Д О Г О В О Р

№ .....

РД-02-29-43/16.10.2026

В гр. София, между:

1. МИНИСТЕРСТВОТО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ, ЕИК 177549112 с адрес: гр. София 1000, ул. „Княз Александър I“ № 12, представлявано от Иван Василев – министър на иновациите и дигиталната трансформация и – директор на дирекция „Финанси и управление на собствеността“, в качеството на ВЪЗЛОЖИТЕЛ и БЕНЕФИЦИЕР, наричано по-долу за краткост ВЪЗЛОЖИТЕЛ

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 и - главен счетоводител, наричано по-долу за краткост ИЗПЪЛНИТЕЛ, от друга страна,

двете наричани по-долу за краткост „страни“, като взеха предвид,че:

- на основание 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, изменен с Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 г. за създаване на европейската рамка за цифрова самоличност, съгласно който всяка държава членка предоставя поне един европейски портфейл за цифрова самоличност (наричан накратко Регламента), и на основание Решение № 754 от 29.09.2026 г. на Министерския съвет за предприемане на действия за осигуряване на Европейски портфейл за цифрова самоличност в България и за изпълнение на свързаните с него задължения, произтичащи от Регламент (ЕС) 910/2014;

- 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, изр. 1-во от Преходните и заключителни разпоредби към ЗЕУ, системната интеграция по чл. 7с от ЗЕУ, в която са включени услуги по изграждане, поддържане, развитие и наблюдение на работоспособността на информационните и комуникационните системи, използвани от административните органи, както и дейности, които осигуряват изпълнението на тези услуги, се извършва от „Информационно обслужване“ АД;

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

- на основание § 45, ал. 2 от ЗЕУ, Министерството на електроното управление, чийто правоприемник е Министерството на иновациите и дигиталната трансформация (МИДТ), е определено като административен орган, който при изпълнение на своите функции ползва дейности по системна интеграция, от системния интегратор „Информационно обслужване“ АД (т. 30 от РМС № 727/05.12.2019 г. с последващи изменения и допълнения, включително с РМС № 447 от 7.07.2022 г.),

- ВЪЗЛОЖИТЕЛЯТ е контролиращ орган на ИЗПЪЛНИТЕЛЯ по смисъла на чл. 12, параграф 1 от Директива 2014/24/ЕС.

- Съгласно чл.7г от ЗЕУ Министърът на иновациите и дигиталната трансформация упражнява върху всички административни органи контрол в рамките на бюджетния процес по отношение на разходите в областта на електронното управление и за използваните от тях информационни и комуникационни технологии и разполага с правомощието да издава задължителни разпореждания до административните органи и лицата по чл. 1, ал. 2 относно спазването на изискванията на ЗЕУ (чл. 7и ЗЕУ);

- Съгласно § 45, ал. 1, изр. 2-ро от Преходните и заключителни разпоредби към ЗЕУ, при необходимост от възлагане на трети лица на дейности по системна интеграция, ИЗПЪЛНИТЕЛЯТ има качеството на публичен възложител и прилага правилата на Закона за обществените поръчки (ЗОП);

сключиха настоящия Договор („Договора/Договорът“), с който се споразумяха за следното:

I. ПРЕДМЕТ НА ДОГОВОРА И МЯСТО НА ИЗПЪЛНЕНИЕ

Чл. 1. (1) ВЪЗЛОЖИТЕЛЯТ възлага, а ИЗПЪЛНИТЕЛЯТ приема да предостави на ВЪЗЛОЖИТЕЛЯ услуги по системна интеграция, попадащи в обхвата на чл. 7с от ЗЕУ, съгласно заложеното в Приложение № 1 – Техническа спецификация за изграждане на национален Европейски портфейл за цифрова самоличност (ЕПЦС/EUDI Wallet), неразделна част от настоящия договор, а именно изграждане на национален Европейски портфейл за цифрова самоличност (ЕПЦС) и свързаната с него рамка на доверие, в съответствие с Регламент (ЕС) № 910/2014, изменен с Регламент (ЕС) 2024/1183, и актовете за изпълнението му.

(2) В обхвата на договора се включват следните дейности, които ще бъдат изпълнени по фази, както следва[1]:

[1] Посочени са основните фази, описани в Техническата спецификация.

1. Фаза 1: „Изграждане на цифров портфейл и доставчик на самоличност“

Дейност №1 „Изграждане на рамка на доверие“;

Дейност №2 „Изграждане на цифров портфейл и доставчик на самоличност“;

Дейност №3 „Изграждане на доставчик на квалифицирани атрибути и верификация“.

2. Фаза 2: „Разширяване на екосистемата“

Дейност №1 „Присъединяване и интеграция на квалифицирани доставчици на удостоверителни услуги, доставчици на квалифицирани електронни удостоверения за атрибути и други допустими доставчици на атрибути“.

(3) В Обхвата на договора се включва и гаранционна поддръжка, съгласно Техническата спецификация – Приложение № 1.

(4) ИЗПЪЛНИТЕЛЯТ се задължава да осигури изпълнението на дейностите по договора в съответствие с изискванията на Техническата спецификация, неразделна част от настоящия договор.

Чл. 2. (1) Място на изпълнение на дейностите по договора: сградата на Министерството на иновациите и дигиталната трансформация, гр. София, ПК 1000, ул. „Княз Александър I“ № 12.

(2) При необходимост, по време на изпълнение на дейностите в обхвата на договора е възможно дейности, които не са свързани с достъп до информация, представляваща служебна тайна, да бъдат извършвани на място, различно от посоченото в ал. 1.

(3) При необходимост от включване на допълнителни дейности в обхвата на услугата, условията за това ще бъдат предмет на допълнителни споразумения, неразделна част от настоящия договор.

II. СРОК НА ДЕЙСТВИЕ И ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ

Чл. 3. (1) Договорът влиза в сила от датата на подписването му от страните и е със срок на действие до приемане на изпълнение на всички задължения на страните по договора.

(2) ИЗПЪЛНИТЕЛЯТ се задължава да изпълни дейностите по чл. 1, ал. 2 в следните срокове[2]:

1. Срокът за изпълнение на дейностите по изграждане на национален Европейски портфейл за цифрова самоличност (ЕПЦС) и свързаната с него рамка на доверие, в

[2] Посочва се общият срок, както и срокове за изпълнение на отделни фази/ отделни етапи на изпълнение на дейности (когато е приложимо)

съответствие с Регламент (ЕС) № 910/2014, изменен с Регламент (ЕС) 2024/1183, и актовете за изпълнението му, по чл. 1 от Договора, е до 30.09.2027 г. За изпълнение на дейностите, ИЗПЪЛНИТЕЛЯТ се задължава до 10 (десет) работни дни след сключване на договора да предостави План-график за изпълнение с разписани междинни срокове за разработване, тестване и внедряване на функционалностите по Фаза 1 и Фаза 2.

2. Срок на гаранционна поддръжка - съгласно Техническата спецификация – Приложение № 1.

(3) При възникване на непредвидени обстоятелства, вкл. обжалване на решения на ВЪЗЛОЖИТЕЛЯ или на ИЗПЪЛНИТЕЛЯ, посоченият/те в ал. 2 срокове се считат за автоматично продължен/и със срока на действие на съответните непредвидени обстоятелства, за което се изготвя констативен протокол. Констативният протокол се съставя като електронен документ и се подписва от лицата по чл. 18 и чл. 19 от Договора с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис.

Чл. 4. (1) Договорът се прекратява:

1. С изтичане на срока на Договора и изпълнение на всички задължения на страните;

2. По взаимно съгласие на страните, изразено в писмена форма;

3. При настъпване на обективна невъзможност за изпълнение на договора, както и при отмяна на правата на системния интегратор за изпълнение на съответните дейности, посредством промяна в нормативната уредба. За избягване на съмнение случаите на изменение на правната уредба включват и приемането на акт от правителството на Република България, който може да уреди по друг начин възлагането на дейността по системна интеграция на настоящия системен интегратор.

(2) В случай, че ИЗПЪЛНИТЕЛЯТ наруши съществено условие на настоящия Договор, и не успее да отстрани нарушението в срок до 30 (тридесет) дни от писмено уведомление за извършеното нарушение, ИЗПЪЛНИТЕЛЯТ е в неизпълнение и ВЪЗЛОЖИТЕЛЯТ има право да развали Договора без предизвестие. При настъпването на всяко „нарушаване на съществено условие по Договора“ от страна на ИЗПЪЛНИТЕЛЯ, се съставя протокол, подписан от лицата по чл. 18 и чл. 19, определени от страните по Договора за отговарящи за изпълнението му. За „съществено условие” по смисъла на изречение първо се счита такова условие, което е свързано с основните права и задължения на страните по Договора, и чието неизпълнение води до неизпълнение на предмета на Договора.

(3) ВЪЗЛОЖИТЕЛЯТ може по своя преценка да удължи 30-дневния период по ал. 2 за такъв период, за който ИЗПЪЛНИТЕЛЯТ продължава нормалните усилия за отстраняване на

неизпълнението.

(4) 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;

(5) При прекратяване на Договора, ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ всички суми за дейностите, изпълнени съгласно този Договор, които са били дължими към момента на прекратяването му.

(6) Независимо от основанието за прекратяване, всяко право на ползване (лиценз) на софтуерни продукти и/или поддръжка на лиценз, осигурени и приети от ВЪЗЛОЖИТЕЛЯ в изпълнение на настоящия Договор, запазва своето действие до изтичане на срока, за който са осигурени.

III. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

Чл. 5. (1) За изпълнение на възложените дейности, съгласно предмета на договора по чл. 1. ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ възнаграждение („обща цена“ или „общо възнаграждение“) в размер на 2 000 000,00 (два милиона) евро без ДДС, съответно 2 400 000,00 (два милиона и четиристотин хиляди) евро с ДДС при действаща 20 % ставка на ДДС, платими, както следва:

1. за изпълнение на дейностите по чл. 1, ал. 2, т. 1 - възнаграждение в размер на 800 000,00 (осемстотин хиляди) евро без ДДС, съответно 960 000,00 (деветстотин и шестдесет хиляди) евро с ДДС;

2. за изпълнение на дейностите по чл. 1, ал. 2, т. 2 - възнаграждение в размер на 1 200 000,00 (един милион и двеста хиляди) евро без ДДС, съответно 1 440 000,00 (един милион четиристотин и четиридесет хиляди) евро с ДДС.

(2) В Цената по ал. 1 са включени всички разходи на ИЗПЪЛНИТЕЛЯ за изпълнение на Услугите, като ВЪЗЛОЖИТЕЛЯТ не дължи заплащането на каквито и да е други разноски, направени от ИЗПЪЛНИТЕЛЯ. При законодателна промяна в размера на приложимата ставка, възнаграждението се актуализира в съответствие с настъпилото изменение, с подписване на допълнително споразумение.

(3) Цената по ал. 1 включва изпълнение на дейностите, посочени в Приложение № 1 към договора.

(4) ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ цената за съответната изпълнена

фаза, предмет на този договор, в срок до 30 (тридесет) дни от получаване на издадена от ИЗПЪЛНИТЕЛЯ оригинална фактура и подписани между ИЗПЪЛНИТЕЛЯ и ВЪЗЛОЖИТЕЛЯ двустранни приемо-предавателни протоколи (за приемането на резултатите от изпълнението на фазите по чл. 1, ал. 2 от договора) от ръководителите на договора за двете страни, при спазване на условията по ал. 5.

(5) Плащането/плащанията по този Договор се извършва/т въз основа на следните документи:

1. двустранни приемо-предавателни протоколи (за приемането на резултатите от изпълнението на фазите на изпълнение на дейности по чл. 1, ал. 2 от договора), съставени като електронни документи и подписани от ръководителите на договора за ИЗПЪЛНИТЕЛЯ и ВЪЗЛОЖИТЕЛЯ с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на ВЪЗЛОЖИТЕЛЯ и ИЗПЪЛНИТЕЛЯ, придружени от съответните документи - резултати от изпълнението на дейностите по чл. 1, ал. 2 от договора в съответствие с изискванията на Техническата спецификация, която е неразделна част от настоящия договор и при съответно спазване на разпоредбите на Раздел VII (Отговорности) от Договора; и

2. фактура, издадена от ИЗПЪЛНИТЕЛЯ, представена на ВЪЗЛОЖИТЕЛЯ и подписана от ръководителя по договора за ВЪЗЛОЖИТЕЛЯ.

(6) Допуска се цената по ал.1 да се заплаща:

1. чрез акредитив, при условия, съгласувани между ИЗПЪЛНИТЕЛЯ и ВЪЗЛОЖИТЕЛЯ. Таксите и комисионните за обслужване на акредитивната сметка се заплащат, както следва: 50 % от ИЗПЪЛНИТЕЛЯ и 50% от ВЪЗЛОЖИТЕЛЯ;

2. авансово - след представяне от страна на ИЗПЪЛНИТЕЛЯ на гаранция, която обезпечава авансово предоставените средства. На основание чл. 113, ал. 4 от Закона за данък върху добавената стойност, ИЗПЪЛНИТЕЛЯТ издава фактура за авансовото плащане не по-късно от 5 дни от датата на получаване на плащането и я предоставя на ВЪЗЛОЖИТЕЛЯ.

(7) Преди извършване на плащане от ВЪЗЛОЖИТЕЛЯ се прилагат правилата на Министерство на финансите за извършване на плащания от разпоредители с бюджет.

Чл. 6. (1) Изплащането на договореното възнаграждение, в размер, определен съгласно чл. 5, ал. 1, се извършва по следната банкова сметка на ИЗПЪЛНИТЕЛЯ:

Банка:	Заличаването на IBAN на Изпълнителя е на основание чл. 72 и чл. 73 от ДОПК.
BIC:	

IBAN:

(2) При промяна на банковата сметка, посочена от ИЗПЪЛНИТЕЛЯ, преди извършване на дължимото плащане, същият уведомява ВЪЗЛОЖИТЕЛЯ писмено в 3-дневен срок от настъпване на промяната. В случай, че не уведоми ВЪЗЛОЖИТЕЛЯ в този срок, плащането по посочената в Договора сметка се счита за валидно извършено.

Чл. 7. Страните се съгласяват, че в случай, че съответната коректно издадена фактура не е получена от ВЪЗЛОЖИТЕЛЯ, 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.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ

Чл. 8. ИЗПЪЛНИТЕЛЯТ се задължава да изпълни дейностите, предмет на договора, съгласно чл. 1 от същия, при спазване на изискванията, посочени в Техническата спецификация – Приложение № 1 към същия.

Чл. 9. (1) ИЗПЪЛНИТЕЛЯТ се задължава да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 21 от Договора. Да опазва и да не разгласява пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена по закон или по силата на Договора информация, която е станала известна при изпълнението на дейностите по чл. 1, ал. 2, като представи декларация по образец – Приложение №2.

(2) При изпълнение на предмета на Договора, посочен в чл. 1, ИЗПЪЛНИТЕЛЯТ се задължава да прилага някои или всички изброени по-долу изисквания, съобразно обхвата на възложената дейност:

а) да спазва изискванията на действащата нормативна уредба в областта на мрежовата и информационната сигурност;

б) да прилага адекватни мерки за мрежова и информационна сигурност, включително да доказва прилагането им чрез документи и/или провеждане на одити при необходимост;

в) да прилага система за прозрачност на веригата на доставките, като при поискване, трябва да може да докаже произхода на предлагания ресурс/ услуга и неговата сигурност;

(3) При възлагане изпълнението на дейностите на трети лица, ИЗПЪЛНИТЕЛЯТ следва да изисква от същите да прилагат всички, изброени в ал. 2, изисквания, съобразно

обхвата на възложената дейност.

(4) При възлагането на дейностите на трети лица, ИЗПЪЛНИТЕЛЯТ действа като публичен възлагащ орган (възложител) и прилага правилата от ЗОП, при стриктно прилагане на принципите на свободна и лоялна конкуренция, равнопоставеност, зачитане на основните права и недопускане на дискриминация.

Чл. 10 (1) При изпълнение на дейностите по договора ИЗПЪЛНИТЕЛЯТ, неговите подизпълнители и служители се задължават:

1. да спазват политиката, правилата и процедурите по информационна сигурност на ВЪЗЛОЖИТЕЛЯ;

2. да опазват и да не разгласяват пред трети лица съдържанието на документацията, която е станала известна при изпълнението на този договор, без писменото съгласие на ВЪЗЛОЖИТЕЛЯ, с изключение на случаите, когато са задължени по закон за това;

3. да опазват и да не разгласяват пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на този договор;

4. да обработва законосъобразно и добросъвестно лични данни, доколкото тези данни са изрично необходими за целите на изпълнение на поетия ангажимент;

5. да предоставя лични данни на публични органи (държавни и общински), когато такива данни са изискани въз основа на валидно законово основание и по законоустановен за целта ред, като своевременно уведоми за това ВЪЗЛОЖИТЕЛЯ;

6. да предприеме всички необходими организационни и технически мерки за осигуряване на целостта и поверителността на данните в случай, че ВЪЗЛОЖИТЕЛЯТ предостави на ИЗПЪЛНИТЕЛЯ достъп до собствени ИТ активи, документи и данни;

7. да опазват и да не разгласяват пред трети лица информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на ВЪЗЛОЖИТЕЛЯ, комуникации, мрежи и информационни системи на ВЪЗЛОЖИТЕЛЯ, изготвени в хода на изпълнението документи и/или всякакви други резултати от изпълнението, както и да не разгласяват, използват или предоставят на трети лица разработена в полза на ВЪЗЛОЖИТЕЛЯ или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящия договор, с изключение на случаите, когато са задължени по закон за това;

8. да спазват вътрешните правила за достъп и режим на работа в сградата/ сградите на ВЪЗЛОЖИТЕЛЯ;

9. да спазват всички процедури и изисквания на ВЪЗЛОЖИТЕЛЯ за работа в информационната инфраструктура на ВЪЗЛОЖИТЕЛЯ;

10. да не осъществяват достъп до компютърни данни в компютърна система без разрешение, да не добавят, променят, изтриват или унищожават компютърна програма или компютърни данни, да не въвеждат компютърен вирус в компютърните системи или мрежи на ВЪЗЛОЖИТЕЛЯ, да не разпространяват пароли или кодове за достъп до компютърна система или до компютърни данни на ВЪЗЛОЖИТЕЛЯ, от което би могло да последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна;

(2) С оглед изпълнението на задълженията по ал. 1, ИЗПЪЛНИТЕЛЯТ (представляващите го лица), както и лицата, ангажирани с изпълнението на дейностите (екипа на ИЗПЪЛНИТЕЛЯ), представят декларация за опазване на информацията.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ

Чл. 11. (1) ВЪЗЛОЖИТЕЛЯТ следва да предоставя на ИЗПЪЛНИТЕЛЯ необходимото съдействие за изпълнение на Договора.

(2) ВЪЗЛОЖИТЕЛЯТ е длъжен да приеме и заплати извършеното от ИЗПЪЛНИТЕЛЯ в съответствие с Договора.

(3) За постигането на резултатите по дейностите, ВЪЗЛОЖИТЕЛЯТ, чрез неговия екип, се задължава да предостави информация за: изградената при ВЪЗЛОЖИТЕЛЯ ИТ архитектура и свързаност на системите, касаещи предмета на договора.

(4) При необходимост, ВЪЗЛОЖИТЕЛЯТ ще осигури условия за провеждане на работни срещи за изпълнението на договора. Местата ще бъдат осигурени на ангажираните от ИЗПЪЛНИТЕЛЯ лица, при съблюдаване на изискванията на Закона за здравословни и безопасни условия на труд (ЗБУТ).

(5) ВЪЗЛОЖИТЕЛЯТ се задължава да осигури на ИЗПЪЛНИТЕЛЯ, достъп до сградата на ВЪЗЛОЖИТЕЛЯ, съгласно вътрешните процедури на ВЪЗЛОЖИТЕЛЯ за осигуряване на достъп, за целите на изпълнение на дейностите по договора.

(6) ВЪЗЛОЖИТЕЛЯТ се задължава да предостави достъп до необходимите за изпълнение на дейностите по договора ИТ активи, документация и данни, при получаване на обосновано искане от ИЗПЪЛНИТЕЛЯ.

(7) За ВЪЗЛОЖИТЕЛЯ няма задължение за осигуряване на офис-техника, консумативи и др. Цялото необходимо оборудване, вкл. техническо, програмно и друго за целите на работата на екипа на ИЗПЪЛНИТЕЛЯ, следва да бъде осигурено от него. За целите

на извършване на работата по Техническата спецификация, ВЪЗЛОЖИТЕЛЯТ се задължава да предостави достъп на ИЗПЪЛНИТЕЛЯ до онази информация, приложения и технологична среда, която е необходима за успешното извършване на работата и при спазване на утвърдените процедури, правила и политики на ВЪЗЛОЖИТЕЛЯ.

VI. ОБЩИ И СПЕЦИАЛНИ УСЛОВИЯ ПО ЗАКОНА ЗА ЗДРАВОСЛОВНИ И БЕЗОПАСНИ УСЛОВИЯ НА ТРУД

Чл. 12 (1) В случаите на осигуряване на работни места, ВЪЗЛОЖИТЕЛЯТ и ИЗПЪЛНИТЕЛЯТ се задължават да осигурят прилагането на правила за съвместно осигуряване на здравословни и безопасни условия на труд (ЗБУТ) за административната сграда, с адрес: гр. София, ПК 1000, ул. „Княз Александър I“ № 12 в изпълнение на разпоредбата на чл. 18 от Закона за здравословни и безопасни условия на труд (ЗЗБУТ), както следва:

1. определят задълженията и отговорностите си за осигуряване на здравословни и безопасни условия на труд при работа на работниците и служителите, както и здравословни и безопасни условия за други лица, които се намират в района на мястото на извършване на дейностите по договора;
2. информират своевременно за възможните опасности и рисковете при работа съгласно ЗЗБУТ и действащите вътрешни правила;
3. координират дейностите си за предпазване на работниците и служителите от тези рискове;
4. прилагат всички нормативни документи, отнасящи се до спазване на изискванията за ЗБУТ.

(2) С възлагане на дейността, ВЪЗЛОЖИТЕЛЯ и ИЗПЪЛНИТЕЛЯТ, следва да поемат следните конкретни задължения за осигуряване на ЗБУТ:

1. На служителите на ИЗПЪЛНИТЕЛЯ се провежда начален и периодични инструктажи от длъжностните лица, определени за това, съгласно изискванията на Наредба № РД-07-2/2009 г. за условията и реда за провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд;

2. ВЪЗЛОЖИТЕЛЯТ следва да запознае служителите на ИЗПЪЛНИТЕЛЯ с разработения, съгласно Наредба № 8121з-647/2014 г. за правилата и нормите за пожарна безопасност при експлоатация на обектите, план за пожарна и аварийна безопасност, план за евакуация, схеми за евакуация с обозначение на евакуационните изходи и средствата за

пожарогасене и да извърши обучение за евакуация и работа с пожарогасителна техника;

3. ВЪЗЛОЖИТЕЛЯТ предоставя на служителите на ИЗПЪЛНИТЕЛЯ информация за рисковете за здравето и безопасността на неговите служители, както и за мерките, които се предприемат за отстраняването, намаляването или контролирането им, при необходимост.

4. Всички останали изисквания по време на изпълнение на дейностите, извън посочените в настоящия документ ангажименти на ВЪЗЛОЖИТЕЛЯ по отношение на работна среда и условията за работа, ще бъдат допълнително уточнени, след получаване на заявка от страна на ИЗПЪЛНИТЕЛЯ, ведно с обосновка на необходимостта за тяхното предоставяне и съгласно възможността от страна на ВЪЗЛОЖИТЕЛЯ за това.

(3) При необходимост, ВЪЗЛОЖИТЕЛЯТ се задължава да осигури:

1. ползване на стационарни телефони с вътрешна и външна линия, като разговорите се заплащат от ИЗПЪЛНИТЕЛЯ въз основа на издадена фактура от ВЪЗЛОЖИТЕЛЯ;

2. условия за провеждане на работни срещи.

VII. ОТГОВОРНОСТИ

Чл. 13. (1) При пълно виновно неизпълнение на договора, ИЗПЪЛНИТЕЛЯТ дължи на ВЪЗЛОЖИТЕЛЯ неустойка в размер на 5 % от общото възнаграждение по чл. 5, ал. 1 без ДДС, която се заплаща от ИЗПЪЛНИТЕЛЯ в 30-дневен срок от уведомяването. За пълно неизпълнение се приема неизвършването на нито една от дейностите, включени в обхвата на договора по чл. 1, ал. 2.

(2) При частично виновно неизпълнение на договора, ИЗПЪЛНИТЕЛЯТ дължи на ВЪЗЛОЖИТЕЛЯ неустойка в размер на 5 % от възнаграждението за съответната фаза по чл. 5, ал. 1 на договора без ДДС, която се заплаща от ИЗПЪЛНИТЕЛЯ в 30-дневен срок от уведомяването. За частично неизпълнение се приема неизвършването на дейност, включена в обхвата на договора по чл. 1, ал. 2.

(3) В случай, че ИЗПЪЛНИТЕЛЯТ е в забава по негова вина, ВЪЗЛОЖИТЕЛЯТ има право да получи неустойка за забавено изпълнение в размер на 0,05 % на ден от възнаграждението за съответната фаза по чл. 5, ал. 1 на договора без ДДС, считано от деня, следващ деня, в който ИЗПЪЛНИТЕЛЯТ е следвало да извърши съответната дейност, но не повече от 1% от общото възнаграждение по чл. 5, ал. 1 без ДДС.

(4) В случай че е налице забава по вина на ВЪЗЛОЖИТЕЛЯ, ИЗПЪЛНИТЕЛЯТ не дължи неустойка за забавено изпълнение.

(5) При констатирано лошо или друго неточно или частично изпълнение или при

отклонение от изискванията на ВЪЗЛОЖИТЕЛЯ, същият има право да поиска от ИЗПЪЛНИТЕЛЯ да изпълни дейността изцяло и качествено, без да дължи допълнително възнаграждение за това. В случай, че и повторното изпълнение на дейността е некачествено, ВЪЗЛОЖИТЕЛЯТ има право да изиска неустойка в размер на 4 % от възнаграждението за съответната фаза по чл. 5, ал. 1 на договора без ДДС.

(6) Всяка забава се удостоверява с констативен протокол, подписан от ВЪЗЛОЖИТЕЛЯ и от ИЗПЪЛНИТЕЛЯ, чрез лицата по чл. 18 и чл. 19.

(7) ВЪЗЛОЖИТЕЛЯТ може да претендира обезщетение за нанесени вреди и/или пропуснати ползи по общия ред, независимо от начислените неустойки, включително при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност.

(8) При забава в плащане на уговореното възнаграждение ВЪЗЛОЖИТЕЛЯТ дължи на ИЗПЪЛНИТЕЛЯ обезщетение в размер на 0,05% на ден върху размера на съответното забавено плащане без ДДС, но не повече от 5% от стойността на забавеното плащане без ДДС.

Чл. 14. Страните запазват правото си да търсят обезщетение за вреди, ако тяхната стойност е по-голяма от изплатените неустойки по реда на този раздел.

VIII. АВТОРСКИ ПРАВА

Чл. 15. (1) Авторските и всички сродни права и собствеността върху изработени софтуерни продукти, техният изходен програмен код, дизайнът на интерфейсите и базите данни, чиято разработка попада в обхвата на чл. 1, ал. 1 от договора и всички съпътстващи изработката им проучвания, разработки, скици, чертежи, планове, модели, документи, софтуер, дизайни, описания, 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 предвидената в договора стойност. ИЗПЪЛНИТЕЛЯТ потвърждава, че Техническата спецификация 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/ третите лица, на които

е възложено изпълнението, единствено адаптират концепцията на ВЪЗЛОЖИТЕЛЯ във вид и по начин, позволяващи използването й за посочените по-горе цели, 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) При разработване на софтуер за ВЪЗЛОЖИТЕЛЯ, настоящият раздел от договора се счита и следва да бъде тълкуван като договор за създаване на обект на авторско право (произведение) по поръчка, съгласно чл. 42 ал. 1 от Закон за авторското право и сродните му права (ЗАПСП), като Страните изрично се съгласяват и споразумяват, че:

1. авторските права върху софтуерните продукти и части от тях, включително имуществените права съгласно раздел II от ЗАПСП и прехвърлимите неимуществени права, съгласно чл. 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 тежести, залози, искове, претенции на трети лица, възбрани и други тежести или права на трети лица;

2. ИЗПЪЛНИТЕЛЯТ предоставя на ВЪЗЛОЖИТЕЛЯ изключителни права по смисъла на чл. 36, ал. 2 от ЗАПСП за използване на Софтуерните продукти и техни елементи, и обектите, изброени в ал. 1 или части от тях, в случай че авторските права върху тях не могат да възникнат директно за ВЪЗЛОЖИТЕЛЯ.

(3) За избягване на съмнение, Страните потвърждават и се съгласяват, че правата на ВЪЗЛОЖИТЕЛЯ върху софтуерните продукти и обектите, изброени в ал. 1, 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 няма и не може да

предявява претенции по отношение на каквито и да било права на интелектуална собственост върху Софтуерните продукти.

(4) С изброените по-горе задължения, ИЗПЪЛНИТЕЛЯТ следва да задължи и трети лица, на които ще възложи за изпълнение дейностите по настоящия договор, да не прехвърлят на други лица каквито и да било права свързани със софтуерни продукти, включително, но не само правото на ползване и/или на промяна, както и нямат право да използват и/или прехвърлят, разкриват или предоставят по какъвто и да било начин на други лица концепцията на ВЪЗЛОЖИТЕЛЯ, съдържаща се в предоставената Техническа спецификация или други документи, предоставени по повод изпълнението на договора.

IX. ДРУГИ УСЛОВИЯ

Чл. 16. Всички съобщения, уведомления и документи по изпълнението на настоящия договор се съставят в електронен вид и се подписват с електронен подпис в PDF-формат. Кореспонденцията се извършва чрез електронна поща на електронните адреси, посочени от страните.

Чл. 17. Спорни въпроси, възникнали при действието на този договор се решават по пътя на споразумения, а нерешените се отнасят за решаване от компетентния съд.

Чл. 18. (1) Отговарящ за изпълнението от страна на ВЪЗЛОЖИТЕЛЯ, наричан ръководител договор за времето на неговото действие е – началник на отдел, дирекция „Дигитална трансформация и автоматизация“, тел: , електронен адрес: , а в нейно отсъствие: – началник на отдел, дирекция „Дигитална трансформация и автоматизация“, тел: ; електронен адрес:

(2) Отговарящ за изпълнението на договора от страна на ВЪЗЛОЖИТЕЛЯ, наричан координатор за времето на неговото действие е – държавен експерт, дирекция „Дигитална трансформация и автоматизация“, тел: ; електронен адрес: , а в нейно отсъствие: държавен експерт, дирекция „Дигитална трансформация и автоматизация“, тел: ; електронен адрес:

Чл. 19. Отговарящ за изпълнението от страна на ИЗПЪЛНИТЕЛЯ, наричан ръководител договор за времето на неговото действие, е – мениджър проекти, тел: , имейл: а в негово отсъствие: - младши мениджър проекти, тел: , имейл:

Чл. 20. Във връзка с изпълнение на изискванията за сигурност на информацията по чл. 10, ал. 2 и ал. 3 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), страните определят следните лица за отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на договора:

1. За ВЪЗЛОЖИТЕЛЯ: - специалист по мрежова и информационна сигурност, дирекция „Киберсигурност и защита“, тел: , ел. адрес: а в негово отсъствие - експерт по мрежова и информационна сигурност IV степен, дирекция „Киберсигурност и защита“, тел: ел. адрес:

2. За ИЗПЪЛНИТЕЛЯ: , Ръководител сектор, Превенция на заплахи и разузнаване тел: , e-mail: а в негово отсъствие , Ръководител сектор, Реагиране при инциденти и управление на заплахи, тел: , ел. адрес:

Чл. 21. (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“). Конфиденциална 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, свързани с изпълнението на Договора.

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

1. съдържанието на документацията, която е станала известна при изпълнението на договора;

2. съдържанието на данъчна и осигурителна информация, лични данни и друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на договора;

3. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на ВЪЗЛОЖИТЕЛЯ, комуникации, мрежи и информационни системи на ВЪЗЛОЖИТЕЛЯ, изготвени в хода на изпълнението документи и/или всякакви други резултати от изпълнението, разработена в полза на ВЪЗЛОЖИТЕЛЯ 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:

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

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

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) Задълженията по този член 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.

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

(8) ИЗПЪЛНИТЕЛЯТ няма право да дава публични изявления и съобщения, да разкрива или разгласява каквато и да е информация, която е получил във връзка с извършване на дейностите, предмет на този договор, независимо дали е въз основа на данни и материали на ВЪЗЛОЖИТЕЛЯ или на резултати от работата на ИЗПЪЛНИТЕЛЯ, без предварителното писмено съгласие на ВЪЗЛОЖИТЕЛЯ, което съгласие няма да бъде безпричинно отказано или забавено.

X. НЕПРЕОДОЛИМА СИЛА

Чл. 22. (1) Страните не отговарят за неизпълнение на задължение по този Договор, когато невъзможността за изпълнение се дължи на непреодолима сила. За целите на този Договор, „непреодолима сила“ има значението на това понятие по смисъла на чл. 306, ал. 2 от Търговския закон.

(2) 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 в срок до 3 *(три)* дни от 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.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира, като страните подписват протокол, в който удостоверяват началната дата на спиране. 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.

(4) След отпадане на непреодолимата сила, засегнатата страна в срок до 3 *(три)* дни уведомява писмено другата страна, като прилага всички релевантни и/или нормативно установени доказателства за отпадането й. Страните подписват протокол, с който удостоверяват датата, от която се възобновява изпълнението на задълженията.

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

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

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

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.

Настоящият договор е изготвен като електронен документ и влиза в сила след подписването му с квалифициран електронен подпис от представителите на страните, като приложенията са негова неразделна част.

Приложения:

1. Приложение № 1 – Техническа спецификация;
2. Приложение № 2 – Образец на декларация за опазване на информацията.

ЗА ВЪЗЛОЖИТЕЛЯ:	ЗА ИЗПЪЛНИТЕЛЯ:
----------	----------
ИВАН ВАСИЛЕВ МИНИСТЪР НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ	ИВАЙЛО ФИЛИПОВ ИЗПЪЛНИТЕЛЕН ДИРЕКТОР НА „ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
-	-- --------
ДИРЕКТОР НА ДИРЕКЦИЯ „ФИНАНСИ И УПРАВЛЕНИЕ НА СОБСТВЕНОСТТА“	ГЛАВЕН СЧЕТОВОДИТЕЛ

Приложение № 1 към чл. 38, ал. 3

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

за

изграждане и въвеждане/внедряване на Портфейл за цифрова самоличност (EU Digital Wallet) и извършване на гаранционна поддръжка

СЪДЪРЖАНИЕ

1 Речник на термини, дефиниции и съкращения 5

1.1 Използвани акроними 5

1.2 Технологични дефиниции 6

1.3 Дефиниции за нива на електронизация на услугите 12

2 Въведение 14

2.1 Цел на документа 14

2.2 За Бенефициера – функции и структура 14

2.3 За проекта 16

2.4 Нормативна рамка 18

2.4.1 Приложими регламенти, директиви, актове за изпълнение, стандарти и препоръки на Европейския съюз 18

2.4.2 Национална нормативна уредба в областта на Европейския портфейл за цифрова самоличност, електронната идентификация и електронното управление 21

2.4.3 Национална нормативна уредба в областта на самоличността, гражданската регистрация и автентичните източници на данни 23

2.4.4 Нормативна уредба в областта на защитата на личните данни и поверителността 24

2.4.5 Нормативна уредба в областта на киберсигурността, информационната сигурност и устойчивостта 25

2.4.6 Нормативна уредба и правила за административно обслужване, електронни услуги и интеграции 26

3 Цели, обхват и очаквани резултати от изпълнение на проекта 26

3.1 Общи и специфични цели на проекта 26

3.2 Обхват на проекта 28

3.3 Целеви групи 29

3.4 Очаквани резултати 31

3.5 Период на изпълнение 33

4 Текущо състояние 34

5 Изисквания към изпълнение на проекта 36

5.1 Общи изисквания към изпълнението 36

5.2 Общи организационни принципи 36

5.3 Управление на проекта 37

5.4 Управление на риска 37

6 Етапи на изпълнение на проекта 38

6.1 Анализ на данните и изискванията 38

6.1.1 Специфични изисквания към етапите на бизнес анализа при разработка, надграждане или внедряване на информационна система 39

6.1.2 Специфични изисквания при оптимизиране на процесите по заявяване на електронни услуги и електронни административни услуги (съгл. §1, т.2 от ЗЕУ) в зависимост от заявителя 40
6.1.3 Изисквания за оптимизиране на процесите по подаване на декларации, изискуеми в съответствие с нормативната уредба и вътрешните правила 43
6.1.4 Изисквания към регистрите и предоставянето на административните услуги ... 44
6.2 Изготвяне на детайлна техническа спецификация 45
6.3 Разработване на софтуерното решение 45
6.4 Тестване 45
6.5 Внедряване 46
6.6 Обучение 46
6.7 Гаранционна поддръжка 46
6.7.1 Обхват на дейностите по гаранционна поддръжка 47
6.7.2 Управление на инциденти (incident management) 48
6.7.3 Управление на проблеми (УП) (problem management) 48
6.7.4 Управление на качеството при отстраняване на инциденти и проблеми. Параметри на качеството. 49
6.7.5 Минимални изисквания към параметрите на качеството 49
7 Общи изисквания за информационни системи в държавната администрация 52
7.1 Функционални изисквания към информационната система 53
7.1.1 Интеграция с външни информационни системи 53
7.1.2 Използване на интеграционния слой на електронното управление 59
7.1.3 Технически изисквания към интерфейсите 61
7.1.4 Електронна идентификация на потребителите 63
7.1.5 Отворени данни 65
7.1.6 Формиране на изгледи 66
7.1.7 Администриране на Системата 67
7.2 Нефункционални изисквания към информационната система 67
7.2.1 Авторски права и изходен код 67
7.2.2 Системна и приложна архитектура 68
7.2.3 Повторно използване (преизползване) на ресурси и готови разработки 72
7.2.4 Изграждане и поддръжка на множество среди 74
7.2.5 Процес на разработка, тестване и разгръщане 75
7.2.6 Бързодействие и мащабируемост 76
7.2.7 Информационна сигурност и интегритет на данните 81
7.2.8 Използваемост 84
7.2.9 Системен журнал 94
7.2.10 Дизайн на бази данни и взаимодействие с тях 95

7.2.11 Изисквания по отношение на киберсигурност в съответствие с чл. 12, ал. 1 от НМИМИС 96
8 Изисквания към изпълнението на дейностите по проекта 99
8.1 Фаза 1 - Изграждане на цифров портфейл и доставчик на самоличност 99
8.1.1 Дейност 1 - Изграждане на рамка на доверие 99
8.1.2 Дейност 2 - Изграждане на цифров портфейл и доставчик на самоличност 106
8.1.3 Дейност 3 - Изграждане на доставчик на квалифицирани атрибути и верификация 115
8.2 Фаза 2 - „Разширяване на екосистемата“ 121
8.2.1 Дейност 1 - Присъединяване и интеграция на квалифицирани доставчици на удостоверителни услуги, доставчици на квалифицирани електронни удостоверения за атрибути и други допустими доставчици на атрибути 121
9 Документация 126
9.1 Изисквания към документацията 126
9.2 Прозрачност и отчетност 127
9.3 Детайлна техническа спецификация 128
9.4 Техническа документация 128
10 Резултати 128

1 Речник на термини, дефиниции и съкращения

1.1 Използвани акроними

Акроним	Описание
2FA	Two-factor Authenticaiton - Двуфакторна автентикация
АПК	Административнопроцесуален кодекс
Clean Pipe	Услуга за защитен интернет капацитет/филтрация на трафик (анти-DDoS/anti-malware на ниво мрежа)
DPIA	Оценка на въздействието върху защитата на данните (Data Protection Impact Assessment)
ДХЧО	Държавен хибриден частен облак
ЕАУ	Електронни административни услуги
ЕГН	Единен граждански номер
ЕЕН	Единен европейски номер
ЕПДЕАУ	Единен портал за достъп до електронни административни услуги
ЕС	Европейски съюз
IDP	Доставчик на идентичност (Identity Provider)
IAM	Управление на идентичности и достъп (Identity and Access Management)
ИИСДА	Интегрирана информационна система на държавната администрация
ИС	Информационна система
КАО	Комплексно административно обслужване
КЕП	Квалифициран електронен подпис
МЕУ	Министерство на електронното управление
МИДТ	Министерство на иновациите и дигиталната трансформация
NF	Нефункционално изискване (Non-Functional Requirement)
НПВУ	Национален план за възстановяване и устойчивост
OAuth	Стандарт/рамка за делегирана авторизация (OAuth)
OIDC	OpenID Connect (протокол за удостоверяване върху OAuth 2.0)
RBAC	Управление на достъп на база роли (Role-Based Access Control)
SAML 2.0	Security Assertion Markup Language 2.0 (протокол за федеративна идентификация/SSO)
SIEM	Security Information and Event Management (събиране/корелация на събития по сигурността)
SSL	Secure Sockets Layer (в практиката – TLS криптиране на връзката)

SSO	Single Sign-On (единно вписване)
TCP	Transmission Control Protocol (мрежов протокол)
UEP	Единна точка за достъп (Unified Endpoint/Entry Point – използвано като „Единна точка за достъп“)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Универсално уникален идентификатор (Universally Unique Identifier)
Viewer	Визуализатор/приложение за преглед на образни изследвания
ВАЕУ	Вътрешно административни електронни услуги
ЗДОИ	Закон за достъп до обществена информация
ЗЕИ	Закон за електронната идентификация
ЗЕУ	Закон за електронното управление
ЗОП	Закон за обществените поръчки
БДС	Български държавен стандарт
MVP	Минимално използваем продукт

1.2 Технологични дефиниции

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

Софтуер с отворен код	Компютърна програма, която се разпространява при условия, които осигуряват безплатен достъп до програмния код и позволяват: Използването на програмата и производните на нея компютърни програми, без ограничения в целта; Промени в програмния код и адаптирането на компютърната програма за нуждите на нейните ползватели; Разпространението на производните компютърни програми при същите условия. Списък на стандартни лицензионни споразумения, които предоставят тези възможности, който може да бъде намерен в подзаконовата нормативна уредба към Закона за електронно управление или на: http://opensource.org/licenses.
Машинночетим формат	Формат на данни, който е структуриран по начин, по който, без да се преобразува в друг формат позволява софтуерни приложения да идентифицират, разпознават и извличат специфични данни, включително отделни факти и тяхната вътрешна структура.
Отворен формат	Означава формат на данни, който не налага употребата на специфична платформа или специфичен софтуер за повторната употреба на съдържанието и е предоставен на обществеността без ограничения, които биха възпрепятствали повторното използване на информация.
Метаданни	Данни, описващи структурата на информацията, предмет на повторно използване.
Официален отворен стандарт	Стандарт, който е установен в писмена форма и описва спецификациите за изискванията как да се осигури софтуерна оперативна съвместимост.
Система за контрол на версиите	Технология, с която се създава специално място, наречено “хранилище”, където е възможно да се следят и описват промените по дадено съдържание (текст, програмен код, двоични файлове). Една система за контрол на версиите трябва да може: • Да съхранява пълна история - кой, какво и кога е променил по съдържанието в хранилището, както и защо се прави промяната; • Да позволява преглеждане разликите между всеки две съхранени версии в хранилището; • Да позволява при необходимост съдържанието в хранилището да може да се върне към предишна съхранена версия; • Да позволява наличието на множество копия на хранилището и синхронизация между тях. Цялата информация, налична в системата за контрол на версиите за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, трябва да може да бъде

	достъпна публично, онлайн, в реално време.
Първичен регистър	Регистър, който се поддържа от първичен администратор на данни - административен орган, който по силата на закон събира или създава данни за субекти (граждани или организации) или за обекти (движими и недвижими) за първи път и изменя или заличава тези данни. Например Търговският регистър е първичен регистър за юридическите лица със стопанска цел, Имотният регистър е първичен регистър за недвижима собственост.
Наличност на Системата в проценти	Процентът на договорените часове, за които компонент или услуга е достъпна за определен период от време.
Работни дни	От Понеделник до Петък без националните и официални празници.
Работни часове (Работно време)	08:00-20:00 всеки работен ден
Инцидент	Инцидент е всяко намаляване на качеството или недостъпност на предоставяна услуга и/или непланираното ѝ прекъсване, както и неизправност на елемент от инфраструктурната конфигурация
Продължително прекъсване	Прекъсване на услугата за повече от четири (4) работни часа
Планирана недостъпност	Планирано прекъсване на една или повече услуги.
Недостъпност	Неспособността на услуга или част от услуга да осигури нормалното обслужване
Непланирана недостъпност	Неочаквано прекъсване на една или повече услуги или значителна деградация на качеството на предлаганата услуга.

Проблем	Проблем е съвкупност от повтарящи се идентични събития или инциденти, които водят до периодично влошаване на дадена услуга, липсата ѝ или неточност в дадена процедура или функционално звено
Портфейлна единица	Портфейлна единица е конкретна активирана инстанция на Портфейла за цифрова самоличност, свързана с определен потребител и конкретно устройство или защитена среда. Тя осигурява възможност за съхраняване, управление и използване на данни за идентификация, електронни удостоверения за атрибути, криптографски ключове и други елементи, необходими за извършване на електронна идентификация, представяне на данни и подписване чрез Портфейла.
Портфейлна операция	Портфейлна операция е всяко действие, извършвано от потребителя, Портфейла или свързан компонент на екосистемата, което води до създаване, промяна, използване, представяне, проверка, блокиране, възстановяване или прекратяване на данни, атрибути, ключове, съгласия или статуси, свързани с портфейлната единица. Такива операции включват например активиране на Портфейл, получаване на данни за идентификация, представяне на атрибут пред доверяваща се страна, потвърждаване или отказ на заявка, подписване, блокиране на устройство или възстановяване на достъп.
Квалифицирани атрибути	Квалифицирани атрибути са удостоверени цифрови данни за лице или организация, издадени от квалифициран доставчик или от оправомощен публичен орган при спазване на изискванията на eIDAS и националната нормативна рамка. В контекста на Портфейла за цифрова самоличност те служат за надеждно доказване на конкретно качество, право, статус, факт или обстоятелство, без да е необходимо представяне на хартиен документ или допълнителна проверка от страна на потребителя. Такива атрибути могат да бъдат например възраст, адрес, гражданство, представителна власт, образователен статус, професионална квалификация, регистрация на юридическо лице или друго обстоятелство, потвърдено от автентичен източник. Квалифицираните атрибути се съхраняват или управляват чрез Портфейла и могат да бъдат предоставяни от потребителя към доверяващи се страни при спазване на принципите за минимизиране на данните, контрол от страна на потребителя, сигурност и проследимост.
Електронно удостоверение за атрибути (EAA)	Удостоверени цифрови данни, които потвърждават конкретно качество, право, статус, факт или обстоятелство, свързано с лице или организация.
Квалифицирано електронно удостоверение за атрибути /	Електронно удостоверение за атрибути, издадено от квалифициран доставчик или оправомощен публичен орган при спазване на изискванията на eIDAS и националната нормативна рамка.

квалифициран атрибут	
Портфейл за цифрова самоличност / EUDI Wallet	Средство за електронна идентификация, чрез което потребителят може да съхранява, управлява и представя данни за самоличност, електронни удостоверения за атрибути и други удостоверени цифрови данни, както и да използва квалифициран електронен подпис.
Доставчик на портфейл	Субект или системен компонент, който предоставя и управлява Портфейла за цифрова самоличност, включително неговата инфраструктура, жизнен цикъл, сигурност, статуси и взаимодействие с останалите участници в екосистемата.
Доставчик на самоличност	Субект или системен компонент, който извършва надеждна проверка на самоличността на потребителя и осигурява издаване или предоставяне на данни за идентификация на лице за нуждите на Портфейла.
Доставчик на атрибути	Субект, който издава или предоставя електронни удостоверения за атрибути въз основа на данни от надежден източник.
Доставчик на квалифицирани атрибути	Доставчик, който издава квалифицирани електронни удостоверения за атрибути при спазване на приложимите изисквания за доверие, сигурност, проверимост и нормативно съответствие.
Данни за идентификация на лице / PID	Данни, чрез които физическо или юридическо лице може да бъде надеждно идентифицирано в рамките на Портфейла и електронните услуги. При физическите лица това могат да бъдат имена, идентификатор, дата на раждане и други данни, определени в приложимата нормативна и техническа рамка.
Автентичен източник на данни	Официален регистър или информационна система, поддържана от компетентен орган, от която се извличат или проверяват данни с правно значение.
Доверяваща се страна	Публична или частна организация, която приема Портфейла като средство за електронна идентификация, удостоверяване или представяне на атрибути и използва предоставените от потребителя данни за конкретна услуга или процес.
Посредник при верификация	Компонент или субект, който подпомага процеса по заявяване, получаване и проверка на данни или атрибути, предоставени чрез Портфейла от потребителя към доверяваща се страна.

Верификация	Процес по проверка на автентичността, валидността, издателя, статуса и допустимостта на данни, атрибути, удостоверения, сертификати или доверителна информация.
Рамка на доверие	Организационна, техническа, процедурна и нормативна основа, която определя правилата за участие, регистрация, контрол, сертифициране, доверие и взаимодействие между участниците в екосистемата на Портфейла.
Регистър на участниците	Регистър, съдържащ информация за участниците в екосистемата, включително доставчици на портфейли, доставчици на самоличност, доставчици на атрибути, посредници при верификация, доверяващи се страни и други допустими субекти.
Доверителен списък	Машинночетим списък с доверителна информация за участници, сертификати, статуси, технически профили и други данни, необходими за проверка на доверие в национален и трансграничен контекст.
Регистратор на доверителни списъци	Компонент, който създава, подписва, публикува, актуализира, валидира и архивира доверителни списъци.
Квалифициран доставчик на удостоверителни услуги / QTSP	Доставчик на удостоверителни услуги, който е квалифициран съгласно eIDAS и предоставя услуги като квалифицирани електронни подписи, квалифицирани електронни печати, квалифицирани удостоверения или други доверителни услуги.
eIDAS възел	Национален инфраструктурен компонент, който осигурява трансгранично взаимодействие и признаване на средства за електронна идентификация между държавите членки на Европейския съюз.
Минимизиране на данните	Принцип, според който се обработват и предоставят само данните, които са необходими за конкретна цел, услуга или операция.
Потребителско потвърждение	Действие, чрез което потребителят изрично одобрява или отказва предоставяне на данни, представяне на атрибут, подписване или друга портфейлна операция.
Жизнен цикъл на портфейла	Последователността от състояния и процеси, през които преминава портфейлната единица - създаване, активиране, използване, актуализация, блокиране, възстановяване, прекратяване и архивиране.

Онбординг на участник	Процес по заявяване, проверка, одобрение, техническа конфигурация, тестване и активиране на участник в екосистемата на Портфейла.
Технически профил	Набор от технически параметри, интерфейси, сертификати, формати, крайни точки, протоколи и настройки, чрез които даден участник взаимодейства със системата.
Sandbox среда	Изолирана тестова среда, предназначена за изпитване на интеграции, технически профили, интерфейси и сценарии от външни участници без риск за продукционната среда и реалните данни.
Защитена среда за криптографски операции	Хардуерна или софтуерна среда, която осигурява сигурно съхранение на ключове и изпълнение на криптографски операции, като например Secure Enclave, StrongBox, Trusted Execution Environment, HSM или еквивалентен механизъм.
Атестация на устройство	Процес по проверка и удостоверяване, че конкретно устройство или защитена среда отговаря на изискванията за сигурност, необходими за използване на портфейлни операции.
Одитна следа / системен журнал	Запис на действия, събития, заявки, отговори, грешки и промени в системата, който позволява проследимост, контрол, анализ на инциденти и доказване на извършени операции.
MVP / минимално използваем продукт	Първоначална версия на решението, която реализира ограничен, но работещ набор от основни функционалности и сценарии, достатъчни за доказване на концепцията и базовата работоспособност на Портфейла.

1.3 Дефиниции за нива на електронизация на услугите

Термин	Описание
Ниво 1	Информация - предоставяне на информация за административни услуги по електронен път, включително за начини и места за заявяване на услугите, срокове и такси.
Ниво 2	Едностранна комуникация - информация съгласно дефиницията за Ниво 1 и осигурен публичен онлайн достъп до шаблони на електронни формуляри.
Ниво 3	Двустранна комуникация - заявяване на услуги изцяло по електронен път, включително електронно подаване на данни и документи, електронна обработка на формуляри и електронна идентификация на потребителите, освен ако със закон се допуска предоставяне на електронна административна услуга без идентификация;.

Ниво 4	Извършване на услуги от ниво 3, за които е осигурена възможност за електронно връчване и електронно плащане, ако за получаването на електронна административна услуга се дължат такси.

2 Въведение

2.1 Цел на документа

Целта на настоящия документ е да опише софтуерните изисквания към изпълнението на проект „Изграждане и въвеждане/внедряване на Портфейл за цифрова самоличност (EU Digital Wallet) и извършване на гаранционна поддръжка“. Навсякъде в документа под „Система/та“ следва да се има предвид портфейла за цифрова самоличност и всички прилежащи към него разработени софтуерни функционалности.

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

Съдържанието на настоящата техническа спецификация е задължително за прилагане от всички лица по чл.1, ал.1 и ал. 2 от ЗЕУ, публичните и секторните Бенефициери по Закона за обществените поръчки, които са публични предприятия по смисъла на Закона за публичните предприятия като в същото може да бъде добавян текст, в зависимост от специфичните нужди на разработваната информационна система, но не може да бъде изтривано настоящото съдържание.

2.2 За Бенефициера – функции и структура

Министерството на иновациите и дигиталната трансформация е централна администрация и орган на изпълнителната власт, който провежда държавната политика в областта на електронното управление, цифровата трансформация, оперативната съвместимост, електронната идентификация, информационната сигурност и развитието на националната цифрова инфраструктура. В рамките на настоящия проект Министерството изпълнява ролята на Бенефициер и компетентен орган, отговорен за стратегическото, нормативното, организационното и координационното обезпечаване на изграждането и въвеждането/внедряването на Портфейл за цифрова самоличност в Република България.

Бенефициерът осигурява цялостната рамка за реализация на проекта, като координира изпълнението му в съответствие с приложимото европейско и национално законодателство, включително изискванията на Регламент (ЕС) № 910/2014, изменен с Регламент (ЕС) 2024/1183, както и с предвидената национална нормативна уредба за Европейския портфейл за цифрова самоличност. Министерството има водеща роля при определянето на националния модел за управление на екосистемата на цифровата самоличност, при въвеждането на националната рамка на доверие, при регламентирането на участниците в процесите и при осигуряването на взаимодействие с институциите на Европейския съюз и държавите членки.

В изпълнение на своите функции Министерството осигурява координация между публичните органи, първичните администратори на данни, доставчиците на портфейли, доставчиците на данни за идентификация на лица, доставчиците на електронни удостоверения за атрибути, квалифицираните доставчици на удостоверителни услуги, доверяващите се страни

и други участници в националната екосистема. Бенефициерът следва да гарантира, че разработваното решение е съвместимо с европейската инфраструктура за цифрова идентичност, с националните регистри, със средата за междурегистров обмен, с националните механизми за електронна идентификация и с приложимите изисквания за сигурност, защита на личните данни и оперативна съвместимост.

Основните функции на Бенефициера във връзка с проекта включват:

- регулаторно и методическо обезпечаване на процесите по изграждане, управление, сертифициране и използване на Портфейла за цифрова самоличност;
- координация на подготовката и прилагането на националната нормативна рамка, включително подзаконови актове, правила, процедури и модели за присъединяване на участниците;
- създаване и поддържане на модел за управление на националната рамка на доверие;
- организация и координация на процесите по регистрация, вписване, контрол и надзор на участниците в екосистемата;
- осигуряване на условия за оперативна съвместимост между Портфейла, националните информационни системи, европейската инфраструктура и системите на публични и частни доставчици на услуги;
- координация с Европейската комисия и с компетентните органи на държавите членки по въпроси, свързани с уведомяване, признаване, валидиране и трансгранично използване на Портфейла;
- осигуряване на механизми за контрол, отчетност, проследимост, управление на риска и гарантиране на съответствието с изискванията за киберсигурност и защита на личните данни;
- приемане, въвеждане в експлоатация и последващо управление на резултатите от проекта, включително координация на гаранционната поддръжка.

Организационно изпълнението на проекта се координира от специализираните административни звена на Министерството, които имат компетентност в областта на електронното управление, цифровата идентичност, информационната сигурност, оперативната съвместимост, правното обслужване, финансовото управление, обществените поръчки, управлението на проекти, комуникацията с институции и внедряването на информационни системи. При необходимост в изпълнението участват и други държавни органи, първични администратори на данни и технически партньори, които предоставят данни, услуги, инфраструктура, експертен капацитет или интеграционни интерфейси, необходими за функционирането на Портфейла.

Министерството упражнява контрол върху изпълнението на проекта чрез определени от него отговорни лица, проектни екипи, работни групи и механизми за приемане на резултатите. В рамките на тези механизми се осигурява съгласуване на бизнес изискванията, архитектурните решения, интеграционните подходи, изискванията за сигурност, тестовите сценарии, документацията, обучението, внедряването и гаранционната поддръжка. По този начин се гарантира, че разработваното решение ще бъде устойчиво, сигурно, мащабируемо, съвместимо с европейските изисквания и приложимо за нуждите на гражданите, бизнеса и публичната администрация.

2.3 За проекта

Проектът „Изграждане и въвеждане/внедряване на Портфейл за цифрова самоличност (EU Digital Wallet) и извършване на гаранционна поддръжка“ има за цел създаване на национално решение за Европейски портфейл за цифрова самоличност, чрез което гражданите и бизнесът в Република България да могат да се идентифицират по електронен път, да получават, съхраняват и предоставят удостоверени цифрови атрибути, да използват квалифициран електронен подпис и да достъпват електронни услуги в България и в останалите държави членки на Европейския съюз.

Проектът се реализира в контекста на новата европейска рамка за цифрова идентичност, въведена с Регламент (ЕС) 2024/1183, с която се създават условия всяка държава членка да предостави на своите граждани, жители и предприятия поне един сертифициран Европейски портфейл за цифрова самоличност. Реализацията на проекта е от стратегическо значение за развитието на електронното управление в Република България, тъй като създава единна, сигурна и оперативно съвместима среда за електронна идентификация, удостоверяване на атрибути, електронно подписване и използване на цифрови административни и частни услуги.

В рамките на проекта ще бъде изградена национална екосистема за цифрова самоличност, която обединява държавна инфраструктура, рамка на доверие, доставчик на портфейл, доставчик на самоличност, механизми за издаване и проверка на атрибути, интеграции с национални регистри, интеграции с квалифицирани доставчици на удостоверителни услуги и механизми за взаимодействие с европейската инфраструктура по eIDAS. Решението следва да осигури както национална приложимост, така и трансгранична оперативна съвместимост, така че българският Портфейл да може да бъде използван при достъп до услуги в други държави членки, а чуждестранни портфейли да могат да бъдат разпознавани и използвани при предоставяне на услуги в Република България.

Проектът предвижда изграждане на цялостна технологична, организационна и интеграционна среда, включваща най-малко следните основни компоненти:

- национална рамка на доверие, която определя правилата, процедурите, техническите изисквания и моделите за доверие между участниците в екосистемата;
- електронен списък на участниците, чрез който се управляват доставчици на портфейли, доставчици на самоличност, доставчици на атрибути, доставчици на квалифицирани атрибути, посредници при верификация и доверяващи се страни;
- регистратор на доверителни списъци, необходим за публикуване, управление и валидиране на доверителна информация;
- доставчик на Портфейл за цифрова самоличност и свързана инфраструктура за управление на жизнения цикъл на портфейлите;
- мобилно приложение за граждани и представители на бизнеса, чрез което се използват функциите на Портфейла;
- доставчик на самоличност, който осигурява надеждна идентификация на лицата и свързване на самоличността с Портфейла;
- доставчик на квалифицирани атрибути от името на публични институции;
- посредник при верификация, чрез който доверяващите се страни ще могат да заявяват, получават и проверяват данни, предоставяни чрез Портфейла;
- интеграционни интерфейси към национални регистри, средата за междурегистров обмен и други съществуващи компоненти на електронното управление;
- интеграции с квалифицирани доставчици на удостоверителни услуги за осигуряване на квалифициран електронен подпис;
- механизми за интеграция с европейската инфраструктура и за трансгранична проверка и използване на цифрови удостоверения и атрибути.

Основните ползи от реализацията на проекта са свързани с намаляване на административната тежест, ограничаване на необходимостта от физическо посещение в администрацията, повишаване на сигурността и проследимостта при достъп до електронни услуги, предоставяне на по-голям контрол на гражданите върху личните им данни, намаляване на разходите за идентификация и KYC процеси за бизнеса и създаване на възможност за дистанционно подписване и сключване на договори. За публичния сектор проектът ще създаде единна национална рамка за доверие и цифрова идентичност, която да подпомогне предоставянето на електронни административни услуги на по-високо ниво на електронизация и с по-висока степен на сигурност.

Очакваният резултат от проекта е изграждане, въвеждане/внедряване и последваща гаранционна поддръжка на национален Портфейл за цифрова самоличност, който отговаря на приложимите европейски и национални изисквания, осигурява оперативна съвместимост с

европейската инфраструктура, позволява използване на удостоверени цифрови атрибути, предоставя възможност за квалифицирано електронно подписване и създава устойчива основа за развитие на цифровата идентичност в Република България.

2.4 Нормативна рамка

Проектът се реализира в съответствие с приложимата нормативна рамка на Европейския съюз и националното законодателство на Република България в областта на електронната идентификация, електронното управление, електронните удостоверителни услуги, защитата на личните данни, киберсигурността, гражданската регистрация, документите за самоличност, административното обслужване, оперативната съвместимост и използването на информационни системи в държавната администрация.

Нормативната рамка е от съществено значение за изпълнението на проекта, тъй като Портфейлът за цифрова самоличност представлява средство за електронна идентификация и доверителна инфраструктура, чрез която гражданите, жителите и юридическите лица ще могат да удостоверяват самоличността си, да получават, съхраняват и представят електронни удостоверения за атрибути, да използват квалифициран електронен подпис и да достъпват електронни публични и частни услуги в национален и трансграничен контекст.

При изпълнението на проекта следва да се спазват принципите на законосъобразност, доброволност при използване на портфейла, защита на личните данни по подразбиране и по проект, минимизиране на данните, контрол на потребителя върху предоставяните атрибути, оперативна съвместимост, технологична неутралност, киберустойчивост, проследимост, отчетност, равнопоставен достъп и недопускане на дискриминационно третиране на участниците в екосистемата.

2.4.1 Приложими регламенти, директиви, актове за изпълнение, стандарти и препоръки на Европейския съюз

Основната европейска правна рамка за изпълнението на проекта се формира от Регламент (ЕС) № 910/2014 относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар, изменен с Регламент (ЕС) 2024/1183 по отношение на създаването на Европейска рамка за цифрова идентичност. Тази рамка въвежда Европейския портфейл за цифрова самоличност като средство за електронна идентификация и определя основните изисквания към неговото предоставяне, използване, сигурност, оперативна съвместимост, сертифициране, уведомяване и приемане от публични и определени частни доставчици на услуги.

При реализацията на проекта следва да бъдат взети предвид най-малко следните актове на Европейския съюз:

- 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 (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 г. за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на Европейска рамка за цифрова идентичност;
- актовете за изпълнение към Регламент (ЕС) № 910/2014, изменен с Регламент (ЕС) 2024/1183, включително актовете, уреждащи основните функционалности на Европейските портфейли за цифрова самоличност, издаването на данни за идентификация на лице и електронни удостоверения за атрибути, поддържаните протоколи и интерфейси, уведомяването на Европейската комисия и сертифицирането на портфейлите;
- Регламент за изпълнение (ЕС) 2024/2977 на Комисията относно правилата за издаване на данни за идентификация на лице и електронни удостоверения за атрибути към единици на Европейски портфейл за цифрова самоличност;
- Регламент за изпълнение (ЕС) 2024/2979 на Комисията относно правилата за основните функционалности на Европейските портфейли за цифрова самоличност;
- Регламент за изпълнение (ЕС) 2024/2980 на Комисията относно правилата за уведомяване на Европейската комисия във връзка с екосистемата на Европейските портфейли за цифрова самоличност;
- Регламент за изпълнение (ЕС) 2024/2981 на Комисията относно сертификационните схеми за Европейските портфейли за цифрова самоличност;
- Регламент за изпълнение (ЕС) 2024/2982 на Комисията относно протоколите и интерфейсите, които следва да се поддържат от Европейската рамка за цифрова идентичност;
- Регламент за изпълнение (ЕС) 2025/846 на Комисията относно трансграничното съпоставяне на самоличността на физически лица;
- Регламент за изпълнение (ЕС) 2025/847 на Комисията относно реакциите при пробиви в сигурността на Европейските портфейли за цифрова самоличност;
- Регламент за изпълнение (ЕС) 2025/848 на Комисията относно регистрацията на доверяващите се страни, използващи Европейските портфейли за цифрова самоличност;
- Регламент за изпълнение (ЕС) 2025/849 на Комисията относно подаването на информация до Комисията и до Групата за сътрудничество за списъка на сертифицираните Европейски портфейли за цифрова самоличност;
- останалите регламенти за изпълнение, приети през 2025 г. и след това въз основа на Регламент (ЕС) № 910/2014, изменен с Регламент (ЕС) 2024/1183, в

актуалната им редакция към датата на изготвяне на детайлната техническа спецификация;

- последващи регламенти за изпълнение, делегирани актове, технически спецификации, референтни стандарти и указания на Европейската комисия и компетентните европейски органи, приложими към EUDI Wallet, електронните удостоверения за атрибути, квалифицираните електронни подписи, квалифицираните електронни печати, управлението на отдалечени устройства за създаване на квалифициран електронен подпис/печат и услугите по доверие;
- Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, известен като Общ регламент относно защитата на данните (GDPR);
- Директива (ЕС) 2016/680 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, когато е приложима спрямо конкретни интеграции или процеси;
- Директива (ЕС) 2022/2555 относно мерки за високо общо ниво на киберсигурност в Съюза (NIS 2), доколкото изискванията ѝ са относими към националната цифрова инфраструктура, доставчиците на услуги, управлението на риска и докладването на инциденти;
- Регламент (ЕС) 2019/881 относно ENISA и сертифицирането на киберсигурността на информационните и комуникационните технологии (Акт за киберсигурността), доколкото е приложим към сертификацията и оценката на сигурността на компоненти и услуги;
- Регламент (ЕС) 2018/1724 за създаване на единна цифрова платформа за предоставяне на достъп до информация, процедури и услуги за помощ и решаване на проблеми, доколкото Портфейлът ще подпомага трансграничното заявяване и използване на електронни услуги;
- Регламент (ЕС) 2022/868 относно европейското управление на данните (Data Governance Act), когато проектът включва модели за доверено споделяне, повторно използване или посредничество при обмен на данни;
- Регламент (ЕС) 2022/2065 относно единния пазар на цифрови услуги (Digital Services Act), доколкото е приложим по отношение на доставчици на онлайн платформи и доверяващи се страни, които следва да приемат или да взаимодействат с EUDI Wallet;

- Директива (ЕС) 2019/1024 относно отворените данни и повторното използване на информацията от обществения сектор, доколкото в рамките на проекта се създават или публикуват публични регистри, списъци или машинночетими данни;
- приложимите спецификации, стандарти, профили и указания, разработени в рамките на European Digital Identity Wallet Architecture and Reference Framework (ARF), включително спецификациите относно участниците в екосистемата, портфейлните единици, PID, електронните удостоверения за атрибути, доверяващите се страни, доставчиците на портфейли, интерфейсите за издаване и представяне, криптографските механизми, журналите, защитата на поверителността и оперативната съвместимост;

2.4.2 Национална нормативна уредба в областта на Европейския портфейл за цифрова самоличност, електронната идентификация и електронното управление

Проектът следва да бъде съобразен с националната нормативна рамка, уреждаща изграждането и използването на Портфейла за цифрова самоличност, електронната идентификация, електронните удостоверителни услуги, електронното управление, обмена на данни между администрации, административното обслужване и функционирането на информационните системи в държавната администрация.

В тази връзка при изпълнението на проекта следва да се вземат предвид най-малко следните нормативни актове:

- Конституцията на Република България, в частта относно основните права на гражданите, защитата на личния живот, правото на информация и задълженията на държавните органи;
- Проектът на Закон за Европейския портфейл за цифрова самоличност, публикуван за обществено обсъждане, както и окончателният закон след неговото приемане и обнародване, доколкото с него ще се уредят условията и редът за изграждане, управление и използване на Европейски портфейли за цифрова самоличност в Република България, изискванията към доставчиците на портфейли, доставчиците на данни за идентификация на лица, доставчиците на атрибути, доверяващите се страни, доверителните списъци, надзора, контрола и взаимодействието с Европейската комисия и държавите членки;
- подзаконовите нормативни актове, които ще бъдат приети въз основа на Закона за Европейския портфейл за цифрова самоличност, включително наредби, правила, процедури, методики и технически изисквания за регистрация, сертифициране, вписване, свързване, контрол, надзор, уведомяване, доверителни списъци, приемане на портфейли, интеграция с доставчици на

удостоверителни услуги и издаване/проверка на електронни удостоверения за атрибути;

- Законът за електронното управление, включително правилата за предоставяне на електронни административни услуги, служебен обмен на данни, електронни документи в администрацията, информационни системи, оперативна съвместимост, регистри, електронни услуги, административни процеси и задължения на административните органи;
- подзаконовите актове към Закона за електронното управление, включително Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги, Наредбата за обмена на документи в администрацията, Наредбата за административния регистър и всички други приложими актове, уреждащи електронни услуги, интерфейси, регистри, метаданни, формати, оперативна съвместимост и интеграционни механизми;
- Законът за електронната идентификация, доколкото урежда обществените отношения, свързани с електронната идентификация на физическите лица, средствата за електронна идентификация, електронните идентификатори, схемите за електронна идентификация, нивата на осигуреност и свързаните с тях органи, регистри, правила и процедури;
- Правилникът за прилагане на Закона за електронната идентификация и приложимите подзаконови нормативни актове, свързани с алгоритмите, методите, организационните и техническите правила за електронна идентификация;
- Законът за електронния документ и електронните удостоверителни услуги, включително правилата относно електронния документ, електронния подпис, електронния печат, електронното удостоверяване, квалифицираните удостоверителни услуги, доставчиците на удостоверителни услуги и правното действие на електронните изявления;
- подзаконовите актове в областта на електронните удостоверителни услуги, включително наредбите, правилата и изискванията, свързани с квалифицираните електронни подписи, квалифицираните електронни печати, квалифицираните удостоверения, удостоверенията за време, електронната препоръчана поща, проверката на валидност и вписването в доверителни списъци;
- Административнопроцесуалният кодекс, включително правилата относно административното производство, електронното заявяване, електронната комуникация, електронното връчване, правата на гражданите и организациите и задълженията на административните органи;

- Законът за администрацията, доколкото урежда организацията и функциите на административните органи и взаимодействието между тях;
- Законът за достъп до обществена информация, доколкото проектът включва публичност на регистри, доверителни списъци, информация за участници в екосистемата, техническа документация, правила за присъединяване и публични данни;

2.4.3 Национална нормативна уредба в областта на самоличността, гражданската регистрация и автентичните източници на данни

Портфейлът за цифрова самоличност изисква надеждно свързване на софтуерната част с данните за идентификация на лицето и с автентични източници на данни, поддържани от компетентни публични органи. Поради това проектът следва да бъде съобразен с нормативната рамка относно гражданската регистрация, българските лични документи, чужденците, пребиваването, адресната регистрация и официалните регистри.

При изпълнението на проекта следва да се вземат предвид най-малко следните нормативни актове:

- Законът за гражданската регистрация, включително правилата относно гражданското състояние, Единната система за гражданска регистрация и административно обслужване на населението (ЕСГРАОН), постоянния и настоящия адрес, актовете за гражданско състояние, регистрите и достъпа до данни;
- Законът за българските лични документи, включително правилата относно издаването, валидността, съдържанието и използването на лични карти, паспорти, свидетелства за управление на МПС и други документи, съдържащи данни за самоличност;
- Законът за чужденците в Република България, доколкото проектът следва да осигури използване на Портфейла и от лица, които пребивават законно в Република България и попадат в обхвата на европейската рамка за цифрова идентичност;
- Законът за българското гражданство, доколкото статутът на гражданството може да бъде релевантен атрибут или част от данните за идентификация;
- Законът за регистър БУЛСТАТ и Законът за търговския регистър и регистъра на юридическите лица с нестопанска цел, доколкото проектът обхваща юридически лица, представителна власт, атрибути за организации и процеси за идентификация на бизнеса;
- нормативните актове, уреждащи първичните регистри и автентичните източници на данни, които могат да бъдат използвани за издаване или проверка на атрибути в Портфейла, включително регистри, поддържани от МВР, ГРАО,

Агенцията по вписванията, НАП, НОИ, МОН, МТСП, Министерството на правосъдието, секторни администрации и други компетентни органи;

- подзаконовите нормативни актове, уреждащи реда за достъп, обмен, проверка, актуализация и предоставяне на данни от автентични източници, включително чрез средата за междурегистров обмен, RegiX, интеграционния слой на електронното управление и други национални инфраструктурни компоненти.

2.4.4 Нормативна уредба в областта на защитата на личните данни и поверителността

Предвид естеството на Портфейла за цифрова самоличност, проектът включва обработване на значителен обем лични данни, включително данни за идентификация, уникални идентификатори, атрибути, данни за представителство, данни от регистри, технически идентификатори, системни журнали, данни за съгласие, транзакционни записи и други данни, свързани с използването на портфейла. Поради това защитата на личните данни следва да бъде заложена като основен принцип при анализа, проектирането, разработката, тестването, внедряването и експлоатацията на системата.

При изпълнението на проекта следва да се вземат предвид най-малко следните нормативни актове и изисквания:

- Законът за защита на личните данни, включително националните правила относно защитата на правата на физическите лица при обработване на лични данни, правомощията на Комисията за защита на личните данни и специалните изисквания при обработване от публични органи;
- приложимите указания, становища и насоки на Европейския комитет по защита на данните, Комисията за защита на личните данни и Европейския надзорен орган по защита на данните, доколкото са относими към електронната идентификация, цифровите портфейли, съгласието, прозрачността, DPIA, проследимостта, минимизирането на данните, селективното разкриване на атрибути и управлението на рискове за субектите;
- изискванията за извършване на оценка на въздействието върху защитата на данните (DPIA) за процесите, които предполагат висок риск за правата и свободите на физическите лица, включително обработване на национални идентификатори, широкомащабна интеграция с регистри, управление на атрибути и трансграничен обмен;
- изискванията за регистри на дейностите по обработване, определяне на роли на администратор, съвместни администратори и обработващи лични данни, договори с обработващи, вътрешни правила, технически и организационни мерки, управление на достъпа, одитен журнал, криптиране, псевдонимизация,

управление на срокове за съхранение и механизми за упражняване на права от субектите на данни.

2.4.5 Нормативна уредба в областта на киберсигурността, информационната сигурност и устойчивостта

Портфейлът за цифрова самоличност представлява критично значим компонент от националната цифрова инфраструктура, тъй като чрез него ще се осъществява електронна идентификация, удостоверяване, подписване, представяне на атрибути и достъп до публични и частни електронни услуги. Поради това проектът следва да бъде реализиран при високи изисквания за киберсигурност, устойчивост, непрекъсваемост, защита на криптографските ключове, управление на уязвимости, наблюдение, реакция при инциденти и възстановяване при бедствия.

При изпълнението на проекта следва да се вземат предвид най-малко следните нормативни актове и изисквания:

- Законът за киберсигурност, включително правилата относно мрежовата и информационната сигурност, управлението на риска, задълженията на административните органи и доставчиците на услуги, докладването на инциденти, компетентните органи и координацията при киберинциденти;
- подзаконовите актове към Закона за киберсигурност, включително Наредбата за минималните изисквания за мрежова и информационна сигурност, доколкото определя минимални организационни и технически мерки за защита на информационните и комуникационните системи;
- Законът за защита на класифицираната информация, доколкото в рамките на проекта се обработва или достъпва класифицирана информация или се изискват специфични мерки за защита на чувствителна информация;
- приложимите стандарти ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27701, ISO/IEC 22301, ISO/IEC 15408/Common Criteria, ETSI стандарти за доверителни услуги, криптографски стандарти, стандарти за мобилна сигурност и други референтни стандарти, доколкото са приложими към архитектурата и сигурността на Портфейла;
- изискванията за сигурно управление на криптографски ключове, сигурно съхранение на ключов материал, защита на мобилни устройства, използване на защитена среда за криптографски операции, дистанционно управление на ключове, отмяна, блокиране, възстановяване, одитен журнал и доказуемост на извършените действия;
- изискванията за провеждане на тестове за сигурност, penetration testing, преглед на кода, анализ на уязвимости, проверка на конфигурации, контрол на достъпа, управление на привилегии, мониторинг, SIEM интеграция, процедури за

реакция при инциденти и планове за непрекъсваемост на дейността и възстановяване при бедствия.

2.4.6 Нормативна уредба и правила за административно обслужване, електронни услуги и интеграции

Проектът следва да бъде съобразен с правилата за предоставяне на електронни административни услуги, електронна комуникация с гражданите и бизнеса, служебен обмен на данни между администрации и повторно използване на вече налична информация. Портфейлът за цифрова самоличност следва да подпомага електронизацията на административните услуги, като осигурява надеждна идентификация, представяне на атрибути, електронно подписване и намаляване на необходимостта от предоставяне на хартиени документи.

При изпълнението на проекта следва да се вземат предвид:

- Административнопроцесуалният кодекс;
- Законът за електронното управление;
- Законът за електронната идентификация;
- Законът за електронния документ и електронните удостоверителни услуги;
- Законът за достъп до обществена информация;
- Законът за ограничаване на административното регулиране и административния контрол върху стопанската дейност, доколкото е относим към намаляване на административната тежест и използване на удостоверени цифрови атрибути;
- приложимите правила за електронно връчване, електронно заявяване, електронно плащане, електронни формуляри, служебно събиране на данни и повторно използване на информация от регистри;
- изискванията за използване на Единния портал за достъп до електронни административни услуги, Системата за сигурно електронно връчване, Системата за електронна автентикация, RegiX, Държавния хибриден частен облак, интеграционния слой на електронното управление и други национални споделени компоненти, когато са приложими към архитектурата на проекта.

3 Цели, обхват и очаквани резултати от изпълнение на проекта

3.1 Общи и специфични цели на проекта

Проектът е насочен към изграждане и въвеждане/внедряване на национален Портфейл за цифрова самоличност (EU Digital Wallet) и осигуряване на последваща гаранционна поддръжка. Основната цел е Република България да изгради сигурна, надеждна, оперативно съвместима и съответстваща на европейската рамка инфраструктура за цифрова самоличност, чрез която гражданите и юридическите лица да могат да се идентифицират по електронен път, да получават, съхраняват, управляват и представят електронни удостоверения за атрибути, както и да използват квалифициран електронен подпис чрез цифровия портфейл. Проектът има

стратегическо значение за развитието на електронното управление, тъй като създава единна национална рамка за доверие, цифрова идентичност и атрибути, която ще позволи предоставяне на електронни административни услуги с по-висока степен на електронизация, по-висока сигурност и по-ниска административна тежест за гражданите, бизнеса и администрацията.

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

- Изграждане на национална рамка на доверие за Портфейла за цифрова самоличност, която да дефинира организационния, техническия, правния и оперативния модел за участие на доставчици на портфейли, доставчици на самоличност, доставчици на атрибути, доставчици на квалифицирани атрибути, посредници при верификация и доверяващи се страни.
- Изграждане на национални доверителни списъци и регистър на участниците в екосистемата, чрез които да се осигури проследимост, публичност, валидиране и управление на участието на всички регистрирани и сертифицирани субекти, свързани с Портфейла за цифрова самоличност.
- Изграждане на доставчик на Портфейл за цифрова самоличност и съпътстваща техническа инфраструктура, която да осигурява издаване, активиране, управление, използване, блокиране, възстановяване и прекратяване на портфейлни единици при спазване на изискванията за сигурност, оперативна съвместимост и защита на личните данни.
- Разработване и внедряване на мобилно приложение за Портфейла за цифрова самоличност, чрез което потребителите да могат да управляват своята цифрова самоличност, да получават и съхраняват електронни удостоверения за атрибути, да предоставят данни към доверяващи се страни, да използват квалифициран електронен подпис и да упражняват контрол върху споделяните от тях данни.
- Изграждане на доставчик на самоличност и механизми за първоначална идентификация, привързване на самоличността към портфейла и последващо удостоверяване на потребителите, включително чрез интеграция с национални регистри, eIDAS възела, съществуващи средства за електронна идентификация и други допустими механизми с необходимото ниво на осигуреност.
- Изграждане на доставчик на квалифицирани атрибути от името на публични институции, чрез който да се предоставя възможност за издаване, получаване, съхраняване, управление и проверка на електронни удостоверения за атрибути, базирани на данни от автентични източници и първични регистри.
- Изграждане на посредник при верификация, чрез който доверяващите се страни да могат да заявяват и проверяват удостоверени цифрови атрибути, предоставяни от потребителите чрез Портфейла, при спазване на принципите за

минимизиране на данните, съгласие/контрол от страна на потребителя, прозрачност и отчетност.

- Осигуряване на интеграция с квалифицирани доставчици на удостоверителни услуги, така че чрез Портфейла да се предоставя възможност за създаване на квалифициран електронен подпис, включително безплатно използване от физически лица за непрофесионални цели съгласно приложимата нормативна рамка.
- Осигуряване на интеграция с националните регистри, средата за междурегистров обмен, RegiX, системите за електронна идентификация, eIDAS възела, Държавния хибриден частен облак и други национални компоненти на електронното управление, необходими за надеждно издаване и проверка на данни за самоличност и атрибути.
- Осигуряване на трансгранична оперативна съвместимост с европейската инфраструктура по eIDAS, така че българският Портфейл за цифрова самоличност да бъде разпознаваем и използваем в други държави членки, а портфейли от други държави членки да могат да бъдат приемани от български доверяващи се страни.
- Осигуряване на високо ниво на информационна сигурност, киберустойчивост, защита на личните данни, криптографска защита, проследимост, управление на риска, сертификация и съответствие с приложимите европейски и национални изисквания.
- Разширяване на екосистемата чрез присъединяване на доставчици на квалифицирани електронни подписи, доставчици на квалифицирани атрибути, публични институции, частни доставчици на услуги и други доверяващи се страни, които да използват Портфейла като средство за идентификация, удостоверяване и обмен на атрибути.
- Осигуряване на гаранционна поддръжка след въвеждане/внедряване на решението, включително поддръжка на приложните компоненти, отстраняване на дефекти, управление на инциденти, поддръжка на интеграции, съдействие при експлоатация и адаптиране към нормативни, технически и организационни промени.

3.2 Обхват на проекта

Обхватът на проекта включва изграждане, въвеждане/внедряване и последваща гаранционна поддръжка на национално решение за Портфейл за цифрова самоличност (EU Digital Wallet), заедно с необходимите инфраструктурни, приложни, интеграционни, административни и доверителни компоненти, които осигуряват функционирането му в съответствие с европейската и националната нормативна рамка.

Проектът следва да осигури реализация на национална екосистема за цифрова самоличност, която позволява електронна идентификация на граждани, жители и юридически лица, издаване и използване на удостоверени цифрови атрибути, създаване на квалифициран електронен подпис, проверка на атрибути от доверяващи се страни, интеграция с национални регистри и трансгранична оперативна съвместимост с европейската инфраструктура по eIDAS.

Обхватът на проекта се структурира в следните основни дейности:

Фаза 1 - „Рамка на доверие, портфейл и идентификация, атрибути и верификация“

Фаза 2 - „Разширяване на екосистемата“

Към всички фази по проекта се прилагат хоризонтални изисквания за бизнес анализ, системен анализ, проектиране, разработка, тестване, контрол на качеството, информационна сигурност, киберсигурност, защита на личните данни, подготовка за сертифициране, DevOps процеси, внедряване, документация, обучение и гаранционна поддръжка.

Изпълнението на всяка фаза следва да включва изготвяне и поддържане на необходимата техническа, функционална, архитектурна, интеграционна, тестова, експлоатационна и потребителска документация. За всеки компонент следва да бъдат проведени функционални, интеграционни, системни, приемателни, регресионни, натоварващи и тестове за сигурност, включително penetration testing и анализ на уязвимости, когато е приложимо.

В рамките на проекта следва да бъдат осигурени необходимите среди за разработка, тестване, приемане, обучение и продукционна експлоатация, както и механизми за мониторинг, проследимост в системен журнал, управление на инциденти, управление на промени, възстановяване при бедствия и гаранционна поддръжка.

3.3 Целеви групи

Реализацията на проекта е насочена към широк кръг целеви групи, които ще използват, администрират, интегрират, поддържат или ще се доверяват на Портфейла за цифрова самоличност и свързаните с него удостоверени цифрови атрибути.

Основните целеви групи по проекта са:

- **Граждани на Република България** - основна целева група са физическите лица, които ще използват Портфейла за цифрова самоличност за електронна идентификация, получаване и управление на удостоверени цифрови атрибути, достъп до електронни административни и частни услуги, квалифицирано електронно подписване и трансгранично използване на цифровата си самоличност в рамките на Европейския съюз.
- **Юридически лица и представители на бизнеса** - целева група са юридическите лица, техните законни представители, упълномощени лица и

служители, които ще използват Портфейла за достъп до електронни услуги, представяне на атрибути, удостоверяване на представителна власт, участие в административни и търговски процеси, дистанционно подписване и намаляване на разходите за идентификация

- **Публични администрации и органи на публичния сектор** - включва държавните органи, общинските администрации, органите на изпълнителната власт, първичните администратори на данни и други публични институции, които ще предоставят електронни услуги, ще приемат Портфейла като средство за идентификация, ще издават или потвърждават атрибути, ще участват в процесите по служебен обмен на данни и ще бъдат включени в националната екосистема.
- **Първични администратори на данни и доставчици на електронни удостоверения за атрибути** - това са институциите и организациите, които поддържат автентични източници на данни и ще предоставят електронни удостоверения за атрибути за нуждите на Портфейла. Това включва органи, поддържащи регистри за самоличност, гражданска регистрация, адресна регистрация, правен статус, образование, социално осигуряване, професионална квалификация, представителна власт и други релевантни обстоятелства.
- **Доверяващи се страни** - включва публични и частни доставчици на електронни услуги, които ще приемат Портфейла за цифрова самоличност като средство за идентификация, удостоверяване или представяне на атрибути. В тази група попадат административни органи, банки, застрахователи, телекомуникационни оператори, образователни институции, работодатели, доставчици на електронна търговия, доставчици на регулирани услуги и други организации, които имат необходимост от надеждна електронна идентификация или проверка на удостоверени данни.
- **Доставчици на портфейли** - целева група са доставчиците на Портфейли за цифрова самоличност, които ще бъдат регистрирани и/или сертифицирани съгласно приложимата нормативна рамка и ще предоставят портфейлни решения на потребителите при спазване на изискванията за сигурност, оперативна съвместимост, защита на личните данни и управление на жизнения цикъл на портфейлите.
- **Доставчици на самоличност** - целева група са субектите, които ще участват в процесите по първоначална идентификация, потвърждаване на самоличност и издаване на данни за идентификация на лице за нуждите на Портфейла. Тази група включва компетентни публични органи и други допустими участници, определени в нормативната и техническата рамка.

- **Доставчици на квалифицирани електронни подписи и други квалифицирани удостоверителни услуги** - или квалифицираните доставчици на удостоверителни услуги, които ще бъдат интегрирани с Портфейла с цел предоставяне на възможност за създаване на квалифициран електронен подпис и други свързани удостоверителни услуги.
- **Доставчици на квалифицирани и неквалифицирани атрибути** - това са доставчиците на електронни удостоверения за атрибути, които ще предоставят квалифицирани или неквалифицирани атрибути за нуждите на Портфейла, включително частни организации и публични институции, които поддържат надеждни източници на данни.
- **Посредници при верификация** - всички субекти и компоненти, които ще подпомагат доверяващите се страни при заявяване, получаване и проверка на цифрови атрибути, предоставяни от потребителите чрез Портфейла.
- **Администратори, оператори и служители по поддръжка** - включва служителите, които ще администрират, наблюдават, поддържат и експлоатират системата и нейните компоненти. Това включва системни администратори, администратори на регистри, администратори на доверителни списъци, оператори по онбординг, експерти по сигурност, екипи за техническа поддръжка, DevOps екипи, QA екипи и служители, участващи в приемане и експлоатация.
- **Контролни, надзорни и сертифициращи органи** – в това число органите и структурите, които ще упражняват контрол, надзор, сертификация, оценка на съответствието, проверка на сигурността, защита на личните данни и мониторинг върху участниците и процесите в екосистемата.
- **Европейска комисия, държави членки и европейска екосистема за цифрова идентичност** - проектът има и трансгранично измерение, поради което целева група са европейските институции, компетентните органи на държавите членки и участниците в европейската екосистема, с които българският Портфейл следва да бъде оперативно съвместим.

3.4 Очаквани резултати

В резултат от изпълнението на проекта следва да бъде изградена, въведена/внедрена и поддържана национална екосистема за Портфейл за цифрова самоличност (EU Digital Wallet), която осигурява електронна идентификация, управление и представяне на удостоверени цифрови атрибути, използване на квалифициран електронен подпис и оперативна съвместимост с европейската инфраструктура по eIDAS.

Очакваните резултати от изпълнението на проекта са:

- Изградена национална рамка на доверие за Портфейла за цифрова самоличност, включително правила, процедури, технически изисквания и механизми за регистрация, присъединяване, контрол и управление на участниците в екосистемата;
- Изградени регистър на участниците, доверителни списъци и необходимата PKI/доверителна инфраструктура за осигуряване на сигурно, проследимо и валидируемо взаимодействие между доставчици на портфейли, доставчици на самоличност, доставчици на атрибути, посредници при верификация и доверяващи се страни;
- Изграден доставчик на Портфейл за цифрова самоличност, който осигурява управление на жизнения цикъл на портфейлните единици, включително издаване, активиране, използване, блокиране, възстановяване и прекратяване;
- Разработено и внедрено мобилно приложение за Портфейл за цифрова самоличност, чрез което потребителите могат да се идентифицират, да получават и съхраняват данни за идентификация и цифрови атрибути, да управляват съгласията си и да представят атрибути пред доверяващи се страни;
- Изграден доставчик на самоличност, осигуряващ надеждна първоначална идентификация на потребителите, проверка на данни от автентични източници и привързване на потвърдена самоличност към портфейлна единица;
- Реализирани интеграции с национални регистри, системи за електронна идентификация, eIDAS възел, RegiX, ЕСГРАОН, регистрите за самоличност и други приложими автентични източници на данни;
- Изграден доставчик на квалифицирани атрибути от името на публични институции, чрез който се осигурява издаване, обновяване, отмяна, съхранение, представяне и проверка на електронни удостоверения за атрибути;
- Изграден посредник при верификация, чрез който доверяващите се страни могат да заявяват и проверяват атрибути, предоставени от потребителя чрез Портфейла, при спазване на принципите за минимизиране на данните, контрол от страна на потребителя, прозрачност и проследимост;
- Осигурена интеграция с квалифицирани доставчици на удостоверителни услуги, така че чрез Портфейла да може да се създава квалифициран електронен подпис при условията, определени в приложимата нормативна рамка;
- Осигурена възможност за присъединяване и интеграция на доставчици на квалифицирани електронни удостоверения за атрибути и други допустими доставчици на атрибути;

- Надградена екосистема с механизми за разширяване на поддържаните доставчици, доверяващи се страни, мобилни устройства, сценарии за използване и интеграции;
- Осигурена трансгранична оперативна съвместимост с европейската инфраструктура по eIDAS, така че българският Портфейл за цифрова самоличност да може да бъде използван в други държави членки, както и портфейли от други държави членки да могат да бъдат приемани в Република България;
- Осигурено високо ниво на информационна сигурност, киберустойчивост, защита на личните данни, криптографска защита, одитен журнал, одитируемост и проследимост на действията в системата;
- Проведени функционални, интеграционни, системни, приемателни, регресионни, натоварващи и тестове за сигурност, включително анализ на уязвимости и penetration testing за приложимите компоненти;
- Подготвено решение за сертифициране и оценка на съответствието съгласно приложимите европейски и национални изисквания към Европейските портфейли за цифрова самоличност;
- Изготвена пълна проектна, техническа, функционална, архитектурна, интеграционна, тестова, потребителска и експлоатационна документация;
- Проведени обучения за администратори, оператори, служители по поддръжка и други участници, определени от Бенефициера;
- Въведени/внедрени необходимите среди за разработка, тестване, приемане, обучение, продукционна експлоатация и поддръжка;
- Осигурена гаранционна поддръжка на разработените компоненти и интеграции, включително управление на инциденти, отстраняване на дефекти, поддръжка на интеграции, актуализация на документация и съдействие при експлоатация.

3.5 Период на изпълнение

Периодът на изпълнение на дейностите по анализ, разработване, тестване и внедряване на Системата (фаза 1 и фаза 2) в срок до 30.09.2027 г. Срокът за конкретното изпълнение на всяка една и конкретна фаза ще бъде съгласуван между страните, чрез подписване на план - график на проекта, не по-късно от 10 (десет) работни дни след подписване на договора между страните. Срокът по дейностите следва да бъде обвързан с приемане на законодателните и нормативните промени. При забавяне приемане на законодателни промени срокът по проекта може да бъде удължаван с промяна в подписания план - график.

За всяка дейност се подписва отделен приемо-предавателен протокол за нейното приемане, тестване и внедряване в реална експлоатация.

Срокът на гаранционната поддръжка на системата е **24** (двадесет и четири) месеца, считано от приемане на всички дейности по проекта, удостоверено с двустранно подписан приемо-предавателен протокол.

4 Текущо състояние

Електронната идентификация и цифровото удостоверяване на самоличност са ключови предпоставки за развитието на електронното управление, електронните административни услуги, трансграничния обмен на данни и цифровото взаимодействие между гражданите, бизнеса и публичната администрация. До настоящия момент в Република България съществуват отделни механизми за електронна идентификация, електронно подписване и достъп до електронни услуги, но липсва завършено, въведено и масово използваемо национално решение, което да отговаря на концепцията и изискванията за Европейски портфейл за цифрова самоличност съгласно Регламент (ЕС) 2024/1183.

Към момента достъпът до електронни административни услуги в България се осъществява чрез различни средства и механизми, включително квалифициран електронен подпис, персонални идентификационни кодове, секторни механизми за автентикация, системи за електронна автентикация, eIDAS възел за трансгранична електронна идентификация, както и отделни частни решения за дистанционна идентификация и електронно подписване. Тези механизми подпомагат използването на електронни услуги, но не формират единна национална екосистема за цифрова самоличност, в която потребителят да може чрез един портфейл да управлява своята цифрова идентичност, удостоверени атрибути, квалифицирани електронни подписи и представянето на данни пред доверяващи се страни.

Наличните към момента средства имат ограничено приложение по отношение на удобство, масовост, потребителско възприемане, мобилност, възможност за селективно представяне на атрибути, трансгранична оперативна съвместимост и интеграция с доставчици на квалифицирани електронни удостоверения за атрибути. В редица случаи използването на електронни услуги продължава да бъде свързано със сложни потребителски процеси, необходимост от отделни регистрации, използване на различни средства за достъп, липса на единен потребителски модел и необходимост от представяне на документи или данни, които вече съществуват в първични регистри на администрацията.

Липсата на такова решение поставя България в ситуация, в която е необходимо ускорено изграждане на национална екосистема за цифрова самоличност. Това включва не само разработване на мобилно приложение, а изграждане на цялостна рамка на доверие, доставчик на портфейл, доставчик на самоличност, доставчик на квалифицирани атрибути от името на публични институции, посредник при верификация, интеграции с национални регистри, интеграция с квалифицирани доставчици на електронни подписи и оперативна съвместимост с европейската инфраструктура по eIDAS.

Развитието на Европейския портфейл за цифрова самоличност не е изолирана национална инициатива, а общоевропейски процес. Съгласно европейската рамка държавите членки следва да предоставят поне един Европейски портфейл за цифрова самоличност на гражданите, жителите и бизнеса. Европейската комисия поддържа обща рамка за изпълнение, включително архитектурна и референтна рамка, актове за изпълнение, пилотни проекти и насоки за оперативна съвместимост. В европейски мащаб вече се изпълняват широкомащабни пилотни проекти, в които участват публични органи, частни доставчици, технологични организации и държави членки, с цел тестване на основни сценарии за използване на EUDI Wallet.

В редица държави членки вече съществуват национални решения за цифрова идентичност, които се използват като основа за адаптиране към новата европейска рамка. Италия развива IT Wallet върху националното приложение IO, като от 2024 г. позволява добавяне на цифрови версии на документи като свидетелство за управление, здравноосигурителна карта и карта за хора с увреждания. Франция развива France Identité на база националната електронна лична карта, като приложението се позиционира като основа за бъдещия френски цифров портфейл. Германия изгражда своя EUDI Wallet в рамките на национална програма за цифрови идентичности и създава правна основа за използването му. Нидерландия разработва публичен NL Wallet, който следва да бъде национално решение, признато по eIDAS. Полша използва натрупания опит от mObywatel, а Естония, Дания и Финландия надграждат вече развити национални екосистеми за електронна идентичност и цифрови услуги.

Този международен контекст показва, че държавите членки подхождат към EUDI Wallet по различен начин, но общата посока е изграждане на национални цифрови портфейли, които надграждат съществуващи системи за електронна идентификация и ги привеждат към общите европейски изисквания за оперативна съвместимост, сигурност, защита на личните данни и трансгранично използване. За България това означава, че проектът следва да компенсира липсата на завършен национален мобилен портфейл и едновременно с това да използва съществуващите национални компоненти - регистри, среда за междурегистров обмен, eIDAS възел, системи за електронна автентикация, квалифицирани доставчици на удостоверителни услуги и инфраструктура за електронно управление.

Проектът на Закон за Европейския портфейл за цифрова самоличност предвижда уредба на условията и реда за изграждане, управление и използване на портфейлите в Република България, регистрацията на доставчици на портфейли, доставчици на данни за идентификация и доставчици на атрибути, правата и задълженията на доверяващите се страни, воденето на доверителни списъци, надзора и взаимодействието с Европейската комисия и държавите членки. В проекта е предвидено министърът на електронното управление да изгражда и поддържа европейски портфейл за цифрова самоличност, както и да осигурява възможност чрез

него да се създава квалифициран електронен подпис, предоставян от квалифицирани доставчици на удостоверителни услуги.

От гледна точка на информационната инфраструктура в България съществуват важни предпоставки за реализиране на проекта - национални регистри, първични администратори на данни, системи за електронни административни услуги, среда за междурегистров обмен, eIDAS възел, доставчици на квалифицирани удостоверителни услуги и натрупан опит в изграждането на централни информационни системи. Въпреки това тези компоненти към момента не са обединени в единна портфейлна екосистема, която да позволява на потребителя да получава, съхранява и представя удостоверени цифрови атрибути, да управлява съгласията си, да използва квалифициран електронен подпис през портфейл и да достъпва трансгранични услуги чрез единен европейски съвместим модел.

Настоящият проект следва да преодолее това състояние чрез изграждане на национален Портфейл за цифрова самоличност и свързаната с него екосистема. Реализацията следва да осигури необходимата технологична, организационна и нормативна свързаност между държавата, гражданите, бизнеса, публичните институции, доставчиците на удостоверителни услуги, доставчиците на атрибути и доверяващите се страни. По този начин България ще може да изпълни европейските изисквания, да въведе съвременно средство за цифрова самоличност и да създаде устойчива основа за развитие на електронни услуги от ново поколение.

5 Изисквания към изпълнение на проекта

5.1 Общи изисквания към изпълнението

Проектът се изпълнява в рамките на бюджета на Министерство на иновациите и дигиталната трансформация по Системна интеграция.

5.2 Общи организационни принципи

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

- Хоризонталният принцип предполага ангажиране на специалисти от различни звена, така че да се покрие пълният набор от компетенции и ноу-хау по предмета на проекта и същевременно екипът да усвои новите разработки на достатъчно ранен етап, така че да е в състояние пълноценно да ги използва и развива и след приключване на проекта;
- Вертикалният принцип включва участие на експерти и представители на различните управленски нива, така че управленският екип да покрива както експертните области, необходими за правилното и качествено изпълнение на проекта, така и управленски и организационни умения и възможности за осъществяване на политиката във връзка с

изпълнението на проекта. Чрез участие на ръководители на звената – ползватели на резултата от проекта, ще се гарантира достатъчно ниво на ангажираност на институцията с проблемите на проекта.

5.3 Управление на проекта

Използваната методология за управление на проекта трябва да съответства на най-добрите световни практики и препоръки (например Project Management Body of Knowledge (PMBOK) Guide, PRINCE2, Agile/ SCRUM/ Kanban, RUP и др. еквивалентни).

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

Доброто управление на проекта трябва да осигури:

- координиране на усилията на експертите от страна на Изпълнителя и Бенефициера 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.

5.4 Управление на риска

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

При изготвянето на списъка с рискове, Изпълнителят следва да вземе предвид следните:

- Промяна в нормативната уредба, водеща до промяна на ключови компоненти на решението – предмет на разработка на настоящия проект;
- Недобра комуникация между екипите на Бенефициера и Изпълнителя по време на аналитичните етапи на проекта;
- Ненавременно изпълнение на всяко от задълженията от страна на Изпълнителя;
- Неправилно и неефективно разпределяне на ресурсите и отговорностите при изпълнението на договора;
- Забавяне при изпълнение на проектните дейности, опасност от неспазване на срока за изпълнение на настоящия проект;

- 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 Бенефициера за всички потенциални проблеми, които биха могли да възникнат в хода на изпълнение на дейностите;
- Риск за администриране на системата след изтичане на периода на гаранционна поддръжка.

6 Етапи на изпълнение на проекта

6.1 Анализ на данните и изискванията

Портфейлът за цифрова самоличност включва доставчик на Портфейл, който управлява целия жизнен цикъл на портфейлната единица: създаване, инициализация, активиране след потвърждаване на самоличността, промени на статуса, блокиране, временно спиране, възстановяване и прекратяване. Доставчикът управлява и свързаните устройства, потребителските сесии, криптографските ключове и атестациите, като поддържа и сценарии при изгубено, сменено или компрометирано устройство. Мобилното приложение за Android и iOS позволява на потребителя да се идентифицира, да получи данните си за идентификация (PID) и да управлява наличните атрибути и удостоверения. Потребителят може да представя данни пред доверяващи се страни онлайн (remote) и лице в лице (proximity), като изрично потвърждава или отказва всяка заявка, а приложението осигурява и резервно копие, възстановяване, експорт и преносимост към друг портфейл. Решението се свързва с доставчика на самоличност и с рамката на доверие, води одитен журнал за всички действия и започва с минимално използваем продукт (MVP), който доказва основните сценарии за използване.

Изпълнителят трябва да изготви Детайлна техническа спецификация за всяка от фазите описани в настоящата техническа спецификация. В нея трябва да са описани всички изисквания за реализирането на дейностите в обхвата на проекта.

Детайлната техническа спецификация подлежи на одобрение от МИДТ. В случай на забележки, корекции или допълнения от страна на МИДТ, Изпълнителят е длъжен да ги отрази в срок до 5 (пет) работни дни от получаването им.

Изготвянето на Детайлната техническа спецификация включва следните основни задачи:

- Дефиниране на детайлни функционални изисквания;
- Описание на бизнес процесите и функциите в системата;
- Подробно описание на потребителите (основни роли, идентифицирани за потребителите, съобразно бизнес-функциите, които реализират и взаимодействията със системата).

Изпълнението на задачите изисква дефиниране на модели на бизнес процеси, модели на справки и анализи, роли в системата и други.

- В процеса на бизнес анализ да бъдат изследвана съвместимостта на бизнес процесите на Бенефициера с вече одобрени оптимизирани референтни модели за предоставяне на услуги и нормативни изисквания на Базисен модел за Комплексно административно обслужване в държавната администрация. При наличие на разработени модели за предоставяне на услуги по „Епизоди от живота“ и „Събития от бизнеса“, които включват услуги, предоставяни от Бенефициера, да бъдат съобразени нуждите от модификации в референтните модели, за да се постигне подобряване на времето и намаляване на административната тежест при комплексно обслужване, спрямо предоставянето на отделните услуги поединично;
- В случай, че се касае за административни услуги, те трябва да бъдат разграничени на базата на разлики в бизнес процесите и да не бъдат генерализирани и/или обобщавани на базата на типа на действие (например, ако Системата издава няколко различни вида удостоверения, с които се удостоверяват различни обстоятелства, административните услуги трябва да бъдат регистрирани отделно);
- Удостоверителните административни услуги трябва да бъдат регистрирани и като вътрешни административни услуги и да бъде реализирана възможност за предоставянето на тези услуги като вътрешни електронно административни услуги за нуждите на комплексното административно обслужване чрез служебен онлайн интерфейс.

6.1.1 Специфични изисквания към етапите на бизнес анализа при разработка, надграждане или внедряване на информационна система

- 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;
- Необходимо е да бъде направен анализ на текущото състояние на данните, които ще се обработват, по отношение на тяхната изчерпателност, пълнота и качество, да се направи оценка на възможността за въвеждане на данни и обстоятелства в регистри, съгласно изискванията на нормативната уредба. Да се предложи модел на данните, съдържащ описание на основните таблици и схематично представяне на връзките между тях;
- В процеса на анализа трябва да се разгледа възможността обменът на данни да се основава на общи стандарти, т.е. условия за използване, формат на данните, машинна

четимост, метаданни, споделени речници/таксономии, честота, детайлност и задължителни атрибути. Задължителното прилагане би гарантирало изпълнението на изискванията за повторни потребители и доставчици на данни.

- Трябва да бъде направен анализ, оценка и описание на работните процеси, заложени в нормативната уредба, да бъде предложена организационна архитектура на базата, на която да бъдат разработени и оптимизирани основните функционалности на Системата.
- Трябва да бъдат предвидени периодични продуктови тествания по време на разработката и внедряването на Системата, с извадка (фокус-група) от бъдещите потребители на Системата, чрез които 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 чрез Центъра за електронна идентификация или на база на ЕГН от КЕП. При необходимост изпълнителят трябва да предложи на Бенефициера адекватни промени в нормативната уредба, които да хармонизират съответните секторни нормативни изисквания с общите разпоредби на Административнопроцесуалния кодекс, Закона за електронно управление, Закона за електронния документ и електронния подпис и приложимите подзаконови актове, ако действащата нормативна уредба изисква:
  - .1 изрично попълване на типов структуриран електронен формуляр, върху който потребителите трябва да се подпишат собственоръчно и/или който да приложат като изискуем документ при заявяването на електронна административна услуга;
  - .2 изрично деклариране или обявяване на обстоятелства или данни, които се администрират и/или удостоверяват от други държавни органи и могат да бъдат получени по служебен път, включително и автоматизирано през съответни интеграционни интерфейси;
  - .3 други нормативни изисквания, които водят до неоптимални или ненужно бюрократични процеси, които биха могли да бъдат оптимизирани при заявяване и предоставяне на електронни административни услуги;

6.1.2 Специфични изисквания при оптимизиране на процесите по заявяване на електронни услуги и електронни административни услуги (съгл. §1, т.2 от ЗЕУ) в зависимост от заявителя

т. 6.1.2. е изцяло неприложима, тъй като в обхвата на проекта няма електронни услуги

- Предвидените за разработка и внедряване електронни административни услуги трябва да бъдат регистрирани предварително в Регистъра на услугите към Административния регистър (съгласно чл. 61 от Закона за администрацията). Услугите, които ще бъдат надградени, и новоразработените услуги трябва да отговарят на изискванията за електронни услуги с минимално Ниво 4, където е приложимо (т.е. услугата изисква заплащане на такса), или Ниво 3, в случаите, в които за предоставяне на услугата не се изисква заплащане на такса; Дефинициите за нивата на електронизация на административните услуги са регламентирани в Наредбата за административния регистър към Закона за администрацията;
- При разработката на информационна система, чрез която се предоставят ЕАУ, да се предвиди изцяло автоматизираното им предоставяне, като се определи задължителното минимално ниво на електронизация на ЕАУ, съгласно т. 1.3 от техническата спецификация, както и нивото на осигуреност на средствата за електронна идентификация при заявяване на ЕАУ, определено съгласно Методика за определяне от лицата по чл. 1, ал. 1 и 2 от ЗЕУ на средствата за електронна идентификация, които се използват при заявяване на ЕАУ и тяхното ниво на осигуреност, и получаване на резултата от нея.
- При анализа трябва да се има предвид, ако АО предоставя ЕАУ от ниво 4, изискваща такса за плащане, тя е с намалена такса спрямо таксата за присъствено заявяване и предоставяне, ако при прилагането на методиката за определяне на разходоориентиран размер на таксите по чл. 7а на Закона за ограничаване на административното регулиране и административния контрол върху стопанската дейност се установи различен размер на разходите, съгласно чл.10а, ал 2 от ЗЕУ.
- Трябва да се разработят информативни текстове за всяка услуга, които включват като минимум:
    .1 условия за предоставяне на услугата;
    .2 срокове за предоставяне на услугата;
    .3 такси за заявяване и съответно предоставяне на услугата;
    .4 начини за получаване на услугата;
    .5 резултат от предоставяне на услугата;
    .6 отказ от предоставяне на услугата.
- Информативните текстове за всяка услуга трябва да бъдат достъпни за потребителите още като първа стъпка от заявяването на услуга;
- Тарифирането на услугите трябва да бъде реализирано така, че Системата да съхранява всички версии на тарифите за услуги (от дата до дата) и да прилага съответната тарифа, в зависимост от момента, в който е заявена дадена услуга;

- Трябва да бъде оптимизиран потребителският път от влизане на сайта до заявяване и получаване на услуга и пътят от регистрация на нов потребител до заявяване и получаване на услуга;
- При оптимизацията на потребителския път трябва да се отчита всяко действие от страна на потребителя (натискане на бутон, въвеждане на данни, прочитане на текст и пр.), което може да се спести.
- Съгласно действащата нормативна уредба допустимите заявители на електронни административни услуги могат да бъдат разделени в няколко групи, като процесите по заявяване на ЕАУ и необходимите процеси по установяване на допустимостта на заявлението зависят от множество фактори. Трябва да бъде обърнато специално внимание на спецификите в процесите в зависимост от качеството, в което действа заявителят, за да се постигне максимална оптимизация на процеса, като същевременно се защити сигурността на търговския и гражданския оборот.
- Предоставянето на ЕАУ от административните органи на гражданите и бизнеса да се извършва през Портала на електронното управление чрез хоризонталната система за е-форми, като се използва Единния модел за заявяване, заплащане и предоставяне на ЕАУ.
- В приложената диаграма са показани възможни разлики в бизнес процесите в зависимост от качеството, в което действа заявител на ЕАУ:

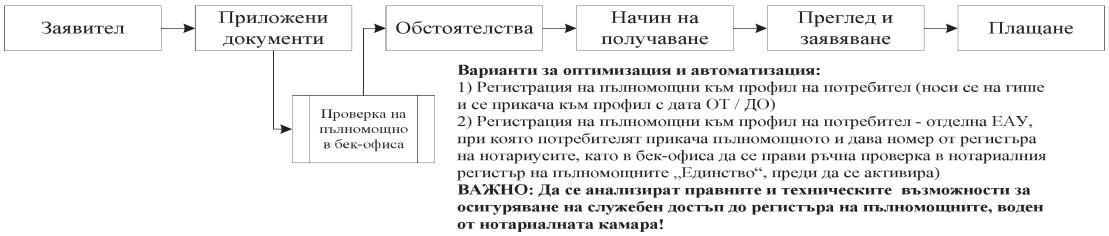
Процес по заявяване „в лично качество“:



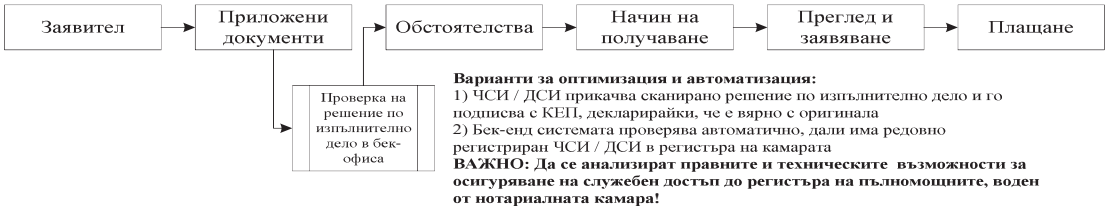
Процес по заявяване на услуга като законен представител на юридическо лице:



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



Процес по заявяване на услуга като длъжностно лице:



В приложената таблица са представени спецификите и разликите в бизнес процесите в

зависимост от качеството, в което действа заявител на ЕАУ, които трябва да бъдат отразени при реализацията на Системата:

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

6.1.3 Изисквания за оптимизиране на процесите по подаване на декларации, изискуеми в съответствие с нормативната уредба и вътрешните правила

Частично приложимо при Изготвянето на Детайлната функционална и техническа

спецификация следва да се прецизира приложението на текущата точка

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

6.1.4 Изисквания към регистрите и предоставянето на административните услуги

Частично приложимо при Изготвянето на Детайлната функционална и техническа спецификация следва да се прецизира приложението на текущата точка

- Всяка удостоверителна административна услуга в обхвата на системата трябва да бъде достъпна като вътрешноадминистративна електронна услуга чрез уеб-услуга, като комуникацията се подписва с електронен печат на институцията и с електронен времеви печат по смисъла на Регламент (ЕС) 910/2014;
- Всяка услуга, за която се допуска представителна власт, трябва да бъде интегрирана с Регистъра на овластяванията по смисъла на Закона за електронната идентификация;
- Системата не трябва да съхранява данни, на които Бенефициерът не е първичен администратор, в случай че данните могат да бъдат извличани в реално време от регистър на съответния първичен администратор при възможност чрез интеграционната шина за обмен на справочна и удостоверителна информация.
- Всички електронни административни услуги, предоставяни от административните органи на гражданите и бизнеса трябва да се заявяват през Портал за електронно управление.

- При предоставянето на ЕАУ е необходимо Изпълнителят да осъществи интеграция с хоризонталните системи на електронното управление.

6.2 Изготвяне на детайлна техническа спецификация

Изпълнителят трябва да изготви детайлна техническа спецификация, която подлежи на одобрение от Бенефициера. В нея трябва да са описани всички изисквания за реализирането на системата. Изготвянето на документа включва следните основни задачи:

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

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

Детайлната техническа спецификация подлежи на одобрение от Бенефициера. В случай на забележки, корекции или допълнения от страна на Бенефициера Изпълнителят е длъжен да ги отрази в документа в срок не по-късно от 10 (десет) работни дни от получаването им.

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 етапи „Тестване“ и „Внедряване“ на проекта.

6.4 Тестване

Изпълнителят трябва да проведе съвместно с Възложителя, приемателно тестване на софтуерното решение в създадена за целта тестова среда, за да демонстрира, че изискванията са изпълнени. Изпълнителят трябва да предложи и опише методология за тестване, която ще използва в план за тестване с описание на обхвата на тестването, вид и спецификация на

тестовете, управление на дефектите, регресионна политика, инструменти, логистично осигуряване и други параметри на процеса.

Приемателното тестване се провежда по предварително изготвени и предоставени тестови сценарии в рамките на Етап „Разработка на софтуерното решение

6.5 Внедряване

Изпълнителят трябва да внедри софтуерното решение в информационната и комуникационна среда на Министерство на иновациите и дигиталната трансформация след успешно приключило приемателно тестване от страна на Бенефициера. Това включва инсталиране, конфигуриране и настройка на програмните компоненти на системата в условията на експлоатационната среда на МИДТ. Условието за пристъпване към внедряване на разработката на софтуерното решение е успешно тествана версия на разработката на Етап „Тестване“.

6.6 Обучение

Изпълнителят трябва да организира и да проведе обучение за работа със Системата на ключови потребители след приключване на фаза 2 от проекта.

За провеждането на обученията Изпълнителят е длъжен да осигури за своя сметка:

- Необходимия софтуер;
- Зала/Зали за провеждане на обученията/ онлайн среда за провеждане на обученията;
- Учебни материали;
- Лектори.

Обучението следва да се проведе след успешно приемане на етап Тестване, при представен предварителен график за провеждането му от страна на Изпълнителя, предоставен списък на служителите, които ще бъдат обучени от страна на Възложителя и потвърждение от страна на Бенефициера за датата/датите на провеждане на обучението. Обучението може да бъде проведено онлайн като е възможно да не е приложимо и да не се провежда обучение за някои от дейностите, при които няма интерфейс. Допустимо е провеждането на отделни обучения за отделните дейности при тяхното успешно финализиране или провеждането на общо обучение за няколко от дейности в една обучителна сесия.

6.7 Гаранционна поддръжка

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за период от 24 (двадесет и четири) месеца след подписване на приемо-предавателен протокол за приемане в експлоатация на фаза 2.

При необходимост, по време на гаранционния период трябва да бъдат осъществявани дейности по осигуряване на експлоатационната годност на софтуера и ефективното му

използване от Бенефициера, в случай че настъпят явни отклонения от нормалните експлоатационни характеристики, заложени в системния проект. За дейностите, включени в обхвата на гаранционната поддръжка не се дължат допълнителни плащания.

Приоритетите на инцидентите и проблемите се определят от Бенефициера в зависимост от влиянието им върху работата на администрацията. Редът на отстраняването им се определя в зависимост от техния приоритет.

6.7.1 Обхват на дейностите по гаранционна поддръжка

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

Дейностите по гаранционна поддръжка трябва да включват следния минимален обхват:

- Извършване на диагностика с цел осигуряване на правилното и безпроблемно функциониране на Системата;
- Регистриране на инцидент в Система за управление на заявки;
- Отстраняване на дефектите, открити в софтуерните и/или хардуерните модули;
- Възстановяването на работоспособността на Системата при евентуален срив;
- Предоставяне на консултации за идентифициране на проблеми в конфигурацията на ИТ средата (операционна система, база данни, middleware, хардуер и мрежи);
- Регулярен мониторинг на неразрешените инциденти, дефиниране на проблеми и оценка на ефектите върху договорените параметри на качеството за наличност и достъпност на Системата;
- Пълно документиране на разрешените инциденти, включително предприетите стъпки за разрешаването им, точното им класифициране, обратна връзка със засегнатите потребители относно предложеното решение, общо изразходвано време за разрешаване;
- Актуализация на документацията 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.

За целите на дейността е необходимо да бъдат изготвени от Изпълнителя и одобрени и подписани от Бенефициера:

- Споразумение за нивото на предоставяните услуги към потребителите на информационни ресурси на АО (SLApm), в които са определени приоритетите за спешно обслужване;
- Параметрите на качество на обслужване на Системата, съобразени с минималните изисквания към параметрите на качеството от т. 6.7.5;
- Комуникационни, анализаторски и документационни средства, с които функционалните звена идентифицират, анализират, проследяват и документират възникването и отстраняването на неработоспособността на информационната система.

6.7.2 Управление на инциденти (incident management)

С цел осигуряване на работоспособността на Системата и повишаване на качеството на обслужване на потребителите ѝ в етапа на нейната експлоатация, Изпълнителят трябва да разработи процедури за бързо и ефективно регистриране на възникнали инциденти и безпроблемно им отстраняване.

Чрез процедурата за управление на инциденти се подпомага и координира работата на въвлечените в тази дейност функционални звена, които изпълняват следните задачи:

I-во ниво на поддръжка – за изпълнение на тези дейности се сформира се екип от експерти на Бенефициера. Задачите на екипа са да извършва дейности по наблюдение на Системата, регистриране, описание и обслужване на инциденти с цел улесняване идентифицирането на причините за възникване, първоначален анализ и класифициране на инциденти, ескалиране на заявки към II-ро ниво поддръжка, документиране на дейностите и изготвяне на доклади.

II-ро ниво на поддръжка – екипът се сформира от експерти на Бенефициера, които разглеждат, анализират и отстраняват всички възникнали инциденти при спазване на процедурата. Екипът изпълнява следните задачи: обслужване на ескалираните от I-во ниво на поддръжка инциденти, анализиране и класифициране на инциденти, разследване и диагностика на инцидента и установяване на средствата и каналите за разрешаване, разрешаване на инцидента и възстановяване на оперативността на всички засегнати компоненти, създаване на база данни за начинът на разрешаване на инцидентите, съдържаща информация както за временните решения (work around), така и за искания за промени;

III-то ниво на поддръжка – екипът се сформира от експерти на Изпълнителя, които разрешават инцидент, ескалиран от екипа на II-ро ниво на поддръжка, осигуряват безпроблемното функциониране на Системата, проактивно изследват инцидент с цел откриване на конкретната причина за възникването му, правят предложения за промени в компонентите, свързани с решаването на регистрирани проблеми, предоставят информация за процеса по управление на проблемите (Problem Management) относно взимане на мерки за предотвратяване повторяемостта на инцидентите.

Процесът на управление на инциденти се осъществява чрез използване на Система за управление на инциденти (Service/ Help Desk), собственост на Бенефициера или Изпълнителя, която гарантира разпознаването им, тяхната проследимост и причините за възникването им, позволява документиране, комуникиране и одобрение по идентификация, разследване и отстраняване на причини за възникване на инциденти и проблеми.

6.7.3 Управление на проблеми (УП) (problem management)

В етапа на гаранционна поддръжка се включва процеса по управление на проблеми, целта на който е да минимизира и/или елиминира влиянието на инцидентите, причинени от

грешки възникнали в компонентите на системите, платформите, функционалните звена и/или процесите, имащи пряко или косвено отношение към влошаване или невъзможност за предоставяне на услугите към крайните потребители. При Управление на промени, екипът от експерти на Изпълнителя трябва:

- да се фокусира върху идентифицирането на причините за възникване на инциденти (root-cause analysis), повторяемостта на идентичните събития и инциденти, които водят до появата и съществуването на грешки.
- да извършва всички необходими дейности за диагностициране и анализиране на причините за възникване на инцидентите и определя начините и методите за разрешаване на проблемите, да дефинира, прилага и да носи пряка отговорност за прилагането на подходящи контролни процедури (Change Management/ Release Management) с цел безпроблемно и качествено имплементиране на одобреното постоянно или временно (work around) решение.
- да подържа база данни инструмент за работа с нея, в която се вписват всички проблеми и съответните им решения (Knowledge Management and Known Error Data Base).
- да обхване двата основни процеса – реактивно и проактивно управление на проблемите, който е част от процеса на непрекъснато подобряване на услугите (Continuous Service Improvement).

6.7.4 Управление на качеството при отстраняване на инциденти и проблеми. Параметри на качеството.

Чрез гаранционната поддръжка Изпълнителят трябва да осигури гарантиране на работоспособността, на мрежовата и информационната сигурност, да поддържа непрекъснатост на работата на Системата, с което се обезпечава неприкосновеността и сигурността на обработваната информация.

Параметрите на качеството на услугите, които Изпълнителят предлага в етапа на гаранционна поддръжка се изпълняват съгласно споразумение за нивото на предоставяните услуги към потребителите на АО (SLApm).

6.7.5 Минимални изисквания към параметрите на качеството

Системата трябва да работи в режим 7/24/365. Конкретните параметри, свързани с достигането на необходимото ниво на работоспособност през гаранционния период, са дадени в Таблици от 1 до 5.

Таблица 1

Наличност на Системата в проценти и часове на годишна база

Система	В рамките на работните часове	Максимално сумарно отпадане на Системата в работно време за една година	Извън рамките на работните часове	Максимално сумарно отпадане на Системата в извън работно време за една година
	99,50%	<15 часа	98,00%	<116 часа

Таблица 2

Планиране на прекъсвания (планирана недостъпност) на Системата		
Продължителност на планирана недостъпност		
< 1 час	от 1 до 6 часа	от 6 до 11 часа
По всяко време	Извън работните часове	В почивни дни или по време на официални празници
Забележка: a) Ако планираното прекъсване може да надхвърли 11 часа трябва да се раздели на две (или повече прекъсвания), които не превишават 11 часа. b) Работните часове са съгласно Таблица „Дефиниции". c) Цитираните в таблицата данни и системи са актуални към датата на изготвяне на настоящия документ. При настъпили промени, системите ще бъдат актуализирани.		
Важно: Обявяването на планирано прекъсване става посредством уведомяване на Бенефициера минимум 7 работни дни предварително. Уведомяването трябва да съдържа: • засегната/и система/и; • начална дата и час; • крайна дата и час; • причина.		

Таблица 3

Приоритети	
Приоритет	**Въздействие върху работните процеси**
1 Критичен	Критично влияние върху работните процеси. Изисква незабавно действие, като работата продължава до неговото отстраняване. 1) Пълно прекъсване на една или повече ЕАУ, предоставяни от администрацията, прекъсване работата на регистри, приложни програмни интерфейси; 2) Недостъпност до предоставяни през функционалността на Системата ЕАУ, които пряко и съществено засягат ключови или голям брой клиенти; 3) Висок риск от финансови загуби и/или засягане на имиджа на администрацията или негови контрагенти; 4) Създава висок риск за компрометиране на информация в Системата;

	5) Нарушена комуникация в инфраструктурата на държавната администрация и с други държави членки на ЕС или на аналогични системи; 6) Риск за съществено прекъсване или излизане от строя на Системата; 7) Критична функционалност не функционира нормално или има критично и негативно отражение върху операциите на потребителите или системната среда във ведомство на Бенефициера или в имиджа на същото 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. 1) Влошаване на качеството на предлагана услуга или достъп до такава, без пълно прекъсване; 2) Създаване на сериозен риск от възникване на инцидент с критичен приоритет; 3) Критична функционалност функционира непълноценно или има силно 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. 1) Ограничено въздействие върху работата на Системата, което засяга или създава неудобство за изпълнение на отделни функции, без да има цялостно отражение върху функциите ѝ. Забавяне на отстраняването му може да доведе до възникване на инцидент от по-високо ниво. 2) Нормалната производителност на Системата 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 1) В момента липсва пряко влияние върху функционирането на Системата, но не решаването му в определен срок крие потенциален риск от възникване на инцидент с по-висок приоритет. 2) Обикновено се свързва с подобряване на функционирането на услуга, предоставяна от Системата или развитието ѝ. 3) Отстраняването се планира съвместно с Бенефициера и е обект на средносрочно планиране. Бенефициерът може да изисква информация или помощ по възможните решения.

Таблица 4

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	1 седмица	В следваща версия	7 работни дни
4	1 работен ден	1 седмица	В следваща версия	14 работни дни

Забележки:

1) Приоритетите се определят от Бенефициера, съгласно таблица 3 „Приоритети“;
2) 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 Системата, Бенефициерът може да снижи приоритета на инцидента без да го закрива.
3) Всички, посочени в таблицата, времена започват да текат от момента на регистриране в Системата за управление на инциденти на Бенефициера.
4) При обективна невъзможност да бъдат спазени сроковете в таблицата, Бенефициерът може да ги промени за конкретен инцидент;

Таблица 5

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 версия	72 часа
3	1 работен ден	1 седмица	В следваща версия	7 работни дни
4	1 работен ден	1 седмица	В следваща версия	14 работни дни

Забележки:

1) 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 Системата, Бенефициерът може да снижи приоритета на инцидента без да го закрива.
2) Всички, посочени в таблицата, времена започват да текат от момента на регистриране в Системата за управление на инциденти на Бенефициера.

7 Общи изисквания за информационни системи в държавната администрация

Всички информационни системи и софтуерните компоненти в администрацията, в т.ч. регистри, интернет страници, вътрешни информационни системи, потребителски интерфейси към съществуващи системи, системи за предоставяне на електронни административни услуги и за електронен документооборот, трябва да отговарят на изискванията на Закона за електронното управление, Закона за киберсигурност, Закона за достъп до обществена информация и Закона за достъп до пространствени данни и подзаконовата нормативна база към тях. Неизпълнението на тези изисквания от страна на изпълнителите по договори за разработка и/или надграждане

на информационни системи/регистри/ЕАУ е основание за неприемане на разработеното софтуерно решение от страна на Бенефициера. Всички описани изисквания ще бъдат детайлно анализирани по време на изпълнение на етап Анализ на изискванията във фаза 1 и фаза 2 от изпълнение на проекта.

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 хоризонталните и централните информационни системи на електронното управление, както следва:

Интеграция с хоризонталните системи на ЕУ

Интеграцията на Системата с хоризонталните системи за електронно управление се осъществява чрез разработване и внедряване на служебен интерфейс за обмен на данни, както следва:

Код	Описание	Приложимост	Забележка*
F1	Информационна система за електронна автентикация версия 2.0	Задължително, до влизане в сила на Националната схема за електронна идентификация по ЗЕИ.	Приложимо. Системата следва да поддържа интеграция със системите за електронна автентикация/идентификация, доколкото това е необходимо за административните портали, онбординг процесите, достъпа на служители и преходните механизми до пълното въвеждане на националната схема и EUDI Wallet.
F2	Информационна система за сигурно електронно връчване	Задължително, ако е приложимо.	Приложимо при необходимост от официално електронно връчване в процесите по регистрация, присъединяване, уведомяване или контрол на доставчици на портфейли, доставчици на атрибути, посредници при верификация и доверяващи се страни. Не е приложимо към стандартните потребителски действия в мобилния портфейл.
F3	Информационна система за	Задължително за информационни	Неприложимо към основния обхват, доколкото проектът

	електронно плащане	системи, чрез които се извършват плащания на такси за ЕАУ с ниво на електронизация 4 и други задължения.	не предвижда заплащане на такси чрез Портфейла или предоставяне на ЕАУ с електронно плащане
F4	Информационна система за електронни форми	Задължително, ако е приложимо.	Приложимо при електронни заявления/форми за регистрация и онбординг на участници в екосистемата, включително доставчици, посредници при верификация и доверяващи се страни. Не е приложимо към самото мобилно приложение
F5	Информационна система за е-валидация	Задължително, ако е приложимо.	Приложимо при валидация на електронни документи, електронни удостоверения за атрибути, подписи, сертификати, доверителни списъци и други данни с правно или техническо значение

Интеграция с други информационни системи

За реализиране на основните бизнес процеси по изграждане, въвеждане/внедряване и експлоатация на Портфейла за цифрова самоличност Системата следва да поддържа интеграция с приложимите хоризонтални, централни, секторни, национални и европейски информационни системи, регистри, инфраструктурни компоненти и доставчици на услуги.

Интеграциите следва да осигурят надежден, защитен, проследим и оперативно съвместим обмен на данни между компонентите на Портфейла, националната рамка на доверие, доставчика на самоличност, доставчика на квалифицирани атрибути, посредника при верификация, регистъра на участниците, доверителните списъци, доставчиците на квалифицирани удостоверителни услуги, доставчиците на атрибути, доверяващите се страни и приложимите национални и европейски инфраструктури.

Интеграционната архитектура следва да бъде реализирана при спазване на изискванията на Закона за електронното управление, Закона за електронната идентификация, Закона за електронния документ и електронните удостоверителни услуги, Закона за защита на личните данни, Закона за киберсигурност, Регламент (ЕС) № 910/2014, изменен с Регламент (ЕС) 2024/1183, както и приложимите актове за изпълнение, стандарти и технически спецификации към Европейската рамка за цифрова идентичност.

Системата следва да поддържа интеграции най-малко в следните направления:

7.1.1.1 Интеграция с хоризонтални системи на електронното управление

Системата следва да се интегрира с приложимите хоризонтални системи на електронното управление, когато това е необходимо за изпълнение на административни, идентификационни, удостоверителни, интеграционни или контролни процеси. Това включва интеграция със системи за електронна автентикация/идентификация, системи за сигурно електронно връчване, средата за междурегистров обмен, интеграционния слой на електронното управление, Единния портал за достъп до електронни административни услуги, системи за електронни формуляри и други споделени компоненти, когато са приложими към конкретните процеси по проекта.

Интеграцията с хоризонталните системи следва да се реализира чрез служебни интерфейси за обмен на данни, при използване на утвърдени протоколи, стандарти, формати и механизми за автентикация, авторизация, защита на обмена, одитен журнал и проследимост.

7.1.1.2 Интеграция с национални регистри и автентични източници на данни

Системата следва да осигури интеграция с национални регистри и автентични източници на данни, необходими за първоначална идентификация на лицата, издаване на данни за идентификация, издаване и проверка на електронни удостоверения за атрибути, удостоверяване на представителна власт и проверка на други обстоятелства, необходими за функционирането на Портфейла.

В обхвата на тези интеграции следва да бъдат включени, когато е приложимо, регистрите за самоличност, ЕСГРАОН, регистри на МВР, регистри на Агенцията по вписванията, регистър БУЛСТАТ, регистри на НАП, НОИ, МОН, МТСП, секторни регистри и други първични регистри, поддържани от компетентни публични органи.

Обменът на данни с регистрите следва да се реализира при спазване на принципа за служебно събиране на данни, използване на автентични източници, минимизиране на обработваните лични данни, защита на данните по проект и по подразбиране, проследимост на заявките и отчетност на достъпа.

7.1.1.3 Интеграция с RegiX и средата за междурегистров обмен

Системата следва да използва RegiX и/или друг утвърден интеграционен механизъм на електронното управление за достъп до данни от първични регистри, когато такива данни са необходими за издаване, актуализация, отмяна или проверка на електронни удостоверения за атрибути.

Интеграцията с RegiX следва да осигурява стандартизиран, защитен и проследим достъп до данни, необходими за функционирането на доставчика на квалифицирани атрибути от името на публични институции, доставчика на самоличност и други компоненти на Системата, които имат основание да използват данни от автентични източници.

7.1.1.4 Интеграция с eIDAS възел и европейската инфраструктура за цифрова идентичност

Системата следва да поддържа интеграция с националния eIDAS възел и приложимите европейски компоненти на инфраструктурата за цифрова идентичност, с цел осигуряване на трансгранична оперативна съвместимост на Портфейла за цифрова самоличност.

Интеграцията следва да позволява използване на българския Портфейл за цифрова самоличност при достъп до услуги в други държави членки, както и приемане и проверка

на портфейли, данни за идентификация и електронни удостоверения за атрибути, издадени в други държави членки, когато това е приложимо и разрешено от нормативната и техническата рамка.

Системата следва да поддържа приложимите протоколи, интерфейси, формати, доверителни списъци, сертификати, метаданни, схеми за уведомяване и технически профили, определени в европейската рамка за EUDI Wallet.

7.1.1.5 Интеграция с доставчици на квалифицирани удостоверителни услуги

Системата следва да поддържа интеграция с квалифицирани доставчици на удостоверителни услуги, вписани в доверителния списък, с цел осигуряване на възможност за създаване на квалифициран електронен подпис чрез Портфейла.

Интеграцията следва да бъде реализирана при равнопоставени, прозрачни и недискриминационни условия за доставчиците, като се осигурят технически интерфейси за заявяване, издаване, използване, проверка, валидиране и управление на квалифицирани удостоверения, когато това е необходимо за предоставяне на услугата през Портфейла.

Когато е приложимо, интеграцията следва да поддържа и механизми за отдалечено съхранение на ключове и извършване на криптографски операции в защитена среда, с цел разширяване на съвместимостта на Портфейла с по-широк кръг мобилни устройства и сценарии за използване.

7.1.1.6 Интеграция с доставчици на квалифицирани и неквалифицирани атрибути

Системата следва да осигури възможност за присъединяване и интеграция на доставчици на квалифицирани електронни удостоверения за атрибути, доставчици на атрибути от името на публични институции и други допустими доставчици на атрибути.

Интеграциите следва да поддържат процеси по издаване, получаване, съхраняване, представяне, проверка, обновяване и отмяна на електронни удостоверения за атрибути, при спазване на приложимите изисквания за доверие, сигурност, защита на личните данни, проследимост, минимизиране на данните и контрол от страна на потребителя.

7.1.1.7 Интеграция с доверяващи се страни

Системата следва да предоставя интерфейси за интеграция с доверяващи се страни, които приемат Портфейла за цифрова самоличност като средство за идентификация, удостоверяване или представяне на атрибути. Доверяващи се страни могат да бъдат публични администрации, доставчици на електронни административни услуги, банки, застрахователи, телекомуникационни оператори, образователни институции, работодатели, доставчици на регулирани услуги и други организации, които имат правно основание и техническа готовност да използват Портфейла.

Интеграцията с доверяващи се страни следва да се реализира чрез посредника при верификация и/или други приложими интерфейси, като се осигури заявяване на конкретни атрибути, проверка на валидност, проверка на издател, контрол върху допустимите цели за обработване, регистриране на заявките, одитна следа и потребителско потвърждение при предоставяне на данни.

7.1.1.8 Интеграция между вътрешните компоненти на Системата

Системата следва да осигури защитена и надеждна интеграция между всички вътрешни компоненти, включително доставчик на Портфейл, мобилно приложение, доставчик на самоличност, доставчик на квалифицирани атрибути, посредник при верификация,

регистър на участниците, регистратор на доверителни списъци, административни портали, системни журнали, мониторинг, конфигурационни услуги и компоненти за управление на сигурността.

Вътрешните интеграции следва да бъдат реализирани по начин, който гарантира модулност, мащабируемост, устойчивост, контрол на достъпа, защита на комуникацията, управление на версиите, наблюдаемост, възможност за независима поддръжка на компонентите и лесно разширяване на екосистемата.

7.1.1.9 Интеграция със системи за мониторинг, одитен журнал и управление на инциденти

Системата следва да поддържа интеграция със системи за мониторинг, централизиран одитен журнал, управление на инциденти, управление на уязвимости, наблюдение на производителност и контрол на достъпа, когато такива системи са налични или бъдат определени от Бенефициера.

Тези интеграции следва да осигурят своевременно откриване на инциденти, проследимост на действията, доказуемост на извършени операции, анализ на събития по сигурността, поддръжка на одитни процеси и изпълнение на изискванията за киберсигурност и защита на личните данни.

7.1.1.10 Интеграция със среди за разработка, тестване и външна интеграция

За нуждите на разработката, приемането и присъединяването на външни участници Системата следва да поддържа отделни среди за разработка, тестване, интеграционно тестване, приемане, обучение, продукционна експлоатация и sandbox среда за външни интегратори.

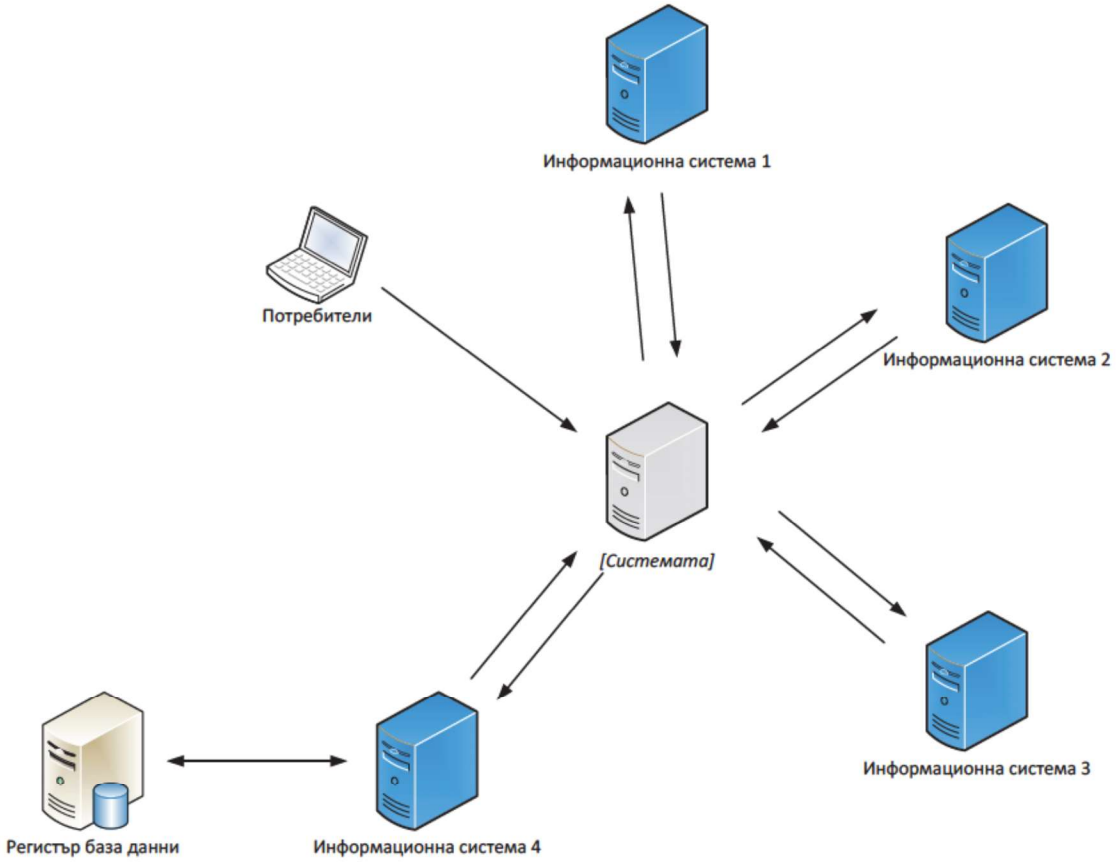
Sandbox средата следва да позволява на доставчици на атрибути, доставчици на квалифицирани удостоверителни услуги, доверяващи се страни, публични институции и други участници да тестват интеграцията си със Системата, без да застрашават продукционната среда, сигурността на реални данни или нормалната работа на компонентите.

При реализацията на интеграциите следва да се прилагат следните принципи:

- използване на стандартизирани и отворени протоколи и формати, когато това е приложимо;
- използване на защитена комуникация и криптографски механизми за защита на обменяните данни;
- автентикация и авторизация на всички системи и участници, които обменят данни със Системата;
- минимизиране на обменяните лични данни и предоставяне само на данни, необходими за конкретния процес;
- пълна проследимост в одитен журнал и проследимост на заявките, отговорите, грешките и действията на участниците;
- водене на версии на интерфейсите и управление на обратната съвместимост;
- възможност за наблюдение, диагностика и анализ на интеграционните процеси;
- механизми за повторение, обработка на грешки, отказоустойчивост и възстановяване при временна недостъпност на външни системи;

- съответствие с изискванията за защита на личните данни, информационна сигурност, киберсигурност и оперативна съвместимост.

Код	Описание	Приложимост	Забележка*
F6	Интегрираната информационна система на държавната администрация (ИИСДА), в частност Регистъра на услугите, в който се вписват допустимите заявители и получатели на административни услуги - например: проверка на достъпа до съответните обстоятелства, посочване на идентификатор на конкретна административна услуга, за която е нужно извличането на съответните обстоятелства от регистрите;	Задължително, ако чрез Системата се предлагат ЕАУ.	Не е приложимо, тъй като в обхвата на проекта не се предвиждат функционалности, свързани с предоставянето на ЕАУ
F7	При реализиране на системи за документооборот на административните органи, касаеща обмена на електронни документи, интеграцията да се извършва съгласно технически протокол, който позволява: 1) обмен на документи между различни системи за документооборот в различни администрации; 2) проследяване на движението на документа и етапа на процедурата по разглеждането или съставянето му.	Задължително, ако е приложимо.	Неприложимо, тъй като в разработката не се предвижда реализиране на система за документнооборот
F8	Интеграциите с външни информационни системи и регистри трябва да се реализира чрез стандартен интеграционен слой, съгласно действащите изисквания за оперативна съвместимост	Задължително	Приложимо. Системата ще има интеграции с национални регистри, RegiX, eIDAS инфраструктура, доставчици на КЕП, доставчици на атрибути и доверяващи се страни, поради което интеграциите следва да се реализират чрез стандартни интерфейси и съобразно изискванията за оперативна съвместимост



7.1.2 Използване на интеграционния слой на електронното управление

Интеграция на Системата чрез използване на интеграционния слой на ЕУ, включващ:

Код	Описание	Приложимост	Забележка*
F9	Интеграционна шина за обмен на справочна и удостоверителна информация (RegiX): 1) В случай, че Системата се явява първичен регистър на данни, с цел присъединяване към интеграционната шина и в последствие използването на първичните данни от други АО, е необходимо да се предвиди разработката на адаптер, който да се реализира съгласно стандарта, публикуван на Портала за електронно управление, в раздел „Разработчици“;	Задължително	Приложимо. Системата ще използва данни от първични администратори на данни и автентични източници чрез RegiX или друг одобрен интеграционен механизъм, особено при издаване и проверка на атрибути и данни за идентификация

	2) При условие, че Системата използва данни от ПАД, трябва да бъде предвидена интеграция с първични регистри чрез стандартен междинен слой или чрез националната схема за електронна идентификация – конкретната реализация трябва да бъде одобрена от Бенефициера след приключване на етапа на бизнес-анализ.		
F10	Интеграционна шина за обмен на електронни документи	Задължително, когато се обменят електронни документи чрез документооборотни системи.	Приложимо е при обмен на електронни документи в административните процеси по регистрация, сертифициране, контрол и уведомяване. Не е приложимо към стандартното представяне на атрибути през Портфейла, когато не се обменят документи чрез документооборотна шина
F11	Интеграционна шина за достъп и управление на ИТ услуги и данни на МИДТ	Препоръчително	Приложимо при наличие на утвърден и използваем компонент на МИДТ за достъп и управление на ИТ услуги и данни, който следва да бъде използван в архитектурата
F12	Информационна система за централизирано поддържане на регистри	Задължително, когато се изграждат регистри, които са били водени на хартия и не са включени в графика за привеждане на регистрите на АО в съответствие със ЗЕУ чрез ИСЦИПР (ПМС 232/20.11.2023	Приложимо. В обхвата се предвиждат регистър на участниците, доверителни списъци и административни регистри/списъци за доставчици, посредници и доверяващи се страни

		г)	
F13	Да се реализира служебен интерфейс за автоматизиран онлайн обмен на данни и предоставяне на вътрешни електронни административни услуги.	Задължително	Не е приложимо, тъй като в обхвата на проекта не се предвиждат функционалности, свързани с ВЕАУ
F14	Трябва да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано машинно поискване и предаване на история на изпълнените транзакции по машинен обмен на данни, предоставените електронни услуги и начислени такси, към информационни системи на други публични институции и доставчици на обществени услуги, с оглед предоставяне на КАО, съгласно действащите изисквания за оперативна съвместимост.	Задължително, ако е приложимо.	Не е приложимо

7.1.3 Технически изисквания към интерфейсите

Код	Описание	Приложимост	Забележка*
F15	**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.	Задължително	Приложимо. Всички служебни онлайн интерфейси, API интерфейси, интеграции с регистри, доставчици на атрибути, доставчици на КЕП и доверяващи се страни следва да бъдат реализирани като надеждни, мащабируеми и производителни уеб услуги
F16	Необходимо е да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на транзакционна история към системата за електронна идентификация, съгласно действащите изисквания за оперативна съвместимост.	Задължително	Приложимо - следва да се осигури проследимост и обмен на транзакционна история с приложимите компоненти за електронна идентификация, доколкото това се

			изисква от нормативната и техническата рамка за EUDI Wallet
F17	Трябва да бъде разработен и внедрен служебен онлайн интерфейс за електронни разплащания чрез интеграция с Централен виртуален ПОС терминал, позволяващ заплащане на такси за ЕАУ и други по електронен път без дължими преводни такси и комисиони.	Задължително за информационни системи, чрез които се извършват плащания на такси за ЕАУ с ниво на електронизация 4 и други задължения	Неприложимо, доколкото в обхвата не се предвиждат електронни плащания, такси за ЕАУ или интеграция с централен виртуален ПОС терминал
F18	Всички публични и служебни онлайн интерфейси трябва да бъдат реализирани с поддръжка на режими “push” и „pull”, в асинхронен и синхронен вариант – практическото прилагане на всяка от комбинациите трябва да бъде определено на етап бизнес-анализ и да бъдат съобразени реалните казуси (use cases), които всеки интерфейс обслужва.	Ако е приложимо	Приложимо. За различните интерфейси следва да се предвидят подходящи режими на обмен – push/pull, синхронен/асинхронен, според конкретния use case: издаване на атрибути, проверка на атрибути, уведомяване, синхронизация на доверителни списъци, интеграции с доставчици и доверяващи се страни
F19	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.	Задължително	Приложимо за публичните и служебните API интерфейси, доколкото изискванията се отнасят до стандартизиране, документиране, сигурност, версия, формат, достъпност и поддръжка на интерфейсите
F20	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	Задължително	Приложимо за публичните и служебните API интерфейси, доколкото изискванията се отнасят до стандартизиране,

	бизнеса, с цел по-лесно и устойчиво интегриране на съществуващите и бъдещи информационни системи.		документиране, сигурност, версия, формат, достъпност и поддръжка на интерфейсите

7.1.4 Електронна идентификация на потребителите

Код	Описание	Приложимост	Забележка*
F21	Електронната идентификация на всички потребители трябва да бъде реализирана в съответствие с изискванията на Регламент ЕС 910/2014 и ЗЕИ.	Задължително	Приложимо за публичните и служебните API интерфейси, доколкото изискванията се отнасят до стандартизиране, документиране, сигурност, версия, формат, достъпност и поддръжка на интерфейсите
F22	До влизане в сила на националната схема за електронна идентификация по ЗЕИ в Системата трябва да бъде осъществена интеграция с хоризонталната система на електронното управление – е-автентикация v2.0, която поддържа интеграция с външни доставчици на идентичност, съгласно §5 от Преходни и Заключителни разпоредби на НОИИСРЕАУ. Реализацията на интеграцията трябва да бъде осъществена по стандартни протоколи SAML 2.0 и/или OpenID Connect.	Задължително	Приложимо
F23	Системата трябва да поддържа и стандартен подход за регистрация на потребители с потребителско име и парола – за потребители, които нямат издадени удостоверения за електронна идентичност, и за потребители, които желаят да продължат да използват електронни административни услуги с КЕП.	Препоръчително	Приложимо
Процес по регистрация на потребители			
F24	Да се предостави възможност за визуализиране на информация относно стъпките по регистрация и информация	Задължително	Приложимо за публичните и служебните API

	във връзка с процеса за потвърждаване на регистрацията и активиране на потребителския профил. Съвети към потребителите за проверка на настройките на имейл клиентите, свързани с блокиране на спам, и съвети за включване на домейна на Бенефициера в „бял списък“.		интерфейси, доколкото изискванията се отнасят до стандартизиране, документиране, сигурност, версия, формат, достъпност и поддръжка на интерфейсите
F25	Да има възможност за избор на потребителско име с контекстна валидация на полетата (in-line validation), включително и за избраното потребителско име и визуализиране на сложността на паролата като „слаба“, „нормална“ и „силна“.	Препоръчително	Приложимо за публичните и служебните API интерфейси, доколкото изискванията се отнасят до стандартизиране, документиране, сигурност, версия, формат, достъпност и поддръжка на интерфейсите
F26	Да се реализира функционалност за потвърждение и активиране на регистрацията чрез изпращане на съобщение до регистрирания имейл адрес на потребителя, с еднократно генериран токън с ограничена времева валидност за потвърждение на регистрацията. Възможност за последващо препращане на имейла за потвърждение, в случай че е бил блокиран от системата на потребителя.	Задължително	Приложимо за публичните и служебните API интерфейси, доколкото изискванията се отнасят до стандартизиране, документиране, сигурност, версия, формат, достъпност и поддръжка на интерфейсите
F27	При реализиране на вход в Системата с удостоверение за електронна идентичност, по Националната схема за електронна идентификация по ЗЕИ, Системата трябва да използва потребителския профил, създаден в нея, чрез интерфейси и по протоколи съгласно подзаконовата нормативна уредба към Закона за електронната идентификация. В случай че даден потребител има регистриран потребителски профил в Системата, който е създаден преди въвеждането на националната схема за електронна идентификация, Системата	Задължително	Приложимо с адаптация към проекта. При реализацията следва да се осигури обвързване на потребителски профил/портфейлна единица с електронната идентичност на лицето, като се спазват изискванията на националната схема, eIDAS 2.0 и проекта на

	трябва да предлага на потребителя възможност за „сливане“ на профилите и асоцииране на локалния профил с този от националната система за електронна идентификация. Допустимо е Системата да поддържа и допълнителни данни и метаданни за потребителите, но само такива, които не са включени като реквизити в централизирания профил на потребителя в системата за електронна идентификация.		Закон за ЕПЦС
F28	Системата трябва да се съобразява с предпочитанията на потребителите, дефинирани в потребителските им профили в системата за електронна идентификация, по отношение на предпочитаните комуникационни канали и канали за получаване на нотификации.	Задължително	Неприложимо, тъй като портфейлът следва да се осигури собствен модел за уведомяване и управление на съгласия, съобразен с eIDAS и GDPR

7.1.5 Отворени данни

Код	Описание	Приложимост	Забележка*
F29	Трябва да бъде разработен и внедрен автоматизиран интерфейс за осигуряване на свободен публичен автоматизиран достъп до документите, информацията и данните в Системата (наричани заедно „данните”). Интерфейсът трябва да осигурява достъп до данните в машинночетим, отворен формат, съгласно всички изисквания на Директива 2013/37/ЕС за повторна употреба на информацията в обществения сектор и на Закона за достъп до обществена информация.	Задължително за системи, които предоставят данни по ЗДОИ	Приложимо
F30	Трябва да бъде разработен и внедрен онлайн интерфейс за предоставяне на пространствени данни, в машинночетим, отворен формат и интеграция с Националния портал за достъп до пространствени данни, съгласно всички изисквания на Директива 2007/2/ЕО и Закона за достъп до пространствени данни. Трябва да се поддържат всички набори от данни, които са изискуеми по Директива 2007/2/ЕО и за които	Задължително за ИС, които обработват пространствени данни	Не е приложимо, тъй като Системата не обработва пространствени данни

	Бенефициерът се явява първичен администратор на данните.		
F31	Да бъде предвидена разработката и внедряването на отворени онлайн интерфейси и практически механизми, които да улеснят търсенето и достъпа до данни, които са на разположение за повторна употреба, като например списъци с основни документи и съответните метаданни, достъпни онлайн и в машинночетим формат, както и интеграция с Портала за отворени данни https://data.egov.bg/, който съдържа връзки и метаданни за списъците с материали, съгласно изискванията на Закона за достъп до обществена информация (ЗДОИ).	Задължително за системи, които предоставят данни по ЗДОИ	Не е приложимо за данни, които не могат да бъдат визуализирани или публикувани поради защита на лични данни, сигурност или доверителен характер
F32	Трябва да се разработи и да се поддържа актуално публично описание на всички служебни и отворени интерфейси, отворените формати за данни, заедно с историята на промените в тях, в структуриран машинночетим формат.	Задължително	Не е приложимо за данни, които не могат да бъдат визуализирани или публикувани поради защита на лични данни, сигурност или доверителен характер
F33	Трябва да се разработят процеси по предоставяне на данни в отворен, машинночетим формат заедно със съответните метаданни. Форматите и метаданните следва да съответстват на официалните отворени стандарти.	Задължително	Приложимо

7.1.6 Формиране на изгледи

Код	Описание	Приложимост	Забележка*
F34	Потребителите на Системата трябва да получават разрези на информацията чрез филтриране, пренареждане и агрегиране на данните. Резултатът се представя чрез: • Визуализиране на таблици; • Графична визуализация на екран; • Експорт на данни в един или в няколко от изброените формати – ODF, Excel, PDF, HTML, TXT, XML, CSV и запис върху електронен носител.	Задължително	Приложимо.

7.1.7 Администриране на Системата

Код	Описание	Приложимост	Забележка*
F35	Системата трябва да осигурява администриране на потребителите и правата за достъп чрез административен панел, с който администраторите на системата да създават профили, управляват, назначават, отнемат роли и права на потребителите.	Задължително	Приложимо. Системата следва да поддържа административни функционалности за управление на потребители, роли, права, участници, конфигурации, интеграции, доверителни списъци, статуси, одит и технически параметри

7.2 Нефункционални изисквания към информационната система

7.2.1 Авторски права и изходен код

Код	Описание	Приложимост	Забележка*
NF1	Всички компютърни програми, които се разработват за реализиране на Системата, трябва да отговарят на критериите и изискванията за софтуер с отворен код.	Задължително	Приложимо
NF2	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, чисто разработване е включено в предмета на проекта, възникват за Бенефициера в пълен обем без ограничения в използването, изменението и разпространението им и представляват произведения, създадени по заявка на Бенефициера съгласно чл. 42, ал. 1 от Закона за авторското право и сродните му права.	Задължително	Приложимо
NF3	Приложимите и допустими лицензи за софтуер с отворен код са: 1) GPL (General Public License) 3.0; 2) LGPL (Lesser General Public License); 3) AGPL (Affero General Public License); 4) Apache License 2.0;	Задължително	Приложимо

	5) New BSD license; 6) MIT License; 7) Mozilla Public License 2.0 8) EUPL (European Union Public License).		
NF4	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.	Задължително	Приложимо
NF5	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.	Задължително	Приложимо
NF6	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.	Задължително	Приложимо

7.2.2 Системна и приложна архитектура

Код	Описание	Приложимост	Забележка*
NF7	Системата трябва да бъде реализирана като разпределена модулна информационна система. Системата трябва да бъде реализирана със стандартни технологии и да поддържа общоприети комуникационни стандарти, които ще гарантират съвместимост на Системата с бъдещи разработки. Съществуващите модули / функционалности трябва да бъдат рефакторирани и/или надградени по начин, който да осигури изпълнението	Задължително	Приложимо

	на настоящето изискване.		
NF8	Бизнес процесите и услугите трябва да бъдат проектирани колкото се може по-независимо с цел по-лесно надграждане, разширяване и обслужване. Системата трябва да е максимално параметризирана и да позволява настройка и промяна на параметрите през служебен (администраторски) потребителски интерфейс; Трябва да бъде реализирана функционалност за текущ мониторинг, анализ и контрол на изпълнението на бизнес процесите в Системата.	Препоръчително	Приложимо
NF9	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).	Задължително	Приложимо
NF10	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.	Задължително	Приложимо
NF11	Приложните програмни интерфейси и информационните обекти задължително да поддържат атрибут за версия.	Задължително	Приложимо

NF12	Програмните интерфейси, изискуемите метаданни и атрибути за версия и достъп до стари версии трябва задължително да са налични и готови за използване минимум 24 месеца след публикуване на нова версия.	Задължително	Приложимо
NF13	Версията на програмните интерфейси, представени чрез уеб-услуги, трябва да поддържа версията по един или няколко от следните начини: 1) Като част от URL-а; 2) Като GET параметър; 3) Като HTTP header (Accept или друг).	Задължително	Приложимо
NF14	За всеки отделен приложен програмен интерфейс трябва да бъде разработен софтуерен комплект за интеграция (SDK) на поне две от популярните развойни платформи (.NET, Java, PHP).	Задължително	Приложимо
NF15	Системата трябва да осигурява възможности за разширяване, резервиране и балансиране на натоварването между множество инстанции на сървъри с еднаква роля.	Задължително	Приложимо
NF16	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.	Задължително	Приложимо
NF17	Изпълнителят трябва да осигури механизми за реализиране на бъдещи промени в Системата без промяна на съществуващия програмен код. Когато това не е възможно, времето за промяна, компилиране и пускане в експлоатация трябва да е сведено до минимум. Бъдещото развитие на Системата ще се налага във връзка с промени в правната рамка, промени в модела на работа на потребителите, промени във външни	Задължително	Приложимо

	системи, интегрирани със Системата, отстраняване на констатирани проблеми, промени в модела на обслужване и др. Такива промени ще се извършват през целия период на експлоатация на Системата, включително и по време на гаранционния период.		
NF18	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).	Задължително	Приложимо
NF19	Мрежата на държавната администрация (EECM) ще бъде използвана като основна комуникационна среда и като основен доставчик на защитен Интернет капацитет (Clean Pipe) – изискванията на софтуерните компоненти по отношение на използвани комуникационни протоколи, TCP портове и пр. трябва да бъдат детайлно документирани от Изпълнителя, за да се осигури максимална защита от хакерски атаки и външни прониквания чрез прилагане на подходящи политики за мрежова и информационна сигурност от Бенефициера в инфраструктурата на Държавния хибриден частен облак и EECM.	Задължително	Неприложимо
NF20	За търсене трябва да се използват системи за пълнотекстово търсене (например Solr, Elastic Search). Не се допуска използването на индекси за пълнотекстово търсене в СУБД.	Задължително	Приложимо
NF21	Системата трябва да бъде разработена така, че да позволява използването ѝ от много различни институции (т.нар. multitenancy), като за използване от нова	Задължително, ако е приложимо	Неприложимо

	институция не трябва да се изисква нова инсталация.		
NF22	Трябва да бъде създаден административен интерфейс, чрез който може да бъде извършвана конфигурацията на софтуера.	Задължително	Приложимо
NF23	Всеки обект в системата трябва да има уникален идентификатор.	Задължително	Приложимо
NF24	Записите в регистрите не трябва да подлежат на изтриване или на промяна, а всяко изтриване или промяна трябва да представлява нов запис	Задължително	Приложимо

7.2.3 Повторно използване (преизползване) на ресурси и готови разработки

Код	Описание	Приложимост	Забележка*
NF25	Проектът следва максимално да преизползва налични публично достъпни инструменти, библиотеки и платформи с отворен код. За реализацията на Системата следва да се използват в максимална степен софтуерни библиотеки и продукти с отворен код.	Задължително	Приложимо
NF26	Изпълнителят следва да представи базов списък със свободните компоненти и средства, които възнамерява да използва. Отворените проекти трябва да отговарят на следните критерии: 1) За разработката им да се използва система за управление на версиите на кода и да е наличен механизъм за съобщаване на несъответствия и приемане на допълнения; 2) Да имат разработена техническа документация за актуалната стабилна версия; 3) Да имат повече от един активен програмист, работещ по развитието им; 4) Да имат възможност за предоставяне на комерсиална поддръжка; 5) Да нямат намаляваща от година на година активност;	Задължително	Приложимо

	6) По възможност проектите да са подкрепени от организации с идеална цел, държавни или комерсиални организации; 7) По възможност проектите да имат разработени unit tests с code coverage над 50%, а проектът да използва Continuous Integration (CI) подходи – build bots, unit tests run, регулярно използване на статични / динамични анализатори на кода и др.		
NF27	Използването на софтуер със затворен код и на инструменти, библиотеки, продукти и системи с платен лиценз става за сметка на Изпълнителя, като е допустимо в случаите, когато липсва подходяща свободна алтернатива с необходимата функционалност или тя не отговаря на горните условия.	Задължително	Приложимо
NF28	Ако Изпълнителят предложи внедряване на Системата чрез използване на софтуерно решение със затворен код, то той трябва да обоснове, че това решение е икономически по-изгодно, отколкото разработка на софтуерно решение с отворен код.	Задължително	Приложимо
NF29	Изпълнителят трябва да осигури поддръжка от комерсиална организация, развиваща основните отворени продукти, които ще бъдат използвани като минимум за операционните системи и софтуерните продукти за управление на базите данни.	Препоръчително	Приложимо
NF30	При използването на свободни имплементации на софтуерни библиотеки е необходимо да се организира копие (fork) на съответното хранилище в общото хранилище за проекти с отворен код, финансирани с публични средства в България (ttps://git.egov.bg/explore/projects). Използващите свободните библиотеки компоненти задават за "upstream repo" хранилищата, като задължително се реферира използваната версия/ commit identificator.	Задължително	Приложимо
NF31	Когато се налага промяна в изходния код	Задължително	Приложимо

	на използван софтуерен компонент, промените трябва да се извършват във fork хранилището в съответствие с изискванията на основния проект. Изпълнителят трябва да извърши необходимите действия за включване на направените промени в основния проект чрез "pull requests" и извършване на необходимите изисквани от разработчиците на основния проект промени до приемането им. Тези дейности трябва да бъдат извършвани по време на целия проект. При установяване на наличие на нови версии на използваните проекти се извършва анализ на влиянието върху настоящата система. В случаите, при които се оптимизира използвана функционалност, отстраняват се пропуски в сигурността, стабилността или бързодействието, новата версия се извлича и използва след успешното изпълнение на интеграционните тестове.		

7.2.4 Изграждане и поддръжка на множество среди

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

Среда	Описание
Среда за развойна дейност (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.
Тестова (Sandbox, Testing)	Чрез Sandbox средата всички, които трябва да се интегрират към Системата, могат да тестват интеграцията си, без да застрашават работата на продукционната среда.
Продукционна (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 Бенефициера, Изпълнителят трябва да съдейства за изграждането на нови системни среди.

Изпълнителят може да предложи изграждането на допълнителни среди според спецификите на предложеното решение.

7.2.5 Процес на разработка, тестване и разгръщане

Код	Описание	Приложимост	Забележка*
NF32	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 те биха могли да съдействат в процесите по развитие и тестване на разработките през целия им жизнен цикъл.	Задължително	Приложимо
NF33	Всички софтуерни приложения, системи, подсистеми, библиотеки и компоненти, които са необходими за реализацията на Системата, трябва да бъдат разработвани като софтуер с отворен код и да бъдат достъпни в публично хранилище. Към настоящия момент следва да се използва общото хранилище за проекти с отворен код, финансирани с публични средства в България (https://git.egov.bg/explore/projects). В случай, че върху част от компонентите, нужни за компилация, има авторски права, те могат да бъдат или в отделно хранилище с подходящия за това лиценз или за тях трябва да бъде предоставен заместващ „mock up“ компонент, така че да не се нарушава компилацията на проекта.	Задължително	Приложимо
NF34	За всеки един разработван компонент Изпълнителят трябва да покрие следните изисквания за гарантиране на качеството на извършваната разработка и на крайния продукт: 1) Документиране на Системата в изходния код, минимум на ниво процедура/функция/клас; 2) Покритие на минимум 50% от изходния код с функционални тестове както и 20%	Задължително	Приложимо

	от съществуващата, тъй като е надграждане; 3) Използване на continuous integration практики; 4) Използване на dependency management.		
NF35	Във всеки един компонент на Системата, който се build-ва и подготвя за инсталация (deployment), е необходимо да присъстват следните реквизити: 1) Дата и час на build; 2) Място/среда на build; 3) Потребител извършил/стартирал build процеса. Идентификатор на ревизията от кодовото хранилище на компонента, срещу която се извършва build-ът.	Задължително	Приложимо

7.2.6 Бързодействие и мащабируемост

7.2.6.1 Контрол на натоварването и защита от DoS/ DDoS атаки

Код	Описание	Приложимост	Забележка*
NF36	Системата трябва да поддържа на приложно ниво "Rate Limiting" и/или "Throttling" на заявки от един и същ клиентски адрес както към страниците с уеб-съдържание, така и по отношение на заявките към приложните програмни интерфейси, достъпни публично или служебно като уеб-услуги (Web Services) и служебни интерфейси.	Задължително	Приложимо
NF37	Системата трябва да позволява конфигуриране от страна на администраторите на лимитите за отделни страници, уеб-услуги и ресурси, които се достъпват с отделен URL/URI.	Задължително	Приложимо
NF38	Системата трябва да поддържа възможност за конфигуриране на различни лимити за конкретни автентикирани потребители (напр. системи на други администрации) и трябва да предоставя възможност за генериране на справки и статистики за броя заявки по ресурси и услуги.	Задължително	Приложимо

7.2.6.2 Кохерентно кеширане на данни и заявки

Код	Описание	Приложимост	Забележка*
NF39	Отделните информационни системи,	Задължително	Приложимо

	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.		
NF40	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.	Задължително	Приложимо
NF41	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.	Задължително	Приложимо
NF42	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.	Задължително	Приложимо
NF43	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.	Задължително	Приложимо
NF44	Като минимум разпределен кохерентен кеш трябва да се предвиди при: 1) Извличане на информация от номенклатури и атомични данни за статус и актуално състояние на партиди от регистри в информационните системи;	Задължително	Приложимо

	2) Извличане на информация от предефинирани периодични справки; 3) Информация от лога на транзакциите при достъп с електронно-ИД до дадена услуга; 4) Информация за извършените плащания; 5) Други, които са идентифицирани на етап бизнес и системен анализ. От кеша следва да бъдат изключени прикачени файлове и големи по обем резултати от справки.		

7.2.6.3 Бързодействие

Код	Описание	Приложимост	Забележка*
NF45	При визуализация на уеб-страници системите трябва да осигуряват висока производителност и минимално време за отговор на заявки - средното време за заявка трябва да бъде по-малко от 1 секунда, с максимум 1 секунда стандартно отклонение за 95% от заявките, без да се включва мрежовото времезакъснение (Network Latency) при транспорт на пакети между клиента и сървъра. Трябва да бъдат създадени тестове за натоварване.	Задължително	Приложимо

7.2.6.4 Използване на HTTP/2

Код	Описание	Приложимост	Забележка*
NF46	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: 1) Включена header compression; 2) Използване на brotli алгоритъм за компресия; 3) Включен HTTP pipelining; 4) HTTP/2 Server push, приоритизиращ специфични компоненти, изграждащи страниците (CSS, JavaScript файлове и др.).	Задължително	Приложимо
NF47	Публичните потребителски интерфейси трябва да поддържат адаптивен избор на TLS cipher suites според вида на	Задължително	Приложимо

	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).		
NF48	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.	Задължително	Приложимо

7.2.6.5 Подписване на документи

Код	Описание	Приложимост	Забележка*
NF49	При реализацията на електронно подписване с всички видове електронен подпис трябва да се подписва сигурен хеш-ключ, генериран на базата на образа/съдържанието, а не да се подписва цялото съдържание.	Задължително	Приложимо
NF50	Минимално допустимият алгоритъм за хеширане, който трябва да се използва при електронно подписване, е SHA-256. В случаите, в които не се подписва уеб съдържание (например документи, файлове и др.), е необходимо да се реализира поточно хеширане, като се избягва зареждането на цялото съдържание в оперативната памет.	Задължително	Приложимо
NF51	Системата трябва да поддържа подписване на електронни изявления и електронни документи и с електронни подписи, издадени от Доставчици на удостоверителни услуги в ЕС, които отговарят на изискванията за унифициран профил на електронните подписи, съгласно подзаконовите правила към Регламент ЕС 910/2014, които влизат в сила и са задължителни от 1 януари 2017 г.	Задължително	Приложимо
NF52	Трябва да бъдат анализирани техническите възможности за реализиране на подписване	Задължително	Приложимо

	на електронни изявления и документи без използване на Java applet и без да се изисква от потребителите да инсталират Java Runtime, като по този начин се осигури максимална съвместимост на процеса на подписване с всички съвременни браузъри. Такава реализация може да бъде осъществена чрез: 1) използване на стандартни компоненти с отворен код, отговарящи на горните условия, които са разработени по други проекти на държавната администрация и са достъпни в хранилището, поддържано от Министерство на иновациите и дигиталната трансформация – при наличие на такива компоненти в хранилището те трябва да се преизползват и само да бъдат интегрирани в Системата; 2) използване на плъгин-модули с отворен код, достъпни за най-разпространените браузъри (Browser Plug-ins), които са адаптирани и поддържат унифицираните профили на електронните подписи, издавани от доставчик на удостоверителни услуги в ЕС, и съответните драйвери за крайни устройства за четене на сигурни носители или по стандартизиран в националната нормативна уредба протокол за подписване извън браузъра; 3) чрез интеграция с услуги за отдалечено подписване, предлагани от доставчици на удостоверителни услуги в ЕС.		

7.2.6.6 Качество и сигурност на програмните продукти и приложенията

Код	Описание	Приложимост	Забележка*
NF53	Да бъде предвидено спазването на добри практики на софтуерната разработка – покритие на изходния код с тестове – над 60%, документиране на изходния код, използване на среда за непрекъсната интеграция (Continuous Integration), възможност за компилиране и пакетиране	Задължително	Приложимо

	на продукта с една команда, възможност за инсталиране на нова версия на сървъра с една команда, система за управление на зависимостите (Dependency Management);		
NF54	Публичните модули, които ще предоставят информация и електронни услуги в Интернет, трябва да отговарят на актуалните уеб стандарти за визуализиране на съдържание.	Задължително	Приложимо

7.2.7 Информационна сигурност и интегритет на данните

Код	Описание	Приложимост	Забележка*
NF55	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).	Задължително	Приложимо
NF56	Да бъде предвидена система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата.	Задължително	Приложимо
NF57	Не се допуска използването на Self-Signed сертификати за публични услуги.	Задължително	Приложимо
NF58	Всички уебстраници (вътрешни и публично достъпни в Интернет) трябва да бъдат достъпни единствено и само през протокол HTTPS. Криптирането трябва да се базира на сигурен сертификат с валидирана идентичност (Verified Identity), позволяващ задължително прилагане на TLS 1.2, който е издаден от удостоверителен орган, разпознаван от най-често използваните браузъри (Microsoft Edge, Google Chorme, Mozilla Firefox). Ежегодното преиздаване и подновяване на сертификата трябва да бъде включено като разходи и дейности в гаранционната поддръжка за целия срок на поддръжката.	Задължително	Приложимо

NF59	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.	Задължително	Приложимо
NF60	Като временна мярка за съвместимост настройките на web сървърите и Reverse Proxy сървърите трябва да бъдат балансирани така, че Системата да позволява използване и на клиентски браузъри, поддържащи по-стария протокол TLS 1.1. Това изключение от общите изисквания за информационна сигурност не се прилага за достъпа на служебни потребители от държавната администрация и доставчици на обществени услуги, които имат служебен достъп до ресурси на Системата.	Задължително	Приложимо
NF61	При разгръщането на всички web услуги (Web Services) трябва да се използва единствено протокол HTTPS със задължително прилагане на минимум TLS 1.2.	Задължително	Приложимо
NF62	Програмният код трябва да включва методи за автоматична санитизация на въвежданите данни и потребителски действия за защита от злонамерени атаки, като минимум SQL инжекции, XSS атаки и други познати методи за атаки, и да отговаря, където е необходимо, на Наредбата за минималните изисквания за мрежова и информационна сигурност.	Задължително	Приложимо
NF63	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	Задължително	Приложимо

	Application Security Project).		
NF64	Трябва да бъде изграден модул за проследимост на действия и събития в Системата. Записът за всяко действие (добавяне, изтриване, модификация, четене) трябва да съдържа следните атрибути: 1) Уникален номер; 2) Точно време на възникване на събитието; 3) Вид (номенклатура от идентификатори за вид събитие); 4) Данни за информационна система, където е възникнало събитието; 5) Име или идентификатор на компонент в информационната система, регистрирал събитието; 6) Приоритет; 7) Описание на събитието; 8) Данни за събитието.	Задължително	Приложимо
NF65	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 (актуално издание, действащо към момента на изпълнение на проекта).	Задължително	Приложимо
NF66	Астрономическото време за удостоверяване настъпването на факти с правно значение и на такива, за които се изисква противопоставеност, 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 от доставчик на удостоверителни услуги или от държавен орган, осигуряващ такава услуга, отговаряща на изискванията на RFC 3161.	Задължително	Приложимо
NF67	Трябва да бъдат проведени тестове за проникване (penetration tests), с които да се идентифицират и коригират слаби места в сигурността на Системата.	Задължително	Приложимо

NF68	При идентификация на регистри и бази данни да се използва електронно удостоверение във формат X.509, издаден за съответния регистър. Идентификацията се осъществява двустранно по протокол TLS (Transport Layer Security – Сигурност на транспортния слой), версия 1.2 или по-висока, дефиниран в Препоръка RFC 5246, приета от IETF	Задължително	Приложимо
NF69	Информационните системи на административните органи да се идентифицират пред регистрите чрез цифров сертификат, двустранно по протокол TLS (Transport Layer Security – Сигурност на транспортния слой), версия 1.2 или по-висока.	Задължително	Приложимо

7.2.8 Използваемост

7.2.8.1 Общи изисквания за използваемост и достъпност

Код	Описание	Приложимост	
NF70	При проектирането и разработката на интернет страници и мобилни приложения трябва да се спазват стандартите за достъпност на потребителския интерфейс за хора с увреждания WCAG 2.1.	Задължително	Приложимо
NF71	Съдържанието на интернет страниците и мобилните приложения на административните органи, на доставчиците на обществени услуги и на лицата, осъществяващи публични функции, трябва да отговаря на последната обнародвана в Официалния вестник на Европейския съюз версия на хармонизирания стандарт EN 301 549, освен в случаите по чл. 58в, ал. 2 или 3 от ЗЕУ.	Задължително	Приложимо
NF72	Всички ресурси трябва да са достъпни чрез GET заявка на уникален адрес (URL). Не се допуска използване на POST за достигане до формуляр за подаване не заявление, за генериране на справка и други.	Задължително	Приложимо
NF73	Функционалностите на потребителския интерфейс на Системата трябва да бъдат независими от използваните от	Задължително	Приложимо

	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). При използване на Captcha, се осигуряват алтернативни форми с използване на изходи за различни видове сетивни възприятия, съобразени с различните увреждания.		
NF74	Не се допуска използване на Captcha като механизъм за ограничаване на достъпа до документи и/или услуги. Алтернативно, Системата трябва да поддържа "Rate Limiting" и/или "Throttling" съгласно изискванията в т. 7.1.1. от настоящите изисквания. Допуска се използването на Captcha единствено при идентифицирани много последователни опити от предполагаем „бот“.	Задължително	Приложимо
NF75	Трябва да бъде осигурен бърз и лесен достъп до електронните услуги и те да бъдат промотирани с подходящи навигационни елементи на публичната интернет страница – банери, елементи от главното меню и др.	Задължително	Приложимо
NF76	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.	Задължително	Приложимо

NF77	Не се допуска използването на HTML Frames, за да не се пречи на оптимизациите за търсещи машини.	Задължително	Приложимо
NF78	При разработката на публични уеббазирани страници трябва да се използват и да се реализира поддръжка на: 1) Стандартните семантични елементи на HTML5 (HTML Semantic Elements); 2) JSON-LD 1.0 (http://www.w3.org/TR/json-ld/); 3) Open Graph Protocol (http://ogp.me) за осигуряване на поддръжка за качествено споделяне на ресурси в социални мрежи и мобилни приложения.	Задължително	Приложимо
NF79	В екранните форми на Системата трябва да се използват потребителски бутони с унифициран размер и лесни за разбиране текстове в еднакъв стил.	Задължително	Приложимо
NF80	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).	Задължително	Приложимо
NF81	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.	Задължително	Приложимо
NF82	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.	Задължително	Приложимо
NF83	Всички търсения трябва да са нечувствителни към малки и главни букви.	Задължително	Приложимо

NF84	Полетата за пароли трябва задължително да различават малки и главни букви.	Задължително	Приложимо
NF85	Полетата за потребителски имена трябва да позволяват използване на имейл адреси като потребителско име, включително да допускат всички символи, регламентирани в RFC 1123, за наименуването на хостове.	Задължително	Приложимо
NF86	Главните и малките букви на въвежданите данни се запазват непроменени, не се допуска Системата да променя капитализацията на данните, въвеждани от потребителите.	Задължително	Приложимо
NF87	Системата трябва да позволява въвеждане на данни, съдържащи както български, така и символи на официалните езици на ЕС.	Задължително	Приложимо
NF88	Наименованията на полетата следва да са достатъчно описателни, като максимално се доближават до характера на съдържащите се в тях данни.	Задължително	Приложимо
NF89	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.	Задължително	Приложимо
NF90	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.	Задължително	Приложимо
NF91	За големите йерархически категоризации трябва да се предвиди възможност за навигация по нива или чрез отложено	Задължително	Приложимо

	зареждане (lazy load).		
NF92	Интернет страниците на администрациите трябва отговарят на правилата за институционална идентичност, определени от министъра на електронното управление. Наименованията на домейните и поддомейните, използвани от административните органи за официалните им интернет страници и портали трябва да отговарят на изискванията на чл. 47 от НОИИСРЕАУ. Ако се използват споделени информационни ресурси от ДХЧО за инсталиране на Системата, за публичен достъп в интернет може да се използват поддомейни на egov.bg със следната конвенция: [име на система].egov.bg. Например: iara-iss.egov.bg, strategy.egov.bg и др.	Задължително	Неприложимо

7.2.8.2 Интернационализация

Код	Описание	Приложимост	Забележка
NF93	Системата трябва да може да съхранява и едновременно да визуализира данни и съдържание, което е въведено/генерирано на различни езици.	Задължително	Приложимо
NF94	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, web услугите и др. трябва да поддържат стандартно и да са конфигурирани изрично за спазване на минимум Unicode 5.2 стандарт при съхранението и обработката на текстови данни, съответно трябва да се използва само UTF-8 кодиране на текстовите данни.	Задължително	Приложимо
NF95	Всички публично достъпни потребителски интерфейси следва да поддържат многоезичност, като минимум български и английски език.	Задължително	Приложимо
NF96	Публичната част на Системата трябва да бъде разработена и да включва набори с	Задължително	Приложимо

	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.		
NF97	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.	Задължително	Приложимо
NF98	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.	Задължително	Приложимо
NF99	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.	Задължително	Приложимо
NF100	При визуализация на числа трябва да се използва разделител за хиляди (интервал).	Задължително	Приложимо
NF101	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	Задължително	Приложимо

	потребителя език/локация в настройките на неговия профил: 1) 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; 2) Системата трябва да поддържа и всички формати съгласно ISO БДС 8601:2006.		

7.2.8.3 Изисквания за използваемост на потребителския интерфейс

Код	Описание	Приложимост	Забележка
NF102	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: 1) Контекстна валидация на въвежданите данни на ниво "поле" от форма и контекстни съобщения за грешка/невалидни данни в реално време; 2) Възможност за избор на стойности от номенклатури чрез търсене в списък по част от дума (autocomplete) и визуализиране на записи, отговарящи на въведеното до момента, без да е необходимо пълните номенклатури да са заредени в браузъра на клиента и потребителят да скорлира дълги списъци с повече от 10 стойности.	Задължително	Приложимо
NF103	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.	Задължително	Приложимо
NF104	Системата трябва да гарантира, че въведените, валидираните и запазените от сървъра данни остават достъпни за потребителите дори за процеси, които не	Задължително	Приложимо

	са приключили, така че при волно, неволно или автоматично прекъсване на потребителската сесия поради изтичане на периода за допустима липса на активност потребителят да може да продължи съответния процес след повторно влизане в системата, без да загуби въведените до момента данни и прикачените до момента електронни документи.		
NF105	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: 1) всяка електронна форма или стъпка от процес, за която има отделен екран/форма; 2) всяка група полета за въвеждане на данни (в случаите, в които определени полета от формата са групирани тематично); 3) всяко отделно поле за въвеждане на данни.	Задължително	Приложимо
NF106	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.	Задължително	Приложимо
NF107	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.	Задължително	Приложимо
NF108	Достъпът на потребителя до контекстната помощна информация трябва да бъде	Задължително	Приложимо

	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.		
NF109	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.	Задължително	Приложимо
NF110	Потребителският интерфейс следва да бъде достъпен за хора с увреждания съгласно изискванията на чл. 48, ал. 5 от ЗОП.	Задължително	Приложимо

7.2.8.4 Изисквания за използваемост в случаи на прекъснати бизнес процеси

Код	Описание	Приложимост	Забележка
NF111	Системата трябва да съхранява перманентно всеки започнал процес/процедура по подаване на заявление или обявяване на обстоятелства, текущия му статус и всички въведени данни и прикачени документи дори ако потребителят е прекъснал волно или неволно потребителската си сесия.	Задължително	Приложимо
NF112	При вход в системата потребителят трябва да получава прегледна и ясна нотификация, че има започнати, но недовършени/ неизпратени/ неподписани заявления, и да бъде подканен да отвори модула за преглед на историята на транзакциите.	Задължително	Приложимо
NF113	Модулът за преглед на историята на транзакциите трябва да поддържа следните функционалности: 1) Да визуализира списък с историята на подадените заявления, като минимум със следните колони –	Задължително	Приложимо

	дата, входящ номер, код на тупа формуляр, подател (име на потребител и имена на физическото лице - подател), статус на заявлението; 2) Да предлага видни и лесни за използване от потребителите контроли/инструменти: a. за филтриране на списъка (от дата до дата, за предефинирани периоди, като "последния един месец", "последната една година"; b. сортиране на списъка по всяка от колоните, без това да премахва текущия филтър; c. свободно търсене по ключови думи по всички колони в списъка и метаданните на прикачените/свързаните документи със заявленията, което да води до динамично филтриране на списъка.		

7.2.8.5 Изисквания за проактивно информиране на потребителите

Код	Описание	Приложимост	Забележка
NF114	За всички публични интернет страници трябва да бъде реализирана функционалност за публикуване на всяко периодично обновявано съдържание (новини, обявления, обществени поръчки, отворени работни позиции, нормативни документи, отговори по ЗДОИ и др.) в стандартен формат (RSS 2.x, Atom или еквивалент), както и поддържането на публично достъпни статистики за посещаемостта на страницата.	Задължително	Приложимо
NF115	Системата трябва да поддържа възможност за автоматично генериране на електронни бюлетини, които да се разпращат периодично или при настъпване на събития по електронна поща до регистрираните в Системата потребители, които са заявили или са се съгласили да получават такива бюлетини;	Задължително	Приложимо

	Потребителите трябва да имат възможност да настройват предпочитанията през потребителския си профил в Системата.		

7.2.9 Системен журнал

Код	Описание	Приложимост	Забележка
NF116	Атрибутите, които трябва да се запазват при всеки запис, трябва да включват като минимум следните данни: 1) дата/час на действието; 2) модул на системата, в който се извършва действието; 3) действие; 4) обект, над който е извършено действието; 5) допълнителна информация; 6) IP адрес и браузър на потребителя.	Задължително	Приложимо
NF117	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.	Задължително	Приложимо
NF118	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.	Задължително	Приложимо
NF119	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.	Задължително	Приложимо
NF120	Трябва да бъде предоставен достъп до системния журнал на органите на реда	Задължително	Приложимо

	чрез потребителски или програмен интерфейс; за достъпа трябва да се изисква електронна идентификация.		

7.2.10 Дизайн на бази данни и взаимодействие с тях

Код	Описание	Приложимост	Забележка
NF121	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.	Задължително	Приложимо
NF122	Базата данни трябва да може да оперира в клъстер, в определени случаи следва да бъде използван т.нар. sharding.	Задължително	Приложимо
NF123	Имената на таблиците и колоните трябва да следват унифицирана конвенция.	Задължително	Приложимо
NF124	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.	Задължително	Приложимо
NF125	Връзките между таблици трябва да са дефинирани чрез foreign key.	Задължително	Приложимо
NF126	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	Приложимо
NF127	Задължително трябва да се използват транзакции, като нивото на изолация трябва да бъде мотивирано в предадената документация.	Задължително	Приложимо
NF128	При операции върху много записи (batch) следва да се избягват дългопродължаващи транзакции.	Задължително	Приложимо
NF129	Заявките трябва да бъдат ограничени в броя записи, които връщат.	Задължително	Приложимо
NF130	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).	Задължително	Приложимо

NF131	При използване на нерелационна база данни трябва да се използват по-бързи и компактни протоколи за комуникация, ако такива са достъпни.	Задължително	Приложимо
NF132	При обработката на данните да се спазват формализираните описания, които подлежат на задължително унифициране: 1) имена; 2) адрес; 3) единен граждански номер; 4) личен номер на чужденец; 5) ЛН - личен номер (за гражданите на Европейския съюз и техните семейства); 6) единен идентификационен код, определен от Агенцията по вписванията; 7) единен идентификационен код (код по БУЛСТАТ); 8) служебен номер по чл. 84, ал. 3 от Данъчно-осигурителния процесуален кодекс; 9) наименование на юридическо лице; 10) телефонни номера; 11) други, определени от министъра на електронното управление.	Задължително	Приложимо
NF133	Във връзка с изискванията за оперативна съвместимост, при разработка на Системата да се предвиди: 1) използването на дефинираните вече обекти в Регистъра на информационните обекти; 2) вписване на формализирани описания на данните, ако чрез Системата се обработват данни, за които АО е първичен администратор.	Задължително	Приложимо

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

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

Код	Описание	Приложимост	Забележка

NF134	Да бъдат включени адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване	Задължително	Приложимо
NF135	Да се представят анализ и оценка на риска, които да послужат като основа за включването на адекватни и комплексни изисквания за мрежова и информационна сигурност.	Задължително	Приложимо
NF136	Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика.	Задължително	Приложимо
NF137	Да се използва отделна, изолирана от другите информационни и комуникационни системи и от интернет, подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуника-ционните системи и техните компоненти. Тази среда трябва да не се използва за други цели.	Задължително	Приложимо
NF138	Да се валидират всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на браузъра, като headers на препращащия и потребителски агент	Задължително	Приложимо
NF139	Всички данни да бъдат кодирани с HTML, изпращани от клиента и показвани в уеб страница.	Задължително	Приложимо
NF140	Да се ограничават заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по URL.	Задължително	Приложимо
NF141	Да се конфигурират типът и размерът на	Задължително	Приложимо

	headers, които уеб сървърът ще приеме.		
NF142	Да се ограничава времетраенето на връзката (connection Timeout) - времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, както и минималният брой байтове в секунда при изпращане на отговор на заявка.	Задължително	Приложимо
NF143	Да се въведе ограничение на броя неуспешни опити за влизане в системата	Задължително	Приложимо
NF144	Да не се допуска извеждането на списък на уеб директориите.	Задължително	Приложимо
NF145	Бисквитките (cookies) задължително да имат: 1) флаг за защита (security flag), който инструктира браузъра, че „бисквитката“ може да бъде достъпна само чрез защитени SSL канали; 2) флаг HTTP only, който инструктира браузъра, че „бисквитката“ може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента.	Задължително	Приложимо
NF146	Да се предвидят и предприемат мерки за защита на DNS, като задължително се прилага DNSSEC (Domain Name System Security Extensions);	Задължително	Приложимо
NF147	По отношение на системните записи (Logs) да бъдат предвидени следните възможности: 1) в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите,	Задължително	Приложимо

	управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи; 2) за всяко от тези събития в записите се отбелязва с астрономическото време, когато е настъпило събитието; 3) да бъде предвидена възможност за синхронизиране на часовниците на компоненти на информационните и комуникационните системи, като се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен; 4) да се предвиди как информацията ще бъде архивирана за срок не по-кратък от дванадесет месеца		

8 Изисквания към изпълнението на дейностите по проекта

8.1 Фаза 1 - Изграждане на цифров портфейл и доставчик на самоличност

8.1.1 Дейност 1 - Изграждане на рамка на доверие

8.1.1.1 Описание на дейността

Дейността обхваща изграждането на национална рамка на доверие за Портфейла за цифрова самоличност, която представлява организационната, техническата, процедурната и доверителната основа за функциониране на цялата екосистема. Рамката на доверие следва да осигури условията, правилата и механизмите, чрез които участниците в екосистемата ще бъдат регистрирани, проверявани, управлявани, валидирани, наблюдавани и, когато е необходимо, временно спирани или заличавани.

Изграждането на рамка на доверие е базова предпоставка за изпълнение на всички следващи дейности по проекта, тъй като чрез нея се определя кои субекти могат да участват в екосистемата, при какви условия, с какви технически параметри, с какъв статус на доверие, чрез какви сертификати и интерфейси, както и по какъв начин тази информация се публикува и валидира от останалите участници. Без такава рамка не може да бъде гарантирано сигурно и оперативно съвместимо взаимодействие между доставчици на портфейли, доставчици на самоличност, доставчици на атрибути, доставчици на квалифицирани атрибути от името на публични институции, посредници при верификация, доверяващи се страни и европейската

инфраструктура по eIDAS.

Дейността включва анализ, проектиране, разработване, внедряване и документиране на следните основни компоненти и процеси:

- правила, политики и процедури за регистрация, присъединяване, промяна, временно спиране, възстановяване и прекратяване на участието на субектите в екосистемата;
- PKI и доверителна инфраструктура, необходима за удостоверяване, подписване, валидиране, защита на обмена, проверка на автентичността и управление на доверителните връзки между компонентите;
- регистър на участниците в екосистемата, чрез който се управляват данните, статусите, техническите профили, сертификатите, ролите и обхватът на участие на отделните субекти;
- регистратор на доверителни списъци, чрез който се създават, подписват, публикуват, актуализират и валидират доверителните списъци, необходими за националната и трансграничната оперативна съвместимост;
- административни интерфейси за управление на участници, заявления, проверки, статуси, конфигурации, доверителни списъци, технически параметри, одитни записи и справки;
- интеграционни интерфейси за обмен на доверителна информация с вътрешните компоненти на системата, с национални инфраструктурни компоненти и с европейската инфраструктура по eIDAS;
- механизми за контрол, проследимост, одитен журнал, мониторинг, управление на риска и съответствие с изискванията за информационна сигурност, киберсигурност и защита на личните данни.

Рамката на доверие следва да бъде изградена като устойчив и разширяем компонент, който да позволява първоначално въвеждане на държавния Портфейл за цифрова самоличност и последващо присъединяване на допълнителни участници - публични институции, доставчици на атрибути, доставчици на квалифицирани удостоверителни услуги, доверяващи се страни и частни доставчици на услуги. Компонентите, реализирани в рамките на дейността, следва да бъдат приложими както за първоначалния минимално използваем продукт, така и за последващо разширяване на националната екосистема.

При изпълнение на дейността следва да бъдат дефинирани основните роли на участниците и техните права и задължения. Най-малко следва да бъдат обхванати следните категории участници:

- доставчици на Портфейл за цифрова самоличност;

- доставчици на самоличност и/или доставчици на данни за идентификация на лица;
- доставчици на електронни удостоверения за атрибути;
- доставчици на квалифицирани електронни удостоверения за атрибути;
- доставчици на квалифицирани атрибути от името на публични институции;
- посредници при верификация;
- доверяващи се страни;
- квалифицирани доставчици на удостоверителни услуги, доколкото рамката на доверие съдържа данни или статуси, необходими за последващото им присъединяване;
- компетентни административни, контролни, надзорни и сертифициращи органи;
- администратори и оператори на националната рамка на доверие.

8.1.1.2 Изисквания към изпълнение на дейността

Изпълнителят следва да извърши детайлен бизнес, нормативен, технически и архитектурен анализ на необходимите процеси и компоненти за изграждане на националната рамка на доверие. Анализът следва да обхване приложимите европейски изисквания по eIDAS 2.0, актовете за изпълнение към европейската рамка за цифрова идентичност, Architecture and Reference Framework, проекта на Закон за Европейския портфейл за цифрова самоличност, националната нормативна уредба в областта на електронното управление, електронната идентификация, електронните удостоверителни услуги, защитата на личните данни и киберсигурността.

Изпълнителят следва да анализира и предложи модел за управление на рамката на доверие, включително роли, отговорности, права за достъп, процеси за одобрение, механизми за контрол, одит, проследимост и управление на жизнения цикъл на участниците. Моделът следва да отчита ролята на Бенефициера/компетентния орган, ролята на техническия оператор на системата, ролята на контролните и надзорните органи, както и ролите на участниците, които се присъединяват към екосистемата.

Изпълнителят следва да разработи процедури за регистрация и присъединяване на участници. Процедурите следва да обхващат най-малко:

- подаване на заявление за регистрация или присъединяване;
- идентифициране на заявителя и проверка на представителна власт;
- подаване и проверка на документи, технически параметри, сертификати, доклади за съответствие, декларации, политики и други доказателства;
- проверка на изпълнението на минималните организационни, технически и нормативни изисквания, както и изискванията за сигурност;
- управление на непълни и нередовни данни;

- одобрение, отказ, вписване, промяна на статус, временно спиране, възстановяване и заличаване;
- уведомяване на заявителя и приложимите компетентни органи;
- публикуване или актуализиране на релевантна информация в регистъра на участниците и доверителните списъци;
- поддържане на пълна история на действията, статусите, документите и решенията.

Процедурите следва да бъдат приложими за различните категории участници, като се отчита спецификата на всеки тип участник. За доставчици на портфейли следва да се предвиди управление на данни за сертифициране, статус на портфейла, технически профили, идентификатори, ключове, сертификати и обхват на предоставяните услуги. За доставчици на самоличност следва да се предвиди управление на източниците на данни, нивото на осигуреност, методите за идентификация и механизмите за валидиране на данни за идентификация на лице. За доставчици на атрибути следва да се предвидят данни за типа атрибути, източниците на данни, правното основание, техническите интерфейси, статуса и обхвата на предоставяните удостоверения. За посредници при верификация и доверяващи се страни следва да се предвиди управление на допустимите цели, заявяваните атрибути, техническите параметри, сертификатите, контактните данни, правното основание и статуса на участие.

Изпълнителят следва да изгради регистър на участниците в екосистемата. Регистърът следва да поддържа структурирана информация за всички вписани участници, включително най-малко: тип участник, наименование, уникален идентификатор, правен статус, контактни данни, технически профил, роли, обхват на участие, сертификати, ключове, крайни точки за интеграция, статус, дата на регистрация, дата на последна промяна, основание за промяна, валидност, връзка с приложими документи, одитна история и публичност на отделни полета.

Регистърът на участниците следва да поддържа различни статуси на участниците, включително най-малко: подадено заявление, в процес на проверка, върнато за корекция, одобрено, активно, временно спряно, отнето/заличено, прекратено, изтекло и архивирано. Статусите следва да бъдат конфигурируеми или разширяеми, като всяка промяна на статус се записва в системния журнал с информация за потребител, дата и час, основание и приложими документи.

Изпълнителят следва да разработи административен интерфейс за управление на регистъра на участниците. Интерфейсът следва да позволява търсене, филтриране, преглед, създаване, редакция, преглед на история, управление на статуси, прикачване и преглед на документи, управление на технически параметри, управление на сертификати, управление на роли, справки и експорти. Достъпът до административния интерфейс следва да бъде ограничен чрез ролеви модел, многостепенна автентикация, управление на права и пълен одитен журнал на действията.

Изпълнителят следва да осигури публичен или ограничено публичен достъп до определени данни от регистъра, когато това се изисква от нормативната рамка или е необходимо за прозрачност и проверка от страна на участниците. Публично достъпните данни следва да бъдат ограничени до информация, която не представлява лични данни, защитена информация, чувствителна техническа информация или информация, чието публикуване би създало риск за сигурността.

Изпълнителят следва да изгради регистратор на доверителни списъци. Регистраторът следва да осигурява създаване, подписване, публикуване, актуализиране, валидиране, управление на версии и архивиране на доверителни списъци, съдържащи информация за участници, сертификати, технически параметри, статуси, доверителни връзки и друга информация, необходима за проверка на доверие в национален и трансграничен контекст.

Доверителните списъци следва да бъдат в машинночетим формат, съобразен с приложимите европейски технически спецификации и профили. Следва да се поддържа механизъм за електронно подписване на списъците, управление на версии, публикуване на актуални и исторически версии, проверка на целостта, управление на валидност, автоматизирана синхронизация и уведомяване при промени в статусите на участниците.

Изпълнителят следва да анализира и реализира достъпа до европейската инфраструктура на рамката на доверие. Това включва анализ на изискванията за участие в европейската екосистема, необходимите технически интерфейси, метаданни, сертификати, доверителни списъци, механизми за уведомяване, протоколи и процеси за валидиране. Резултатът от анализа следва да бъде приложен в архитектурата и интеграционните интерфейси на Системата.

Изпълнителят следва да изгради необходимата PKI и доверителна инфраструктура или да интегрира Системата със съществуваща такава, когато това е допустимо и одобрено от Бенефициера. PKI инфраструктурата следва да осигурява издаване, управление, съхранение, подновяване, отмяна и проверка на сертификати и ключове, необходими за вътрешните и външните доверителни процеси.

PKI и криптографската инфраструктура следва да отговарят на приложимите изисквания за сигурно управление на ключове, защита на частни ключове, използване на HSM или друга защитена среда, разделение на роли, контрол на достъпа, одитен журнал, резервираност, възстановяване, ротация на ключове, управление на компрометиране и процедури при инциденти. Когато се използват сертификати, списъци за отмяна или услуги за проверка на статус, следва да бъдат реализирани механизми за валидиране, актуализация и проследимост.

Изпълнителят следва да осигури вътрешни и външни приложни програмни интерфейси за достъп до данни от рамката на доверие. Интерфейсите следва да позволяват проверка на статус на участник, проверка на доверителна информация, проверка на сертификати, получаване на

технически параметри, синхронизация на доверителни списъци и други операции, необходими за работата на доставчика на портфейл, доставчика на самоличност, доставчика на атрибути, посредника при верификация и доверяващите се страни.

Всички API интерфейси следва да бъдат документирани, управление на версии, защитени и съобразени с принципите за оперативна съвместимост. Документацията следва да включва описание на методи, параметри, формати на заявки и отговори, кодове за грешки, механизми за автентикация и авторизация, примери, тестови сценарии, ограничения, правила за използване и процедури при промяна на версия.

Изпълнителят следва да осигури sandbox или тестова среда за присъединяване на участници към рамката на доверие. Средата следва да позволява тестване на технически профили, сертификати, интерфейси, доверителни списъци, проверки на статус, интеграционни сценарии и обмен на тестови данни, без риск за продукционната среда и без обработка на реални лични данни, освен ако това не е изрично допустимо и обезпечено с необходимите мерки.

Изпълнителят следва да осигури механизми за мониторинг, одитен журнал на всички действия, извършвани в рамките на дейността. Следва да се записва най-малко: вход и изход на потребители, преглед и промяна на данни, подаване и обработка на заявления, промяна на статуси, управление на сертификати, публикуване на доверителни списъци, системни грешки, неуспешни опити за достъп, интеграционни заявки, административни действия и действия с повишен риск.

Одитните журнали следва да бъдат защитени от нерегламентирана промяна и изтриване, да поддържат необходимите срокове за съхранение, да позволяват справки и одит, да бъдат достъпни само за оправомощени лица и да не съдържат повече лични данни от необходимото за целите на проследимостта, сигурността и отчетността.

Изпълнителят следва да осигури съответствие с изискванията за защита на личните данни. При проектирането на регистъра на участниците, административните интерфейси, доверителните списъци, журналите и интеграциите следва да се прилагат принципите за минимизиране на данните, ограничаване на целите, контрол на достъпа, криптиране, анонимизация, защита по проект и по подразбиране, отчетност и възможност за доказване на законосъобразността на обработването.

Изпълнителят следва да осигури съответствие с изискванията за киберсигурност и информационна сигурност. Системата следва да бъде защитена срещу неоторизиран достъп, подправяне на данни, компрометиране на ключове, инжекционни атаки, неоторизирано използване на интерфейси, злоупотреба с привилегии, отказ от услуга, нерегламентирано публикуване на доверителна информация и други релевантни заплахи.

За компонентите по дейността следва да бъдат проведени функционални, интеграционни,

системни, регресионни, натоварващи и тестове за сигурност. Следва да бъдат извършени анализ на уязвимости и penetration testing за публичните, административните и интеграционните интерфейси. Установените критични и високи уязвимости следва да бъдат отстранени преди приемане и внедряване в продукционна среда.

Изпълнителят следва да осигури необходимите среди за разработка, тестване, приемане, обучение, sandbox и продукционна експлоатация на компонентите по дейността. Средите следва да бъдат логически и/или физически разделени, с различни настройки за достъп, тестови данни, конфигурации, сертификати и механизми за наблюдение.

Изпълнителят следва да осигури DevOps процеси за управление на разработката, версиите, конфигурациите, миграциите, разгръщането, rollback процедури, наблюдение, автоматизирано тестване и проследимост на промените. Всеки компонент следва да бъде доставен с необходимите скриптове, конфигурации, инструкции и процедури за инсталиране, надграждане и възстановяване.

При изпълнението на дейността следва да се осигури възможност за бъдещо разширяване на рамката на доверие, включително добавяне на нови типове участници, нови технически профили, нови видове атрибути, нови доверителни списъци, нови интеграционни интерфейси, нови европейски изисквания, нови национални процедури и нови механизми за контрол и сертифициране.

8.1.1.3 Очаквани резултати

Очакваните резултати от изпълнението на дейността са:

- извършен бизнес, нормативен, технически и архитектурен анализ на процесите, компонентите и участниците, необходими за изграждане на национална рамка на доверие;
- дефиниран модел за управление на националната рамка на доверие, включително роли, отговорности, процеси, права за достъп, механизми за контрол, проследимост и управление на риска;
- разработени правила, политики и процедури за регистрация, присъединяване, промяна, временно спиране, възстановяване и прекратяване на участие на субекти в екосистемата;
- дефинирани процедури за регистрация на доставчици на портфейли, доставчици на самоличност, доставчици на квалифицирани атрибути, доставчици на квалифицирани атрибути от името на публични институции, посредници при верификация и доверяващи се страни;
- изграден регистър на участниците в екосистемата, поддържащ структурирана информация, статуси, технически профили, сертификати, документи, история и справки;

- реализирани административни интерфейси за управление на заявления, участници, статуси, документи, сертификати, технически параметри, доверителна информация, справки и одитни записи;
- изградена или интегрирана необходимата PKI и доверителна инфраструктура за управление на сертификати, ключове, доверителни връзки, подписване, валидиране и защита на обмена;
- изграден регистратор на доверителни списъци, осигуряващ създаване, подписване, публикуване, актуализиране, валидиране, управление на версии и архивиране на доверителни списъци;
- реализирани машинночетими доверителни списъци, във формат съгласно ETSI TS 119 612 и ETSI TS 119 602 (списъци на доверени субекти), съобразени с приложимите европейски и национални изисквания;
- извършен анализ и реализирани необходимите механизми за достъп и взаимодействие с европейската инфраструктура на рамката на доверие;
- реализирани вътрешни и външни API интерфейси за проверка на статуси, доверителна информация, сертификати, технически параметри и синхронизация на доверителни списъци;
- осигурена sandbox/тестова среда за тестване на присъединяване, технически профили, сертификати, доверителни списъци и интеграционни сценарии;
- реализирани механизми за мониторинг, одитен журнал, справки, проследимост и контрол на действията в рамката на доверие;
- осигурени механизми за информационна сигурност, киберсигурност, защита на личните данни, управление на достъпа и защита на доверителната информация;
- проведени функционални, интеграционни, системни, регресионни, натоварващи и тестове за сигурност на компонентите по дейността;
- изготвени доклади от тестове, анализ на уязвимости и penetration testing за приложимите компоненти;
- внедрени компонентите по дейността в съответните среди за разработка, тестване, приемане, обучение, sandbox и продукционна експлоатация;
- осигурена възможност за последващо разширяване на рамката на доверие с нови типове участници, нови доверителни списъци, нови технически профили, нови интеграции и нови нормативни изисквания.

8.1.2 Дейност 2 - Изграждане на цифров портфейл и доставчик на самоличност

8.1.2.1 Описание на дейността

Дейността обхваща изграждането на основните компоненти, чрез които крайният

потребител ще използва Портфейла за цифрова самоличност, както и компонентите, чрез които потвърдената самоличност на лицето ще бъде свързвана с конкретна инстанция на портфейла. Дейността включва изграждане на доставчик на Портфейл за цифрова самоличност, разработване на мобилно приложение за крайни потребители, изграждане на доставчик на самоличност и реализиране на необходимите процеси за първоначална идентификация, издаване на данни за идентификация на лице, активиране на портфейл, управление на отделните записи в портфейла на потребителя (наричани още: портфейлни единици) и използване на базови сценарии за електронна идентификация.

Дейността е ключова за проекта, тъй като чрез нея се изгражда потребителският и идентификационният слой на националната екосистема за цифрова самоличност. Докато рамката на доверие определя правилата, участниците и доверителната инфраструктура, Реализацията на дейността включва практическия механизъм, чрез който гражданите, жителите и, когато е приложимо, представителите на юридически лица, ще могат да използват Портфейла за цифрова самоличност в реални електронни процеси.

Доставчикът на Портфейл за цифрова самоличност следва да осигури техническата и приложната инфраструктура за управление на жизнения цикъл на портфейлните единици. Това включва създаване, активиране, свързване с потвърдена самоличност, използване, обновяване, блокиране, възстановяване, прекратяване и архивиране на портфейлна единица, както и управление на устройствата, ключовете, атестациите, сесиите и настройките за сигурност.

Мобилното приложение следва да бъде основният потребителски интерфейс към Портфейла. Чрез него потребителят следва да може да премине през процес на първоначално активиране, да потвърди своята самоличност, да получи данни за идентификация на лице, да управлява наличните в портфейла данни и атрибути, да представя данни пред доверяващи се страни, да дава или отказва съгласие за предоставяне на данни, да преглежда история на действията, да управлява настройките за сигурност и да използва базови сценарии за електронна идентификация.

Доставчикът на самоличност следва да осигури надежден механизъм за потвърждаване на самоличността на лицето и за издаване или предоставяне на данни за идентификация на лице за нуждите на Портфейла. Този компонент следва да работи в тясна връзка с националните регистри, приложимите средства за електронна идентификация, eIDAS възела, системите за електронна автентикация и други допустими източници или механизми, чрез които може да бъде постигнато ниво на осигуреност „високо“.

Дейността следва да осигури и реализация на минимално използваем продукт (MVP), чрез който да бъдат доказани основните сценарии на работа на Портфейла. Минимално използваемият продукт следва да включва най-малко процес по първоначална идентификация на потребител, активиране на портфейл, получаване на данни за идентификация на лице,

използване на портфейла за електронна идентификация и представяне на базов удостоверен атрибут, включително сценарий за проверка на възраст.

При изпълнението на дейността следва да се осигури съответствие с европейските изисквания за EUDI Wallet, включително изискванията за сигурно управление на портфейлни единици, защита на криптографските ключове, потребителски контрол върху данните, селективно предоставяне на атрибути, защита на личните данни, оперативна съвместимост, достъпност и проследимост. Решението следва да бъде проектирано така, че да може да се използва като основа за последващо надграждане с допълнителни доставчици на атрибути, доставчици на квалифициран електронен подпис, доверяващи се страни и трансгранични сценарии.

8.1.2.2 Изисквания към изпълнение на дейността

Изпълнителят следва да извърши детайлен бизнес, нормативен, технически, архитектурен и потребителски анализ на процесите, свързани с изграждането и използването на Портфейла за цифрова самоличност. Анализът следва да обхване процесите по първоначална идентификация, активиране на портфейл, издаване на данни за идентификация на лице, управление на портфейлна единица, управление на устройство, управление на ключове, управление на потребителски съгласия, представяне на данни към доверяващи се страни, блокиране, възстановяване и прекратяване на портфейл.

Изпълнителят следва да проектира и реализира доставчик на Портфейл за цифрова самоличност като сървърен и интеграционен компонент, който управлява жизнения цикъл на портфейлните единици и осигурява взаимодействие между мобилното приложение, доставчика на самоличност, рамката на доверие, доставчика на атрибути, посредника при верификация, доставчиците на удостоверителни услуги и приложимите национални и европейски инфраструктури.

Доставчикът на Портфейл следва да поддържа най-малко следните процеси:

- създаване и инициализация на портфейлна единица;
- активиране на портфейл след успешно потвърждаване на самоличността на потребителя;
- свързване на портфейлна единица с потвърдена самоличност;
- управление на статус на портфейлна единица;
- управление на свързани устройства;
- управление на сесии и потребителски достъп;
- управление на криптографски ключове и атестации;
- управление на настройки за сигурност;
- блокиране, временно спиране, възстановяване и прекратяване на портфейл;

- поддръжка на процеси при изгубено, сменено или компрометирано устройство;
- одитен журнал и проследимост на действията;
- предоставяне на интерфейси към вътрешни и външни компоненти на екосистемата.

Изпълнителят следва да разработи мобилно приложение за Портфейл за цифрова самоличност за основните мобилни платформи, като минимално следва да се поддържат Android и iOS. Приложението следва да бъде разработено като native или друг еквивалентен технологичен подход, който гарантира високо ниво на сигурност, производителност, достъп до защитените възможности на устройството, стабилност, поддръжка и съответствие с изискванията на платформите.

Мобилното приложение следва да осигурява ясен, достъпен и сигурен потребителски интерфейс за изпълнение на основните портфейлни операции. Потребителят следва да може да разбира какви данни се съхраняват в портфейла, кой ги е издал, за каква цел се заявяват, на кого се предоставят и какви последици има потвърждаването или отказът на конкретна операция.

Мобилното приложение следва да включва най-малко следните функционални области:

- първоначално стартиране и активиране на приложението;
- процес по идентификация и свързване на портфейла със самоличността на потребителя;
- получаване и преглед на данни за идентификация на лице;
- управление на налични атрибути и удостоверения;
- представяне на данни и атрибути пред доверяващи се страни – онлайн (remote) и при физическо присъствие (proximity);
- потвърждаване, отказ и управление на заявки за предоставяне на данни;
- създаване на резервно копие на данните в Портфейла и възстановяване от него при смяна, загуба или компрометиране на устройството;
- експорт на данните и преносимост към друг Портфейл, включително към портфейл на друг доставчик;
- управление на настройки за сигурност;
- управление на устройство, включително възможности за блокиране или деактивиране;
- уведомления към потребителя за важни действия, промени, рискове, заявки или статуси;
- помощна информация, инструкции и условия за използване.

Приложението следва да поддържа механизми за потребителски контрол върху данните. Преди всяко предоставяне на данни към доверяваща се страна потребителят следва да получава ясна информация най-малко за: идентичността на доверяващата се страна, целта на заявката,

конкретните заявени данни или атрибути, издателя на атрибутите, последиците от предоставянето, възможността за отказ и, когато е приложимо, срока или контекста на използване.

Изпълнителят следва да осигури сигурно съхранение на криптографски ключове и чувствителни данни в мобилното устройство. За първоначалния обхват следва да се предвиди поддръжка на устройства, които разполагат със защитено хардуерно или системно ниво за съхранение на ключове и извършване на криптографски операции, като Apple Secure Enclave, Android StrongBox, Trusted Execution Environment или еквивалентен механизъм, съобразен с възможностите на конкретната платформа и приложимите европейски изисквания.

Когато дадено устройство не покрива минималните изисквания за сигурно съхранение и криптографски операции, приложението следва да има механизъм за информиране на потребителя и ограничаване на достъпа до функционалности, които не могат да бъдат изпълнени при необходимото ниво на сигурност. Следва да се предвиди възможност за последващо разширяване на поддържаните устройства чрез допълнителни механизми, включително отдалечено съхранение на ключове и криптографски операции в защитена среда, когато това бъде реализирано в следващите дейности.

Изпълнителят следва да изгради доставчик на самоличност, който осигурява процесите по първоначална идентификация и потвърждаване на самоличността на потребителя. Доставчикът на самоличност следва да работи при ниво на осигуреност, „високо“ по смисъла на чл. 8, параграф 2, буква „в“ от Регламент (ЕС) № 910/2014 и Регламент за изпълнение (ЕС) 2015/1502, съгласно чл. 5а, параграф 11 от Регламент (ЕС) № 910/2014. Издаването на данни за идентификация на лице (PID) и активирането на портфейлната единица се извършват само при постигнато ниво на осигуреност „високо“.

Доставчикът на самоличност следва да поддържа механизми за идентификация на потребителя чрез допустими национални и европейски средства. Възможните механизми следва да бъдат анализирани и предложени от Изпълнителя, като могат да включват електронна идентификация чрез съществуващи национални средства, квалифициран електронен подпис, eIDAS трансгранична идентификация, физическа идентификация чрез определени офиси или други допустими механизми, които покриват необходимото ниво на доверие.

Изпълнителят следва да осигури интеграции с приложимите национални регистри и автентични източници, необходими за проверка на самоличността и издаване на данни за идентификация на лице. В обхвата следва да бъдат анализирани и, когато е приложимо, реализирани интеграции с регистри за самоличност, ЕСГРАОН, регистри на МВР, eIDAS възела, системи за електронна автентикация, RegiX и други приложими компоненти на електронното управление.

Данните за идентификация на лице следва да бъдат издавани и управлявани в съответствие с приложимите европейски изисквания за PID, като се осигурява точност, актуалност, проверимост, защита на личните данни, контрол на достъпа, възможност за проверка на валидност и проследимост на процеса по издаване.

Изпълнителят следва да осигури механизми за повторна проверка, актуализация или отмяна на данни за идентификация, когато това е необходимо поради промяна на данни, изтичане на валидност, компрометиране, блокиране, прекратяване или друг нормативно или технически предвиден случай.

В рамките на дейността следва да бъде реализирана връзката между доставчика на самоличност и доставчика на Портфейл. След успешно потвърждаване на самоличността следва да бъде възможно сигурно свързване на самоличността с конкретна портфейлна единица, без да се допуска нерегламентирано създаване на портфейл, свързване с чужда самоличност, дублиране, подправяне или компрометиране на процеса.

Изпълнителят следва да осигури механизми за управление на потребителския профил в рамките на Портфейла. Тези механизми следва да позволяват преглед на основни данни, статус на портфейла, свързани устройства, налични атрибути, история на използване, настройки за сигурност, предпочитания за уведомяване, помощна информация и действия при загуба или компрометиране на устройството.

Следва да се осигури механизъм за блокиране или деактивиране на портфейл при изгубено, откраднато, сменено или компрометирано устройство. Процесът следва да бъде проектиран така, че да защитава потребителя от неоторизирано използване, но и да позволява възстановяване на достъпа при доказване на самоличността по надежден начин.

Изпълнителят следва да осигури механизми за водене на одитен журнал, мониторинг и одит на действията, свързани с доставчика на портфейл, мобилното приложение и доставчика на самоличност. Следва да се записват най-малко действията по идентификация, активиране, издаване на PID, промяна на статус, блокиране, възстановяване, представяне на данни, откази, грешки, административни действия и интеграционни заявки. Журналите не следва да съдържат повече лични данни от необходимото за целите на сигурността, проследимостта и нормативното съответствие.

Изпълнителят следва да осигури механизми за защита на личните данни по проект и по подразбиране. Решението следва да бъде проектирано така, че да се обработват само данните, необходими за конкретния процес, да се избягва ненужно централизирано съхранение на потребителски атрибути, да се осигурява потребителски контрол върху предоставянето на данни и да се поддържат механизми за прозрачност и отчетност.

При проектирането на мобилното приложение и сървърните компоненти следва да се

осигурят мерки за защита срещу злоупотреби, включително защита срещу подправяне на приложението, неоторизиран достъп, reverse engineering, компрометирани устройства, root/jailbreak среда, replay атаки, подправяне на заявки, неоторизирано използване на API, подмяна на доверяваща се страна, man-in-the-middle атаки и други релевантни заплахи.

Изпълнителят следва да осигури съвместимост на мобилното приложение с актуалните версии на Android и iOS, както и с минимални версии, които ще бъдат определени в хода на анализа и съгласувани с Бенефициера. Следва да се дефинира политика за поддръжка на версии на операционните системи, устройства, криптографски възможности и механизми за актуализация на приложението.

Мобилното приложение следва да бъде публикувано и поддържано съгласно изискванията на съответните официални магазини за приложения, когато това е приложимо. Изпълнителят следва да осигури необходимите материали, технически настройки, версии, описания, политики за поверителност, тестови версии и съдействие при процесите по публикуване и актуализация.

Изпълнителят следва да осигури достъпност и използваемост на мобилното приложение и приложимите уеб интерфейси. Потребителските процеси следва да бъдат ясни, последователни, разбираеми и съобразени с принципите за достъпност, включително за потребители с увреждания. Следва да се избягват излишно сложни стъпки, неясни съобщения, технически термини без обяснение и действия, които могат да доведат до неволно предоставяне на данни.

Изпълнителят следва да реализира минимално използваем продукт, който да демонстрира работоспособността на основните компоненти по дейността. MVP следва да включва най-малко: инсталиране и активиране на мобилно приложение, идентификация на потребител, издаване/получаване на данни за идентификация на лице, представяне на данни към доверяваща се страна и проверка на възраст чрез цифров атрибут. Конкретните сценарии, данни, участници и ограничения на MVP следва да бъдат уточнени в хода на анализа и съгласувани с Бенефициера.

Изпълнителят следва да осигури интеграция на компонентите по дейността с рамката на доверие, изградена по Дейност 1. Това включва проверка на статуси, доверителни списъци, сертификати, технически профили, регистрирани участници, доверяващи се страни и приложими правила за предоставяне на данни.

Изпълнителят следва да осигури интеграция с компонентите, които ще бъдат изградени или надградени в следващи дейности, включително доставчик на квалифицирани атрибути, посредник при верификация, доставчици на квалифицирани електронни подписи и доставчици на атрибути. Архитектурата следва да бъде модулна и разширяема, така че последващите интеграции да не изискват цялостна преработка на вече реализираните компоненти.

Изпълнителят следва да осигури необходимите среди за разработка, тестване,

интеграционно тестване, приемане, обучение, sandbox и продукционна експлоатация на компонентите по дейността. Средите следва да бъдат разделени, контролирани и конфигурирани така, че да позволяват надеждно тестване на мобилното приложение, доставчика на портфейл, доставчика на самоличност, интеграциите и MVP сценариите.

За компонентите по дейността следва да бъдат проведени функционални, интеграционни, системни, приемателни, регресионни, натоварващи, потребителски и тестове за сигурност. За мобилното приложение следва да бъдат проведени тестове за съвместимост с различни устройства, версии на операционни системи, механизми за защитено съхранение, мрежови условия и сценарии на прекъсване или възстановяване.

Следва да бъдат извършени анализ на уязвимости и penetration testing на мобилното приложение, сървърните компоненти, административните интерфейси, API интерфейсите и интеграциите. Установените критични и високи уязвимости следва да бъдат отстранени преди въвеждане в продукционна експлоатация.

Изпълнителят следва да осигури DevOps процеси за управление на разработката, версиите, конфигурациите, подписването на мобилните приложения, публикуването в тестови и продукционни канали, миграциите, мониторинга, автоматизираните тестове, rollback процедурите и проследимостта на промените.

При изпълнението на дейността следва да се осигури възможност за последващо разширяване на функционалностите, включително добавяне на нови методи за идентификация, нови типове атрибути, нови сценарии за представяне на данни, нови доверяващи се страни, нови механизми за подписване, поддръжка на допълнителни устройства и съвместимост с бъдещи версии на европейската рамка за цифрова идентичност.

8.1.2.3 Очаквани резултати

Очакваните резултати от изпълнението на дейността са:

- извършен бизнес, нормативен, технически, архитектурен и потребителски анализ на процесите по изграждане и използване на Портфейла за цифрова самоличност;
- проектирана и реализирана архитектура на доставчик на Портфейл за цифрова самоличност;
- изграден доставчик на Портфейл, който управлява жизнения цикъл на портфейлните единици;
- реализирани функционалности за създаване, активиране, използване, управление, блокиране, възстановяване и прекратяване на портфейлни единици;
- реализирани механизми за управление на устройства, сесии, ключове, атестации, настройки за сигурност и статуси на портфейла;

- разработено мобилно приложение за Портфейл за цифрова самоличност за основните мобилни платформи;
- реализиран потребителски интерфейс за идентификация, получаване на данни за идентификация, управление на атрибути, представяне на данни, управление на съгласия и преглед на история на използване;
- реализирани механизми за сигурно съхранение на ключове и чувствителни данни в мобилното устройство чрез защитените възможности на съответната платформа;
- реализирани механизми за проверка на съвместимостта на устройството и ограничаване на функционалности при липса на необходимото ниво на сигурност;
- изграден доставчик на самоличност, който осигурява надеждна първоначална идентификация на потребителя;
- реализирани механизми за привързване на потвърдена самоличност към портфейлна единица;
- реализирани интеграции с приложимите национални регистри, автентични източници, eIDAS възел, системи за електронна автентикация и други компоненти, необходими за идентификация и издаване на данни за идентификация на лице;
- реализирани механизми за издаване, получаване, съхранение, актуализация и отмяна на данни за идентификация на лице;
- реализирани механизми за потребителски контрол върху предоставянето на данни и съгласие при представяне на данни пред доверяващи се страни;
- реализирани механизми за блокиране, деактивиране и възстановяване при изгубено, сменено, откраднато или компрометирано устройство;
- реализирани механизми за водене на одитен журнал, мониторинг, одит и проследимост на действията, свързани с Портфейла и доставчика на самоличност;
- реализиран минимално използваем продукт, доказващ основните сценарии за използване на Портфейла, включително идентификация на потребител и проверка на възраст чрез удостоверен цифров атрибут;
- осигурена интеграция на компонентите по дейността с рамката на доверие и готовност за последваща интеграция с доставчик на квалифицирани атрибути, посредник при верификация, доставчици на КЕП и доставчици на атрибути;
- осигурена съвместимост на мобилното приложение с определените версии на Android и iOS и подготвен процес за публикуване, тестване и актуализация на приложението;
- осигурени мерки за информационна сигурност, киберсигурност, защита на личните данни, криптографска защита и защита на мобилното приложение;
- проведени функционални, интеграционни, системни, приемателни, регресионни, натоварващи, потребителски и тестове за сигурност;

- изготвени доклади от тестове, анализ на уязвимости и penetration testing за приложимите компоненти;
- внедрени компонентите по дейността в съответните среди за разработка, тестване, приемане, обучение, sandbox и продукционна експлоатация;
- осигурена възможност за последващо разширяване на Портфейла с нови сценарии, нови методи за идентификация, нови атрибути, нови доверяващи се страни, нови механизми за подписване и допълнителни устройства.

8.1.3 Дейност 3 - Изграждане на доставчик на квалифицирани атрибути и верификация

8.1.3.1 Описание на дейността

Дейността обхваща изграждането на компонентите, чрез които Портфейлът за цифрова самоличност ще може да предоставя удостоверени цифрови атрибути и чрез които доверяващите се страни ще могат да заявяват, получават и проверяват предоставени от потребителя данни. Дейността включва изграждане на доставчик на квалифицирани атрибути от името на публични институции и изграждане на посредник при верификация.

Доставчикът на квалифицирани атрибути от името на публични институции следва да осигури възможност за издаване на електронни удостоверения за атрибути въз основа на данни от автентични източници и първични регистри, поддържани от компетентни публични органи. Чрез този компонент Портфейлът следва да може да получава и използва удостоверени цифрови данни, които удостоверяват определено качество, право, статус, факт или обстоятелство, свързано с физическо или юридическо лице.

Като примери за атрибути могат да бъдат посочени възраст, адрес, гражданство, представителна власт, образователен статус, професионална квалификация, регистрационен статус на юридическо лице, принадлежност към определена категория лица, право на достъп до определена услуга или друг атрибут, който може да бъде потвърден чрез автентичен източник. Конкретният обхват на атрибутите следва да бъде определен в хода на анализа, съобразно нормативната рамка, техническата готовност на източниците на данни и приоритетните сценарии за използване на Портфейла.

Посредникът при верификация следва да осигури техническа и организационна възможност доверяващите се страни да заявяват и проверяват атрибути, предоставяни от потребителя чрез Портфейла. Той следва да бъде компонентът, чрез който се управляват процесите по заявяване на необходимите атрибути, проверка на доверяващата се страна, валидиране на статуса на участниците, контрол на допустимите цели за обработване, проверка на валидността и автентичността на предоставените удостоверения и поддържане на одитна следа за извършените действия.

Дейността е пряко свързана с Дейност 1 и Дейност 2. Доставчикът на квалифицирани

атрибути и посредникът при верификация следва да използват рамката на доверие, регистъра на участниците, доверителните списъци, доставчика на Портфейл, доставчика на самоличност, мобилното приложение и приложимите национални и европейски интеграции. По този начин се осигурява цялостен процес, при който атрибутите се издават от надежден източник, съхраняват се или се управляват чрез Портфейла, предоставят се от потребителя при изрично действие или съгласие и се проверяват от доверяваща се страна в съответствие с приложимите правила.

Дейността следва да осигури възможност за реализиране на основни сценарии, включително проверка на възраст, проверка на идентификационни данни, проверка на представителна власт или друг приоритетен атрибут, определен от Бенефициера. Сценариите следва да бъдат реализирани по начин, който гарантира минимизиране на данните - например предоставяне на резултат „лицето е над определена възраст“, когато не е необходимо предоставяне на пълна дата на раждане.

При изпълнението на дейността следва да се осигури възможност за последващо разширяване на набора от атрибути, източници на данни, доверяващи се страни, верификационни сценарии и интеграционни интерфейси, без необходимост от цялостна преработка на архитектурата.

8.1.3.2 Изисквания към изпълнение на дейността

Изпълнителят следва да проектира и реализира доставчик на квалифицирани атрибути от името на публични институции. Компонентът следва да позволява издаване на електронни удостоверения за атрибути въз основа на данни от автентични източници, като гарантира точност, актуалност, проверимост, защита на данните, проследимост на издаването и възможност за проверка на валидността.

Доставчикът на квалифицирани атрибути следва да поддържа най-малко следните процеси:

- заявяване на атрибут от потребителя или от приложим компонент на екосистемата;
- проверка на самоличността и правото на лицето да получи съответния атрибут;
- извличане или проверка на данни от автентичен източник;
- издаване на електронно удостоверение за атрибут;
- предоставяне на атрибута към Портфейла;
- съхраняване или управление на необходимите метаданни;
- проверка на валидност и статус на атрибута;
- актуализация на атрибута при промяна на данните в източника;
- отмяна, временно спиране или прекратяване на валидността на атрибута;
- поддръжка на история и одитен журнал;
- предоставяне на интерфейси за вътрешни и външни компоненти.

Изпълнителят следва да осигури интеграция с RegiX, средата за междурегистров обмен и/или други утвърдени интеграционни механизми за достъп до данни от първични регистри. Когато даден атрибут изисква директна интеграция с конкретна система или регистър, Изпълнителят следва да анализира и предложи технически подход, съобразен с възможностите на съответния администратор на данни и с изискванията за сигурност.

Обменът на данни с автентични източници следва да бъде реализиран при спазване на принципите за служебно събиране на данни, минимизиране на обработваните лични данни, ограничаване на целите, защита на обмена, проследимост на заявките и отчетност на достъпа. Системата не следва да съхранява повече данни от необходимото за издаване, валидиране, проследимост и нормативно изискуема отчетност.

Изпълнителят следва да осигури механизми за управление на жизнения цикъл на атрибутите. За всеки тип атрибут следва да бъдат определени правила за валидност, актуализация, повторно издаване, отмяна, блокиране, проверка на статус, архивиране и прекратяване. Когато атрибутът е обвързан с динамични данни, следва да се предвиди механизъм за проверка на актуалност или за ограничаване на срока на валидност.

Изпълнителят следва да реализира подходящи формати и технически профили за електронните удостоверения за атрибути, съобразени с приложимите европейски спецификации, актове за изпълнение и Architecture and Reference Framework. Следва да се осигури поддръжка най-малко на форматите ISO/IEC 18013-5 (mdoc) и SD-JWT VC, на протокола OpenID for Verifiable Credential Issuance (OpenID4VCI) с профила HAIP за издаване, както и на криптографски механизми, които позволяват оперативна съвместимост с Портфейла, доверяващите се страни и европейската инфраструктура.

Изпълнителят следва да осигури възможност за селективно представяне и минимизиране на данните, когато това е приложимо спрямо конкретния атрибут и техническите възможности на избрания формат. При сценарии като проверка на възраст следва да се предоставя само необходимото твърдение или резултат, без да се разкриват повече лични данни от необходимото.

Изпълнителят следва да изгради посредник при верификация, който да осигурява процесите по заявяване и проверка на атрибути от доверяващи се страни. Посредникът следва да работи в съответствие с рамката на доверие и да проверява дали доверяващата се страна е регистрирана, активна, има право да заявява конкретния тип атрибут и използва коректен технически профил.

Посредникът при верификация следва да поддържа най-малко следните процеси:

- регистрация или избор на доверяваща се страна от регистъра на участниците;
- проверка на статуса и правата на доверяващата се страна;

- заявяване на конкретен атрибут или група атрибути;
- дефиниране на цел на заявката и основание за обработване;
- генериране или обработка на заявка към Портфейла;
- предоставяне на ясна информация към потребителя за исканите данни;
- получаване на потвърждение или отказ от потребителя;
- проверка на предоставения атрибут или удостоверение;
- проверка на издателя, валидността, статуса, подписа и доверителната информация;
- връщане на резултат към доверяващата се страна;
- одитен журнал на процеса.

Изпълнителят следва да разработи приложни програмни интерфейси за интеграция на доверяващи се страни с посредника при верификация. Интерфейсите следва да бъдат ясно документирани, водене на версии, защитени и реализирани съгласно протоколите и профилите по ARF, най-малко: OpenID for Verifiable Presentations (OpenID4VP) с профила OpenID4VC High Assurance Interoperability Profile (HAIP) – за онлайн представяне; ISO/IEC 18013-5 – за представяне при физическо присъствие; ISO/IEC 18013-7 и W3C Digital Credentials API – за онлайн представяне чрез браузър. Документацията следва да включва описание на процесите, методите, параметрите, формата на заявките и отговорите, кодовете за грешки, механизмите за автентикация и авторизация, тестови сценарии и примерни интеграции.

Изпълнителят следва да разработи административен интерфейс за управление на посредника при верификация. Интерфейсът следва да позволява управление на доверяващи се страни, технически профили, допустими атрибути, цели на заявяване, конфигурации, статуси, справки, одитни записи и интеграционни параметри.

Изпълнителят следва да осигури възможност за ограничаване на заявяваните атрибути според типа доверяваща се страна, правното основание, целта на заявката и статуса на участника. Системата не следва да позволява доверяваща се страна да заявява атрибути, за които няма основание, разрешение или техническа конфигурация.

Изпълнителят следва да осигури възможност за проверка на атрибути в онлайн режим. Задължително следва да бъде осигурено и представяне и проверка на атрибути при физическо присъствие (proximity) в съответствие с ARF и ISO/IEC 18013-5, при което доверяваща се страна извършва проверка чрез мобилно устройство или друг технически компонент.

При реализация на proximity сценариите следва да бъдат спазени изискванията за сигурност, защита от подправяне, контрол на потребителя, ограничаване на данните, проверка на доверяващата се страна и проследимост на операцията.

Изпълнителят следва да осигури интеграция на доставчика на квалифицирани атрибути и посредника при верификация с Портфейла, доставчика на самоличност и рамката на доверие.

Всички операции по издаване, представяне и проверка на атрибути следва да бъдат обвързани с валиден участник, валидно доверително състояние, валиден технически профил и коректно идентифициран потребител.

Изпълнителят следва да осигури механизми за потребителско потвърждение при предоставяне на атрибути. Потребителят следва да вижда кой заявява данните, какви данни се заявяват, за каква цел, дали заявката е от регистрирана доверяваща се страна и какъв резултат ще бъде предоставен. Потребителят следва да има възможност да потвърди или откаже предоставянето, освен в случаите, в които нормативната рамка предвижда друг допустим модел.

Изпълнителят следва да осигури пълен одитен журнал, мониторинг и одит на процесите по издаване, актуализация, отмяна, представяне и проверка на атрибути. Журналите следва да съдържат достатъчна информация за проследимост и сигурност, без да включват повече лични данни от необходимото.

Изпълнителят следва да осигури защита на личните данни по проект и по подразбиране. При проектирането на процесите по атрибути следва да се спазват принципите за минимизиране на данните, прозрачност, контрол на потребителя, ограничаване на целите, ограничаване на съхранението, криптиране, управление на достъпа и отчетност.

Изпълнителят следва да осигури високо ниво на информационна сигурност и киберсигурност. Компонентите по дейността следва да бъдат защитени срещу неоторизиран достъп, подправяне на атрибути, злоупотреба с API, заявяване на неразрешени данни, replay атаки, подмяна на доверяваща се страна, компрометиране на сертификати, неоторизирана промяна на статуси и други релевантни заплахи.

За компонентите по дейността следва да бъдат проведени функционални, интеграционни, системни, приемателни, регресионни, натоварващи и тестове за сигурност. Следва да бъдат проведени и тестове с примерни доверяващи се страни, примерни атрибути, тестови регистри или тестови услуги, така че да се докаже цялостният процес от издаване до проверка на атрибут.

Следва да бъдат извършени анализ на уязвимости и penetration testing на доставчика на атрибути, посредника при верификация, административните интерфейси, API интерфейсите и интеграциите. Установените критични и високи уязвимости следва да бъдат отстранени преди приемане и внедряване в продукционна среда.

Изпълнителят следва да осигури необходимите среди за разработка, тестване, интеграционно тестване, приемане, обучение, sandbox и продукционна експлоатация. Sandbox средата следва да позволява на доверяващи се страни и други участници да тестват процесите по заявяване и проверка на атрибути без риск за продукционната среда.

8.1.3.3 Очаквани резултати

Очакваните резултати от изпълнението на дейността са:

- извършен бизнес, нормативен, технически и архитектурен анализ на процесите по издаване, управление, представяне и проверка на атрибути;
- дефиниран първоначален каталог от атрибути, източници на данни, правила за валидност, технически профили и сценарии за използване;
- изграден доставчик на квалифицирани атрибути от името на публични институции;
- реализирани механизми за заявяване, издаване, получаване, съхраняване, представяне, актуализация, проверка и отмяна на електронни удостоверения за атрибути;
- реализирани интеграции с RegiX, средата за междурегистров обмен, автентични източници и приложими национални регистри;
- реализирани механизми за проверка на валидност, актуалност, статус и издател на атрибути;
- реализирани механизми за минимизиране и селективно предоставяне на данни, включително за сценарии като проверка на възраст;
- изграден посредник при верификация за заявяване и проверка на атрибути от доверяващи се страни;
- реализирани интерфейси за интеграция на доверяващи се страни с посредника при верификация;
- реализиран административен интерфейс за управление на доверяващи се страни, допустими атрибути, цели на заявяване, технически профили, конфигурации, статуси, справки и одитни записи;
- осигурена проверка на статуса и правата на доверяващите се страни чрез рамката на доверие;
- реализирани механизми за потребителско потвърждение или отказ при предоставяне на атрибути;
- реализирани механизми за водене на одитен журнал, мониторинг, одит и проследимост на процесите по атрибути и верификация;
- реализирани мерки за защита на личните данни, информационна сигурност, криптографска защита и киберсигурност;
- проведени функционални, интеграционни, системни, приемателни, регресионни, натоварващи и тестове за сигурност;
- проведени тестове с примерни атрибути и примерни доверяващи се страни;
- изготвени доклади от тестове, анализ на уязвимости и penetration testing за приложимите компоненти;

- изградена или конфигурирана sandbox среда за тестване на интеграции с доверяващи се страни и сценарии за проверка на атрибути;
- внедрени компонентите по дейността в съответните среди за разработка, тестване, приемане, обучение, sandbox и продукционна експлоатация;
- осигурена възможност за последващо разширяване на набора от атрибути, източници на данни, доверяващи се страни и верификационни сценарии.

8.2 Фаза 2 - „Разширяване на екосистемата“

8.2.1 Дейност 1 - Присъединяване и интеграция на квалифицирани доставчици на удостоверителни услуги, доставчици на квалифицирани електронни удостоверения за атрибути и други допустими доставчици на атрибути

8.2.1.1 Описание на дейността

Дейността обхваща надграждането на изградената национална екосистема за цифрова самоличност чрез присъединяване и интеграция на квалифицирани доставчици на удостоверителни услуги, доставчици на квалифицирани електронни удостоверения за атрибути и други допустими доставчици на атрибути. Дейността има за цел да разшири функционалния обхват на Портфейла и да осигури възможност за реално използване на Портфейла като средство за квалифицирано електронно подписване и като отворена платформа за управление на различни видове удостоверени цифрови атрибути.

Чрез изпълнението на дейността Портфейлът следва да бъде интегриран с квалифицирани доставчици на удостоверителни услуги, така че потребителите да могат да създават квалифициран електронен подпис чрез Портфейла при условията, определени в приложимата нормативна рамка. Това включва техническа възможност за заявяване, издаване, използване, проверка и управление на квалифицирани удостоверения и свързани процеси, когато те са необходими за предоставяне на услугата през Портфейла.

Дейността следва да осигури равнопоставено, прозрачно и недискриминационно присъединяване на квалифицирани доставчици на удостоверителни услуги, вписани в съответните доверителни списъци, така че Портфейлът да не бъде обвързан с един конкретен доставчик, а да позволява работа с всички доставчици, които отговарят на изискванията и са присъединени към екосистемата.

В рамките на дейността следва да бъде реализирано и присъединяване на доставчици на квалифицирани електронни удостоверения за атрибути и други доставчици на атрибути. По този начин екосистемата ще може да бъде разширявана с нови източници на удостоверени цифрови данни, извън първоначално реализирания доставчик на квалифицирани атрибути от името на публични институции.

Дейността надгражда резултатите от предходните дейности. За да функционират

интеграциите с доставчици на КЕП и атрибути, следва да бъдат използвани рамката на доверие, регистърът на участниците, доверителните списъци, доставчикът на Портфейл, мобилното приложение, доставчикът на самоличност, доставчикът на квалифицирани атрибути и посредникът при верификация. Всеки нов участник следва да бъде регистриран, проверен, вписан, технически конфигуриран, тестван и управляван чрез механизмите на националната рамка на доверие.

Когато е необходимо за осигуряване на по-широка съвместимост с мобилни устройства и за реализиране на квалифицирано електронно подписване, дейността може да включва изграждане или интеграция на услуга за отдалечено съхранение на ключове и извършване на криптографски операции в защитена среда. Тази възможност следва да бъде анализирана и реализирана при спазване на изискванията за квалифицирани удостоверителни услуги, сигурно управление на ключове, контрол от страна на потребителя и съответствие с европейската рамка.

Дейността следва да осигури устойчивост и разширяемост на екосистемата, като даде възможност в бъдеще да бъдат присъединявани нови доставчици, нови типове атрибути, нови бизнес сценарии, нови доверяващи се страни и нови механизми за подписване, без да се нарушава работоспособността на вече изградените компоненти.

8.2.1.2 Изисквания към изпълнение на дейността

Изпълнителят следва да анализира и предложи модел за присъединяване на квалифицирани доставчици на удостоверителни услуги. Моделът следва да включва организационни, правни и технически условия за присъединяване, процес по заявление, проверка на статуса на доставчика, проверка на вписване в доверителен списък, проверка на техническа готовност, тестова интеграция, приемане, активиране, мониторинг, временно спиране и прекратяване.

Интеграцията с квалифицирани доставчици на удостоверителни услуги следва да осигурява възможност за използване на квалифициран електронен подпис чрез Портфейла. В зависимост от конкретния технически модел и услугите на съответния доставчик, това може да включва процеси по заявяване на квалифицирано удостоверение, идентификация или препотвърждаване на потребителя, активиране на подписване, потвърждаване на операцията от потребителя, създаване на подпис, проверка на резултата, управление на удостоверения и обработка на грешки.

Изпълнителят следва да осигури технически интерфейси за интеграция с доставчици на КЕП. Интерфейсите следва да бъдат защитени, документирани, водене на версии и съобразени с приложимите стандарти и спецификации. Документацията следва да включва методи, параметри, формати на заявки и отговори, кодове за грешки, механизми за автентикация и авторизация, механизми за подписване и криптиране, тестови сценарии и примерни процеси.

Изпълнителят следва да осигури потребителски процес в мобилното приложение за

използване на квалифициран електронен подпис. Процесът следва да бъде ясен, сигурен и разбираем за потребителя, като преди създаване на подпис потребителят следва да получава информация за документа или данните, които се подписват, доставчика на услугата, правното значение на действието и необходимите стъпки за потвърждение.

При реализация на подписване чрез Портфейла следва да се осигури изрично потвърждение от потребителя и защита срещу подписване без знание или съгласие на потребителя. Следва да се използват подходящи механизми за автентикация, локално потвърждение, биометрия или друг допустим фактор, съобразен с изискванията за сигурност и приложимите технически спецификации.

Изпълнителят следва да осигури механизми за проверка на валидността на квалифицираните удостоверения, статуса на доставчика, валидността на сертификатите, доверителните списъци и резултатите от подписването. Всяка операция по подписване следва да бъде проследима, като се спазват изискванията за защита на личните данни и минимизиране на информацията в одитните журнали.

Когато нормативната рамка предвижда предоставяне на безплатен квалифициран електронен подпис за физически лица за непрофесионални цели, системата следва да бъде проектирана така, че да поддържа необходимите процеси по издаване, използване, отчетност, валидност, компенсация към доставчици или други свързани механизми, доколкото те са възложени в обхвата и са нормативно определени.

Изпълнителят следва да анализира необходимостта от услуга за отдалечено съхранение на ключове и извършване на криптографски операции в защитена среда. Ако бъде потвърдена необходимостта от такава услуга, тя следва да бъде реализирана или интегрирана по начин, който гарантира защита на ключовия материал, контрол на потребителя, разделение на роли, силна автентикация, одитен журнал, висока наличност, устойчивост и съответствие с изискванията за квалифицирани удостоверителни услуги.

Изпълнителят следва да осигури модел за присъединяване на доставчици на квалифицирани електронни удостоверения за атрибути и други доставчици на атрибути. Моделът следва да включва заявление, проверка, техническо тестване, вписване в регистъра на участниците, публикуване в доверителни списъци, конфигуриране на допустими атрибути, управление на статуси и контрол на съответствието.

Интеграцията с доставчици на атрибути следва да осигурява възможност за получаване, съхраняване, представяне, проверка, актуализация и отмяна на атрибути чрез Портфейла. Всеки доставчик следва да бъде обвързан с конкретни типове атрибути, правно основание, технически профил, срокове на валидност, правила за актуализация, правила за отмяна и механизми за проверка на статус.

Изпълнителят следва да осигури възможност за управление на множество доставчици на атрибути за един и същ или сходен тип атрибут, когато това е допустимо. Системата следва да може да различава издателя, нивото на доверие, квалифицирания или неквалифицирания характер на атрибута, валидността, статуса и приложимия сценарий за използване.

Изпълнителят следва да разшири административните функционалности за онбординг и управление на доставчици. Административните интерфейси следва да позволяват управление на заявления, доставчици, технически профили, сертификати, крайни точки, тестови резултати, статуси, допустими атрибути, доверителни връзки, справки, одитни записи и конфигурации.

Изпълнителят следва да осигури sandbox среда за доставчици на КЕП и доставчици на атрибути. Средата следва да позволява тестване на интеграции, сертификати, подписване, издаване на атрибути, проверка на атрибути, обработка на грешки, съвместимост с Портфейла и съвместимост с посредника при верификация.

Изпълнителят следва да осигури механизми за мониторинг, одитен журнал на интеграциите с доставчици на КЕП и атрибути. Следва да се проследяват заявките, отговорите, грешките, статусите, техническата достъпност, промяната на конфигурации, операциите с повишен риск, действията на администраторите и резултатите от критични операции, без да се съхраняват ненужни лични данни или съдържание на подписвани документи извън необходимото.

Изпълнителят следва да осигури механизми за управление на грешки, временна недостъпност и отказоустойчивост при взаимодействие с външни доставчици. Системата следва да обработва коректно случаи на недостъпен доставчик, невалиден сертификат, изтекло удостоверение, отказ от потребителя, неуспешно подписване, невалиден атрибут, отменен атрибут, неразрешена заявка или несъвместим технически профил.

Изпълнителят следва да осигури защита на личните данни по проект и по подразбиране. При интеграцията с доставчици на КЕП и атрибути следва да се обменят само данните, които са необходими за конкретната операция. Следва да се избягва ненужно съхраняване на подписвани документи, лични данни, атрибути, резултати от проверки и технически данни, които не са необходими за доказуемост, сигурност или нормативно изискуема отчетност.

Изпълнителят следва да осигури високо ниво на киберсигурност и защита на интеграционните интерфейси. Компонентите по дейността следва да бъдат защитени срещу неоторизиран достъп, злоупотреба с API, подправяне на доставчик, подмяна на заявка за подписване, подмяна на атрибут, man-in-the-middle атаки, replay атаки, компрометиране на ключове, ескалация на привилегии и други релевантни заплахи.

Всички интеграции следва да бъдат реализирани чрез стандартизирани, документирани и водене на версии на интерфейсите. Следва да се поддържа управление на версии и обратна

съвместимост, доколкото е приложимо, така че промени в интерфейсите да не водят до нерегламентирани прекъсвания на услугите.

Изпълнителят следва да осигури възможност за добавяне на нови доставчици без промени в основната архитектура. Процесът по присъединяване следва да бъде параметризиран в максимална степен чрез технически профили, конфигурации, сертификати, доверителни списъци и правила, вместо чрез твърдо кодирани интеграции.

За компонентите по дейността следва да бъдат проведени функционални, интеграционни, системни, приемателни, регресионни, натоварващи и тестове за сигурност. Следва да бъдат проведени тестове с поне един или повече примерни квалифицирани доставчици на удостоверителни услуги и доставчици на атрибути, когато това е възможно и съгласувано с Бенефициера.

Следва да бъдат извършени анализ на уязвимости и penetration testing на интерфейсите за интеграция с доставчици на КЕП и атрибути, административните интерфейси, sandbox средата и приложимите потребителски процеси. Установените критични и високи уязвимости следва да бъдат отстранени преди приемане и внедряване.

8.2.1.3 Очаквани резултати

Очакваните резултати от изпълнението на дейността са:

- извършен бизнес, нормативен, технически и архитектурен анализ на процесите по интеграция с доставчици на КЕП и доставчици на атрибути;
- дефиниран модел за присъединяване на квалифицирани доставчици на удостоверителни услуги;
- реализирани технически интерфейси за интеграция с квалифицирани доставчици на удостоверителни услуги;
- осигурена възможност за създаване на квалифициран електронен подпис чрез Портфейла;
- реализиран потребителски процес в мобилното приложение за подписване чрез Портфейла;
- реализирани механизми за проверка на доставчик, удостоверение, сертификат, статус, доверителна информация и резултат от подписване;
- осигурена възможност за поддръжка на процеси, свързани с безплатен квалифициран електронен подпис за физически лица, когато това е приложимо и нормативно определено;
- анализирана и при необходимост реализирана или интегрирана услуга за отдалечено съхранение на ключове и криптографски операции в защитена среда;

- дефиниран модел за присъединяване на доставчици на квалифицирани електронни удостоверения за атрибути и други доставчици на атрибути;
- реализирани технически интерфейси за интеграция с доставчици на атрибути;
- осигурена възможност за получаване, съхраняване, представяне, проверка, актуализация и отмяна на атрибути, издавани от външни доставчици;
- надградени административни интерфейси за онбординг, управление, мониторинг, статуси, технически профили, сертификати, справки и одит на доставчици;
- осигурена sandbox среда за тестване на интеграции с доставчици на КЕП и атрибути;
- реализирани механизми за мониторинг, одитен журнал и проследимост на интеграционните процеси;
- реализирани механизми за управление на грешки, отказоустойчивост и обработка на временна недостъпност на външни доставчици;
- реализирани мерки за защита на личните данни, информационна сигурност, криптографска защита и киберсигурност;
- осигурена възможност за добавяне на нови доставчици без промяна в основната архитектура на системата;
- проведени функционални, интеграционни, системни, приемателни, регресионни, натоварващи и тестове за сигурност;
- проведени тестове с примерни или реални доставчици на КЕП и доставчици на атрибути, когато това е възможно и съгласувано с Бенефициера;
- изготвени доклади от тестове, анализ на уязвимости и penetration testing за приложимите компоненти;
- внедрени надградените компоненти и интеграции в съответните среди за разработка, тестване, приемане, обучение, sandbox и продукционна експлоатация;
- осигурена възможност за последващо разширяване на екосистемата с нови доставчици, нови атрибути, нови сценарии за подписване, нови доверяващи се страни и нови технически профили.

9 Документация

9.1 Изисквания към документацията

- Цялата документация и всички технически описания, ръководства за работа, администриране и поддръжка на Системата, включително и на нейните съставни части, трябва да бъдат налични и на български или английски език;
- Всички документи трябва да бъдат предоставени от Изпълнителя в електронен формат (ODF/ Office Open XML / MS Word DOC / RTF / PDF / HTML или др.), позволяващ пълнотекстово търсене/търсене по ключови думи и копиране на части от съдържанието от оригиналните документи във външни документи, за вътрешна употреба на Бенефициера;

- 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 web услуги, команди, структури от данни и др. Документацията да бъде придружена и с примерен програмен код и/или библиотеки (SDK) за реализиране на интеграция с външни системи, разработен(и) на Java или .NET. Примерният код трябва да е напълно работоспособен и да демонстрира базови итерации с API-то:
  .1 Регистриране на крайна точка (end-point) за получаване на актуализации от Системата в реално време;
  .2 Заявки за получаване на номенклатурни данни (списъци, таксономии);
  .3 Заявки за актуализиране на номенклатурни данни (списъци, таксономии);
  .4 Регистрация на потребител;
  .5 Идентификация и оторизация на потребител или уеб услуга;
- Документацията за приложния програмен интерфейс (API) трябва да бъде публично достъпна;
- Всеки предоставен REST приложно-програмен интерфейс трябва да бъде документиран чрез API Blueprint (https://github.com/apiaryio/api-blueprint), Swagger (http://swagger.io) или чрез аналогична технология. Аналогично представяне трябва да бъде изготвено и за SOAP интерфейсите;
- Детайлна техническа документация за схемата на базата данни – структури за данни, индекси, дялове, съхранени процедури, конфигурации за репликация на данни и др.
- Ръководства на потребителя и администратора за работа и администриране на Системата, където в разработените компоненти има интерфейс за управление и само в случаите, когато надграждането по дадена дейност предвижда функционална промяна при използването или администрирането на дадения компонент или Система.

9.2 Прозрачност и отчетност

- В обхвата на проекта е включено извършване на дейности по анализ на бизнес процеси и нормативна уредба, проектиране на системна и приложна архитектура, разработване на компютърни програми и други дейности, свързани с предоставяне на специализирани професионални услуги. Изпълнителят и Бенефициерът трябва да публикуват подробни месечни отчети в машинночетим отворен формат за извършените дейности, включително количеството изработени човекодни по дейности, извършени от консултанти, експерти, специалисти и служители на изпълнителя и Бенефициера.
- Документацията, предоставена от изпълнителя на Бенефициера, трябва да бъде:
  .1 на български или английски език;

.2 само в електронен формат, като копирането и редактирането на предоставените документи следва да бъде лесно осъществимо;

.3 актуализирана в съответствие със съгласувана с Бенефициера процедура, която следва да включва документи, подлежащи на промяна/актуализация, крайни срокове и нужната за случая методология.

Минимално изискуемата документация по проекта включва долу изброените документи.

9.3 Детайлна техническа спецификация

Изпълнителят на проекта 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 Бенефициера. В случай на забележки, корекции или допълнения от страна на Бенефициера, Изпълнителят е длъжен да ги отрази в детайлната техническа спецификация (системен проект).

9.4 Техническа документация

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

- Ръководство за администратора, включващо всички необходими процедури и скриптове по инсталиране, конфигуриране, архивиране, възстановяване и други, необходими за администриране на Системата, където в разработените компоненти има интерфейс за управление и само в случаите, когато надграждането по дадена дейност предвижда функционална промяна при администрирането на дадения компонент или Система;
- Документи за крайния ползвател – Изпълнителят трябва да предостави главното Ръководство на ползвателите на софтуера, където в разработените компоненти има интерфейс за крайни потребители и само в случаите, когато надграждането по дадена дейност предвижда функционална промяна при използването на дадения компонент или Система. 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 структурата на базата данни;
- Описание на изходния програмен код.

10 Резултати

Очакваните резултати от изпълнението на настоящия проект са следните:

- Изградена национална рамка на доверие за Портфейла за цифрова самоличност, включително правила, процедури, регистър на участниците, доверителни списъци, PKI/доверителна инфраструктура и механизми за управление, контрол и проследимост на участниците в екосистемата;
- Изграден и внедрен доставчик на Портфейл за цифрова самоличност, осигуряващ управление на жизнения цикъл на портфейлните единици, включително създаване, активиране, използване, блокиране, възстановяване и прекратяване;
- Разработено и внедрено мобилно приложение за Портфейл за цифрова самоличност, чрез което потребителите могат да се идентифицират, да получават, съхраняват и управляват данни за идентификация и удостоверени цифрови атрибути, както и да предоставят данни към доверяващи се страни;
- Изграден доставчик на самоличност, осигуряващ надеждна първоначална идентификация на потребителите, проверка на данни от автентични източници и привързване на потвърдена самоличност към портфейлна единица;
- Реализирани интеграции с приложимите национални регистри, автентични източници на данни, RegiX, eIDAS възел, системи за електронна автентикация и други компоненти на електронното управление, необходими за функционирането на Портфейла;
- Изграден доставчик на квалифицирани атрибути от името на публични институции, осигуряващ издаване, обновяване, отмяна, съхранение, представяне и проверка на електронни удостоверения за атрибути;
- Изграден посредник при верификация, чрез който доверяващите се страни могат да заявяват и проверяват атрибути, предоставяни от потребителя чрез Портфейла, при спазване на принципите за минимизиране на данните, контрол от страна на потребителя, прозрачност и проследимост;
- Осигурена възможност за присъединяване и интеграция на доставчици на квалифицирани електронни удостоверения за атрибути и други допустими доставчици на атрибути;
- Надградена екосистема за цифрова самоличност с механизми за онбординг, управление, тестване, мониторинг и поддръжка на доставчици, доверяващи се страни и други участници;
- Осигурена трансгранична оперативна съвместимост с европейската инфраструктура по eIDAS, така че българският Портфейл за цифрова самоличност да може да бъде използван в други държави членки, както и портфейли от други държави членки да могат да бъдат приемани в Република България;
- Осигурено високо ниво на информационна сигурност, киберсигурност, криптографска защита, защита на личните данни, одитни журнали и проследимост на действията в системата;

- Въведени/внедрени необходимите среди за разработка, тестване, интеграционно тестване, приемане, обучение, sandbox и продукционна експлоатация;
- Изградена устойчива, сигурна и разширяема национална инфраструктура за цифрова самоличност, която създава основа за развитие на електронното управление, намаляване на административната тежест и предоставяне на електронни услуги от ново поколение.

Приложение №2

към Договор № ……

(Образец)

Д Е К Л А Р А Ц И Я
ЗА ОПАЗВАНЕ НА ИНФОРМАЦИЯ

Долуподписаният/ та ……..,

ЕГН: .....,[3] в качеството ми на ……., декларирам, че ще пазя в тайна, станалата ми известна във връзка с изпълнението на Договор № ……/…..... г.[4] 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.[5] 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 иновациите и дигиталната трансформация (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 връзка с

---

[3] *В случай, че лицето е чужденец, се вписват съответните идентификационни данни.*

[4] *Вписва се референтен номер на Договора, в договорния регистър на ВЪЗЛОЖИТЕЛЯ.*

[5] Съгласно § 5, ал.1 от Преходните и заключителните разпоредби на Закона за въвеждане на еврото в Република България „действащите нормативни актове, които уреждат задължения за плащане на такси, санкции, глоби и други публични задължения към държавата и общините в български левове, продължават да се прилагат в съответствие с предвидените в този закон правила за превалутиране.“.

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 МИДТ, 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)