ДОГОВОР

№ ……/……..2022 г.

В гр. София, между:

1. МИНИСТЕРСТВОТО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ, с адрес: гр. София 1000, ул. „Ген. Гурко“ № 6, БУЛСТАТ 180680495, представлявано от Божидар Божанов – министър на електронното управление и Ангел Петров - главен секретар на Министерство на електронното управление, наричано по-долу за краткост ВЪЗЛОЖИТЕЛ от една страна и

2. „ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД, ЕИК 831641791, със седалище и адрес на управление: гр. София 1504, район Оборище, ул. „Панайот Волов“ № 2, представлявано от Ивайло Филипов – изпълнителен директор на дружеството, наричано по-долу за краткост ИЗПЪЛНИТЕЛ, от друга страна,

двете наричани по-долу за краткост „Страни/Страните“, като взеха предвид че:

- Услугите, предмет на настоящия договор, представляват дейности по системна интеграция, по смисъла на чл. 7с от ***Закона за електронното управление*** (ЗЕУ)
- Съгласно § 45, ал.1, предл. първо от Преходните и Заключителни разпоредби към Закона за изменение и допълнение на ЗЕУ (Обн. - ДВ, бр. 94 от 2019 г., в сила от 29.11.2019 г., доп. ДВ, бр.102 от 2019 г., в сила от 29.11.2019 г.) системната интеграция по чл. 7с от ЗЕУ се извършва от „Информационно обслужване“ АД, т.е. ИЗПЪЛНИТЕЛЯТ по закон притежава правото да предоставя услуги по изграждане, поддържане, развитие и наблюдение на работоспособността на информационните и комуникационните системи, използвани от административните органи, определени с Решение № 727/05.12.2019 г. на Министерския съвет, както и дейности, които осигуряват изпълнението на тези услуги;
- Съгласно § 45, ал.1, предл. второ от Преходните и Заключителни разпоредби към Закона за изменение и допълнение на ЗЕУ (Обн. - ДВ, бр. 94 от 2019 г., в сила от

29.11.2019 г., доп. ДВ, бр.102 от 2019 г., в сила от 29.11.2019 г.) „Информационно обслужване“ АД е публичен възложител само при възлагане на дейностите по чл. 7с.

- Възлагат се услуги от възложител на публичен възложител, който има изключителни права за предоставяне на съответните услуги по силата на ЗЕУ (§ 45, ал. 1);

- На основание § 45, ал. 2 от ЗЕУ с РМС № 727/05.12.2019 г. с последващи изменения и допълнения Министерство на електронното управление (МЕУ) е определено като административен орган, който при изпълнение на своите функции, свързани с дейности по системна интеграция, възлага изпълнението на тези дейности на „Информационно обслужване“ АД - за дейностите по системна интеграция на информационни и комуникационни системи, свързани с електронна идентификация, а за останалите информационни и комуникационни системи и мрежи – за доставка на хардуер, мрежово оборудване и софтуерни лицензи, включително свързани с доставката други дейности, услуги и абонаменти, и за извършване на тестове за информационна и киберсигурност, анализи и даване на препоръки за съществуващи или планирани информационни и комуникационни системи и мрежи (т. 30).

- на основание чл. 7с от ***Закона за електронното управление*** (ЗЕУ), § 45. (1) от Преходните и Заключителни разпоредби към ***Закона за изменение и допълнение на ЗЕУ,*** както и чл. 9 от ***Закона за задълженията и договорите (ЗЗД),*** се сключи този договор („Договора“) за следното:

I. ПРЕДМЕТ НА ДОГОВОРА

Чл. 1. Предмет на договора е изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID, наричано за краткост „Система/Системата“, съгласно заложеното в „ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ за изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID“ на ВЪЗЛОЖИТЕЛЯ (наричана за краткост Приложение № 1), която е неразделна част от настоящия договор.

II. СРОК НА ДЕЙСТВИЕ И ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ

Чл. 2. (1) Настоящият Договор влиза в сила, считано от датата на двустранното му подписване и е със срок на действие до изтичане на срока за гаранционна поддръжка (36 (тридесет и шест) месеца от внедряването на Системата в експлоатация) и изпълнение на всички задължения на страните по договора.

(2) Срокът за изпълнение на дейностите по изграждане на мобилното приложение (Дейности 1, 2, 3 и 4) по чл. 1 е 9 (девет) месеца, считано от датата на сключване на договора, който срок се разпределя, както следва:

т. 1 Срокът за изпълнение на Дейност 1 по точка 8.1 на Приложение № 1 е до 1 (един) месец след сключване на договора.

т. 2 Срокът за предаване на работеща базова функционалност за електронна идентификация, част от Дейност 2, 3 и 4 по точки 8.2 до 8.4 наПриложение № 1 е до 6 (шест) месеца след сключване на договора.

т. 3 Срокът за изпълнение на Дейност 2 по точка 8.2 на Приложение № 1, на Дейност 3 по т.8.3 от Приложение № 1 и на Дейност 4 по т.8.4 от Приложение №1 е до 9 (девет) месеца след сключване на договора.

т. 4 Срокът за изпълнение на Дейност 5 по т.8.5. на Приложение № 1 и на Дейност 6 по т.8.6 от Приложение № 1 е до 6 (шест) месеца от приемане на изпълнението на Дейност 2, Дейност 3 и Дейност 4 (след внедряване на Системата).

(3) Срокът на гаранционната поддръжка на мобилното приложение по чл. 1 е 36 (тридесет и шест) месеца от внедряването на системата в експлоатация.

(4) При непредвидени обстоятелства, както и обжалване на решения на ИЗПЪЛНИТЕЛЯ, свързани с изпълнението на договора, посочените в ал. 2 срокове се считат за автоматично продължени със срока на действие на съответните непредвидени обстоятелства, за което между страните се подписва констативен протокол.

Чл. 3. (1) Договорът се прекратява:

т. 1. При изтичане на срока по чл. 2, ал. 1 от договора;

т. 2. Преди изтичане на срока по чл.2, ал.1 - по взаимно съгласие на страните, изразено писмено;

т. 3. При настъпване на обективна невъзможност за изпълнение на договора;

т. 4. При пълно неизпълнение на задълженията на страните, извън случаите по т. 3.

(2) В случай, че ИЗПЪЛНИТЕЛЯТ наруши съществено условие на настоящия Договор, в срок от 3 (три) дни от констатиране на нарушението, ВЪЗЛОЖИТЕЛЯТ изпраща писмено уведомление за извършеното нарушение на ИЗПЪЛНИТЕЛЯ. За „съществено условие" по смисъла на изречение първо се счита такова условие, което е свързано с правата и задълженията на страните по Договора, и чието неизпълнение води до неизпълнение на предмета на Договора.

(3) В случай, че ИЗПЪЛНИТЕЛЯТ наруши съществено условие на настоящия Договор, и не успее да отстрани нарушението в срок от 30 (тридесет) дни от писменото уведомление за извършеното нарушение, то тогава ИЗПЪЛНИТЕЛЯТ е в неизпълнение и ВЪЗЛОЖИТЕЛЯТ има право да развали Договора без предизвестие Правото за ВЪЗЛОЖИТЕЛЯ възниква, считано от деня, следващ крайната дата за отстраняване на нарушението.

(4) При настъпването на всяко „нарушаване на съществено условие по договора" от страна на ИЗПЪЛНИТЕЛЯ, което води до прекратяване на договора от страна на ВЪЗЛОЖИТЕЛЯ без предизвестие, се съставя протокол, подписан от лицата, определени от страните по договора, отговарящи за изпълнението му. Протоколът по изречение първо се съставя в срок до 3 (три) дни от изтичането на тридесетдневния срок за отстраняване на нарушението от страна на ИЗПЪЛНИТЕЛЯ. В протокола задължително се описват извършеното от ИЗПЪЛНИТЕЛЯ нарушение на съществено условие по договора и възникналите за ВЪЗЛОЖИТЕЛЯ последици от него, както и изпълнените до момента дейности по договора.

(5) При прекратяване на договора ВЪЗЛОЖИТЕЛЯТ ще заплати всички дължими суми за дейностите съгласно този Договор, които са били изпълнени качествено и в срок и надлежно приети към момента на прекратяване на договора.

(6) При прекратяване на договора по реда на ал. 3 и ал. 4 на настоящия член ВЪЗЛОЖИТЕЛЯТ ще заплати всички дължими суми за дейностите съгласно този Договор,

които са били изпълнени качествено и в срок и надлежно приети към момента на прекратяване на договора.

(7) Ако ИЗПЪЛНИТЕЛЯТ е в неизпълнение, и не успее да отстрани такова неизпълнение в срок от 30 (тридесет) дни, ВЪЗЛОЖИТЕЛЯТ има право на обезщетение по чл.9, ал.1. от настоящия договор.

(8) ВЪЗЛОЖИТЕЛЯТ може по своя преценка да удължи 30-дневния срок по ал. 3 с толкова време, за което ВЪЗЛОЖИТЕЛЯТ счита, че е необходимо на ИЗПЪЛНИТЕЛЯ да продължи нормалните усилия за отстраняване на неизпълнението. След изтичане на удължения срок правоотношенията между страните се уреждат по реда на ал. 3.

(9) По преценка на ВЪЗЛОЖИТЕЛЯ случай, в който ИЗПЪЛНИТЕЛЯТ наруши съществено условие на настоящия Договор, и не успее да отстрани нарушението в срок от 30 (тридесет) дни от писменото уведомление за извършеното нарушение и това неизпълнение води до неизпълнение на предмета на Договора, се приравнява на пълно неизпълнение и непостигане целите на настоящия договор, които са изграждане на пълнофункционална, въведена в експлоатация и действаща Система. В този случай договорът се прекратява, а извършените и приети предходни дейности, които вече са заплатени на ИЗПЪЛНИТЕЛЯ, ще се разглеждат като неефективни и безрезултатни, а оттам и неизвършени, съответно заплатеното по тях, ще се счита за недължимо платено и следва да се възстанови на ВЪЗЛОЖИТЕЛЯ.

(10) При пълно неизпълнение на задълженията на страните, изправната страна прекратява договора едностранно без предизвестие. За констатиране на пълно неизпълнение на задълженията на неизправната страна се съставя констативен протокол от изправната страна и протоколът се представя на неизправната за подпис. Договорът се прекратява, считано от датата на подписване на протокола от двете страни. В случай, че неизправната страна откаже да подпише протокола в знак на несъгласие с направените констатации в него, то той следва да се счита за едномесечно предизвестие за прекратяване на договора.

(11) По взаимно съгласие на страните, изразено писмено, сроковете по ал. 3, ал.

7, ал. 8, съответно по ал. 9 могат да бъдат и по-кратки, като страните договарят по-кратките срокове, отчитайки тежестта на нарушението на същественото условие по договора, както и всяко друго неизпълнение на договора и възможния разумен срок за отстраняване на неизпълнението.

(12) ВЪЗЛОЖИТЕЛЯТ има право едностранно да прекрати договора:

1. при започване на процедура по ликвидация на ИЗПЪЛНИТЕЛЯ;

2. при откриване на производство за обявяване в несъстоятелност на ИЗПЪЛНИТЕЛЯ, както и при обявяване в несъстоятелност на ИЗПЪЛНИТЕЛЯ.

III. ЦЕНА И НАЧИН НА ПЛАЩАНЕ

Чл. 4. (1) За изпълнение на възложените дейности, съгласно предмета на договора по чл. 1, ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ възнаграждение в размер на 1 747 400 (един милион седемстотин четиридесет и седем хиляди и четиристотин) лева без ДДС, съответно 2 096 880 (два милиона деветдесет и шест хиляди осемстотин и осемдесет) лева с ДДС при действаща 20% ставка на ДДС.

(2) При законодателна промяна в размера на приложимата ставка на ДДС, възнаграждението се актуализира в съответствие с настъпилото изменение, без необходимост от подписване на допълнително споразумение, считано от датата на влизане в сила на законодателната промяна.

(3) Цената по ал. 1 включва извършване на дейностите, посочени в Приложение № 1 при условията на настоящия договор.

(4) Възнаграждението по ал. 1 се заплаща, както следва:

т. 1. 20 % (двадесет на сто) от възнаграждението по ал.1 - в срок до 30 дни, след приемане на изпълнението на Дейност 1 по точка 8.1 от Приложение № 1, удостоверено с одобрен от ВЪЗЛОЖИТЕЛЯ междинен доклад и издадена от ИЗПЪЛНИТЕЛЯ фактура.

т. 2. 30 % (тридесет на сто) от възнаграждението по ал.1 - в срок до 30 дни, след предаване на работеща базова функционалност за електронна идентификация, част от Дейност 2, 3 и 4 по точки 8.2 до 8.4 от Приложение № 1, удостоверено с одобрен от ВЪЗЛОЖИТЕЛЯ междинен доклад и издадена от ИЗПЪЛНИТЕЛЯ фактура.

т. 3. 40 % (четиридесет на сто) - в срок до 30 дни, след приемане на изпълнението на Дейност 2 по точка 8.2 на Приложение № 1, на Дейност 3 по т.8.3 от Приложение № 1 и на Дейност 4 по т.8.4 от Приложение №1, удостоверено с одобрен от ВЪЗЛОЖИТЕЛЯ междинен доклад и издадена от ИЗПЪЛНИТЕЛЯ фактура.

т. 4. 10 % (десет на сто) от възнаграждението по ал.1 - в срок до 30 дни, след приемане на изпълнението на Дейност 5 по т.8.5. на Приложение № 1 и на Дейност 6 по т.8.6 от Приложение № 1, удостоверено с одобрен от ВЪЗЛОЖИТЕЛЯ междинен доклад и издадена от ИЗПЪЛНИТЕЛЯ фактура.

(5) Допуска се възнаграждението по ал. 1 да се заплати изцяло или частично чрез акредитив, при спазване изискванията на чл.153 ал. 7 от Закона за публичните финанси и раздел IV от съвместно писмо на МФ и БНБ БДС № 11/2001 г., при условията на настоящия договор. Таксите и комисионните за обслужване на акредитивната сметка се заплащат както следва: 50 % (петдесет на сто) от ИЗПЪЛНИТЕЛЯ и 50% (петдесет на сто) от ВЪЗЛОЖИТЕЛЯ.

Чл. 5. (1) Изплащането на договореното възнаграждение по чл. 4, ал. 1 ще бъде извършвано по следната посочена от ИЗПЪЛНИТЕЛЯ банкова сметка:

Банка: Юробанк България АД

BIC: BPBIBGSF

IBAN: BG10BPBI79401053711101

(2) Страните се съгласяват, че в случай, че издадената фактура не е получена от ВЪЗЛОЖИТЕЛЯ в срок от 10 (десет) дни от датата на издаването й, няма да е налице забава от страна на ВЪЗЛОЖИТЕЛЯ за плащане на дължимите суми и не се дължи лихва за забава за периода, с който е забавено представянето на фактурата.

Чл. 6. (1) Представянето на междинните доклади се извършва чрез подписване на двустранни предавателно-приемателни протоколи, подписани от представители на ИЗПЪЛНИТЕЛЯ и на ВЪЗЛОЖИТЕЛЯ.

(2) В срок до 5 (пет) работни дни от датата на получаване на документите по ал.1 ВЪЗЛОЖИТЕЛЯТ има право:

1. Да приеме изпълнението, когато отговаря на договореното, като одобри представения от ИЗПЪЛНИТЕЛЯ междинен доклад;

2. Да откаже да приеме изпълнението при констатирани отклонения от договореното, като конкретизира недостатъците в констативен протокол и предостави подходящ срок за отстраняване.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ

Чл. 7. (1) ИЗПЪЛНИТЕЛЯТ се задължава да изпълнява дейностите, предмет на договора, съгласно чл. 1 от същия, при спазване на изискванията на ВЪЗЛОЖИТЕЛЯ, дадени в Приложение № 1 към договора.

(2) ИЗПЪЛНИТЕЛЯТ се задължава да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 16 от Договора. Да опазва и да не разгласява пред трети лица съдържанието на лични данни и друга защитена по закон или по силата на Договора информация, която е станала известна при изпълнението на дейностите по чл.1, като представи декларация по образец – Приложение №2. Това задължение се отнася и за лицата, които имат достъп до системите на ВЪЗЛОЖИТЕЛЯ във връзка с изпълнението на договора.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ

Чл. 8. (1) ВЪЗЛОЖИТЕЛЯТ следва да предостави на ИЗПЪЛНИТЕЛЯ необходимото съдействие за изпълнение на договора, както и да приеме и заплати извършеното от ИЗПЪЛНИТЕЛЯ в съответствие с договора, в случай че не е констатирано неизпълнение/няма забележки.

(2) За внедряване на Системата в експлоатация, ВЪЗЛОЖИТЕЛЯТ следва да предостави на ИЗПЪЛНИТЕЛЯ провизирана продукционна среда с необходимите параметри и функционалности, в която да се изпълнят всички дейности по инсталиране и конфигуриране на инфраструктурата, необходима за пускането в експлоатация и функционирането на Системата, не по-късно от 2 (два) календарни месеца преди срока за внедряване на мобилното приложение (Дейности 1, 2, 3 и 4).

VI. ОТГОВОРНОСТИ

Чл. 9. (1) При забавено изпълнение на задължения по Договора от страна на ИЗПЪЛНИТЕЛЯ в нарушение на сроковете предвидените в Приложение № 1, същият заплаща на ВЪЗЛОЖИТЕЛЯ неустойка в размер на 0,05% (нула цяло нула пет на сто) от цената по чл. 4, ал.1 за всеки просрочен ден, но не повече от 10 % (десет на сто) от цената, а за сроковете, които се смятат в часове, дължимата неустойка е 0,01 % (нула цяло, нула един процент) от сумата по чл. 4, ал.1 за всеки просрочен час, но не повече от 10 % (десет на сто) от тази сума.

(2) При системно (три и повече пъти) неизпълнение на задълженията за гаранционна поддръжка в срока по гаранцията, ИЗПЪЛНИТЕЛЯТ дължи на ВЪЗЛОЖИТЕЛЯ неустойка в размер на 5 % (пет на сто) от цената по чл. 4, ал. 1. За неизпълнение ще се счита забава от страна на ИЗПЪЛНИТЕЛЯ да отстрани инцидент или проблем в срока посочен в Таблица 3 „Параметри на качеството при отстраняване на инцидент“ и Таблица 4 „Параметри на качеството при отстраняване на проблем“ от Приложение № 1 към „ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ за изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID“.

(3) В случай на пълно неизпълнение ВЪЗЛОЖИТЕЛЯТ има право да прекрати договора, както и да изиска неустойка в размер на 10% (десет на сто) от стойността на договора по чл. 4, ал. 1. без ДДС.

При пълно неизпълнение на задълженията за гаранционна поддръжка или при отказ за изпълнение на задълженията за гаранционна поддръжка в срока на гаранцията, Възложителят има право да прекрати незабавно Договора, като в този случай ИЗПЪЛНИТЕЛЯТ дължи неустойка в размер на 10 % (десет на сто) от цената по чл. 4, ал. 1.

(4) Под пълно неизпълнение се разбира надвишаване със 120 (сто и двадесет) часа и повече на сроковете за отстраняване на проблем или инцидент или 10 (десет) и повече случая на забава от страна на Изпълнителя да отстрани инцидент или проблем в сроковете, посочени в Таблица 3 „Параметри на качеството при отстраняване на инцидент“ и Таблица 4 „Параметри на качеството при отстраняване на проблем“ от Приложение № 1.

(5) Не е налице забава, системно или пълно неизпълнение, когато ВЪЗЛОЖИТЕЛЯТ, въз основа на мотивирано предложение от страна на ИЗПЪЛНИТЕЛЯ, с писмено изявление се е съгласил да бъдат удължени сроковете за изпълнение на задълженията за гаранционна поддръжка на ИЗПЪЛНИТЕЛЯ, посочени в Таблица 3 „Параметри на качеството при отстраняване на инцидент“ и Таблица 4 „Параметри на качеството при отстраняване на проблем“ от Приложение № 1. Сроковете за изпълнение на задълженията за гаранционна поддръжка, посочени в Таблица 3 и Таблица 4 от Приложение 1 могат да бъдат удължени за определен период или за целия срок на гаранционна поддръжка, както и за всички или само за част от дейностите на гаранционната поддръжка. В този случай под пълно неизпълнение по ал. 4 се разбира надвишаване на новите, договорени между страните срокове, със 120 (сто и двадесет) часа и повече на сроковете за отстраняване на проблем или инцидент или 10 (десет) и повече случая на забава от страна на ИЗПЪЛНИТЕЛЯ да отстрани инцидент или проблем.

(6) При нарушение от страна на ИЗПЪЛНИТЕЛЯ на правата на Интелектуална собственост на ВЪЗЛОЖИТЕЛЯ, ИЗПЪЛНИТЕЛЯТ дължи неустойка в размер на 10% (десет на сто) от стойността на Договора по чл. 4, ал.1.

(7) При забава на ВЪЗЛОЖИТЕЛЯ за изпълнение на задълженията му за плащане по Договора, същият заплаща на ИЗПЪЛНИТЕЛЯ неустойка в размер на 0,05% (нула цяло нула пет на сто) от съответната дължима сума по чл. 4, ал. 4 за всеки просрочен ден, но не повече от 10 % (десет на сто) от съответната дължима сума по чл. 4, ал. 4.

(8) Дължимите неустойки се заплащат в срок до 7 (седем) дни от съответната страна, при писмено поискване от изправната страна, обективирано в писмо или протокол, по следните банкови сметки:

1. Банкова сметка на ВЪЗЛОЖИТЕЛЯ:
БНБ Централно управление
IBAN: BG28BNBG96613000142901
BIC код на БНБ – BNBGBGSF

2. Банкова сметка на ИЗПЪЛНИТЕЛЯ:
Банка: Юробанк България АД

BIC: BPBIBGSF

IBAN: BG10BPBI79401053711101

(9) В случай че банковата сметка на ВЪЗЛОЖИТЕЛЯ не е заверена със сумата на неустойката в срок до 7 (седем) дни от искането на ВЪЗЛОЖИТЕЛЯ за плащане на неустойка, ВЪЗЛОЖИТЕЛЯТ има право да извърши прихващане от следващото плащане по договора.

Чл. 10. Страните запазват правото си да търсят обезщетение за претърпени вреди и пропуснати ползи, ако тяхната стойност е по-голяма от изплатените неустойки по общия ред.

Чл.11. При констатирано лошо или друго неточно или частично изпълнение на отделна дейност или при отклонение от изискванията на ВЪЗЛОЖИТЕЛЯ, същият има право да поиска от ИЗПЪЛНИТЕЛЯ да изпълни изцяло и качествено, без да дължи допълнително възнаграждение за това. В случай, че и повторното изпълнение на услугата е некачествено, ВЪЗЛОЖИТЕЛЯТ има право да прекрати договора, както и да изиска неустойка в размер на 10% (десет на сто) от стойността на съответната дейност без ДДС.

VII. АВТОРСКИ ПРАВА

Чл. 12. (1) Страните се споразумяват изрично и потвърждават, че авторските и всички сродни права и собствеността върху софтуерните продукти, техният изходен програмен код, дизайнът на интерфейсите и базите данни, чиято разработка е предмет на Договора, и всички съпътстващи изработката им проучвания, разработки, скици, чертежи, планове, модели, документи, софтуер, дизайни, описания, документи, данни, файлове, матрици или каквито и да било средства и носители и свързаната с тях документация и други продукти, възникват директно за ВЪЗЛОЖИТЕЛЯ, в пълния им обем, съгласно действащото законодателство, а в случай че това не е възможно, ще се считат за прехвърлени на ВЪЗЛОЖИТЕЛЯ в пълния им обем, без никакви ограничения в използването, изменението и разпространението им и без ВЪЗЛОЖИТЕЛЯТ да дължи каквито и да било допълнителни плащания и суми, освен договорената цена по чл.4, ал. 1. Соф-

туерните продукти трябва да отговарят на критериите за софтуер с отворен код. За разработка трябва да се използват хранилището и системата за контрол на версиите, поддържани от ВЪЗЛОЖИТЕЛЯ, или друго хранилище и система за контрол на версиите, определени от ВЪЗЛОЖИТЕЛЯ. ИЗПЪЛНИТЕЛЯТ потвърждава, че документ „ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ за изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID“ на ВЪЗЛОЖИТЕЛЯ и цялата информация предоставена му от ВЪЗЛОЖИТЕЛЯ за изпълнение на задълженията му по настоящия Договор, са изключителна собственост на ВЪЗЛОЖИТЕЛЯ и същият притежава авторските права върху тях, като ИЗПЪЛНИТЕЛЯТ единствено адаптира концепцията на ВЪЗЛОЖИТЕЛЯ във вид и по начин, позволяващи използването й за успешната реализация на Системата, като всички адаптации, направени в изпълнение на този Договор, както и авторските права върху тях, остават изключителна собственост на ВЪЗЛОЖИТЕЛЯ и могат да бъдат използвани по негово собствено усмотрение свободно в други проекти, развивани или осъществявани от него.

(2) Настоящият Договор се счита и следва да бъде тълкуван като договор за създаване на обект на авторско право (произведение) по поръчка, съгласно член 42 (1) от Закон за авторското право и сродните му права („ЗАПСП“), като страните изрично се съгласяват и споразумяват, че:

т. 1. авторските права върху софтуерните продукти и части от тях, включително имуществените права съгласно раздел II от ЗАПСП и прехвърлимите неимуществени права, съгласно член 15 от ЗАПСП ще възникнат и принадлежат изцяло и безусловно на ВЪЗЛОЖИТЕЛЯ, като ИЗПЪЛНИТЕЛЯТ декларира и гарантира, че те няма да бъдат обременени с каквито и да било залози, искове, възбрани и други тежести и претенции или права на трети лица;

т. 2. ИЗПЪЛНИТЕЛЯТ предоставя на ВЪЗЛОЖИТЕЛЯ изключителни права по смисъла на член 36, ал. 2 от ЗАПСП за използване на софтуерните продукти и всички техни елементи и обектите или части от тях, в случай че авторските права върху тях не могат да възникнат директно за ВЪЗЛОЖИТЕЛЯ, като страните потвърждават, че договорената цена по чл. 4, ал. 1, включва предоставянето на правата съгласно настоящата

ал. 2 и че така определената цена е достатъчна, справедлива и определена по взаимно съгласие на страните.

(3) За избягване на съмнение, страните потвърждават и се съгласяват, че правата на ВЪЗЛОЖИТЕЛЯ върху всички софтуерни продукти и обекти, включително и изключителното право на ползване по ал. 2, т. 2 обхващат всички видове използване, както е предвидено в ЗАПСП, без никакви ограничения по отношение на срокове и територия, включително, но не само: право на ползване, промяна, изменение, възпроизвеждане, публикуване, разпространение, продажба, адаптиране, прехвърляне, представяне, маркетинг, разпореждане по какъвто и да било начин и с каквито и да било средства в най-широк възможен смисъл и по най-широк възможен начин за целия срок на действие и закрила на авторското право, за всички държави, където това право може да бъде признато. Това право на ВЪЗЛОЖИТЕЛЯ е без ограничение по отношение на броя на възпроизвеждането, разпространението или представянето и е валидно за всички държави, езици и начин на опериране. Освен това ИЗПЪЛНИТЕЛЯТ потвърждава и се съгласява, че цялата търговска репутация и ползи, произтичащи от софтуерните продукти, ще възникват и принадлежат на ВЪЗЛОЖИТЕЛЯ и ИЗПЪЛНИТЕЛЯТ няма да има каквито и да било права и/или претенции в това отношение. ИЗПЪЛНИТЕЛЯТ също потвърждава и се съгласява, че не притежава, няма и не може да предявява претенции по отношение на каквито и да било права на интелектуална собственост върху софтуерните продукти.

(4) ИЗПЪЛНИТЕЛЯТ няма право да прехвърля на трети лица каквито и да било права свързани със софтуерните продукти, включително, но не само правото на ползване и/или на промяна, както и няма право да използва и/или прехвърля, разкрива или предоставя по какъвто и да било начин на трети лица концепцията на ВЪЗЛОЖИТЕЛЯ, съдържаща се в Приложение № 1 и останалите договорни документи.

VIII. ДРУГИ УСЛОВИЯ

Чл. 13. (1) Всички съобщения и уведомления между страните по настоящия дого-

вор ще се извършват само в писмена форма, като условие за действителност. Кореспонденция, свързана непосредствено с извършване на дейностите по гаранционна поддръжка, може също така да бъдат извършвана чрез електронна поща на електронните адреси, заявени от ВЪЗЛОЖИТЕЛЯ в хода на предоставяне на услугите.

(2) Всички документи, описани в договора и приложенията към него, ще се съставят като електронни документи и ще се подписват от представителите на страните с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис.

Чл. 14. Спорни въпроси, възникнали при действието на този договор, се решават по пътя на споразумения, а нерешените се отнасят за решаване от компетентния съд.

Чл. 15. (1) Отговарящ за изпълнението на договора от страна на ВЪЗЛОЖИТЕЛЯ и координатор за времето на неговото действие е Мариана Цвяткова- директор на дирекция „Електронна идентификация“, Държавна агенция „Електронно управление“ (в ликвидация), телефон: +359 2949 2402, +359 876455290 , електронна поща: mtsvyatkova@e-gov.bg.

(2) Отговарящ за изпълнението на договора от страна на ИЗПЪЛНИТЕЛЯ за времето на неговото действие е: Александър Станев, Директор на дирекция „Системна интеграция и иновации“ телефон: +359 888 514 544, електронна поща: a.stanev@is-bg.net , а в негово отсъствие Стилян Горанов, Бизнес анализатор, информационни технологии, Одел „Бизнес анализ“, тел. +359 895 528 691, електронна поща: s.goranov@is-bg.net .

Чл. 16. (1) Всяка от страните по този Договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала ѝ известна при или по повод изпълнението на Договора („Конфиденциална информация“). Конфиденциалната информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и да е естество или в каквато и да е форма, включително, финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи,

спецификации, диаграми, планове, уведомления, данни, образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство. Настоящият договор и Приложение № 1 „ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ за изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID“ не съставляват Конфиденциална информация.

(2) Конфиденциалната информация за целите на настоящия договор включва и:

т. 1. съдържанието на документацията, която е станала известна при изпълнението на този договор;

т. 2. лични данни и друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на този договор;

т. 3. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на МЕУ, комуникации, мрежи и информационни системи на МЕУ, изготвени в хода на изпълнението документи и/или всякакви други резултати от изпълнението, разработени в полза на МЕУ или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящия договор.

(3) Лични данни се обработват от Страните единствено за целите на изпълнение на Договора, при стриктно спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и действащата нормативна уредба.

(4) С изключение на случаите, посочени в ал.5 на този член, Конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата Страна, като това съгласие не може да бъде отказано безпричинно.

(5) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

т. 1. информацията е станала или става публично достъпна, без нарушаване на този Договор от която и да е от Страните;

т. 2. информацията се изисква по силата на закон, приложим спрямо която и да е от Страните; или

т. 3. предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната Страна е длъжна да изпълни такова изискване;
В случаите по точки 2 или 3 Страната, която следва да предостави информацията, уведомява незабавно другата Страна по Договора.

(6) Задължения на ИЗПЪЛНИТЕЛЯ във връзка с изискванията за конфиденциалност:

т. 1. да спазва вътрешните правила за достъп и режим на работа в сградите на МЕУ;

т. 2. да спазва всички процедури и изисквания на МЕУ за работа в информационната инфраструктура на МЕУ;

т. 3. да пази в поверителност и да не разкрива или разпространява информация за другата страна, станала му известна при или по повод изпълнението на услугите, предмет на договора;

т. 4. представляващите ИЗПЪЛНИТЕЛЯ и лицата, които имат достъп до системите на МЕУ е необходимо да предоставят подписани декларации за опазване на информацията, по образец – Приложение № 2, при подписването на договора и при необходимост от предоставяне на достъп до системите на МЕУ.

(7) Задълженията по тази клауза се отнасят до ИЗПЪЛНИТЕЛЯ, всички негови поделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, като ИЗПЪЛНИТЕЛЯТ отговаря за изпълнението на тези задължения от страна на такива лица.

(8) Задълженията, свързани с неразкриване на Конфиденциалната информация, остават в сила и след прекратяване на Договора на каквото и да е основание.

<u>Непреодолима сила</u>

Чл. 17. (1) Страните не отговарят за неизпълнение на задължение по този Договор, когато невъзможността за изпълнение се дължи на непреодолима сила.

(2) За целите на този Договор, „непреодолима сила“ има значението на това понятие по смисъла на чл. 306, ал. 2 от Търговския закон. Страните се съгласяват, че за непреодолима сила ще се считат и изменения в приложимото право, касаещи дейността на която и да е от тях, и възпрепятстващи изпълнението или водещи до невъзможност за изпълнение на поетите с Договора задължения.

(3) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата Страна незабавно при настъпване на непреодолимата сила. Към уведомлението се прилагат всички релевантни и/или нормативно установени доказателства за настъпването и естеството на непреодолимата сила, причинната връзка между това обстоятелство и невъзможността за изпълнение, и очакваното времетраене на неизпълнението.

(4) Докато трае непреодолимата сила, изпълнението на задължението се спира. Засегнатата Страна е длъжна, след съгласуване с насрещната Страна, да продължи да изпълнява тази част от задълженията си, които не са възпрепятствани от непреодолимата сила.

(5) Не може да се позовава на непреодолима сила Страна:

т. 1. която е била в забава или друго неизпълнение преди настъпването на непреодолима сила;

т. 2. която не е информирала незабавно другата Страна за настъпването на непреодолима сила; или

т. 3. чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на Договора.

(6) Липсата на парични средства не представлява непреодолима сила.

Този Договор е изготвен като електронен документ и е подписан с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис, от представители на всяка от Страните, като приложенията са негова неразделна част.

Приложения:

1. Приложение № 1 – „ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ за изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID“ на ВЪЗЛОЖИТЕЛЯ;
2. Приложение № 2 – Образец на декларация за опазване на информацията.

ВЪЗЛОЖИТЕЛ:	**ИЗПЪЛНИТЕЛ:**
_____	_____
Божидар Божанов **Министър на електронното управление**	**Ивайло Филипов** **Изпълнителен директор на "Информационно обслужване" АД**
_____	_____
Ангел Петров **Главен секретар**	**Камелия Софрониева** **Главен счетоводител**

Kremena Ivanova Kancheva-Simeonova
Digitally signed by Kremena Ivanova Kancheva-Simeonova
Date: 2022.04.21 15:51:13 +03'00'

Приложение № 1

Министерство на електронното управление

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

За

Изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID

СЪДЪРЖАНИЕ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ 6
1.1. Използвани акроними 6
1.2. Технологични дефиниции 6
2. ВЪВЕДЕНИЕ 8
2.1. Цел на документа 8
2.2. За Възложителя – функции и структура 8
2.3. За проекта 9
2.4. Нормативна рамка 9
3. Цели, обхват и очаквани резултати от изпълнение на проекта 11
3.1. Общи и специфични цели на проекта 11
3.2. Обхват на проекта 12
3.3. Целеви групи 12
3.4. Очаквани резултати 12
3.5. Период на изпълнение 13
4. ТЕКУЩО СЪСТОЯНИЕ 13
5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО 15
5.1. Управление на проекта 15
5.2. Управление на риска 15
5.3. Изисквания по сигурността 16
6. ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА 16
6.1. Анализ на данните и изискванията 16
6.1.1. Функционален обхват на проекта (не е приложимо) 16
6.1.2. Специфични изисквания към етапите на бизнес анализа и разработка 17
6.2. Изготвяне на системен проект 18
6.3. Разработване на софтуерното решение 18
6.4. Тестване 19
6.5. Внедряване 19
6.6. Обучение 19
6.7. Гаранционна поддръжка 19

Параметри на гаранционната поддръжка 24

7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ 25

7.1. Функционални изисквания към информационната система 25

7.1.1. Интеграция с външни информационни системи 25

7.1.2. Технически изисквания към интерфейсите 26

7.1.3. Администриране на Системата 27

7.2. Нефункционални изисквания към информационната система 27

7.2.1. Авторски права и изходен код 27

7.2.2. Системна и приложна архитектура 28

7.2.3. Изграждане и поддръжка на множество среди 29

7.2.4. Процес на разработка, тестване и разгръщане 30

7.2.5. Информационна сигурност и интегритет на данните 31

7.2.6. Бързодействие и мащабируемост 33

7.2.7. Използваемост 35

7.2.8. Системен журнал 40

7.2.9. Дизайн на бази данни и взаимодействие с тях 40

7.2.10. Изисквания за киберсигурност 41

8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА 43

8.1. Дейност 1 Проектиране на модел на създаване, разпределение и използване на криптографски ключове 43

8.1.1. Описание на дейността 43

8.1.2. Очаквани резултати 44

8.2. Дейност 2 - Разработване на сървърна част за регистрация и използване на електронна идентичност 45

8.2.1. Описание на дейността 45

8.2.2. Регистрация на физически лица 45

8.2.3. Управление и използване на ключовите двойки 46

8.2.4. Управление на списъка с локации, които поддържат валидация на идентичността 47

8.2.5. Функционалност за валидация на идентичността от страна на служител 47

8.2.6. Управление на потребители 48

8.2.7. Процес на автентикация и атрибути 48
8.2.8. Процес на подписване 49
8.2.9. Очаквани резултати 50
8.3. Дейност 3 - Разработване на мобилно приложение за потребители за Android и iOS 50
8.3.1. Описание на дейностите 50
8.3.2. Регистрация 50
8.3.3. Идентификация 51
8.3.4. Подписване 52
8.3.5. Валидация за повишаване на нивото на електронна идентификация 53
8.3.6. Напомняне и подновяване на изтичащ сертификат 53
8.3.7. Управление на устройствата 53
8.3.8. Очаквани резултати 54
8.4. Дейност 4 - Разработване на служебно мобилно приложение за Android и iOS54
8.4.1. Описание на дейностите 54
8.4.2. Служебна валидация за повишаване на нивото на осигуреност при електронна идентификация 55
8.4.3. Очаквани резултати 55
8.5. Дейност 5 - Разработване на софтуерни библиотеки за надграждане на системи с функционалности за подписване и идентификация 55
8.5.1. Описание на дейността 55
8.5.2. Очаквани резултати 56
8.6. Дейност 6 - Консултантски услуги по пилотна интеграция в администрацията .56
8.6.1. Описание на дейността 56
8.6.2. Очаквани резултати 57
9. ДОКУМЕНТАЦИЯ 58
9.1. Изисквания към документацията 58
9.2. Прозрачност и отчетност 59
9.3. Системен проект 59
9.4. Техническа документация 59
9.5. Комуникация и доклади 60
9.5.1. Междинни доклади 60

9.5.2. Окончателен доклад 60
9.5.3. Комуникация 61
Приложение 1 към Техническа спецификация..... 62

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

1.1. Използвани акроними

Акроним	Описание
МЕУ	Министерство на електронното управление
ЗДОИ	Закон за достъп до обществена информация
ЗЕУ	Закон за електронното управление
ДХЧО	Държавен хибриден частен облак
SDK	Software development kit
API	Application programming interface/Приложно програмен интерфейс
АПК	Административнопроцесуален кодекс

1.2. Технологични дефиниции

Термин	Описание
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	Компютърна програма, която се разпространява при

Термин	Описание
код	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;

Термин	Описание
	▪ 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.
Мобилно приложение	Определението в т. 45 на ДР на ЗЕУ

2. ВЪВЕДЕНИЕ

2.1. Цел на документа

Целта на настоящия документ е да опише софтуерните изисквания към изпълнението на проект „**Изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID**“

В настоящата техническа спецификация са описани и изискванията към проектната организация, документацията и отчетността.

2.2. За Възложителя – функции и структура

Министерството е юридическо лице на бюджетна издръжка със седалище в гр. София.

Министерството на електронното управление има функции по издаване, налагане и контрол на политики, правила и добри практики в областта на електронното управление, стратегическо планиране и инициативи, бюджетно програмиране и контрол, координация на секторни политики и секторни и междуведомствени проекти.

Министърът на електронното управление провежда държавната политика в следните области:

- електронно управление;
- електронни удостоверителни услуги;
- електронна идентификация;
- мрежова и информационна сигурност;
- инфраструктура за пространствена информация;
- информация от обществения сектор в машинночетим отворен формат;
- информационните технологии и информационното общество.

При осъществяването на държавната политика в посочените области министърът на електронното управление изпълнява правомощия, възложени му със Закона за електронното управление (ЗЕУ), Закона за електронната идентификация (ЗЕИ), Закона за електронните съобщения (ЗЕС), други закони или с акт на Министерския съвет.

2.3. За проекта

Настоящият проект обхваща дейности по изграждане на приложение за мобилна електронна идентификация и подписване BGID, като целите на проекта са да се реализира въвеждане на използването на идентификация на потребителите посредством национален електронен идентификатор.

2.4. Нормативна рамка

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

Национално законодателство:

- Закон за електронното управление;
- Закон за електронната идентификация;
- Закон за електронния документ и електронните удостоверителни услуги;
- Закон за защита на личните данни и подзаконовите нормативни актове по прилагането му;
- Закон за администрацията;
- Правилник за прилагане на Закона за електронната идентификация;
- Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги;

Наредба за минималните изисквания за мрежова и информационна сигурност;

Закон за платежните услуги и платежните системи (във връзка с идентификацията на лица)

Европейско законодателство:

Регламент (ЕС) 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО;

Регламент за изпълнение (ЕС) 2015/1501 на Комисията от 8 септември 2015 г. относно рамката за оперативна съвместимост съгласно чл. 12, параграф 8 от Регламент (ЕС) 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар;

Регламент за изпълнение (ЕС) 2015/1502 на Комисията от 8 септември 2015 година за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно член 8, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар;

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните);

Регламент (ЕС) 2018/1724 на Европейския парламент и на Съвета от 2 октомври 2018 година за създаване на единна цифрова платформа за предоставяне на достъп до информация, до процедури и до услуги за оказване на помощ и решаване на проблеми, както и на произлизащите от него актове за изпълнение.

Национални стратегически документи:

Актуализирана стратегия за развитие на електронното управление в Република България 2019-2023 г.;

Актуализирана Пътна карта за изпълнение на Стратегията за развитие на електронното управление в Република България за периода 2019 - 2023 г.;

Единен модел за заявяване, заплащане и предоставяне на електронни административни услуги - https://e-gov.bg/wps/portal/agency/systems/unified-model;

Модел на интеграция с хоризонтална система за електронна автентикация - https://e-gov.bg/wps/portal/agency/systems/info-systems/e-authentication.

Актуализирана Национална стратегия за киберсигурност „КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023“

Международни стандарти:

ISO/EIC 29115:2013

БДС ISO/IEC 27001:2017

EN ISO 9001:2015

ISO 20000-1:2018

ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

ETSI EN 319 411-1/2 Policy and security requirements for Trust Service Providers issuing certificate;

ETSI EN 319 412-1 V1.1.1 (2016-02)

ICAO 9303: Машинно четими пътни документи;

NIST FRVT: Биометрично лицево разпознаване;

ISO/IEC 30107 - 3: Биометрично разпознаване на атака;

ISO/IEC 19795 - 1:2006: Ефективност на биометрична проверка;

Посочените нормативни актове и документи в областта на електронното управление и административното обслужване не са изброени изчерпателно. Изпълнението на проекта трябва да е съобразено и с всички произтичащи от законовата уредба и подзаконовите актове за нейното прилагане изисквания, включително нови промени на националното и европейското законодателство, извън посочените по-горе, имащи отношение към настоящия проект.

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

3.1. Общи и специфични цели на проекта

Проектът е насочен към изграждане на удобно и достъпно средство за електронна идентификация на потребителите на електронни административни услуги, както и за електронно подписване на заявления за електронни административни услуги чрез мобилни устройства.

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

Предоставяне на удобно и достъпно мобилно средство за електронна идентификация и подписване на електронно съдържание (с усъвършенстван електронен подпис);

Предоставяне на софтуерни компоненти за надграждане на съществуващи информационни системи с компонента за мобилно подписване;

3.2. Обхват на проекта

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

Дейност 1: Проектиране на модел на създаване, разпределение и използване на криптографски ключове;

Дейност 2: Разработване на сървърна част за регистрация и използване на електронна идентификация;

Дейност 3: Разработване на мобилно приложение за потребители за Android и iOS;

Дейност 4: Разработване на служебно мобилно приложение за Android и iOS;

Дейност 5: Разработване на софтуерни библиотеки за надграждане на информационни системи с функционалности за подписване и идентификация;

Дейност 6: Пилотна интеграция.

3.3. Целеви групи

Целевите групи, към които е насочен проектът, обхващат:

Министерство на електронното управление;

Доставчици на електронни административни услуги - административните органи, лицата, осъществяващи публични функции и организациите, предоставящи обществени услуги;

Граждани и бизнес.

3.4. Очаквани резултати

Очакваните резултати от изпълнението са:

Изградени мобилни приложения за електронна идентификация и подписване

Надградени пилотни системи с високо ниво на използване от граждани и бизнес за използване на мобилна идентификация и подписване

Повишаване на използването на вече съществуващи електронни административни услуги

Високо ниво за готовност за покриване на изискванията на предложението за изменение на Регламент (ЕС) 910/2014 за т.нар. европейски дигитален портфейл, след влизането му в сила

3.5. Период на изпълнение

Периодът на изпълнение на Дейности 1, 2, 3 и 4 е 9 месеца, считано от датата на сключване на договора.

Изпълнителят трябва да изготви подробен график, в който следва да се конкретизират сроковете за изпълнение на всяка дейност. Графикът за изпълнение трябва да бъде съобразен с продължителността на дейността и не може да надвишава периода на изпълнение.

Посоченият период на изпълнение не обхваща Дейност 5 и Дейност 6. Срокът за приключване на Дейност 5 и Дейност 6 е до 6 месеца след внедряване на системата.

При изпълнението на Дейности 1-4, Изпълнителят трябва да представи работеща базова функционалност за електронна идентификация не по-късно от 6 месеца от сключване на договора.

4. ТЕКУЩО СЪСТОЯНИЕ

Пътната карта за изпълнение на Стратегия за развитие на електронното управление в Република България за периода 2019-2023 г. предвижда реализиране на единна национална схема за електронна идентификация, базирана на средства за идентификация, издавани от държавата. Схемата е регламентирана в Закона за електронната идентификация (ЗЕИ) и Правилника за неговото приложение.

Съгласно ЗЕИ физическите лица се идентифицират в електронна среда чрез електронен идентификатор, който се съдържа в удостоверение за електронна идентичност.

Субекти в схемата са: органът за електронна идентификация в лицето на министъра на вътрешните работи, който е издател на удостоверенията за електронна идентичност, помощни органи (администратори на електронна идентичност) и центровете за електронна идентификация, които извършват проверка на електронната идентичност.

Към настоящия момент Министерството на вътрешните работи е обявило обществена поръчка с наименование „Проектиране, изграждане и управление на Система за издаване на български лични документи поколение 2019“. Проектът предвижда в дейностите по реализиране на Централизираната система за персонализация на български лични документи да бъде включено проектирането и изграждането на Централизирана система за електронна идентификация. Предвижда се още българските лични документи да бъдат носители на удостоверение за електронна идентичност, а двете системи – за електронна идентификация и за персонализация на личните документи, да бъдат изградени едновременно и в необходимата логическа съвместимост. Министерството на вътрешните работи с решение № 5785мпр-35/29.04.2020 г. е определило изпълнител за горепосочената обществена поръчка. Решението е обжалвано пред ВАС. В Закона за българските лични документи се предвижда от 01.10.2020 г. личните документи да съдържат удостоверения за електронна идентичност, но спазването на посочения срок зависи от влизане в сила на

решението за избор на изпълнител, което към настоящия момент не би могло да се предвиди.

Съгласно чл. 22, ал. 1 от Закона за електронното управление „българските граждани и дългосрочно пребиваващите чужденци, получатели на електронни административни услуги и автори на електронните изявления, се идентифицират по ред, определен със закон“. Към момента, това е ЗЕИ, но както бе посочено, електронните идентификатори все още не се предоставят на българските граждани.

Поради липсата на национална схема за електронна идентификация към момента се използват средствата, регламентирани в § 5 от ПЗР на Наредбата за общите изисквания за информационните системи, регистрите и електронните административни услуги, а именно: квалифициран електронен подпис (КЕП), персонален идентификационен код (ПИК) на НАП/НОИ и уникален код за достъп (УКД) на НЗОК, ако съответните публични органи предвиждат възможност гражданите да се идентифицират пред тях чрез тези средства. Чрез посочените средства обаче българските граждани не могат да се идентифицират, когато заявяват електронни административни услуги в други държави-членки на Европейския съюз, което препятства възможността за ползване на трансгранични електронни услуги в рамките на ЕС. Този проблем се решава само частично с решението за одобряване на нотифициране на частни схеми за електронна идентификация, прието от Министерския съвет през 2021 г.

Наред с посоченото, част от средствата за електронна идентификация като ПИК и УКД, не отговарят на изискванията на Регламент (ЕС) № 910/2014 за нива на осигуреност „значително“ или „високо“ и чрез тях не могат да се заявяват всички административни услуги. КЕП по своята същност не е средство за електронна идентификация и само временно е предвиден като такъв – ще се използва за идентификация до 1 година след влизане в продукционен режим на националната схема по ЗЕИ.

Настоящият проект ще създаде условия за сигурна и надеждна електронна идентификация на гражданите при предоставяне на електронни административни услуги, която ще отговаря на изискванията на Регламент № 910/2014 г. и предстоящите му изменения.

Позитивен аспект на настоящото състояние е наличието на хоризонталната система за електронна автентикация (еАвт 2.0), която се явява в ролята на т.нар „брокер“ в процеса на идентификация, и изпълнява частично функцията на „център за електронна идентификация“ по смисъла на ЗЕИ.

Към настоящия момент текат обсъждания по предложението за изменения на Регламент (ЕС) 910/2014, чрез които ще се въведе Европейски дигитален портфейл, които са взети предвид при подготовката на настоящата документация, доколкото това е възможно предвид липсата на финални текстове и подзаконови актове.

5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

5.1. Управление на проекта

Възложителят изисква методология за управление на проекта, която изпълнителят трябва да приложи и която съответства на най-добрите практики и препоръки, а именно Agile/Scrum/Kanban или еквиваленти.

Дейностите по управление на проекта трябва да включват като минимум управление на реализацията на всички дейности и постигане на очакваните резултати, както и разпределението на участниците в екипа за управление по роли, график и дейностите.

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.

Изпълнителят трябва да предложи график за изпълнение на проекта съгласно предвидените периоди в т.3.5 , където трябва да опише 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 изготвените документи.

5.2. Управление на риска

Изпълнителят трябва да поддържа 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 Изпълнителят следва да поддържа актуален списък с рисковете.

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

- Промяна в нормативната уредба, водеща до промяна на ключови компоненти на системата;

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;

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.

5.3. Изисквания по сигурността

Всички действия на Изпълнителя по поддържане нивото на сигурност, по отношение на поддръжката и развитието на информационните системи, следва да отговарят на изискванията на Закона за електронното управление и всички подзаконови актове по прилагането му, Закона за киберсигурност и всички подзаконови актове по прилагането му, Закона за защита на класифицираната информация, Закона за защита на личните данни и подзаконовите актове по тяхното прилагане.

6. ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА

Изпълнението на проекта включва следните етапи:

6.1. Анализ на данните и изискванията

6.1.1. Функционален обхват на проекта (не е приложимо)

Разработка и внедряване на нови публични електронни административни услуги;

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).

6.1.2. Специфични изисквания към етапите на бизнес анализа и разработка

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), както и органите, осъществяващи първоначално удостоверяване на идентичност (присъствена валидация). Чрез тестванията да се изпита и оцени използваемостта на услугите и потребителските интерфейси, както и за да бъдат отстранени затруднения и несъответствия със спецификацията;

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. При необходимост изпълнителят трябва да предложи на Възложителя адекватни промени в нормативната уредба, които да хармонизират съответните секторни нормативни изисквания с общите разпоредби на Административно-процесуалния кодекс, Закона за електронно управление, Закона за електронния документ и електронните удостоверителни услуги и приложимите подзаконови актове;

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.

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 спецификацията;
- Да се онагледи основният процес и свързаните подпроцеси, които се описват в съответните дейности за изпълнение;
- 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;
- Начин на интеграция с други системи съгласно изискванията на настоящата спецификация;

Изпълнението на задачите изисква дефиниране на модели на бизнес процеси, модели на стандартни справки и анализи, 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 или еквивалент.

Системният проект подлежи на одобрение от Възложителя в срок до 10 работни дни след предаване. 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 модулите на информационната система съгласно изискванията на настоящата техническа спецификация и системния проект;
- Провеждане на вътрешни тестове на Системата (в среда на разработчика);
- Изготвяне на детайлни сценарии за провеждане на приемателните тестове за етап „Тестване“ на проекта.

За изпълнение на дейностите по разработка на системата изпълнителят трябва да опише в системния проект приложим подход (методология) за софтуерна разработка, която ще използва, както и инструментите за разработка и средата за провеждане на вътрешните тестове. Изпълнителят трябва да опише как предложеният подход ще бъде адаптиран за успешната реализация на Системата.

6.4. Тестване

Изпълнителят, съвместно с Възложителя, трябва да проведе приемателно тестване на софтуерното решение в създадена за целта тестова среда, за да бъде валидирано , че изискванията са изпълнени.

6.5. Внедряване

Изпълнителят трябва да внедри софтуерното решение в информационната и комуникационна среда, осигурена от Министерството на електронното управление. Това включва инсталиране, конфигуриране и настройка на програмните компоненти на системата в условията на експлоатационната среда.

6.6. Обучение

Изпълнителят трябва да организира и да проведе обучения, свързани с експлоатацията на Реализираната система за екипа на Възложителя за целите на администрирането на системата.

Изпълнителят трябва да подготви обучителни материали за други административни органи, извършващи присъствена валидация.

6.7. Гаранционна поддръжка

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за период от минимум 36 месеца след внедряване 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 подаване на информация за инциденти и несъответствия.

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.

Гаранционната поддръжка включва:

- предприемане от страна на Изпълнителя на всички необходими действия, за разрешаване на назначената му заявка;
- възпроизвеждане, анализиране и разрешаване на назначената му заявка, включително създаване на временен процес на работа при невъзможност за отстраняване на инцидента в параметрите на качеството, посочени в Приложение № 1 на настоящата техническа спецификация;
- при необходимост назначаване на нови операции към заявка - в случай че е необходимо извършване на действия и от други екипи от второ ниво или заявката да бъде ескалирана към трето ниво и проследява прогреса на изпълнението ѝ до намиране на решение;
- проактивно изследване на събития с цел откриване на проблеми – коренната причина за възникването на инцидентите;
- следене на цялостния процес на развитие на заявката до постигане на решението ѝ;
- наблюдение на детайлите на инцидента, включително засегнатите други компоненти на приложението;
- при необходимост докладва на Възложителя за установени проблеми в приложението;
- при необходимост прави предложения до Възложителя за промени, свързани с решаването на регистрирани проблеми;
- промяна в конфигурационни параметри на приложението;
- оказване на съдействие на Възложителя при инсталация и оптимизация, включващи:

➢ наблюдение на основни параметри и оптимизация на отделните елементи;

➢ инсталация на разработени нови подверсии, пачове и други на системата и на използвани средства за разработка;

- поддръжка и настройка на приложението при въвеждане на нови версии или пачове на операционната система, базата от данни и сървъра за работа на приложението или при доставка на ново оборудване (хардуер и системен софтуер);

- контрол на версиите на приложния софтуер. Контролът на версиите се осъществява чрез специализиран софтуер на Възложителя или на Изпълнителя, ако такъв няма при Възложителя. Използваният софтуер ще бъде уточнен след подписване на договора.

Изпълнителят трябва да оказва съдействие на екипа на Възложителя при създаването, наблюдението и управлението на системната среда на системата, при:

- анализ и оптимизация на системната среда;
- управление на сигурността на системата и данните;
- осигуряване на работа на системата върху и с последните нови версии на софтуер от системната и приложна среда на системата.

Изпълнителят трябва да оказва съдействие на екипа на Възложителя при настройка, поддръжка и оптимизация на базата данни на системата, включващо:

- наблюдение на производителността и оптимизиране на базата данни, индекси и изпълнявани операции;
- наблюдение и диагностика на сървърите на базата данни и грешките при работа на СУБД и оказване на съдействие на Възложителя при необходимост от решаване на възникнали проблеми;
- проверка за нарушаване на консистентността на базата данни и решаване на възникнали проблеми съвместно с Възложителя, изготвяне и актуализиране на политика за създаване и актуализация на статистики на базата данни.
- преглед на дизайна на базата данни;
- възстановяване на базата данни след настъпили критични и аварийни ситуации;
- извършване на профилактика на базата данни, чрез тестване на Системата на определен период от време не по-дълъг от три месеца при различни параметри и натоварвания;

- анализ на подадените от екипите на Възложителя данни от мониторинга на функционирането на системата и производителността (статистически файлове, логове, др.).

Дейностите по гаранционна поддръжка включват корективни действия за осигуряване на нормалната работоспособност на приложението. Извършват се при възникване на проблем във функционирането на системата или при постъпила заявка от страна на Възложителя и включват:

- възстановяване на системата при пълна или частична неработоспособност в следствие на инцидент/проблем, съгласно времената, заложени в Приложение 1 към настоящата спецификация;
- възстановяване на нормалната работа на приложението при нарушаване на параметрите на качеството на обслужване, посочени в Приложение1 към настоящата техническа спецификация;
- възстановяване и коригиране на информация при неправилна работа със системата или при неправилна работа на същата, включително с директна намеса в изходния код и базите данни в случаите, когато с вградените му софтуерните инструменти не може да се извърши възстановяването или корекцията;
- преинсталиране на системата при необходимост;
- конфигуриране – промени в конфигурацията в продукционна среда;
- предоставяне на Възложителя на пачове, актуализации, специални версии и нови версии веднага, след като са налични. Всеки пач, актуализация, специална и нова версия задължително се придружава с документ, описващ отстранените грешки, извършените промени в софтуера и интерфейсите с други системи (release notes), препоръки за конфигурирането на параметрите на системната среда и персоналните компютри на потребителите, като при необходимост се извършва конфигуриране на място. В случай на извършени промени се актуализира ръководството на потребителя, описващо начина на използване на актуализираната функционалност. Изпълнителят следва да гарантира, че всички пачове, актуализации, специални и нови версии са предварително тествани и изчистени от грешки преди въвеждането им в ИТ инфраструктурите на Възложителя.
- отстраняване на открити грешки в работата на системата;

- изготвяне на справки по искане на Възложителя, свързани с функционирането на системата;
- актуализиране на функционалната и техническата документация, включително ръководствата за администратора и потребителите и изходния код на приложението с означена нова версия при извършени промени в софтуера и базата данни.

➢ Трансфер на знания към екипите на Възложителя. При изпълнението на тази група дейности Изпълнителят следва да осигури:

- оказване помощ на потребителите при работа със системата, в т.ч. консултации на място, по телефон, електронна поща (e-mail) или др.;
- оказване съдействие на Възложителя при изготвяне/актуализиране на организационни правила, процедури и други документи, свързани с използването на системата;
- провеждане на обучения на място при Възложителя за работа с приложението и изготвяне на обучителни материали. Време за изпълнение – според естеството на обучението и броя на обучаваните;
- участие при въвеждане на промените на приложението в тестова и/или продуктивна среда и провеждане на тестовите изпитания;
- актуализиране на документи, номенклатури, списъци, чек-листове, справки, декларации, удостоверения, писма, отчети и др. по искане на Възложителя поради настъпили промени в нормативната уредба, в работни процеси, процедури, организационни промени и извършване на всички необходими актуализации в базата данни и функционалностите на системата, в рамките на съществуващата функционалност. Актуализирането се извършва до 5 (пет) дни от поискването им;
- актуализиране и промени в системата, базата данни и интерфейсите към други системи във връзка с настъпили нормативни промени, промени в работни процеси, процедури, организационни промени в рамките на съществуващата функционалност. Промените се извършват в срок съгласуван между страните, но не повече от 30 (тридесет) дни;
- унифициране на етикети на полета, формат на визуализираната информация, наименование на данните/информацията в справочната част и използвана терминология в системата до 5 (пет) дни от поискването им;

- развитие на съществуващите процеси, функционалности и валидации в системата за обработка на информацията и данните в срок, съгласуван с Възложителя, но не по дълъг от 30 (тридесет) дни от поискването им;
- реализация на подобрения или разширения в справочните части или в оперативните модули - в частта им за извеждане (визуализация) на данни и допълнителна информация. Сроковете за Реализация на поисканите подобрения/разширения е до 15 (петнадесет) дни от поискването им, по график, съгласуван с Възложителя;
- създаване, разработване, генериране и предоставяне на Възложителя на различни справки и отчети, при невъзможност те да бъдат извлечени с наличната функционалност на системата;
- развитие на възможността за добавяне и съхраняване на историята на извършените действия от потребителите на системата в системен журнал, достъпен през потребителски интерфейс в изпълнение на чл. 12 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги;
- развитие на съществуващи интерфейси на системата за обмен на информация между системата и останалите системи на Възложителя и между системата и външни за Възложителя информационни системи. Сроковете за развитие на всеки интерфейс е до 15 (петнадесет) дни от заявяването му.

➢ 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.

Параметри на гаранционната поддръжка

Гаранционната поддръжка на системата се извършва в режим 8x5, като Изпълнителят следва да предложи адекватна схема на работа на служителите си за покриване на заявки за обслужване на инциденти при спазване на параметрите на качеството на обслужване, посочени в Приложение № 1 към настоящата техническа спецификация.

За да се приеме, че изпълнението е с необходимото ниво на качество за тази дейност, трябва да са изпълнени (постигнати) кумулативно и следните параметри:

- съотношение между предадени и внедрени версии на системата, не по-голямо от 3:2 (предадени: внедрени) версии;
- не повече от 5% повторно отворени инциденти;
- не повече от 10% прекъснати или грешни по време на инсталирането версии/под-версии.

При изтичане на гаранционния срок се предават актуализирани версии на системата и свързаните с нея документи и модели, в които са отразени всички коригиращи дейности, извършени от Изпълнителя в рамките на периода на гаранционната поддръжка.

7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

7.1. Функционални изисквания към информационната система

7.1.1. 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:

Национална база данни “Население” – широк набор от данни за целите на първоначалната регистрация, както и статуса на лицето при всяка идентификация (изпълнителят трябва да предложи подходящо решение за реализиране на достатъчно бързи справки, които да не забавят процеса на идентификация). Възложителят ще извърши необходимите процедури по осигуряване на локално копие за Изпълнителя на Национална база данни „Население“ за нуждите на BGID. Справките ще се извършват през това копие, както и през RegiX въз основа на идентификатор и номер на документ за самоличност;

Регистър на българските документи за самоличност - при първоначална регистрация за проверка на документ за самоличност;

Система за електронна автентикация - както като средство за идентификация през еАвт, така и при първоначална регистрация с КЕП или ПИК на НАП/НОИ. За целта Възложителят е предвидил актуализиране и доработка на необходимата функционалност в еАвт;

Система за сигурно електронно връчване - за автоматизирано създаване на профил при регистрация в системата за е-идентификация и връчване на първоначално съобщение. За реализиране на комуникацията Възложителят ще предостави пълна детайлна документация за интеграция на Системата за сигурно електронно връчване.

7.1.2. 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;

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. Тестовата среда не трябва да използва данни от продукционната среда.

7.1.3. Администриране на Системата

Системата трябва да осигурява администриране на служебните потребители и правата за достъп.

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, 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:

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

Изходният код (Source Code), разработван по проекта, както и цялата техническа документация трябва да 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.

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.

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;

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)

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;

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);

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);

Мрежата на държавната администрация (ЕЕСМ) 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 ЕЕСМ;

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. 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.
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.

7.2.4. 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

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.

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
- Използване на continuous integration практики;
- Използване на dependency management.

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.

За тестване на мобилните приложения следва да се използват инструменти, подобни на Browserstack.

7.2.5. 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; системата за ежедневен бекъп на данните следва да бъде организирана по два параметъра: географски и локален. Географският е за сигурност на съхранението на данните и застраховка (защита) от непредвидени ситуации - пожар, земетресение и др. Локалният е за скорост на възстановяване.

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

Всички модули на реализираната система (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 Edge, Google Chrome, Mozilla Firefox, Apple Safari). Преиздаването и подновяването 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;

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 информацционна 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, като предоставянето на услугата Secure TimeStamp не е включено в проекта;

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

7.2.6. Бързодействие и мащабируемост

7.2.6.1. Контрол на натоварването и защита от DoS/DDoS атаки

Системата трябва да поддържа "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.

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;

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

7.2.6.3. Бързодействие

При визуализация на екрани 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;

Изключение при бързодействието е допустимо единствено в процеса на регистрация и обработка на изпратеното от потребителя видео. Извършване на enrollment и liveness detection е възможно да отнеме повече време в зависимост от оценката на алгоритъма и натоварването на 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. 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 50%, 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 уеб стандарти за визуализиране на съдържание.

7.2.7. Използваемост

7.2.7.1. Общи изисквания за използваемост и достъпност

Да бъде предвидена възможност за изпълнение на изискванията за 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 и други, съгласно формализираните описания в чл. 14 и чл. 41 от НОИИСРЕАУ.

При проектирането и разработката на софтуерните компоненти и потребителските интерфейси същите трябва да отговарят на хармонизирания европейски стандарт БДС EN 301549:2021 като референтен стандарт и на Указанията за достъпност на уеб съдържание WCAG 2.1, ниво на съответствие – АА, 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 на 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);

Да се спазват изискванията за достъпност както на настолните и мобилните приложения, така и на уеб услугите.

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, посочени

по-горе. Допуска се използването на Captcha единствено при идентифицирани много последователни опити от предполагаем „бот“;

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 уеб базирани 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.

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).

7.2.7.2. 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, уеб услугите и др. трябва да поддържат стандартно кодиране 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;

7.2.7.3. 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 скролира 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;

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 максимално да покрива ниво на достъпност според последните стандарти на World Wide Web Consortium - Web Content Accessibility Guidelines 2.0 (WCAG 2.0), като използва най-добрите практики и техники.

7.2.8. 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.

7.2.9. Дизайн на бази данни и взаимодействие с тях

При използване на база данни (релационна или нерелационна) следва да бъдат следвани добрите практики за дизайн и взаимодействие 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.

7.2.10. Изисквания за киберсигурност

Изпълнителят да представи анализ и оценка на риска, които да послужат като основа за включване на адекватни и комплексни изисквания за мрежова и информационна сигурност. (чл. 12, ал. 1 от НМИМИС).

Изпълнителят да разработи 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 е заложено още в етапа на разработка и внедряване

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

Да се използва подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуникационните системи и техните компоненти.

Всички входни данни, постъпващи от потребителя, включително съдържанието, предоставено от потребителя и съдържанието на браузъра, като headers на препращащия и потребителски агент, трябва да бъдат валидирани.

Всички данни, изпращани от клиента и показвани в уеб страница, трябва да бъдат кодирани с HTML, за да се гарантира, че съдържанието се изобразява като текст вместо HTML елемент или JavaScript.

За защита на уеб сървърите:

- да се предвиди ограничение на заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по URL за защита от атаки от типа отказ от услуги (DoS);
- да се конфигурират типът и размерът на headers, които уеб сървърът ще приеме;
- да се предвиди ограничение във времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка, за да се минимизира въздействието и на slow HTTP атаки.
- За защита от brute force атаки да се въведе ограничение на броя неуспешни опити за влизане в системата.
- (Неприложимо) Да не се допуска извеждане на списък на уеб директориите.

Бисквитките (cookies) трябва да имат:

- флаг за защита (security flag) - този флаг инструктира браузъра, че "бисквитката" може да бъде достъпна само чрез защитени SSL канали;
- флаг HTTP only - инструктира браузъра, че "бисквитката" може да бъде достъпна само от сървъра, а не от скриптовете от страна на клиента.
- Да се предприемат мерки за защита на DNS, като задължително се прилага DNSSEC (Domain Name System Security Extensions).

Да бъдат конфигурирани CSP headers

Всички хипервръзки да имат rel=”noopener”

Да бъде изключен HTTP методът TRACE, където е приложимо

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 да 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.

- Получената информация да се архивира и се съхранява за период не по-малък от дванадесет месеца при спазване на изискванията на чл. 32 от НМИМИС.
- В записите за всяко от посочените събитията, да е отбелязано астрономическото време, когато е настъпило събитието.
- Да бъде предвидена възможност за синхронизиране на часовниците на компоненти на информационните и комуникационните системи да 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.

8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА

8.1. Дейност 1 Проектиране на модел на създаване, разпределение и използване на криптографски ключове

8.1.1. Описание на дейността

В рамките на тази дейност трябва да бъде изграден и одобрен модел за създаване, разпределение и използване на криптографски ключове за целите на реализирането на електронната идентификация и подписване. Моделът трябва да следва добрите практики и да използва т.нар. threshold signature scheme, така че да не се налага събирането на криптографски материал на едно място. Примери за реализиране на такъв модел са естонското решение Smart-ID, документирано на следния адрес:

https://github.com/SK-EID/smart-id-documentation и следния документ на IETF: https://datatracker.ietf.org/doc/html/draft-hallambaker-threshold-sigs-05.

Моделът трябва да даде отговори на следните въпроси:

вид на използваните асиметрични алгоритми

колко ключови двойки на потребител трябва да бъдат създадени за целите на идентификацията и подписването

по какъв начин трябва да бъдат разпределени частите от ключовите двойки между устройството на потребителя и сървърни модули

по какъв начин се използват сървърните хардуерни модули (HSM) и необходимо ли е закупуване на нови такива, както и какви точно характеристики са необходими

какви и колко удостоверителни вериги са необходими и каква инфраструктура на публичния ключ (PKI) следва да бъде изградена

какви стандарти да бъдат използвани за съхранение на усъвършенстваните електронни подписи

необходим ли е PIN от страна на сървъра, който съответно да бъде скрит от потребителя в приложенията, в случай, че избере биометрично отключване

какви са сценариите за възстановяване на профил при загубено устройство - повторна регистрация, съхраняване на резервни ключове и др.

какви са начините на съхранение на ключовите двойки в устройствата и минималните версии на операционните системи/среди, гарантиращи достатъчно сигурно съхранение

какъв е подходът при използване на повече от едно устройство (различни под-акаунти към една идентичност или различни акаунти; унифициране на PIN-овете)

какъв е моделът на подновяване на ключовите двойки и сертификатите и с какъв срок на валидност по подразбиране за различните нива на осигуреност

какви канали за комуникация ще бъдат използвани при заявка за идентификация - push-нотификация след посочване на ЕГН, QR код на екран, deep link и др.

по какъв начин се осъществява подписването – с QR код на екрана и deep link или с повторна идентификация и връщане на подписа в рамките на SAML 2.0 assertion.

дали и какъв подход да се използва за т.нар. liveness detection при първоначална регистрация. Условията за използване следва да включват изцяло on-premise инсталиране на системата и липса на трансфер на лични данни към трети страни.

по какъв ред и протокол да се поддържа включване и електронно подписване от други доставчици на услуги за електронно подписване в рамките на приложението (напр. настоящите доставчици на квалифицирани удостоверителни услуги, предоставящи мобилно подписване)

8.1.2. Очаквани резултати

Резултатът от тази дейност трябва да бъде системен проект, съдържащ детайлна архитектура и отговори на горепосочените въпроси, където е нужно да бъдат подкрепени със съответните анализи и данни.

8.2. Дейност 2 - Разработване на сървърна част за регистрация и използване на електронна идентичност

8.2.1. Описание на дейността

Сървърната част на системата трябва да изпълнява следните функции:

регистрация на физически лица

управление и използване на ключовите двойки

управление на списъка с локации, които поддържат валидация на идентичността

функционалност за валидация на идентичността от страна на служител

управление на устройствата за достъп на потребител

управление на административните потребители

8.2.2. Регистрация на физически лица

Сървърната част трябва да поддържа регистрация по следните начини:

Чрез идентификация с КЕП през портала на BGID. Процесът следва да преминава през няколко кратки стъпки, при които потвърдената идентификация с КЕП през портала да бъде прехвърлена към мобилното приложение чрез сканиране на QR код. Тази форма на регистрация ще дава ниво на осигуреност „високо“ на потребителя;

Чрез Модула за електронна автентикация (е-Автентикация), при което потребителят да може да използва всички допустими методи за вход, в това число ПИК на НАП и др. След потвърждаване на вход през е-Автентикация, мобилното приложение ще изисква също така процес на лицево разпознаване чрез заснемане на снимка и видео в selfie режим. Данните ще се сравняват чрез автоматизиран процес на база сравнение със снимката на заявителя, извлечена от Национална база данни „Население“. Тази форма на регистрация ще дава ниво на осигуреност „значително“ на потребителя;

Изцяло чрез мобилното приложение със заснемане на документ за самоличност, в това число лична карта или паспорт. След изпращане на снимката към сървъра, ще се извличат личните данни на лицето от машинночетимата зона на документа (MRZ зона). След потвърждаване на идентичността на потребителя, мобилното приложение ще изисква също така процес на лицево разпознаване чрез заснемане на снимка и видео в selfie режим. Данните ще се сравняват чрез автоматизиран процес на база сравнение със снимката на заявителя, извлечена от Национална база данни „Население“. Тази форма на регистрация ще дава ниво на осигуреност „значително“ на потребителя.

На гражданите трябва да бъде предоставена възможност за повишаване на нивото на осигуреност. Процесът за повишаване ще може да се прави от служител на администрация, работеща с BGID, като се изисква задължително потвърждаване на самоличността на потребителя от страна на служителя, като ще му се предоставя извлечено изображение от Национална база данни „Население“ за съпоставка.

При регистрация гражданите могат да посочат и мобилен телефон и имейл адрес за получаване на известия, както и кое от двете е предпочитаният канал за известия (по подразбиране следва да е избран имейл адресът). Въведените данни се попълват в регистрирания профил в системата за сигурно електронно връчване.

В сървърната част на системата трябва да се съхранява:

- анонимен уникален идентификатор на средството за идентификация, обвързан с конкретно издаденото eID на лицето на дадено устройство (UUID)
- личен идентификатор (ЕГН/ЛНЧ)
- необходимият криптографски материал и X.509 удостоверения, като в X.509 удостоверенията трябва да се записва анонимният уникален идентификатор на лицето (UUID)
- информацията, на база на която са издадени удостоверенията (изпратените лични данни при регистрация), в криптиран вид.
- контактна информация (имейл и телефон)

След успешна регистрация, на гражданите се създава автоматично профил в системата за сигурно електронно връчване (чрез извикване на съответно API, документация за което ще бъде предоставена от Възложителя на Изпълнителя).

Същата функционалност трябва да бъде използвана и при подновяване на изтекли сертификати спрямо периода, определен за това в Дейност 1.

8.2.3. Управление и използване на ключовите двойки

- Сървърната част трябва да съхранява и управлява части от ключовите двойки съгласно механизма, описан в Дейност 1.
- Сървърната част трябва да предоставя програмен интерфейс за подписване с частичните ключови двойки. За всяко подписване трябва да бъде подаден необходимия криптографски материал от страна на клиента за създаването на threshold електронния подпис.

Идентификаторът на потребителя следва да се съхранява в мобилните приложения, заедно с прилежащия криптографски материал.

8.2.4. Управление на списъка с локации, които поддържат валидация на идентичността

Администраторите на системата трябва да могат да добавят и премахват локации с географски координати на всяка една администрация, която борави с BGID.

За всяка локация трябва да се посочва адрес, имена на институция, геокоординати и работно време, като в случай, че част от тази информация е налична в административния регистър, тя трябва да бъде извлечена от там. За този модел на извличане на данните Възложителят следва да предостави пълна детайлна документация за API за извличане на данните на Изпълнителя.

Изборът на геокоординати трябва да става с помощта на карта или друг улеснен метод за избор на местонахождение.

Видовете институции трябва да бъдат предварително дефинирани и да се избират от списък (напр. РУП(МВР), Общинска администрация, Български пощи, както и частни субекти, разполагащи с мрежа за обслужване на граждани). Към тях трябва да бъде посочвано териториалното звено (напр. РУП (МВР) – гр. Казанлък).

За всяка организация управлението на достъпа на служителите ще става посредством идентификация през централизирана активна директория на държавната администрация, която се изгражда от Възложителя. След идентификация през АД в административен модул на портала на BGID, ще се актуализира автоматично списък с лица, които могат да използват служебните административни функционалности за служители.

8.2.5. Функционалност за валидация на идентичността от страна на служител

Тъй като различните начини на първоначална регистрация водят до различни нива на осигуреност, има необходимост от предоставяне на възможност за повишаване на нивото на осигуреност (напр. от „значително“ към „високо“). Това ще се осъществява посредством еднократно присъствено идентифициране на титулярите на електронна идентичност.

На обучени за целта служители в административни структури, Български пощи и други организации трябва бъде предоставена функционалност за

валидиране на идентичността на физическите лица и съответно повишаване на нивото на осигуреност.

Системата ще работи с мобилно устройство, на което е инсталирана необходимата функционалност. При валидация служителят качва снимка на личната карта/паспорта, направена с приложението, след като сканира QR код от екрана на приложението на потребителя. Функционалностите на служебното приложение са описани в т. 8.4 – Дейност 4.

8.2.6. Управление на потребители

Системата трябва да поддържа Role Based Access Control (RBAC), като проверките за достъп до грануларни функционалности трябва да бъдат извършвани в сървърния бек-енд (Server Authoritative RBAC). Това изискване не изключва имплементиране на аналогични проверки и във фронт-енд приложенията, за да се осигури по-добра ползваемост за служебните потребители и администраторите, но такива проверки във фронт-енд приложенията не могат да заместят проверките в бек-енда.

Системата трябва да поддържа като минимум следните роли, със следните права:

- Администратор – пълни права върху системата, вкл. да създава и изтрива локални администратори
- Редактор на локации – с права да добавя, редактира и изтрива локации за присъствена валидация
- Локален администратор – има право да създава и изтрива валидатори за дадена организация (напр. МВР, общинска администрация, Български пощи)
- Валидатор – служител, който извършва присъствена валидация по 8.1.1.4 с цел повишаване на нивото на осигуреност

Правата за достъп до функционалности трябва да бъдат дефинирани в йерархична номенклатура (таксономия) на няколко нива и трябва да се реализира функционалност за създаване на допълнителни роли, за които се да може да се дефинират различни комбинации от права за достъп до функционалности от номенклатурата.

Идентификацията на вътрешните потребители трябва да се извършва по същия начин, както и за всеки гражданин, използващ приложението, но да се изисква ниво на осигуреност „високо“.

8.2.7. Процес на автентикация и атрибути

В случай, че бъде избран подход с push-нотификация, процесът на идентификация е както следва:

- Потребителят заявява идентификация в интернет страница на доставчик на услуги
- Потребителят бива препратен към системата за е-автентикация, където избира средство за идентификация BG EID. Има опция тази стъпка да бъде пропусната, ако на страницата на доставчика на услугата бъде избрано, че желаното средство е именно това.
- Без значение дали услугите се използват на мобилно или на настолно устройство, след като потребителят въведе ЕГН, се изпраща Push-заявка към мобилното устройство на потребителя за потвърждаване на идентификацията. Следва да има разумни ограничения за броя идентификации за период от време.
- Системата връща съответния отговор на системата за е-автентикация по SAML 2.0 (или OpenID Connect, ако той се поддържа)

В случай, че бъде избран подход със сканиране на QR код, процесът на идентификация се различава от гореописания в частта, в която вместо посочване на ЕГН и push-нотификация, се сканира QR код, генериран от сървърната част.

Атрибутите, които системата трябва да връща, трябва да са съобразени с изискванията за системата за електронна автентикация. В допълнение, трябва да има атрибут с анонимен индентификатор, който е случайно генериран за всеки отделен ключ (тоест за всяко устройство или за всяко отделно генерирано ID на даден потребител) Този анонимен индентификатор ще се използва и при подписването на документи с приложението.

Във всички компоненти адресът на системата за електронна автентикация трябва да бъде конфигурируем, за да позволява в бъдеще добавяне на системи, различни от еАвт 2.0.

8.2.8. Процес на подписване

Съществуват различни възможности за реализация на процес на подписване, като най-подходящата следва да бъде предложена и избрана в Дейност 1.

В случай, че в рамките на Дейност 1 бъде избран подход за подписване чрез повторна идентификация, системата трябва да обработва SAML 2.0 заявки, съдържащи хеш и описание на подписвания документ/документи, като изпрати тези данни и на мобилното приложение при заявката за идентификация, и съответно върне отговор с резултата от подписа под формата на атрибут(и).

В случай, че бъде избран подход със сканиране на QR код, съдържащ хеша за подписване, в сървърната част следва да бъде реализирана единствено базова функционалност за подписване на подадения хеш със сървърната част от частния ключ.

Изпълнителят трябва да предложи вариант, в който оригиналният документ за подписване да бъде изпратен на лицето (към профила му за електронно връчване), както и да бъде предоставен вариант за проверка на хеша на този документ, за да има възможност подписващият да се увери, че подписва правилния хеш.

8.2.9. Очаквани резултати

Като резултат от дейността трябва да бъде реализирана и разгъната на продукционна среда сървърна част на системата, към която да бъдат насочени приложенията по Дейност 3 и Дейност 4.

8.3. Дейност 3 - Разработване на мобилно приложение за потребители за Android и iOS

8.3.1. Описание на дейностите

В рамките на Дейност 3 трябва да бъдат разработени мобилни приложения за най-популярните операционни системи, както следва:

- Android 9;
- Apple iOS 14 и Apple iPadOS 14;

Функционалностите на двете приложения трябва да са идентични;

Потребителският интерфейс и облика на двете приложения трябва да са идентични, доколкото е възможно, предвид особеностите на двете популярни мобилни платформи;

Двете приложения трябва да бъдат разработени поотделно като т.нар. “native” приложения, освен ако Изпълнителят не аргументира, а Възложителят приеме, алтернативен подход с използване на универсален фреймуърк, който таргетира множество платформи.

Двете приложения трябва поддържат и да работят:

- На смарт-телефони (напр. с размер на екраните 4.7“ – 6.7“), и на фаблети и таблети (напр. с размер на екраните >6.8“), поддържащи съответните версии на операционните системи, включително и на HDPI дисплеи;
-
- В режим “portrait” през цялото време, без значение от ориентацията на устройството;
- В режим „day mode” и в режим “night/dark mode”.

8.3.2. Регистрация

Мобилните приложения трябва да предоставят възможност за регистрация по един от начините, посочени в Дейност 2.

При използване на международен паспорт следва приложението да изчита необходимата информация от MRZ зоната на документа за прочитане на съдържанието на електронния носител на информация в паспорта съгласно ICAO стандарта по т.нар. BAC (Basic Access Control) и SAC (Supplemental Access Control).

За генерирането на ключовите двойки трябва да се използва secure random функционалността на операционната система.

Частта от ключовите двойки, която се съхранява в мобилното устройство, трябва да бъде съхранявана в сигурното хранилище за ключове, поддържано от съответното устройство.

.

8.3.3. Идентификация

В случай, че по Дейност 1 е избран вариант за идентификация с QR код, съответно deep link, мобилното приложение трябва да поддържа сканирането на QR кода и обработването на deep link.

В случай, че в Дейност 1 е избран подход с push-нотификация, при стартиране на идентификация от браузър (без значение на настолно или мобилно устройство), на мобилното устройство трябва да се появи известие, след натискането на което, потребителят трябва да може да потвърди идентификация.

И при двата подхода на екрана на устройството трябва да бъдат показани данни на доставчика на услугата и какви лични данни ще получи. Трябва да бъдат поддържани следните подходи на тази функционалност:

- Информативен, за идентификация към местни административни органи, при които данните ще бъдат получавани по друг канал, но доставчикът на услугата трябва да опише в SAML или OpenId Connect заявката си какви данни от първични регистри използва за лицето
- Автоматичен, за интегрираните доставчици на услуги, които изискват идентификация. При този подход данните, които ще са необходими и ще се извличат, ще са предварително регистрирани и дефинирани в BGID и респективно ще бъдат ограничени като формат и количество още при интеграцията.

Идентификацията трябва да се извърши с биометрично потвърждение и/или с PIN код. При нужда PIN-кодът за отключване на локалните части на ключа трябва да се съхранява в пространство, достъпно само за приложението. Изпълнителят следва да предложи анализ на риска във връзка с използването само на едно от двете средства (биометрия и PIN). Също така

да бъде прецизирана възможността за минимизиране на необходимостта от многократно въвеждане на PIN код/биометрия от страна на потребителя.

След идентификация пред BGID потребителят ще трябва да има достъп до следните функционалности:

- Информация за текущото лице;
- Визуализация на уникален за сесията персонален QR код, идентифициращ потребителя на конкретното устройство, който да може да се използва за сдвояване в различни сценарии;
- Преглед на извършените електронни идентификации и електронни подписвания, включително и информация за устройството и IP адреси;
- Унищожаване на електронната идентичност/сертификата за електронен подпис.

8.3.4. Подписване

В зависимост от избрания метод за подписване в Дейност 1, приложенията трябва да отговарят на следните изисквания:

Подписването на електронно съдържание ще бъде достъпно след успешното преминаване на процеса на електронна идентификация.

(В случай на използване на повторна идентификация за подписване) - да предостави идентичен процес както при идентификацията, с изключение на визуализираното на екрана съобщение, което трябва да съдържа информация за подписваните документи

8.3.5. (В случай на използване на QR код/deep link) – да има отделна секция за подписване, при която сканираното (или отвореното през deep link) съдържание да бъде подписано и изпратено с POST заявка към еднократния линк, съдържащ се в QR кода / deep link-а. BGID трябва да може да гарантира идентичността на приложението, което генерира съдържанието. По този начин потребителите ще бъдат предпазени от имитиращи сайтове, които изискват автентикация и крадат личните данни на потребителя. За целта QR кодът следва да съдържа само идентификатор на системата и идентификатор на документа, а самия хеш за подписване ще се получава от сървърната част на BGID след проверка на самоличността на приложението, което ги изисква. За целта всяка интеграция с BGID ще трябва да е предварително дефинирана.

Валидация за повишаване на нивото на електронна идентификация

Приложенията трябва да поддържат функционалност за валидация. При избор на „Валидация“ от менюто или заглавния екран трябва да се визуализира QR код и инструкция той да бъде показан, заедно с документ за самоличност, на служител в една от одобрените локации.

Системата (както сървърната част, така и мобилните приложения), трябва да показва и списък с локации на карта, с възможност за търсене по населено място или пощенски код и с опция за отваряне на приложение за навигация до съответната локация.

Бутонът за валидация не следва да се показва, ако нивото на осигуреност е високо.

8.3.6. Напомняне и подновяване на изтичащ сертификат

3 месеца преди изтичане на валидността на сертификата приложенията трябва да позволяват подновяване по начин, определен в Дейност 1.

Подновяването трябва да използва същата функционалност, както при регистрация, в случай че съответното удостоверение е изтекло.

Подновяването в рамките на валидността на удостоверението (до 3 месеца преди датата на изтичане) трябва да може да става с използване на все още валидните удостоверения, без необходимост от повторно преминаване на процесите по валидация.

8.3.7. Управление на устройствата

В приложението трябва да има секция, в която да се визуализират всички устройства на текущия потребител. За всяко устройство трябва да бъде визуализиран последния IP адрес, от който е било използвано.

- При повече от едно устройство, потребителят трябва да може да деактивира устройство от списъка, като последващи действия с това устройство трябва да са невъзможни. При деактивирането трябва да бъде избрана причина „Загубено устройство“, „Подмяна на старо устройство“ и др.

При добавяне на ново устройство трябва да бъде изпращано известие, вкл. на регистрираните с първото устройство имейл и/или телефон.

Всяко ново устройство, което се добавя, преминава през стандартния процес на регистрация, описан в Дейност 2. При регистрация на ново устройство, всички регистрирани устройства получават ниво на осигуреност до най-

високото, получено при която и да е от регистрациите. Процесът на Валидация повишава нивото на всички устройства.

В случай, че приложението бъде изтрито и няма друго устройство, на което съответното физическо лице има инсталирано приложение, то трябва да се премине към повторна първоначална регистрация.

Премахването на регистрация в случай на ограничен достъп до единствено устройство ще става чрез съдействие от екип на Центъра за поддръжка.

8.3.8. Очаквани резултати

Като резултат от тази дейност трябва да има:

Подадени за публикуване приложения в Google Play Store и Apple App Store с отстранени всички технически забележки, възникнали в процеса на одобрение от страна на проверяващите администратори на съответните мобилни платформи.

Публикуван изходен код на приложенията.

Сториборд „walkthrough" клип за основните функционалности на приложенията и начинът им на използване.

8.4. Дейност 4 - Разработване на служебно мобилно приложение за Android и iOS

8.4.1. Описание на дейностите

В рамките на Дейност 4 трябва да бъдат разработени служебни мобилни приложения за най-популярните операционни системи, както следва:

- Android 9;
- Apple iOS14;

Служебните мобилни приложения ще бъдат достъпни и ще се използват от служебни лица, които имат специфични функции, свързани с администрирането на крайни потребители на системата.

За служебните мобилни приложения важат и трябва да бъдат изпълнени всички изисквания, дефинирани в т. 8.3.1 - 8.3.8, с изключение на изискванията в т. 8.3.5, които трябва да бъдат реализирани от гледна точка на служебните потребители, които имат ролята „Валидатор".

Възможна е реализацията на функционалността по Дейност 4 да бъде включена като част от приложението по Дейност 3, като тя ще бъде достъпна след електронната идентификация на съответното длъжностно лице.

8.4.2. Служебна валидация за повишаване на нивото на осигуреност при електронна идентификация

Приложенията трябва да поддържат функционалност за валидация. При избор на „Валидация“ от менюто или заглавния екран, трябва да се включва камерата за сканиране на QR код на потребител от екрана на неговото устройство, който е активирал функцията за „Валидация“ на клиентското приложение.

Бутонът за валидация не следва да предизвиква действие, ако след сканиране на QR кода на потребителя се окаже, че нивото на осигуреност вече е валидирано до „Високо“, но събитието трябва да се регистрира в бек-енда.

На следваща стъпка, служителят трябва да може да види в служебното приложение снимката на документа за самоличност на потребителя и да я сравни със:

- Същият документ за самоличност, представен физически от лицето за „Валидация“;
- Образ на документа за самоличност, изтеглен от Национална база данни „Население“;

Служителят трябва да снима представения физически документ за самоличност, както и заявителя, и да потвърди изрично в приложението, че сравнението е извършено и че документите за самоличност съвпадат;

8.4.3. Очаквани резултати

Като резултат от тази дейност трябва да има:

Подадени за публикуване приложения в Google Play Store и Apple App Store с отстранени всички технически забележки, възникнали в процеса на одобрение от страна на проверяващите администратори на съответните мобилни платформи.

Публикуван изходен код на приложенията.

8.5. Дейност 5 - Разработване на софтуерни библиотеки за надграждане на системи с функционалности за подписване и идентификация

8.5.1. Описание на дейността

В рамките на тази дейност трябва да бъдат разработени софтуерни библиотеки за следните нужди:

Генериране на бутон/линк за идентификация и подписване в рамките на интернет страницата на доставчиците на услуги

Генериране на QR кодове (ако е приложимо) в рамките на интернет страницата на доставчиците на услуги

Обработка на отговор на заявка за подписване (в случай, че се използва метода на повторната идентификация)

Подписване на подаден QR код (в случай, че се използва метода за подписване с QR код)

Обработка на изпратена директно заявка за подписване (в случай, че се използва метода с QR код)

При генериране на заявката за подписване, следва да се използва подходящ канал за обмяна на данните в съответствие с описаният подход в Дейност 1 (напр. SAML 2.0 AuthnRequest extensions атрибута).

При генериране на линк за автентикация, библиотеката трябва да позволява посочване на минимално необходимо ниво на осигуреност, което е допустимо за вход в съответната системата.

Библиотеките трябва да бъдат разработени за следните програмни езици:

За клиентската част – JavaScript

За сървърната част – Java, C#, PHP

8.5.2. Очаквани резултати

Библиотеките ще бъдат подписани (където е приложимо) и публикувани в популярните хранилища за библиотеки – напр. Maven Central, NuGet, PEAR.

Документация, съдържаща примери за използването на библиотеките, ще бъде публикувана заедно с библиотеките на публично хранилище.

8.6. Дейност 6 - Консултантски услуги по пилотна интеграция в администрацията

8.6.1. Описание на дейността

В рамките на проекта, координирано с други институции, трябва да бъде реализирана идентификация чрез системата за електронна автентикация и настоящата система, както и подписване, със следните най-често използвани системи в администрацията:

Портал за електронни услуги на НАП – идентификация през системата за електронна автентикация

Електронни услуги на НОИ – идентификация през системата за електронна автентикация

Портал за електронни услуги на МВР

Система за електронни форми на МЕУ

Публичните ЕАУ на АВ

Публичните ЕАУ на АГКК

Изпълнителят трябва да предостави консултантски услуги на съответната институция и да подкрепи усъвършенстването на системите.

Изпълнителят трябва да изпълни софтуерна разработка на функционалности, част от портала в проекта, които да бъдат използвани от екип за поддръжка на BGID. Изграждането на необходимата инфраструктура и свързаност, офис помещения, екип и техника за извършване на самата поддръжка не са част от настоящия проект и следва да бъдат осигурени от Възложителя.

Софтуерната разработка на модулите за центъра за поддръжка включват следните функционалности:

- В случаите, когато по време на регистрация възниква проблем с лицевото разпознаване или удостоверяването на документите, на мобилното приложение на потребителя ще се извежда съобщение, че следва да изчака обработка. Данните ще се подават на екипа за поддръжка, който ще преглежда ръчно всяка незавършена регистрация и ще има възможност или да я потвърди директно през портала, или да я прекрати, като изпрати отговор с искане на повторен процес на идентификация към потребителя;

- Центърът за поддръжка ще отговаря на въпроси по електронна поща, телефон или изпратени през мобилното приложение въпроси, когато това е приложимо;

- Екипът на центъра за поддръжка ще отговаря и за предоставяне на инструкции и съдействие на представителите на администрациите, които използват BGID, като осигуряват техническо съдействие по служебните им задължения и функционалности за това как се работи с BGID, за управлението на потребителските групи и др.

8.6.2. Очаквани резултати

В резултат на дейността, входът в горе посочените системите трябва да може да се осъществява с изграденото по този проект средство за електронна идентификация и

услуги в рамките на тези системи трябва да могат да бъдат заявявани чрез подписване с разработената система.

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 на български език;

Допуска се генерираната документация на базата на изходният код да бъде на английски език;

Всички документи трябва да бъдат предоставени от Изпълнителя в електронен формат (ODF/Office Open XML/MS Word DOC/RTF/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 уеб услуги, команди, структури от данни и др.

Документацията за публичния приложен 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

Документацията и помощните материали изискуеми за различните дейности на проекта, които Изпълнителят предоставя на Възложителя, трябва да бъдат:

- на български език;
- в електронен формат;
- копирането и редактирането на предоставените документи и материали следва да бъде лесно осъществимо;

9.3. Системен проект

Изпълнителят 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 приложения, 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 Ръководство за ползвателите на приложението. 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. Комуникация и доклади

За успешното изпълнение на проекта изпълнителят трябва да предложи 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:

9.5.1. Междинни доклади

Междинните доклади трябва да бъдат представяни, както следва:

- При приключване на Дейност 1, включващ етап 1 и етап 2 от т. 6 от настоящия документ;
- При предаване на работеща базова функционалност за електронна идентификация като част от изпълнението на Дейности 2, 3 и 4, включващ част от етап 3 от т. 6 от настоящия документ;
- При приключване на Дейности 2, 3 и 4, включващ етапи 3, 4 и 5;
- При приключване на Дейности 5 и 6, включващ етап 6 от т. 6 от настоящия документ;

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

Междинният доклад 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.

9.5.2. Окончателен доклад

В края на периода за изпълнение, включващ дейности от 1 до 6, както и етапи от 1 до 6, с изключение на етап 7 „Гаранционна поддръжка“, трябва да се представи окончателен доклад. Окончателният доклад трябва да съдържа описание на изпълнението и постигнатите резултати.

9.5.3. Комуникация

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. Докладите се одобряват от отговорния/отговорните служител/служители в срок до 5 работни дни.

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.

Приложение 1 към Техническа спецификация

Параметри на качеството на обслужване на мобилното приложение за електронна идентификация и електронно подписване – BGID

Таблица 1 Дефиниции

Термин	Дефиниция
Работоспособност	Процентът на договорените часове, за които мобилното приложение BGID е достъпно за определен период от време.
Светла част на денонощието	От 08.00 часа до 20.00 часа
Извън светлата част на денонощието	От 20:00 – 08:00 часа всеки работен ден, събота, неделя, национални и официални празници
Работни часове (Работно време)	08:00-20:00 всеки работен ден
Инцидент	Всяко събитие, което причинява или може да предизвика прекъсване и/или намаляване на качеството на услуга, предоставяна чрез мобилното приложение BGID.
Продължителна неработоспособност	Прекъсване на услуга, предоставяна от мобилното приложение BGID за повече от четири (4) работни часа.
Планирана неработоспособност	Планирано прекъсване на работата на мобилното приложение BGID.
Неработоспособност	Неспособността на мобилното приложение BGID да осигури нормално обслужване на потребителите, съгласно определените параметри на качеството.
Непланирана неработоспособност	Неочаквано прекъсване на една или повече услуги, предоставяни чрез мобилното приложение BGID или значително намаляване на параметрите на качеството на предлаганата услуга.

Термин	Дефиниция
Осигуряване на нормално обслужване	Постигане на работоспособност на мобилното приложение BGID, съгласно посочените проценти за наличност и достъпност на месечна база.
Критична функционалност не функционира нормално	Функционалност, която не позволява обслужване на потребителите или забавянето в изпълнението им надвишава нормалните в конкретния случай.
Услуга, предоставяна чрез мобилното приложение BGID	Електронна идентификация на потребителите на електронни административни услуги, както и електронно подписване на заявления за електронни административни услуги чрез мобилно устройство.
Наличност	Процент на договорените часове, за които мобилното приложение BGID е достъпно за определен период от време.
Достъпност	Способността на мобилното приложение BGID да осигури нормалното обслужване и работа на крайните потребители с него.
Непланирано прекъсване	Всяко прекъсване, за което Възложителя не е уведомен 7 работни дни предварително.
Система за управление на инциденти/проблеми	Софтуерният инструмент, който се използва от Възложителя за регистриране и управление на инциденти/проблеми.
Регистриране на инцидент	Действия на оторизирано лице по описание на възникнал инцидент в Системата за управление на инциденти/проблеми.
Процедура за управление на инциденти и проблеми	Процедурата е детайлно описана в настоящата техническа спецификация.
Време на реакция	Времето от регистрирането на инцидент/проблем в Системата за управление на инциденти/проблеми до започване на работа от страна на Изпълнителя по отстраняването му.

Термин	Дефиниция
План за решение	Описание на действията на Изпълнителя за отстраняване на инцидент/проблем или предлагане на временно решение, което да възстановява поне частично работоспособността на мобилното приложение BGID.
Специална версия	Версия, създадена за да се реши конкретно възникнал един или няколко инцидента със степен на критичност 1 или 2. Предава се от Изпълнителя в определените от Възложителя срокове от момента на изтичане на времето за реакция.
Следваща версия	Версия за отстраняване на инциденти/проблеми съгласно плана за дейностите по договора.
Срок за отстраняване на инцидент	Максималното време за реализиране на плана за решение.
НКГ	Наличност за календарна година.
МОД	Максимално сумарно отпадане на денонощие.
МБрО	Максимален брой отпадане на денонощие.

Определяне на степента на критичност на инцидент

Степента на критичност на възникнал инцидент се определя съгласно критериите, описани в

Таблица 2 Приоритети:

Таблица 2 Приоритети

Приоритет	Въздействие върху работните процеси
1 Критичен	Критично влияние върху работните процеси. Изисква незабавно действие, като работата продължава до неговото отстраняване.

Приоритет	Въздействие върху работните процеси
	Пълно прекъсване в работата на мобилното приложение BGID. Недостъпност до предоставяните от мобилното приложение BGID функционалности, която пряко и съществено засяга способността на ключови или голям брой потребители да използват приложението и ЕАУ, достъпни чрез него. Висок риск от финансови загуби и/или засягане на имиджа на ДАЕУ или негови контрагенти; Създава висок риск за компрометиране на информация в системите на електронното управление. Нарушена комуникация с аналогични системи на електронното управление вследствие на дефект или отпадане на BGID. Риск за съществено прекъсване или излизане от строя на мобилното приложение BGID. Критична функционалност - не функционира нормално или има критично и негативно отражение върху операциите на потребителите или системната среда на Възложителя или е възникнало непланирано преустановяване на достъпността.
2 Висок	Съществено влияние върху работните процеси. Изисква ангажиране на необходимите ресурси за отстраняването на проблема, като работата продължава в нормалните работни часове до неговото отстраняване. Влошаване на качеството на предлагана услуга или достъп до такава, без пълно прекъсване; Създаване на сериозен риск от възникване на инцидент с критичен приоритет; Критична функционалност - функционира непълноценно или има силно

Приоритет	Въздействие върху работните процеси
	неблагоприятно отражение върху работните процеси вследствие на неприемлива производителност или генериране на грешни данни.
3 Среден	Несъществено влияние върху работните процеси. Изисква ангажиране на необходимите ресурси за отстраняване на проблема, като работата за неговото отстраняване е не повече от 7 работни дни. Ограничено въздействие върху работата на мобилното приложение BGID, което засяга или създава неудобство за изпълнение на отделни функции, без да има цялостно отражение върху функциите му. Забавяне на отстраняването му може да доведе до възникване на инцидент от по-високо ниво. Нормалната производителност на мобилното приложение BGID или част от него е влошена, но по-голяма част от функционалната му способност е незасегната.
4 Нисък	Няма пряко влияние върху работните процеси в момента на възникването му. Изисква ангажирането на необходимите ресурси за отстраняване на проблема, като работата за неговото отстраняване е не повече от 14 работни дни В момента липсва пряко влияние върху функционирането на мобилното приложение BGID, но нерешаването му в определен срок крие потенциален риск от възникване на инцидент с по-висок приоритет. Обикновено се свързва с подобряване на функционирането на услуга, предоставяна от мобилното приложение BGID или развитието й. Отстраняването се планира съвместно с Възложителя и е обект на средносрочно планиране. Възложителят може да изисква информация или помощ по възможните решения.

Параметри на качеството при отстраняване на инцидент

Таблица 3 Параметри на качеството при отстраняване на инцидент

Приоритет на инцидента	Време за реакция, max	План за решение, max	Начин на отстраняване	Срок за отстраняване на инцидента, max
1	30 минути	2 ч.	В специална версия	6 часа
2	1 час	4 ч.	В специална версия	12 часа
3	1 работен ден	3 работни дни	В следваща версия	7 работни дни
4	1 работен ден	1 седмица	В следваща версия	14 работни дни

Забележки:

(a) Всички понятия са съгласно Таблица 1 Дефиниции;

(b) Приоритетите се определят от Възложителя, съгласно точка „Определяне на степента на критичност на инцидент“;

(c) За инциденти от 1 и 2 приоритет, ако за времето на отстраняване на проблема бъде намерено временно решение, с което изцяло се възстановява работоспособността на мобилното приложение BGID, Възложителят може да снижи приоритета на инцидента без да го закрива.

(d) Всички, посочени в таблицата, времена започват да текат от момента на регистриране в Системата за управление на инциденти на Възложителя.

(e) При обективна невъзможност да бъдат спазени сроковете в таблицата, Възложителят може да ги промени за конкретен инцидент.

Параметри на качеството при отстраняване на проблем

Таблица 4 Параметри на качеството при отстраняване на проблем

Приоритет на проблема	Време за реакция, max	План за решение, max	Начин на отстраняване	Срок за отстраняване на проблема, max
1	1 час	4 часа	В специална версия	24 часа
2	2 часа	24 часа	В специална	72 часа

Приоритет на проблема	Време за реакция, max	План за решение, max	Начин на отстраняване	Срок за отстраняване на проблема, max
			версия	
3	1 работен ден	4 работни дни	В специална версия	7 работни дни
4	1 работен ден	1 седмица	В следваща версия	14 работни дни

Забележки:

(a) Всички понятия са съгласно Таблица 1 Дефиниции;

(b) За инциденти от 1 и 2 приоритет, ако за времето на отстраняване на проблема бъде намерено временно решение, с което изцяло се възстановява работоспособността на мобилното приложение BGID, Възложителят може да снижи приоритета на инцидента без да го закрива.

(c) Всички, посочени в таблицата, времена започват да текат от момента на регистриране в Системата за управление на инциденти на Възложителя.

(d) Времената за отстраняване на проблем не включват времето, необходимо за преглед на мобилните приложения според политиките за публикуване в съответната платформа за приложения.

Наличност и достъпност на Мобилното приложение за електронна идентификация и електронно подписване – BGID

Таблица 5 Наличност и достъпност на Мобилно приложение BGID

Приложно поле	Наличност за календарна година - НКГ	Максимално сумарно отпадане на денонощие - МОД	Максимален брой отпадане за денонощие МБрО
1. Мобилно приложение BGID	99,680 %	Не повече от 60 минути	4 броя

(a) Всички понятия са съгласно Таблица 1 Дефиниции

Приложение № 2

(Образец)

Д Е К Л А Р А Ц И Я

ЗА ОПАЗВАНЕ НА ИНФОРМАЦИЯ

Долуподписаният/ та ……..,

ЕГН: .....,[1] в качеството ми на ……., декларирам, че ще пазя в тайна, станалата ми известна във връзка с изпълнението на Договор № ……/…..... г.[2] информация, съдържаща данни, представляващи данъчна и осигурителна информация, лични данни или друга защитена от закон или по силата на договора информация. За неизпълнение на тези задължения ми е известно, че нося предвидената в съответните нормативни актове отговорност.

Запознат/а съм с разпоредбата на чл. 270 от ***Данъчно-осигурителния процесуален кодекс***, съгласно която, ако разглася, предоставя, публикувам, използвам или разпространя по друг начин факти и обстоятелства, представляващи данъчна и осигурителна информация, ако не подлежа на по-тежко наказание, ще бъда наказан/а с глоба от 1000 лв. до 5000 лв., а в особено тежки случаи - от 5000 лв. до 10 000 лв.

Декларирам, че ще пазя в тайна, станалата ми известна информация, относно съдържанието на документация, вътрешни правила, процедури, организация, структура, начин на функциониране, комуникации, мрежи и информационни системи на Министерството на електронното управление (ВЪЗЛОЖИТЕЛЯ), изготвени в хода на изпълнението документи и/или всякакви други постигнати резултати от изпълнението, както и че няма да разгласявам, използвам или предоставям на трети лица разработена в полза на ВЪЗЛОЖИТЕЛЯ документация или програмен код в явен и изпълним вид във

---

1 *В случай, че лицето е чужденец, се вписват съответните идентификационни данни.*

2 *Вписва се референтен номер на Договора, в договорния регистър на ВЪЗЛОЖИТЕЛЯ.*

връзка с изпълнението на този договор, с изключение на случаите, когато съм задължен по закон за това.

При обработването на данните се задължавам да спазвам разпоредбите на ***Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО*** и ***Закона за защита на личните данни***.

Известна ми е отговорността по чл. 284 от ***Наказателния кодекс***, а именно: налагане на наказание лишаване от свобода до две години или пробация, ако във вреда на държавата, на предприятие, организация или на частно лице съобщя другиму или обнародвам информация, която ми е поверена или достъпна по служба и за която зная, че представлява служебна тайна.

Ще спазвам изискванията на действащата нормативна уредба в областта на мрежовата и информационната сигурност.

Известна ми е отговорността по Глава 9а от Особената част на ***Наказателния кодекс***, относно достъп до компютърни данни в компютърна система без разрешение, добавяне, промяна, изтриване или унищожаване на компютърна програма или компютърни данни, въвеждане на компютърен вирус в компютърните системи или мрежи на ВЪЗЛОЖИТЕЛЯ, разпространение на пароли или кодове за достъп до компютърна система или до компютърни данни и от това последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна.

Подпис:

(подписване с електронен подпис)