечатване на визов стикер в консулската система eConsulate (КБДИ) се извършват автоматично (невидимо за потребителя) следните действия:

o Да се генерира набора от данни, необходим за запис в 2d баркода;

o Да се изпрати горния набор от данни към системата, обслужваща Certificate Authority, която ще ги подписва криптографски;

o Системата, обслужваща Certificate Authority връща криптографски подписаните данни на консулската система;

o Така получените данни трябва да се кодират във формат на 2d баркод, според ICAO-VDS-TR, ISO/IEC 16022 и добрите практики, от останалите страни в ЕС, имплементирали т. нар. 2d баркод.

- Така кодираните данни в 2d баркод формат, се визуализират върху визовия стикер в клетка 16 на екрана за печат;

- След потвърждение от потребителя визуализираните данни се изпечатват върху визовия стикер;

 Стъпките по генериране и изпечатване на 2d баркод върху визовия стикер приключват със запис на криптографски подписаните данни в заявлението за виза в консулската система.

Проверката за коректност на изпечатания 2d баркод е извън функционалността на консулската система.

Приложението за изчитане на 2d баркода от визовите стикери е извън функционалността на консулската система.

Тъй като практиката в другите страни от ЕС е показала, че един от основните проблеми при изпечатването на 2d баркода е качеството и начина на печат на различните принтери, то Изпълнителят трябва да проведе тестове на различни принтери, предоставени от Възложителя за съвместимост на печата.

В случай че с никой, от предоставените от Възложителя, принтери не може да се постигне печат, който да гарантира успешно изчитане на отпечатания 2d баркод, то Възложителя ще трябва да закупи принтери, които покриват изискванията за отпечатване на четим 2d Баркод.

Изпълнителят следва да осигури актуализиране/надстройване на софтуера в отговор на каквито и да са установени несъответствия във функционирането на системното и приложното програмно осигуряване.

За предоставяне на гаранционната поддръжка, Изпълнителят следва да разполага с помощно бюро (хелп деск). Достъпът до Помощното бюро следва да е осигурен чрез телефонен номер 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. Следва да бъде предоставен достъп до система за обработване на заявки (helpdesk).

Гаранционната поддръжка следва да включва възможност за получаване на обновления на софтуера (updates, patches, firmwareupdates).

При дефектиране на носител на информация по време на гаранционната поддръжка, същият не се връща

8.2.3. Очаквани резултати

Разработена допълнителна функционалност към консулската система eConsulate (КБДИ)

9. ДОКУМЕНТАЦИЯ

9.1. Изисквания към документацията

▪ Цялата документация и всички технически описания, ръководства за работа, администриране и поддръжка на Системата, включително и на нейните съставни части, трябва да бъдат налични и на български език;

▪ Всички документи трябва да бъдат предоставени от Изпълнителя в електронен формат (ODF/ /Office Open XML/MS Word DOC/RTF/PDF/HTML или др.), позволяващ пълнотекстово търсене/търсене по ключови думи и копиране на части от съдържанието от оригиналните документи във външни документи, за вътрешна употреба на възложителя;

▪ Навсякъде, където в документацията има включени диаграми или графики, те трябва да бъдат вградени в документите в оригиналния си векторен формат;

▪ Детайлна техническа документация на програмния приложен интерфейс (API), включително за поддържаните уебуслуги, команди, структури от данни и др. Документацията да бъде придружена и с примерен програмен код и/или библиотеки (SDK) за реализиране на интеграция с външни системи, разработен(и) на Java или .NET. Примерният код трябва да е напълно работоспособен и да демонстрира базови итерации с API-то:

- Регистриране на крайна точка (end-point) за получаване на актуализации от Системата в реално време;
- Заявки за получаване на номенклатурни данни (списъци, таксономии);
- Заявки за актуализиране на номенклатурни данни (списъци, таксономии);
- Регистрация на потребител;
- Идентификация и оторизация на потребител или уебуслуга;

▪ Документацията за приложния програмен интерфейс (API) трябва да бъде публично достъпна;

▪ Всеки предоставен REST приложно-програмен интерфейс трябва да бъде документиран чрез API Blueprint (https://github.com/apiaryio/api-blueprint), Swagger (http://swagger.io) или чрез аналогична технология. Аналогично представяне трябва да бъде изготвено и за SOAP интерфейсите;

▪ Детайлна техническа документация за схемата на базата данни – структури за данни, индекси, дялове, съхранени процедури, конфигурации за репликация на данни и др.

▪ Ръководства на потребителя и администратора за работа и администриране на Системата

▪ Обща информация, инструкции и процедури за администриране и поддръжка на приложните сървъри, сървърите за бази данни и др.

▪ Обща информация, инструкции и процедури за администриране, архивиране и възстановяване, и поддръжка на сървъра за управление на бази данни.

9.2. Прозрачност и отчетност

- В обхвата на проекта е включено извършване на дейности по анализ на бизнес процеси и нормативна уредба, проектиране на системна и приложна архитектура, разработване на компютърни програми и други дейности, свързани с предоставяне на специализирани професионални услуги. Изпълнителят и Възложителят трябва да публикуват подробни месечни отчети в машинночетим отворен формат за извършените дейности, включително количеството изработени човекодни по дейности, извършени от консултанти, експерти, специалисти и служители на Изпълнителя и Възложителя.

Документацията, предоставена от Изпълнителя на Възложителя, трябва да бъде:

- на български език;
- на хартия и в електронен формат; копирането и редактирането на предоставените документи следва да бъде лесно осъществимо;
- актуализирана в съответствие със съгласувана с възложителя процедура, която следва да включва документи, подлежащи на промяна/актуализация, крайни срокове и нужната за случая методология.

Минимално изискуемата документация по проекта включва долу изброените документи.

9.3. Системен проект

Изпълнителят на настоящата поръчка трябва да дефинира в детайли конкретния обхват на реализация на софтуерната разработка и да документира изискванията към софтуера в детайлна техническа спецификация (системен проект), която ще послужи за пряка изходна база за разработка.

При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, е необходимо да се използва утвърдена нотация за описание на бизнес модели. Изготвената детайлна техническа спецификация (системен проект) се представя за одобрение на Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят е длъжен да ги отрази в детайлната техническа спецификация (системен проект).

9.4. Техническа документация

Всички продукти, които ще се доставят, трябва да са със специфична документация за инсталиране и/или техническа документация, в това число:

- Ръководство за администратора, включващо всички необходими процедури и скриптове по инсталиране, конфигуриране, архивиране, възстановяване и други, необходими за администриране на Системата;

- Документи за крайния ползвател – Изпълнителят трябва да предостави главното Ръководство на ползвателите на софтуера. Документът е предназначен за крайните ползватели. Той трябва да описва цялостната функционалност на приложния софтуер и съответното му използване от крайни ползватели;
- Детайлно описание на базата данни;
- Описание на софтуерните модули;
- Описание на изходния програмен код.

9.5. Протоколи

Изпълнителят трябва да изготвя протоколи от изпълнението на различните етапи на проекта, описани в раздел 8 на настоящия документ, заедно със съпътстващите ги документи – резултати от изпълнението на етапите.

9.6. Комуникация и доклади

За успешното изпълнение на проекта участниците в настоящия проект трябва да предложат адекватен механизъм за управление на проектната комуникация, който е неразделна част от предлаганата цялостна проектна методология.

Управлението на комуникацията трябва да включва изготвяне на минимум следните регулярни доклади за статуса и напредъка на изпълнението на поръчката:

9.6.1. Встъпителен доклад

Встъпителният доклад трябва да бъде предоставен до един месец от подписването на договора и да съдържа описание минимум на:

- Подробен работен план и актуализиран времеви график за периода на проекта;
- Начини на комуникация;
- Отговорни лица и екипи.

Встъпителният доклад следва да бъде одобрен от Възложителя.

9.6.2. Междинни доклади

Междинните доклади трябва да бъдат представяни и да се предават при приключване на всяка от дейностите и поддейностите и/или при настъпване на събитие.

Междинните доклади трябва да съдържат информация относно изпълнението на дейностите и поддейностите по предварително изготвения проектен план.

Докладът за междинния напредък трябва да бъде подготвен по следния начин:

- Общ прогрес по дейностите през периода;
- Постигнати проектни резултати за периода;
- Срещнати проблеми, причини и мерки, предприети за преодоляването им;
- Рискове за изпълнение на свързани дейности и на проекта като цяло и предприети мерки;
- Актуализиран план за изпълнение, ако има такъв.

Всеки междинен доклад следва да бъде одобрен от Възложителя.

9.6.3. Окончателен доклад

В края на периода за изпълнение трябва да се представи окончателен доклад. Окончателният доклад трябва да съдържа описание на изпълнението и резултати.

Докладите се изпращат до отговорния служител на Възложителя. За тази цел Възложителят ще определи в договора отговорния/отговорните служител/служители. Всички доклади се представят на български език в електронен формат и на хартиен носител. Докладите се одобряват от отговорния/отговорните служител/служители в срок до 5 работни дни.

Всички доклади трябва да се представят на възложителя на български език на хартиен и на електронен носител. Представянето на докладите трябва да се извършва чрез подписване на двустранни предавателно-приемателни протоколи, подписани от представители на Изпълнителя и на Възложителя.

Възложителят разглежда представените доклади и уведомява Изпълнителя за приемането им без забележки или ги връща за преработване, допълване и/или окомплектоване, ако не отговарят на изискванията, като чрез упълномощено в договора лице дава указания и определя срок за отстраняване на констатираните недостатъци и пропуски.

9.7. Други условия

1. Навсякъде в техническата спецификация Възложителя (посочени в колона, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство) да се чете и разбира „или ЕКВИВАЛЕНТ“. Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.

2. Изискванията, поставени в настоящата Техническа спецификация, са минимални. Предложеното от участника оборудване и софтуер трябва да съответства или да надвишава в техническо отношение минималните изисквания в Техническата спецификация на Възложителя.

9. РЕЗУЛТАТИ

Очакваните резултати от изпълнението на настоящия проект са следните:
В резултат на изпълнението на настоящия проект ще бъдат закупени:

- сървър за софтуер за генериране на видим цифрово подписан печат – 2 бр.
- Хардуерен модул за сигурност HSM – 2 бр.
- Специализиран софтуер за генериране на видим цифрово подписан печат – 2 бр.
- Ще бъде разработена допълнителна функционалност към консулската система eConsulate (КБДИ)
- провеждане на обучение за служители на МВнР
- гаранционна поддръжка на хардуерен модул за сигурност
- работна станция за наблюдение и управление на системата – 1 бр